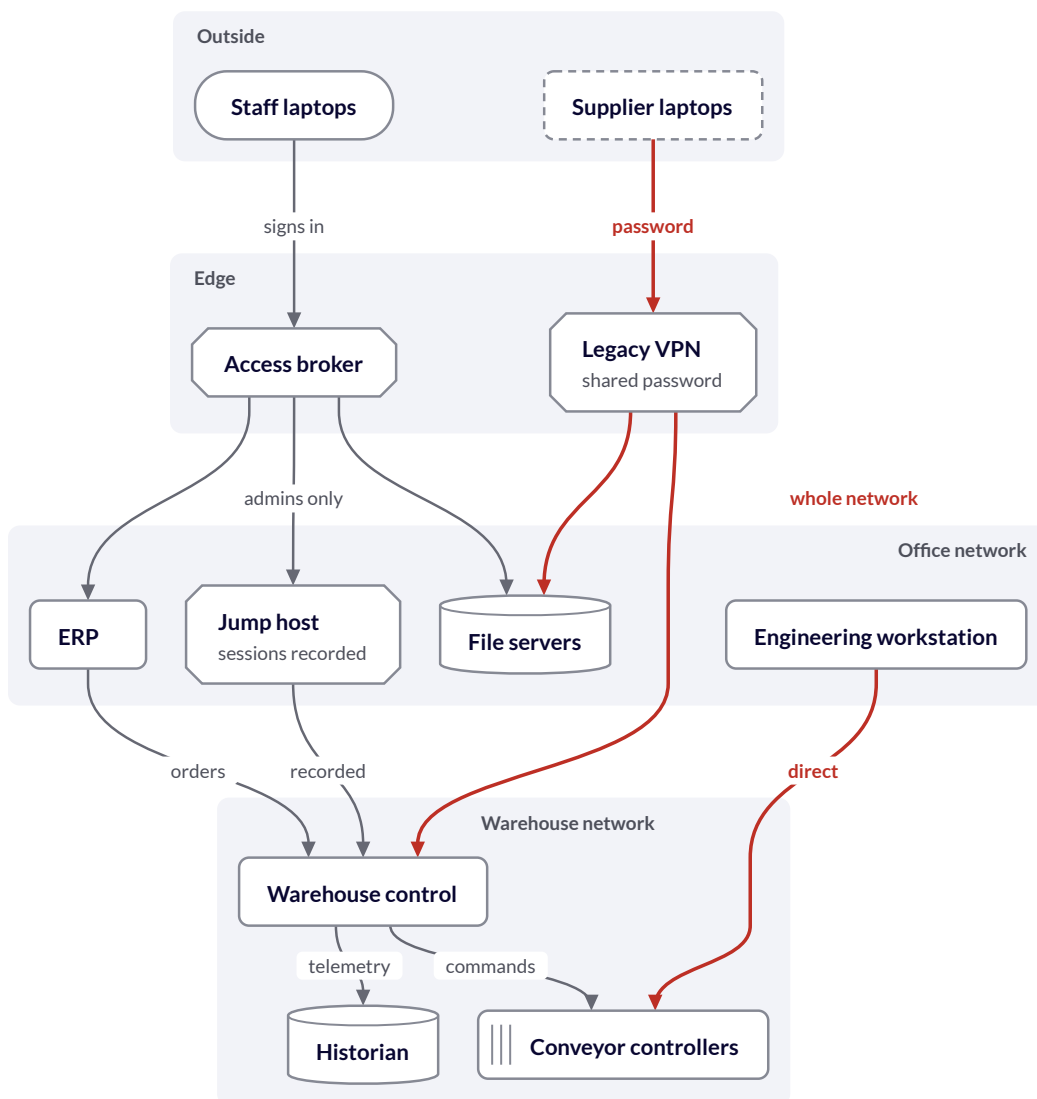


Two routes reach the warehouse controls unchecked

Three connections, drawn in red, skip the controls that the others pass

Who can reach what, from outside to the warehouse floor. Point at a system to trace what feeds it and what it feeds

— Call — Skips the controls



Source: firewall rules and flow records, 1 to 30 September 2026. Dots show direction; more dots, more sessions.

