

GUIDE · INTEGRATION

EdgeGate as Your OT Router and Firewall

Routing, segmentation, industrial protocols, remote access and a tamper-evident record of who was on the network — deploying one fanless appliance inline, where the traffic already is.

Contents

1	Why a plant needs its own router	3
2	A rule list is a list of what is permitted	4
3	Industrial protocols, natively	6
4	A backup should never delay a poll	7
5	Remote access, and a record of who was there	8
6	A log that cannot be quietly edited	9
–	Specifications and next steps	10
–	Sources and related reading	11

Most network equipment is designed for offices, then sold to factories. EdgeGate was designed the other way round. This guide covers what it takes to deploy EdgeGate as the router and firewall at an OT boundary – segmentation that holds, protocols the plant already speaks, traffic that cannot be starved by a backup, and a record of every change that is good enough to hand to an auditor.

Product	EdgeGate — industrial edge router
Replaces	Router, firewall, traffic shaper, protocol gateway, remote-access server, compliance logger
Audience	Network and OT engineers planning or hardening a plant-floor or branch boundary

1. Why a plant needs its own router

An OT network is not an IT network with machines on it. Three things about a plant floor shape every decision inside EdgeGate.

- **Availability first.** A control network can survive being read. It cannot survive being interrupted. Blocking a legitimate command to a filler is worse than most intrusions, so nothing here fails closed by surprise: policy changes that could cut you off apply behind a rollback timer — any change that would cut off the person making it, not merely one page's worth — and a rule that stops matching says so instead of going quiet.
- **Already inline.** Everything EdgeGate sees, it sees because the traffic passes through it. No SPAN port, no tap, no agent on a PLC that has not been patched since 2014 — and because it is inline, it can *prevent* rather than merely report.
- **One small box.** Fanless, DIN-mountable, no moving parts, and sized for a cabinet rather than a rack. Steady-state it uses about 75 MB of RAM and one per cent of a core, which is what lets it sit at every line instead of one per site.

Plain language, on every screen. Plant engineers are not network engineers, and should not have to become them. Every screen in EdgeGate explains what a setting changes, not just what it is called — in English, Turkish or Spanish, chosen per browser, so the operator on shift and the integrator who commissioned the line can each read it in their own language.

ONE APPLIANCE, REPLACING FIVE

- **Router and firewall** — VLAN segmentation between process, office, guest and CCTV networks, default-deny.
- **Traffic optimiser** — five priority bands, so a backup cannot delay a poll.
- **Protocol gateway** — reads Modbus, S7, OPC UA and CoAP natively and forwards the readings on.
- **Remote access** — WireGuard, or IKEv2 with the client every laptop and phone already has; IPsec or WireGuard site tunnels to headquarters.
- **Asset discovery** — a live inventory built entirely from traffic it was already forwarding.
- **Compliance recorder** — who was on the network and what they connected to, in a log that cannot be quietly edited.

8

PORTS · 6 COPPER, 2 SFP

4

OT PROTOCOLS NATIVE

5

PRIORITY BANDS

3

INTERFACE LANGUAGES

2. A rule list is a list of what is permitted

Forwarding is denied by default, so every rule adds capability rather than removing it — and reading the list tells you the whole policy. Rules are evaluated top to bottom, first match decides, in one global order that is the same order the kernel enforces.

#	ACTION	SOURCE	DESTINATION	SERVICE	HITS / MIN
01	ACCEPT	OT-HISTORIAN	SCADA-HMI	MODBUS/TCP	842
02	ACCEPT	VLAN200/ANY	HISTORIAN-01	OPC-UA:4840	311
03	DROP	ANY	EDGEGATE-MGMT	HTTPS:443	14
—	DROP	ANY — UNMATCHED	ANY	ANY	0

DEFAULT ACTION: DROP

FIRST MATCH WINS · REPLIES TO ACCEPTED CONNECTIONS ARE PERMITTED AUTOMATICALLY · NOTHING BETWEEN ZONES IS ALLOWED UNLESS A RULE SAYS SO

