FÜRTINET

CASE STUDY

School District in British Columbia Secures Its Network and Enables BYOD with Network Access Control

ABBOTSFORD SCHOOL DISTRICT

The Abbotsford School District in the city of Abbotsford, British Columbia, Canada, has about 18,500 students and 2,100 teachers and staff at its 46 schools. Every classroom has wireless devices, including document cameras, projectors, and a laptop/desktop for the teacher. The district also provides tablets, laptops, and lab devices for students—about 10,000 devices in total.

The district's network was under siege. Students were flooding the network with their cell phones, taking up valuable bandwidth needed for instruction and putting the network, students, and the district at risk. Moreover, passwords to school-owned devices were constantly being compromised, allowing unknown devices onto the network, and the IT department had no way of identifying the devices or their owners. "We had to send teams out to reset passwords—it was unworkable," says Shelley Wilcox, director of technology at Abbotsford School District. "We needed a solution that would give us better control of our network—a solution that would tell us who's trying to connect and then could automatically route them to the right network. We also needed to be able to track devices as they moved around the district and locate them if used inappropriately."

Flexible Access Policies, Enforced Automatically

The Fortinet FortiNAC[1] network access control (NAC) solution identifies all endpoint devices as they connect to the Abbotsford School District network, performs compliance checks to make sure they have antivirus protection and are not jail broken, and puts them on the appropriate virtual local-area network (VLAN) based on predefined policies for each user group and device type. There's a VLAN for district-owned devices used for learning in the classroom and labs; a bring-your-own-device (BYOD) network for teachers, staff, and special-needs students; and a BYOD network for students and guests, which for safety and bandwidth management reasons is routed outside the district to the Provincial Learning Network. "Now you can walk into any facility, and the FortiNAC solution will automatically recognize your device and put you on the right network," says Wilcox.

Recent initiatives necessitated changes to the BYOD networks. Devices must now be routed through the firewalls to filter websites and content yet remain independent of networked servers and printers. "Thanks to the FortiNAC solution, we can do this easily," adds Wilcox.

> *"Using Fortinet's FortiNAC solution, we have much higher security because we know exactly what's on the network, how each device is connected, where it's located, and who is using it. And when people come to any school in our district, they know they will get safe, seamless connectivity. FortiNAC network access control enables us to provide better service and increased user satisfaction, and that's huge."*
>
> – *Shelley Wilcox, Director of Technology, Abbotsford School District*

Details

Customer: Abbotsford School District
Industry: Education
Location: Abbotsford, British Columbia, Canada

Business Impact

- Automatically provisions network access based on predefined BYOD policies

- Ensures that only authorized users and devices can access the network

Wilcox specifically highlights the FortiNAC solution's flexible network access and remediation policies if a device is out of compliance: "We now have the ability to specify where, when, and how we want to allow access. As an IT director, I can say this is one project where we haven't had a lot of resistance."

In addition to controlling access, the FortiNAC solution detects and identifies devices that are already on the network. "We discovered more than 1,000 unregistered, rogue devices, which we can now register or block, since authentication occurs through active directory," says Wilcox. "Using FortiNAC network access control, we now have much higher security."

Reduces Administrative Overhead

NAC also eliminates the need to manage multiple service set identifiers (SSIDs) at each school, and Wilcox no longer needs to send teams to different schools to reset compromised SSID passwords—something that was very time-consuming for the IT department. "Schools thank us because we're no longer constantly resetting passwords that students had hacked and texted to everyone, and their networks are no longer overwhelmed," comments Wilcox. Her employees are happy too. "Using the FortiNAC solution, it's now easy for us to identify users and manage access to resources using appropriate VLANs. Device registration is handled quickly through online registration or by uploading lists of devices into NAC."

Blocks Cyber Threats and Identifies the Perpetrator

The FortiNAC solution is also used to detect and block inappropriate activity on the network as part of Abbotsford's integrated security solution, which includes their firewall and filtering software. When the threat-detection solution detects a problem, such as the transmission of inappropriate content or a cyber threat, the FortiNAC solution identifies the offending device and user and can block access. Wilcox notes that this visibility and access control are very helpful when investigating an incident. "When you have a powerful tool in the pocket of every kid, you can't see everything all the time," observes Wilcox. "Now, using FortiNAC network access control with our firewall, we can identify the device, where it is, what it's doing, and who is using it. It's a very powerful combination."

"Using Fortinet's FortiNAC solution, we have much higher security because we know exactly what's on the network, how each device is connected, where it's located, and who is using it," says Wilcox. "When people come to any school in our district, they know they will get safe, seamless connectivity. FortiNAC network access control enables us to provide better service and increased user satisfaction, and that's huge."

Business Impact (cont.)

- Remediates noncompliant devices

- Integrates with firewalls to help remediate devices on the network if cyber abuse or inappropriate activity is identified

- Tracks all devices across the school district

- Cuts administrative overhead and improves the user experience

Solution

- FortiNAC

"We discovered more than 1,000 unregistered, rogue devices, which we can now register or block, since authentication occurs through active directory."

– Shelley Wilcox, Director of Technology, Abbotsford School District

[1] Formerly Bradford Networks.

FÜRTINET®

www.fortinet.com