



Learn how Penn State protected and segmented their building control systems in record time and enabled secure remote access.

Secured infrastructure and simplified management for Penn State University

Airwall provides secure network connections for the Penn State campus in record time with no additional infrastructure or head count required.



Challenges

The university's shared infrastructure of over 640 buildings statewide featured no isolation or segmentation and was exposed to thousands of attack vectors. Downtime, incessant alarms, and unrestricted vendor access further complicated their network management.



Solution

The team deployed the Airwall Solution on their own without support from other teams, new hires, or additional infrastructure. They connected, isolated, and cloaked building controls across their entire infrastructure and segmented network access control for employees, clients, and vendors.



Wins

Deploying 10 times faster than alternative solutions and with significant hardware cost savings, the university reduced their attack surface by 90%, eliminated broadcast storms, reduced alarms by 50%, and easily connected new and remote buildings.

“Our increasingly connected world can certainly bring exciting opportunities and efficiencies, but we can only be successful if we can network systems in a highly secure and scalable way.”

Tom Walker
Head of Facilities Automation Services (FAS)

The challenge

The facilities automation services (FAS) group at Penn State needed to centralize and isolate plant services across university buildings statewide — a seemingly impossible task, given that building-specific systems were on the same flat network as servers for HR, finance, etc. A lack of adequate segmentation and isolation completely exposed the entire network to lateral attacks.

“I took over this infrastructure when it was a flat, Layer 2 network across the main campus about four years ago,” explained Tom Walker, system design specialist and head of the FAS group. The network had grown organically over the years and added a new routed Layer 3 network, consisting of more than 600 switches and routers across 24 physical campuses.

The university’s large vendor ecosystem only made things worse, as manually configuring remote VPN access for outside vendors was both complicated and ineffective. On-site vendors increased security risks by adding their own switches, access points, and wireless routers to the Layer 2 network.

As if the FAS group didn’t have enough on their hands, frequent broadcast storms and 100,000-plus weekly HVAC and other alarms further limited their availability for larger security concerns.

The solution

Finding a solution that met the FAS team’s requirements wasn’t easy.

“We looked at creating separate VLANs or [private VLANS] within the buildings, doing MAC filtering, doing access control lists, or doing building-level firewalls,” Walker explained.

“But when we started looking at scalability, it [got] crazy. For some of those options, I’d have to hire at least two more people just to manage and coordinate the combination of tools.”

A proof-of-concept of the Airwall showed them that it didn’t have to be so complicated. “In less than 20 minutes, we were able to install our first cloaked overlay network without having to modify systems or involve external departments,” Walker said.

This ease of management and non-disruptive deployment was crucial to the FAS group, allowing them to manage the network re-architecture and deploy on their own — without involving other teams, hiring more people, or purchasing additional infrastructure.

Customer success

Quick, cost-effective deployment: Tom and his team connected 50 buildings in just five days and all buildings in 75 days, deploying 10 times faster than alternative solutions. They now manage their own updates and changes from a single pane of glass.

Enhanced network security: The Airwall overlay network allowed the FAS group to isolate and cloak all systems within their BAS infrastructure, eliminated the need for public IP addresses, and segmented network access control for employees, contractors, and vendors — reducing their total attack surface by almost 90%.

Superior network availability: Isolating and segmenting their BAS allowed the team to eliminate broadcast storms, increase network performance, and reduce alarms by 50% in the first two months, freeing them up to focus on proper data tolerance.

Better business intelligence: The FAS group centralized control and data collection with a solution that allowed them to easily and securely connect any building across the state. Analyzing the collected data helps them save money through improved building efficiency and predictive maintenance.

Taking it further

As the FAS group continues to expand campus properties, they're finding that they can connect to increasingly remote sites across separate networks using Tempered's broad connectivity options. Most recently, they connected a building in the middle of a cornfield using cellular, where it would have cost over \$100,000 to establish a

fiber connection. "We're able to deploy in places that we weren't able to get to before," Walker explained.

"I wanted something that we could easily deploy and rapidly secure the infrastructure down. Now we have a private and isolated network for all our legacy and new BACnet systems. It's now simple and fast to connect and segment any building controls, over any network."

Tom Walker
Head of Facilities Automation Services

Deployed Airwall Solution components

Airwall Conductor, Airwall Relays, Airwall Servers, Airwall Gateways, and Airwall Agents created a solution that enabled the FAS team to segment and cloak all Penn State's building control systems.



Airwall Conductor: The orchestration engine allowed the FAS team to provision, segment, allocate, and revoke network access in the cloud. They deployed the Conductor so they could visualize their segmentation and whitelist endpoints at a granular level.



Airwall Relay: The FAS team deployed Relays (identity-based routing devices) in front of the overlay network in the cloud to securely connect and route traffic across the enterprise WAN using encrypted tunnels. The routing devices enable traffic from other locations to access databases and applications at Penn State quickly and securely — without the need for expensive firewalls or a complicated VPN.



Airwall Server: Airwall Servers allowed the team to enable software-defined segmentation for building systems, encrypt at the individual server level, and enforce a perimeter around each server. Additionally, each server is now cloaked, so only authenticated and authorized endpoints can discover and communicate with it.



Airwall Gateways: Physical Airwall Gateways were deployed in front of buildings to cloak and segment the building control systems.



Airwall Agents: Secure remote access was enabled for employees and technicians who needed access to building control systems, with Airwall Agent software on their devices.



Tempered delivered defense-in-depth

- 1 Zero-Trust Network Access (ZTNA)
- 2 Software-Defined Network (SDN)
- 3 Software-Defined Perimeter (SDP)
- 4 Multi-Factor Authentication (MFA)
- 5 Micro-segmentation for every endpoint
- 6 Lateral movement eliminated

without expense-in-depth

 25% of the cost of traditional IT solutions

 Deployed in 75 FTE days instead of 2,500 FTE days

 Did not require additional network admins

**Want to see what Airwall can do for you?
Schedule a meeting with our experts to learn more.**

experts@tempered.io | +1 206.452.5500