EdgeGate console · firewall rules, illustrative configuration

FOUR THINGS THE MODEL GUARANTEES

- **Changes cannot half-apply.** The whole rule set is rebuilt in a single kernel transaction. There is no window in which some rules are loaded and others are not — the state before and the state after are the only two states that ever exist.
- **Rules explain themselves.** Expand any rule and it is drawn out in packet order and restated as a sentence. Reading a rule back in words is how you notice it says something other than you meant — before the line stops rather than after.
- **It shares the box politely.** EdgeGate writes only into chains it owns. Container networking, VPN rules and anything else on the appliance survive every rebuild untouched.
- **Return traffic is understood.** A rule only has to describe the direction a connection starts in. The reply is accepted automatically, which removes the single most common cause of a rule set that half works.

Address translation, both ways. Masquerade hides plant networks behind the uplink; port forwards publish a single service inward. The firewall rule that lets a forward through is written for you and removed with it, so there is no orphaned opening left behind when a service is retired.

A RULE SET THAT STAYS READABLE AS IT GROWS

Every firewall is legible on the day it is written. The question is what it looks like after three years of small exceptions — and whether anybody can still answer “what applies to the plant floor?” without reading forty rules while holding the segmentation plan in their head.

- **Name a set of ports once.** A zone is a name for a group of interfaces — lan, ot, guest — and a rule written against the name follows the group, including ports added to it years later.
 - **Then read it back three ways.** *In order* is what the appliance will do. *By interface* answers “what have we written for M5?”, including the ones a port with no rules names as a finding rather than an omission. *By zone* gathers rules that name the segment and rules that name one of its ports.
 - **Is this rule doing anything?** Every rule carries the packets and bytes it has matched, so a rule that has done nothing for a year is visible — the beginning of a conversation about whether it should still be there.
 - **Rules that admit they are broken.** A rule that can never fire, because an earlier one already covers it, is marked. A rule naming a VLAN or a zone that no longer exists is reported as unable to apply rather than shown as active.
-

WHAT THE ROUTER ACCEPTS FOR ITSELF

Most appliances are hardened everywhere except at their own management interface. EdgeGate treats that as a policy in its own right: which ports may reach the API and SSH, what answers a ping, and which services are open — with the list of open services derived from the features actually enabled rather than maintained by hand.

- **A lock-out you can survive.** Any change that would cut off the person making it — not merely this page’s worth — applies behind a countdown. Confirm it and it stays; lose access and it reverts on its own, unattended.
 - **Turn a feature off, close its port.** Because openings follow the features that need them, disabling DHCP on a port closes its opening on that port and nowhere else.
 - **Contractors, gated and time-limited.** A captive portal can be placed on any port. Devices are blocked until someone signs in with an account that has its own expiry, bound to both the address and the hardware address.
-

3. Industrial protocols, natively

EdgeGate reads industrial equipment directly. Modbus/TCP, S7, OPC UA and CoAP are built in — polled on a schedule, converted to one common shape, and forwarded to wherever the data is needed. No separate protocol gateway, no OPC tunneller licence, and no second box in the cabinet.

OT ROUTING · POLLING PROFILES

PROFILE	PROTOCOL	DEVICE	READS	EVERY
Line 3 filler	S7	192.168.32.11	rack 0 · slot 1 · DB120	1 s
Flowmeter bank	Modbus	192.168.32.24	unit 1 · holding 40001 ×8	2 s
Capper torque	OPC UA	192.168.32.31	ns=2;s=Capper.Torque	5 s
Ambient sensors	CoAP	inbound listener	/sensors/temp, /sensors/rh	push

Forwarding channels → Historian (MQTT), SIEM (syslog), common JSON per tag

Each profile polls one device on its own schedule and forwards readings to a named channel

TIMING THAT SUITS THE EQUIPMENT

Poll intervals are per profile, because a modern PLC and a twenty-year-old RTU do not tolerate the same rate. Short intervals against slow devices cause timeouts that look exactly like faults, so the interval is a first-class setting rather than a global default someone has to discover.

