Barracuda
Your journey, secured.

On Keolis buses, Dutch riders got fast, reliable, secure Wi-Fi.

See how a new kind of firewall for distributed networks made it possible.

KEOLIS NEDERLAND
Keolis Nederland is de nieuwe naam van Syntus

ICTVISION

About Keolis

Keolis is a regional public transportation provider operating several hundreds of buses with public Wi-Fi in the provinces of Gelderland, Veluwe, Overijssel, Twente, and Utrecht. Keolis is extending public bus services throughout the area connecting Almere municipality by December 2017, and a train route between Zwolle, Kampen, and Enschede, located in the Overijssel province.

About ICT Vision B.V.

Located in Eindhoven in the Netherlands, ICT Vision B.V. is a multivendor ICT consulting company and system integrator with certified partnerships for Microsoft, Google, VMware, Netapp, Aruba Networks, and Barracuda Networks. ICT Vision specialises on ICT networking and infrastructure solutions, including SAN storage, hosted environments, office automation, and business continuity. All services are continuously monitored and managed 24x7 from ICT Vision's own network operations center.

The Challenge

For the Utrecht province in the Netherlands, more than a hundred public buses that provide clean, reliable, timely, and entertaining transportation were to be equipped with public Wi-Fi that needed to be secured from network-based threats and reliably connected to the data center. Via a secure VPN connection from every bus to the data center, ongoing updates were provided for the on-board infotainment system. As every bus is equipped with a reliable 4G data modem uplink, speeds weren't an issue— keeping the Wi-Fi network safe and protected from internet-based hacking and denial-of-service

Profile Keolis

- Public Transportation company.
- Founded 1999. Based in Netherlands.
- 182 Staff, 1750 drivers.
- More than 30 million passengers a year.

Profile ICT Vision B.V.

- Founded in 2006. Based in Netherlands.
- Specialises in information and communication technology with focus on network connectivity, cloud, and storage solutions.

Challenges

- Provide secure and reliable Wi-Fi services for several hundred public transportation buses.

Solution

On-board 4G modem connected to Barracuda Secure Connector SC1 IoT devices, which are connected to a Barracuda Secure Access Controller virtual image. Central Management by a Firewall Control Center virtual image.

Results

- Secure VPN connection from every bus to the datacenter.
- Fast reliable Wi-Fi, protected from internet based hacking and denial of service available after Terms and Conditions agreement.

attempts was difficult. Keolis needed an affordable solution that can scale and secure the thousands of remote public buses.

The Solution

To find a manageable Solution, Keolis turned to ICT Vision B.V., a long time Barracuda Partner that provides networks-as-a-service. After evaluating several options, Keolis chose the Barracuda solution for IoT. The Secure Connector SC1 appliances connected to the stackable machines access security brokers was the perfect fit since it is able to provide secure and reliable tunnels to the public transport system, offering Wi-Fi access and central management.

Fast Troubleshooting and Efficient Daily Management

All security, networking, and connectivity benefits are easily accomplished with the management console, a small Microsoft Windows OS executable. Using this standalone application enables rich, low-latency live views of all the traffic flowing through the firewall, with the ability to easily manage the firewall even when under heavy loads.

Configuration changes are done quickly and applied almost instantaneously. And with "Firewall History View," troubleshooting can be done in a matter of seconds, without the need to go through tons of log files or use of complicated commands in a CLI window.

Quick Deployment

Configuring and maintaining multiple security appliances can be a complicated and time-consuming task. For IoT environments, the Barracuda solution is fully configurable via a template-based management system that is tightly integrated with the central management capabilities of Firewall Control Center. Once a template is changed, Barracuda Cloud Generation Firewall appliances linked to this template are automatically updated within seconds.

The "Automatic Network Setup" takes care of cumbersome setup and routing configurations. Administrators just define a single, large network that is automatically translated into smaller subnets, which, in turn, are then automatically assigned to the remote appliances. The encrypted connection between the FSC1 security appliance and the data center is established with Barracuda's proprietary, enhanced IPsec protocol TINA. Without relinquishing any security aspects, TINA is significantly more resilient and effective for low latency 4G internet connections than standard IPsec solutions.

Central management scales to tens of thousands of remote locations by using a three-tiered management and load-share approach:

> "With the Barracuda Secure Connector SC1 the Wi-Fi access points on the public buses kept secure, always connected to the datacenter and central management is no longer an issue."
>
> **Frank van Tuyl**
> Consultant
> ICT Vision B.V.

Learn more about Barracuda CloudGen Firewall and Barracuda CloudGen WAF.

barracuda.com/products/cloudgenfirewall
barracuda.com/products/webapplicationfirewall

Barracuda
Your journey, secured.