CITY OF GREATER SUDBURY SECURES MISSION CRITICAL INFRASTRUCTURE WITH UNIFIED ACCESS CONTROL

Summary

Company: City of Greater Sudbury

Industry: Government

Challenges: Secure access to the city's water treatment network and support secure wireless access for city employees

Selection Criteria: An 802.1X network access control solution that could secure access to both wired and wireless networks

Solution:

- Unified Access Control
- IC4500 UAC Appliance
- Odyssey Access Client

Results:

- Meets compliance requirements and mitigates risk from guest access to networks
- Supports access control for mission critical infrastructure
- Meets business demand for wireless LAN (WLAN) connectivity

The City of Greater Sudbury, the largest city in Northern Ontario, Canada, is located in a region known for its natural resources, rich mineral deposits, and mining heritage. As a municipal government, the City of Greater Sudbury provides a wide range of public services, including zoning and by-law development, arts and culture, parks and recreation, and public utilities, including water treatment.

Challenges

Sudbury needed to comply with regulations from the province of Ontario that called for protection of the data and infrastructure for its water treatment facility. The Public Works Department looked to the city's IT organization to protect its mission critical infrastructure by securing access to its water treatment facility network at dozens of unmanned sites.

In the past, well-meaning contractors had connected unauthorized notebooks at remote sites. This could potentially bring down the entire water treatment network and potentially introduce malware to the mission critical infrastructure. If the water treatment network is disrupted, the City requires that attendants are dispatched to all remote sites to restore service within the environment.

The city also had a major initiative to provide wireless LAN (WLAN) access to employees ranging from city offices to public arenas. Before that business goal could be met, IT had to be confident that city staff could securely authenticate and access the WLAN. "We needed to make sure our front gate was secure," said Peter Houle, systems specialist at the City of Greater Sudbury.

Selection Criteria

"There was no golden rule for how to control access in our environment," said Aaron Green, network specialist at the City of Greater Sudbury. "We had to choose the right solution that would work for both our wired and wireless networks."

The City of Greater Sudbury IT Department determined that 802.1X would provide the best standards-based, open solution to control access to its water treatment facility network and meet the growing demands for wireless LAN connectivity. The network access control (NAC) solution needed to support Supervisory Control and Data Acquisition (SCADA) and other nontraditional IT equipment on the water treatment network. In addition, the City needed a cross-platform solution, including support for Mac OS, Windows, and Linux-based endpoints, as well as for "unmanaged" devices that could not support 802.1X Extensible Authentication Protocol (EAP) authentication.

The IT team quickly found that Juniper Networks® Unified Access Control fit their needs. In particular, Houle noted that the IT team liked the Juniper solution's support for 802.1X authentication, integrated RADIUS, as well as the ability to perform endpoint health checks prior to granting user access to the network.

Solution

The City of Sudbury now uses Unified Access Control to control network access in more than 50 municipal buildings and to more than 70 unmanned water treatment facilities.

UAC is a standards-based, scalable network access control system that reduces threat exposure and mitigates risk, protects the network from unauthorized access, and provides comprehensive control, visibility, and monitoring. UAC also addresses potential vulnerabilities such as insider threats, guest access, outsourcing, and regulatory compliance.

The City of Sudbury chose the Juniper Networks IC4500 Unified Access Control Appliance. The IC4500 UAC Appliance scales from 35 to 5,000 simultaneous users in either or both agent and agentless mode. UAC allows the City to gather user credentials, endpoint security state, and device location to implement dynamic, identity- and location-based access and security policies which it distributes to enforcement points across the network. Enforcement points may be any 802.1X-enabled access point and switch—including the Juniper Networks EX Series Ethernet Switch, or any Juniper firewall, including the Juniper Networks SRX Series Services Gateway or other security devices.

When guests and contractors authenticate to the City of Sudbury's network, they are directed to a guest VLAN instead of directly to the SCADA network. If an endpoint fails the device posture check, it is quarantined to mitigate risk of a crossover infection. From there, the user is directed to contact the help desk to resolve the issue, for example, by updating out-of-date antivirus signatures.

The City of Sudbury has equipped more than 250 notebooks and 50 workstations with Juniper Networks Odyssey Access Client for secure access and connectivity to its growing number of wireless LANs. OAC is an 802.1X client software that ensures that users connect to the appropriate network, that login credentials are not compromised, and that user and network credentials and transmitted data are secure. OAC is quick and easy to deploy, distribute, and upgrade without requiring an IT staffer to touch every device.

UAC's open-standard support was critical for the support of dumb devices and a speedy rollout. UAC leverages the new Trusted Networks Connect (TNC) open standard Interface for Metadata Access Point (IF-MAP), which allows UAC to integrate with third-party network and security devices. With IF-MAP support, for example, UAC integrated with Great Bay's MAC Authentication and Beacon Endpoint Profiler software. The MAC Authentication capability allowed SCADA and other non-EAP clients to be identified and monitored via their media access control (MAC) addresses. The City used Great Bay's Beacon to discover network-attached endpoints, which sped deployment of the system.

Results

Network access control has allowed the City of Greater Sudbury to provide contractors and employees with secure access to its water treatment facility networks while reducing overall downtime and associated support costs. UAC controls contractor and employee access to the water treatment network, delivers the appropriate differentiated access based on the user's role and identity, and vets user endpoints to ensure that up-to-date antivirus signatures and other security health indicators are loaded and running.

UAC has proven flexible in adapting to changing business requirements. The UAC solution is also used to provide secure access to the city's growing wireless LAN infrastructure. The city's arena is host to many trade shows, and event producers increasingly want wired and WLAN connectivity. With Unified Access Control, the City of Sudbury can meet the business demand for convenient wireless LAN access while ensuring that its security and compliance obligations are met.

> **"We've secured our staff's access to the wireless LAN with Juniper, and we're relying on Juniper to bring the same level of secure access control when we roll out wireless coverage essentially everywhere in the city."**
>
> Aaron Green,
> network specialist, City of Greater Sudbury

With IF-MAP integration between UAC and Great Bay, the City of Sudbury was able to significantly reduce the time required to inventory all devices attached to the water treatment network. IT was able to locate, map, and secure all of the SCADA and unintelligent devices on the network using Great Bay in a matter of days, as opposed to weeks.

Houle is matter-of-fact about what he likes best about UAC: "We almost never login to the UAC appliance. It chugs along in the background and assigns people to the right VLAN. It's hands-off for us."

Next Steps and Lessons Learned

The IT team at the City of Sudbury is expanding its wireless LAN service to 20 additional facilities. "We've secured our staff's access to the wireless LAN with Juniper, and we're relying on Juniper to bring the same level of secure access control when we roll out wireless coverage essentially everywhere in the city," said Green.

For More Information

To find out more about Juniper Networks products and solutions, please visit **www.juniper.net**.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3520325-001-EN June 2011

♻ Printed on recycled paper