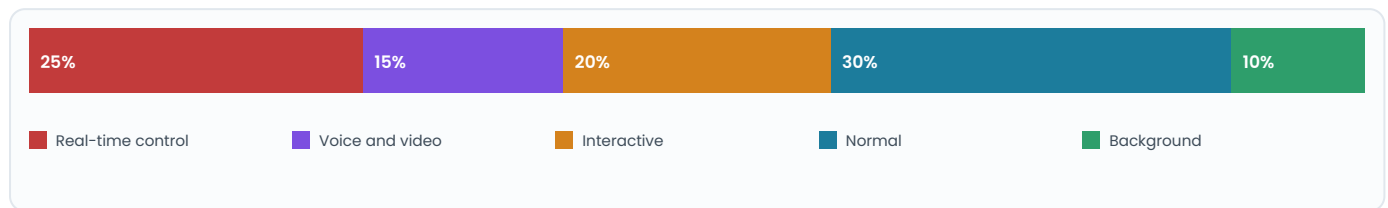
TRY IT BEFORE YOU COMMIT

A probe tool reads one device once, using exactly the same readers the scheduler uses. A successful probe means a profile with those settings will work — not merely that the machine answers a ping. When it fails, the reason comes from the protocol itself: a refused connection reads differently from a timeout, and both differently from a device that answered and rejected the request.

And the priority policy knows about all of it. The application catalogue recognises Modbus, S7, OPC UA, EtherNet/IP, PROFINET, DNP3, IEC 60870-5-104, BACnet/IP, CoAP, MQTT and more than 40 protocols in total — so “this is control traffic and it goes first” is one rule, written in the words the plant already uses.

4. A backup should never delay a poll

When the uplink fills, something has to wait. EdgeGate lets you decide what — by person and by application, not merely by address.



Five priority bands share the uplink; each gets a guaranteed floor, not a cap

- **Say what it is.** A rule names whose traffic it is — a signed-in person, a fixed HMI, a whole VLAN — and which application, from a catalogue of forty-four industrial and business protocols.
- **Say what it is worth.** Five bands, from real-time control down to background. Each gets a guaranteed share of the link — a floor it is entitled to whenever it has traffic, not a cap it is held to when the link is quiet.
- **Own the queue.** Set the link's rate just under what it really carries, and the backlog forms here, where the policy is — instead of in the carrier's equipment, where nothing can reorder it.

PRIORITISING A PERSON, NOT AN ADDRESS

An address is a lease. The shift supervisor who has to reach the line at two in the morning keeps that claim whichever laptop they picked up, so a rule names an identity and EdgeGate resolves it to whatever addresses that person currently holds — updated the moment they sign in or out. The same seam is already in place for 802.1X.

