



FOUNDRY
NETWORKS

CASE STUDY: NFBC

Niagara Falls Bridge Commission



SUMMARY

Niagara Falls attracts multitudes of U.S. and Canadian tourists and honeymooners with its spectacular scenery and numerous attractions. Linking the two sides of the Niagara Falls region, the Niagara Falls Bridge Commission (NFBC) is a joint U.S. and Canadian agency that owns and operates three bridges that traverse the Niagara River. Although the NFBC does not handle customs and immigration between the two countries, the organization is charged with keeping the Niagara Falls bridges safe and ensuring that traffic flows efficiently and unhindered between the U.S. and Canada.

Network security and traffic management functions are overseen remotely from NFBC's Operations Center at the agency's administrative headquarters in Lewiston, NY. From this state-of-the-art Operations Center, which operates 24 hours a day, 7 days a week, NFBC management and staff analyze information streaming in from 160 video cameras, 96 access control points and 6 U.S./Canadian customs plazas distributed along the bridges.

OBJECTIVE

Due to the critical nature of maintaining unimpeded traffic along the fourth busiest U.S.-Canadian border, NFBC required a converged network and security solution to automate consolidation and interpretation of a wide array of disparate data sources, such as:

- Switch/router interface logs
- User activities
- Network traffic statistics
- Log-in, log-out logs
- Host behaviors
- Other systems

The goal of this best-of-breed communications and advanced security solution was to cost-effectively automate once manual correlation efforts in order to rapidly reduce the time to resolution of both network and security incidents. Often, the existing manual efforts were unable to identify repeat issues and required reproducing each scenario.

"We needed a network infrastructure capable of supporting our intensive environment, but we also wanted a network behavior analysis solution that would allow us to view information about that network more efficiently," explains Dave Woods, Manager of IT.

With a 10Gb international network with more than 500 nodes across seven locations, the NFBC found that network management was taking up more time and becoming more complex. As the network grew, network and host behavior anomalies became harder to detect. The agency needed a solution to address these issues and ensure that its network securely supported its' high performance requirements.

SOLUTION

Foundry's converged network solution Lancope's StealthWatch Network Behavior Analysis (NBA) solution met each of NFBC's requirements providing them with their ideal solution. Foundry's networking and wireless hardware transports on-demand data, voice, and video throughout the agency's operations. Lancope's StealthWatch System integrates security awareness with Foundry's network infrastructure to significantly reduce network risks and maximize network availability. This joint Foundry/Lancope solution rapidly identifies, prioritizes, mitigates, and resolves critical network and security incidents and threats—regardless of signature availability.

The joint solution includes a number of Foundry and Lancope products:

- Foundry sFlow-capable BigIron® RX backbone switches
- Foundry sFlow-capable FastIron® family of Power over Ethernet (PoE) switches

WWW.NIAGARAFALLSBRIDGES.COM

INDUSTRY

Government

COMPANY DESCRIPTION

The Niagara Falls Bridge Commission (NFBC) is a joint U.S./Canadian agency that owns and operates three bridges that traverse the Niagara River at the fourth busiest border crossing between the two countries. The bridges handle about 12 million crossings a year, and about \$32 billion in trade goes back and forth across border.

OBJECTIVE

- Deploy a converged networking solution to consolidate the many types of data coming in to the NFBC's Operations Center
- Include advanced security features to keep this busy border crossing between the U.S. and Canada safe
- Create a robust, reliable networking environment that is as mission-critical as the bridges it serves

SOLUTION

- The network includes Foundry's BigIron RX backbone switches, FastIron family of Power over Ethernet (PoE) switches, IronPoint Mobility Series, IronView Network Manager (INM) software as well as Lancope's StealthWatch Network Behavior Analysis and response solution

RESULTS

- NFBC staff are able to analyze incoming video, voice, and data and coordinate responses 24 hours a day and seven days a week
- By integrating Lancope's StealthWatch with INM, the NFBC is able to combine network behavior analysis with network management to detect flow-based anomalies and threats

