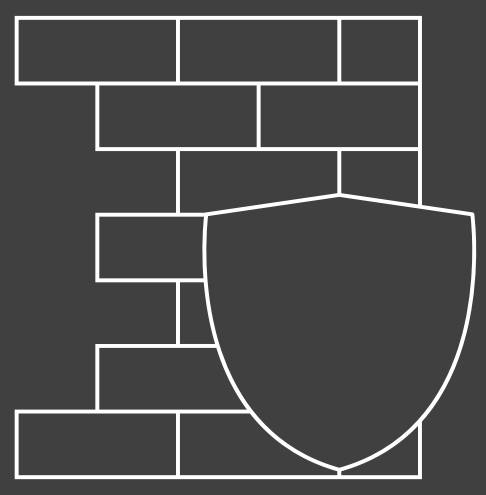
8 Reasons Firewalls Are Failing Us

(and What We're Doing About It)



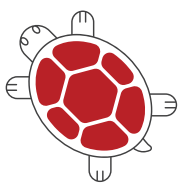
Let's be honest. Next Generation Firewalls are nearly two decades old — launched in 2008, not long after the first iPhone. They weren't built for the world we live in now — especially not for OT environments. Here's where they're falling short — and why it matters more than ever:

Outbound = Inbound

When you allow outbound connections—even to a website—you're opening the door to command—and—control malware.
That's how ransomware moves in.

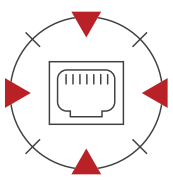
Default "Permit All" Rules

Too many firewalls ship with open rules for the sake of convenience.
Unless you catch every single default setting, you're exposed.



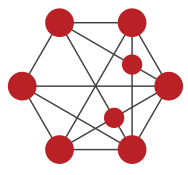
Patching Takes Too Long

Industrial sites can't just reboot for every new patch. About 35% of industrial CVE's won't be patched because the vendor EOL'd that system or, in some cases, the vendor is out of business.
Attackers know exactly which outdated versions to look for — and they find them fast.



Admin Interfaces Left Wide Open

Web consoles. Serial ports. Default passwords are still in place.
All it takes is one forgotten interface for someone to walk right in.

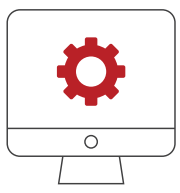


Complexity Is the Enemy

Managing firewalls is a full-time job. When key staff leave or get stretched too thin, mistakes happen — and attackers are waiting.

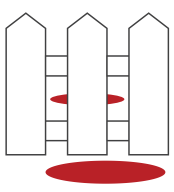
Weak Segmentation

Most OT environments are flat, for a very good reason - performance. Segmenting can lead to process disruption if too much latency is introduced. Therefore, in these cases, if an attacker compromises one system, they shouldn't be able to move sideways.
But without strong segmentation, they usually can — and do.



Trusting Old Tech

Legacy systems don't age well.
They weren't built for today's threats, but they're still running the critical operations that keep society moving.



Thinking the Perimeter Still Matters

When every contractor, cloud app, and remote user punches a hole through your perimeter, what's left to defend?
You need security that's built for an always-connected, distributed footprint world.

How BlastShield Protects You

- Passwordless Authentication
- Network Cloaking (Invisible Networks)
- True Segmentation
- Protection for Legacy Systems
- Easy, Lightweight Deployment

Protect your critical infrastructure before attackers get in.

SCHEDULE A DEMO AT WWW.BLASTWAVE.COM

BlastWave

www.blastwave.com