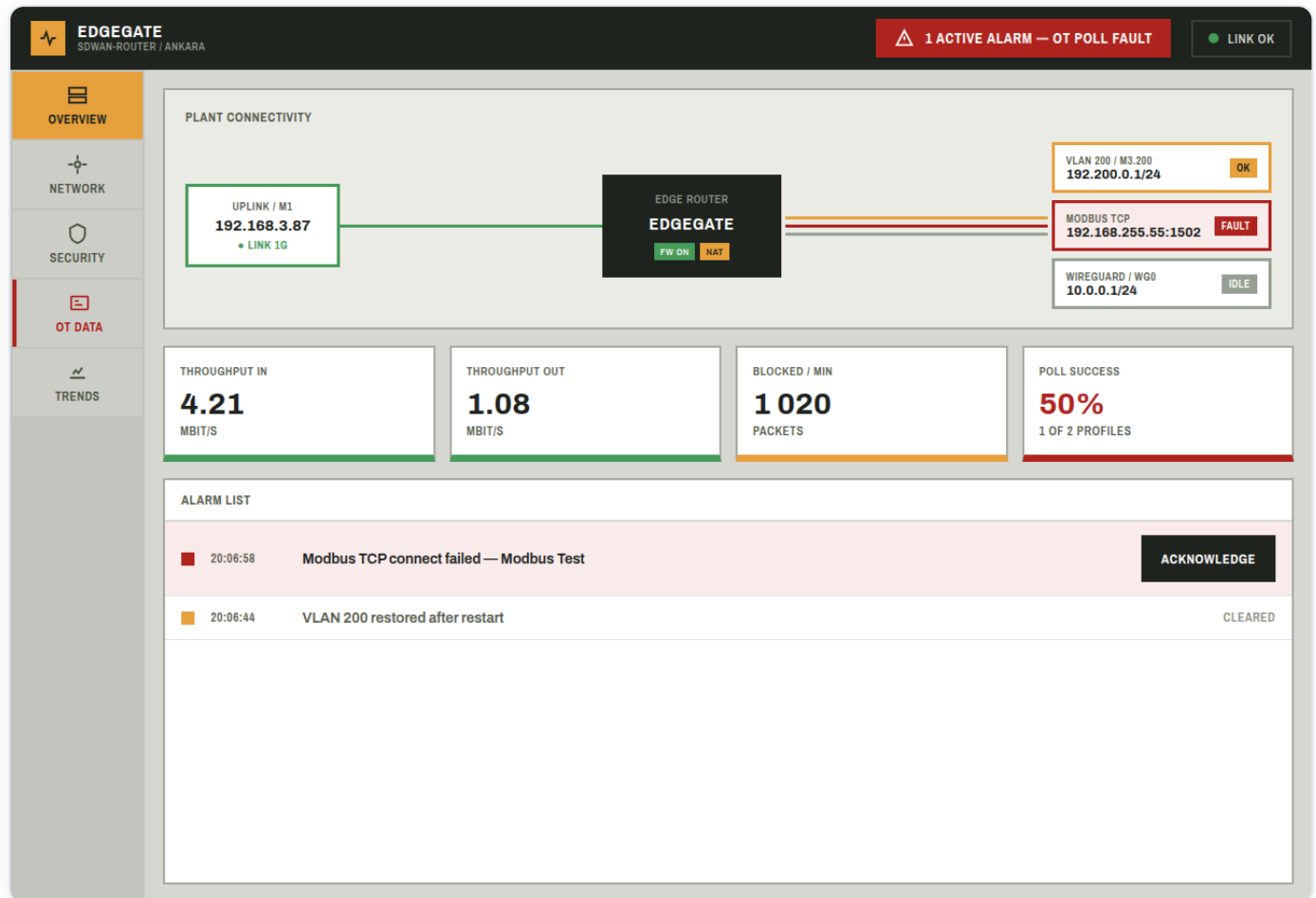
BOTH DIRECTIONS OF A CONVERSATION, ALWAYS TOGETHER

A flow is classified once, on its first packet, and the answer is carried on the connection. The reply — arriving on a different port with the addresses reversed — inherits it. That is what makes it impossible for one half of a control exchange to be prioritised while the other half queues behind a file copy.

And it says when it is not working. Priority means nothing on a link the appliance is not queueing for. Rather than let a correct-looking policy quietly do nothing, EdgeGate reports which links are actually being managed — and a packet tracer will tell you, for any flow you describe, which band it lands in and whether that band is worth anything on the port it leaves by.

5. Remote access, and a record of who was there

Two opposite directions, kept deliberately separate. Remote access brings people in: one server, many clients, each with its own key and its own reachable networks. Site tunnels join this plant to headquarters or to another site. Confusing the two is how remote-access setups end up routing more than they were meant to.



