

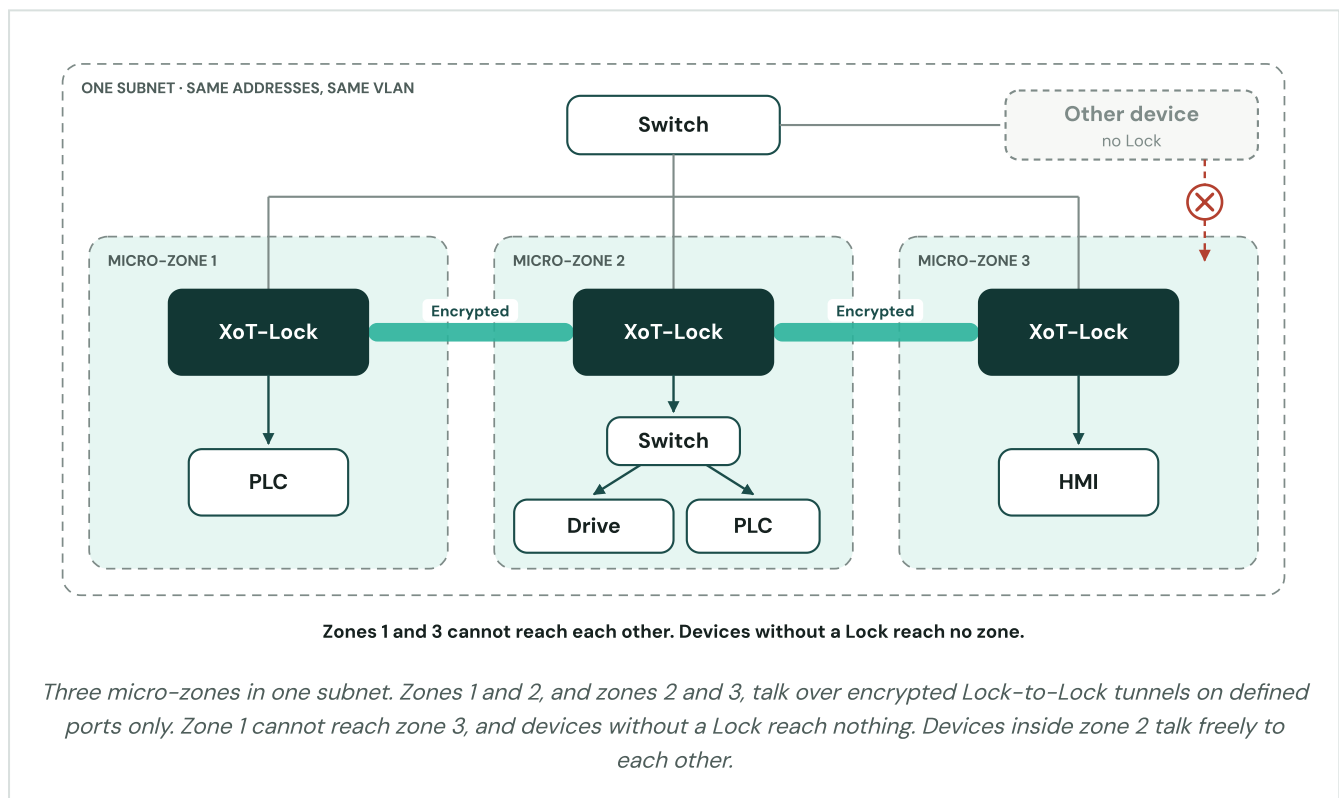
GUIDE IN SEVEN STEPS

Micro-segmentation with Hide and Protect

This guide describes a seven-step method. With it, you divide an existing network into policy-controlled micro-zones using XoT-Lock and the Hide and Protect licence. The equipment keeps its IP addresses, VLANs and settings, and the method reduces the risk of disrupting operations. Micro-zones can span subnets and VLANs, or sit inside a single flat subnet.

01 Target state

Each micro-zone sits behind its own XoT-Lock in transparent mode. Everything is denied by default. Permitted traffic between zones runs in encrypted Lock-to-Lock tunnels, on defined ports only. The example shows one possibility: micro-segmentation inside a single subnet.



02 The method at a glance



Steps 1–2 are desk work. Steps 4–5 are a temporary learning period. No traffic is blocked until step 7.