Prepared by Hunt & Hackett for the head of infrastructure, Meridian Freight. 14 October 2026.

Nine of twelve flows pass a control; three do not

Every managed route into the warehouse network goes through one recorded door, the jump host. The legacy VPN and one engineering workstation go around it, and the VPN also opens the file servers.

We listed every flow that crosses a zone boundary and asked one question of each: what checks who is connecting? For nine, the answer is the access broker, the jump host or a fixed service account. For three, it is a shared password or nothing.

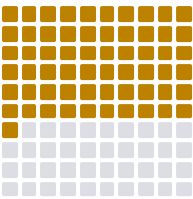
Flows across zone boundaries, September 2026

From	To	What checks it	Sessions a day	Finding
Staff laptops	Access broker	Sign-in, device check	2,400	● Managed
Access broker	ERP	Per application	1,900	● Managed
Access broker	File servers	Per application	420	● Managed
Access broker	Jump host	Administrators only	80	● Managed
Jump host	Warehouse control	Recorded session	80	● Managed
ERP	Warehouse control	Service account, one port	3,100	● Managed
Supplier laptops	Legacy VPN	Shared password	46	◆ Close
Legacy VPN	Warehouse control	Nothing: whole network	15	◆ Close
Legacy VPN	File servers	Nothing: whole network	31	◆ Close
Engineering workstation	Conveyor controllers	Nothing: direct	12	◆ Move to jump host
Warehouse control	Conveyor controllers	Fixed addresses	8,600	● Managed
Warehouse control	Historian	Fixed addresses	1,440	● Managed

The firewall allows far more than the flows need

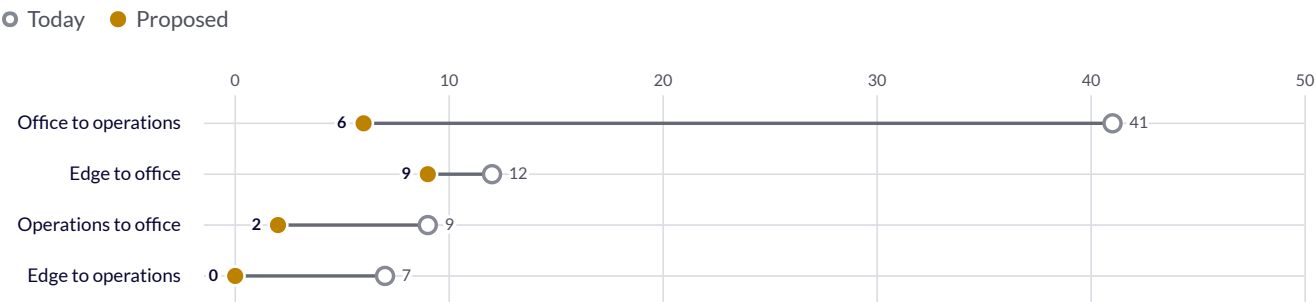
The three red routes exist because the rules permit them. Between office and operations, 61 of every 100 rules allow any port. Rewriting the rules around the nine managed flows closes most of what is open and breaks nothing we observed in September.

61 of 100 rules allow any port



The proposed rules close 35 of the 41 open paths from office to operations

Pairs of systems that can connect across each boundary, today and under the proposed rules



Source: firewall configuration of 30 September 2026, and the rule set proposed in annex B.

Three changes, in the order we would make them

1 Move both suppliers to the access broker

Then switch the legacy VPN off. Removes three of the three red routes' starting point. Six weeks.

2 Put the engineering tool on the jump host

The vendor supports it. Sessions to the controllers are then recorded like every other. Two weeks.

3 Replace the "any" rules with the nine flows

Run the new rules in log-only mode for a month first, so nothing breaks unseen.

Method

Flows are from firewall and switch records for 1 to 30 September 2026, grouped by source and destination system. A "session" is one connection from start to end. Open paths were counted from the rule set, not from traffic, so they include paths nobody used.