EdgeGate console · plant connectivity overview, illustrative configuration

- **Least privilege, per person.** Each client is routed only to the networks it is given. A contractor reaching one device reaches that device, and nothing else on the plant — the safe default rather than an accident.
- **Keys generated on the appliance.** For WireGuard, EdgeGate produces the client's whole configuration, including its key, so nobody exchanges material by hand. For a contractor who will not install software, the same page serves IKEv2 instead — a username, a password and the client already built into Windows, macOS, iOS and Android.
- **Honest status.** WireGuard keeps no connection, so “up” means the interface exists and “connected” means a handshake happened recently. EdgeGate shows both rather than collapsing them into a single light that means neither.
- **Overlapping addresses, solved.** When two sites number their networks identically, which they very often do, a tunnel can translate one side onto a different range of the same size, so the link works without renumbering a plant.

Every session is on the record. Remote sessions, portal sign-ins and the connections they opened all land in the tamper-evident store described overleaf. “Who was on the network last Tuesday, and what did they reach?” is a query, not an investigation.

6. A log that cannot be quietly edited

Every record carries the fingerprint of the one before it. Change a record, remove one, reorder two — the chain breaks from that point on, and verification names the exact record where it broke. That is the difference between a log file and a record: one is evidence, the other is a text file anyone with root can rewrite.

What is recorded	Detail
Portal activity	Sign-ins, failures and expiries, with addresses, ports and timing
Connections	Every connection a signed-in device opened, protocol, timing and the translated address it left by
Configuration	Every read and write of the records themselves, including who did it
Never recorded	Content. Traffic data only, ever — packet capture exists as a separate, administrator-only tool with its own limits

- **Deleted only for age.** Records are removed when they pass their retention period and for no other reason. If the disk runs short, the appliance raises an alarm rather than making room — the opposite of a ring buffer, and the only behaviour a retention obligation can survive.
- **Off the box, on a schedule.** A retention obligation that lives only on the appliance is one failed disk from being unmet, so records are shipped daily or weekly over HTTPS or SFTP, with the host key pinned. Shipping never deletes the local copy, and every attempt — successful or not — is itself written into the chain.

Said plainly, because your compliance officer will ask. A qualified timestamp from a licensed provider is on the roadmap for the append path. Today, the chain proves ordering and integrity against itself, not against trusted external time.

Specifications and next steps

Hardware	
Processor	Intel Atom C3558, 4 cores
Memory	16 GB
Network	6 × copper (M1–M6), 2 × SFP (T1–T2)
Cooling	Fanless, no moving parts
Security and audit	
Firewall	Default-deny forwarding; private rule chains rebuilt atomically
Management plane	Rollback timer on any change that would cut off its own author; service openings derived from enabled features
Remote access	WireGuard or IKEv2 (no client software); site tunnels over WireGuard or IPsec
Records	Hash-chained, append-only store; scheduled archiving over HTTPS or SFTP with pinned host key
OT and management	
Protocols polled	Modbus/TCP, Siemens S7, OPC UA, CoAP
Recognised for priority	EtherNet/IP, PROFINET, DNP3, IEC 60870-5-104, BACnet/IP, MQTT, FINS, MELSEC and more
Discovery	Entirely passive — vendor registry, DHCP fingerprinting, LLDP/CDP, mDNS/SSDP, behavioural inference
Fleet management	Optional Sphere Central: templates, canary-then-batch rollouts, hourly drift detection

Specifications describe the current release. Confirm exact figures for a given deployment against current Connexite product documentation at docs.connexite.co.uk.

Sources and related reading

Connexite. connexite.co.uk/edgegate — product page, and docs.connexite.co.uk for current configuration reference.

EdgeGate for multi-site estates. The companion datasheet on fleet rollout with Sphere Central, available from the Resources page.

Complementing OT Visibility Platforms. How ConnexSight, ConnexGate and ConnexONE sit alongside Claroty, Dragos and Nozomi Networks — also in Integration Guides.

Talk to us about your deployment

Our engineering team can help you plan a single-site rollout or a multi-branch estate running from one standard build.

connexite.co.uk/contact

connexite.co.uk/edgegate