03 Step by step

1 Identify devices

Know exactly what is on the network

- **Inventory every device** in the network to be segmented: IP address, MAC address, function, vendor and who maintains it.
- **Rate criticality.** Which devices are vulnerable, legacy or safety-relevant? They get the tightest protection.
- **Use existing sources:** network drawings, switch MAC tables, SCADA configuration and vendor documentation.
- **Decide the classification** for policies: Asset Type and Asset Group (what), Country, City, Address and Room (where).

OUTPUT

Asset list with classification tags.

2 Identify layer 2 domains

Decide the micro-zones

- **Only IP traffic crosses a Lock.** Layer 2 protocols do not. Find devices that depend on layer 2 communication with each other, such as PROFINET RT or IEC 61850 GOOSE.
- **Put devices that communicate at layer 2 behind the same Lock,** for example via a small switch on the Lock's DEVICE port.
- **Everything else gets its own zone.** Ideally one Lock per device.
- **Remember:** traffic between devices in the same zone does not pass the Lock and is not filtered.

OUTPUT

Zone map: which devices sit behind which Lock, and how many Locks are needed.

3

Install Locks, keep IPs

Insert enforcement without re-addressing

- **Plan each Lock's own address:** IP, gateway, DNS and NTP. Verify the path to the XMS on TCP 443 via the NETWORK port.
- **Install inline in transparent mode:** NETWORK port to the existing switch, DEVICE port to the device or cell switch.
- **Enrol each Lock** in the XMS and define the protected devices as assets with the tags from step 1.
- **No device changes** IP address, netmask, gateway or VLAN.

OUTPUT

Enrolled Locks, assets defined in the XMS.

IMPORTANT The Lock denies everything by default. A Lock without an active policy forwards nothing. Create the allow-all policy (step 4) before the Lock is inserted, or do both in the same maintenance window.

4

Set an allow-all policy

Keep operations running while learning

- **Create a temporary any-to-any policy** per Lock: any source, any destination, all ports and protocols.
- **Name it clearly** as temporary, with a date, so it is never forgotten.
- **Verify** that the process runs exactly as before the Locks were installed.

OUTPUT

Locks in place, operations running as before.

5

Enable Traffic Discovery

Capture the real communication

- **Enable Traffic Discovery** on each Lock. Each flow is recorded with source, destination, ports and protocol, and sent to the XMS.
- **Capture a full operating cycle:** all shifts, batch runs, weekly jobs such as backups, and maintenance or vendor sessions.
- **Rare events matter most.** A flow that only happens once a month will otherwise be blocked later.

OUTPUT

Traffic list per device: who it talks to, on which ports and how much.

6 Analyse data and create policies

Turn observed flows into least privilege

- **Device** → **device in another zone** → Lock-to-Lock policy (client Lock → server Lock) on the exact ports.
- **People** (operators, engineers, vendors) → user-group policies via XoT-Desktop Client or XoT-WebAccess, time-limited where possible.
- **Device** → **systems outside the Locks** (historian, SCADA, patch server) → outbound policy, preferably to a registered Unprotected Asset.
- **Unknown or unexpected flows** → investigate before allowing. Not every observed flow is needed.
- **Review the policy set** with operations and the device owners before it goes live.

OUTPUT

Reviewed policy set, saved but not yet active (Inactive).

7 Apply policies

Switch to default deny

- **Plan a maintenance window** and go zone by zone, starting with the least critical.
- **Activate the scoped policies and remove the allow-all policy** for that zone.
- **Verify operations** with the process owner before moving to the next zone.
- **Rollback:** keep the allow-all policy saved as Inactive, so it can be re-activated in seconds.

OUTPUT

Micro-segmented network.
Documented zones and policies.

04 Rules that apply throughout

- ☐ **Licence:** micro-segmentation requires the Hide and Protect licence for each protected machine. With Remote Access alone, the Lock runs in open mode and cannot block LAN traffic or restrict outbound traffic.
- ☐ **Capacity:** encryption limits how much traffic a Lock can carry. Plan for large flows between zones, and use the software Lock for the heaviest flows.
- ☐ **Timing:** permanent policies for machine-to-machine flows, time-limited policies for people.
- ☐ **Support:** your partner provides first-line support. For harder questions, the partner gets help from Xertified.

CRITICAL The XMS, NTP and DNS servers must never be defined as a protected asset or appear as a destination in any policy, not even when they sit in the same subnet. The Lock has a single routing table, and management traffic must stay outside the tunnels.