Barracuda
Your journey, secured.

Building facilities company secures, connects, and automates technical installations and building management

Van Dam Groep combines security, automation and better services with Barracuda CloudGen Firewall Secure Connector solutions.

van dam groep

About Van Dam Groep

The Van Dam Group was founded in 1935 as a plumbing company. Over the years, the disciplines heating, electricity, and ventilation have been added. With over 350 employees, the Van Dam Group is one of the larger and leading organizations in the installation sector in the Netherlands. Partly due to years of experience and knowledge building, the Van Dam Group has acquired an important position within the Dutch market.

Facility Management 4.0

Over the last couple of years literally all technology used for technical installation of home or office buildings got IP and networking aware. While this offered great opportunities for home automation it also provides challenges when protecting against the notoriously unsafe internet. Before switching to the Secure Connector solution, Van Dam Groep was using small firewall/VPN devices to protect the remote locations. Whilst this was secure, they were more expensive, harder to manage and all in all too much of a complicated solution. More user-friendly alternatives with better pricing almost always used an internet based central management approach. Access control and building automation is a vital part of the service, so potentially exposing confidential customer data to the internet was not an option. Van Dam Groep was looking for a solution that is secure, user friendly, cost effective, fast to deploy with complete control over every aspect of the security credentials. This is where the Secure Connector solution got involved.

Profile

- Leading organization for installations and maintenance electrical systems, solar, heating, air condition, and home automation in the area
- Located in the Netherlands.
- More than 350 employees.
- More than 80 years of experience in the sector.

Challenges

- Replace existing firewall / VPN solution that was hard to manage and expensive.
- Replace existing connections with a future-proof solution.
- Secure uninterrupted connectivity from all buildings to private management cloud.
- Anytime anywhere connectivity to remote systems.
- Edge intelligence to monitor remote equipment and create work orders only if needed.

Solution

- Barracuda Secure Connector 2 appliances with LTE failover and custom Linux container for edge intelligence.
- SC2's connected to Barracuda Secure Access Controllers hosted in private cloud.
- Everything managed via Barracuda Firewall Control Center.

Results

- Secure always on connectivity for every managed building.
- Easy to roll out solution for new buildings

Automated deployment, fully confidential

Rolling out a larger number of security devices is only possible with Barracuda's zero-touch deployment capabilities available on all Secure Connector units. With no need for manual configuration on-site, zero-touch deployment allows shipping the devices directly to the remote location where they just need to be plugged in. They automatically authenticate to the Firewall Control Center in the private cloud to receive configuration instructions. The process ensures full confidentiality of any type of customer data, accelerates deployment times, and helps to make large-scale rollouts in an economic manner possible at all.

"Always on and secure IP connectivity to the buildings technical systems saves time, travel expenses and allows for a better service to our customers."

Tom Stevens
Sr. Security & Automation engineer
Van Dam Groep

Easy to use, always on full confidentiality

The small Barracuda Secure Connector devices utilize a proprietary VPN encryption to automatically establish a secure and redundant connection to the Barracuda Secure Access Controller hosted in a private cloud datacenter. This guarantees full confidentiality of all traffic to and from the buildings. Access Control and security scanning is done entirely on the backhauled traffic. The always-on VPN connection enables maintenance and status data to be read out and controlled at any time.

In case of a technical issue, service technicians access the buildings systems for further investigation and fix/workaround application at any time without having to manually dial-in or even travel to the remote building. This saves time and increases service levels, resulting in happier customers.

Predictive maintenance use cases

The edge intelligence functionality provided by Barracuda Secure Connector devices enable advanced use cases like automatic maintenance ticket generation.

As an example: For an air filter as part of a heating system a simple air pressure sensor before the filter and after the unit gives a reliable indication when the filter needs to be replaced. The edge intelligence functionality of the Secure Connector devices reads out the pressure difference and - once it exceeds a certain threshold - automatically generates a maintenance ticket. This makes sure the filter is renewed exactly at the time it is needed without generating additional cost.

"Deployment of the Barracuda Secure Connector appliances with zero-touch deployment was straightforward and fast."

Tom Stevens
Sr. Security & Automation engineer
Van Dam Groep

About Barracuda Industrial IoT Solutions

Barracuda CloudGen Firewall solutions for Industrial IoT are a family of highly secure, small form-factor devices for advanced network security, encrypted communications, and cost-effective connectivity. Full integration into Barracuda Firewall Control Center architecture guarantees hassle-free centralized management for tens of thousands of remote devices. The encrypted connection between the 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 than other competitive VPN solutions. Advanced security functions include application enforcement, IPS, URL filtering, antivirus, sandboxing (ATP), and denial-of-service protection. These functions are handled centrally and scalable on the Secure Access Controller.

Learn more about Barracuda securing the internet of things

barracuda.com/iot

Barracuda
Your journey, secured.