OT Network Segmentation

Implementing Defense in Depth for Industrial Networks

OT Security Learning Series

Document 300 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Network segmentation is the practice of dividing a network into smaller, isolated segments to limit the spread of attacks and control traffic flow. In OT environments, proper segmentation is one of the most effective security controls available.

Information

Network segmentation is consistently identified as a critical missing control in post-incident analyses. Flat networks allow attackers to move laterally from initial compromise directly to critical control systems.

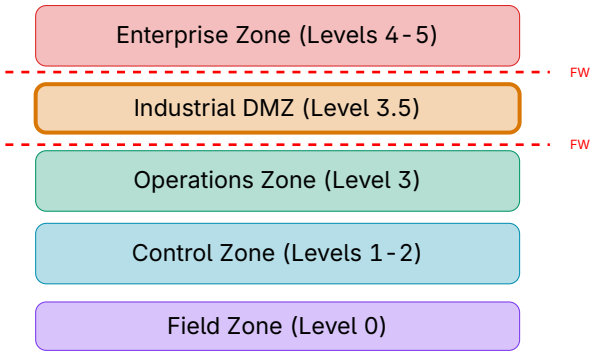
1.1 Why Segmentation Matters

- **Limits blast radius:** Compromises contained to single segment
- **Controls data flow:** Only authorized traffic between zones
- **Enables monitoring:** Choke points for traffic inspection
- **Supports compliance:** Required by IEC 62443, NIST, NERC CIP

2 Segmentation Models

2.1 Purdue Model Application

The Purdue Model provides the conceptual framework; segmentation is the implementation:



2.2 Zone and Conduit Model (IEC 62443)

Zones and Conduits

- **Zone:** Grouping of assets with common security requirements
- **Conduit:** Controlled communication path between zones
- **Security Level:** Target security capability for each zone (SL 1-4)

3 Implementation Approaches

3.1 Physical Segmentation

- **Separate physical networks:** Different cables, switches, infrastructure
- **Air gaps:** Complete physical isolation (increasingly rare)
- **Data diodes:** Hardware-enforced unidirectional communication

Tip

Physical segmentation provides the strongest isolation but is costly and inflexible. Use for the most critical systems where risk justifies the expense.

3.2 Logical Segmentation

- **VLANs:** Layer 2 separation on shared infrastructure
- **Firewalls:** Layer 3/4 traffic filtering between segments
- **ACLs:** Router-based access control lists
- **Software-defined networking:** Centralized policy enforcement

3.3 Comparison

Method	Security	Cost	Flexibility
Air Gap	Highest	High	Very Low
Data Diode	Very High	High	Low
Physical Separation	High	Medium-High	Low
Firewalls + VLANs	Medium-High	Medium	High
VLANs Only	Low-Medium	Low	High

4 Industrial DMZ Design

4.1 Purpose

The Industrial DMZ (Level 3.5) serves as a buffer zone:

- **No direct IT-OT connections:** All traffic proxied through DMZ
- **Services hosted in DMZ:** Jump servers, historians, patch servers
- **Dual-firewall architecture:** Separate firewalls on each side

Critical

Never allow direct connections from enterprise networks (Level 4-5) to control systems (Level 0-2). All communication must pass through the DMZ.

4.2 Common DMZ Services

Service	Purpose
Jump Server / Bastion Host	Controlled remote access point
Historian Mirror	Replicated process data for business use
Patch Repository	Staging area for OT software updates
AV Update Server	Antivirus signatures for OT systems
Remote Access Gateway	VPN termination and access control

5 Firewall Rule Design

5.1 Principles

Key Point

Firewall rule design principles:

1. **Default deny:** Block all traffic not explicitly permitted
2. **Least privilege:** Allow only required protocols and ports
3. **Source/destination specific:** No “any” rules
4. **Direction matters:** OT initiates outbound; block inbound
5. **Log denied traffic:** For detection and troubleshooting

5.2 Example Rule Set

DMZ to OT Zone (Level 3) rules:

Action	Source	Dest	Port	Proto	Purpose
Allow	Historian-DMZ	Historian-OT	1433	TCP	DB replication
Allow	Jump-Server	Eng-WS	3389	TCP	Remote access
Allow	Patch-Server	OT-Servers	445	TCP	Updates
Deny	Any	Any	Any	Any	Default deny

6 Common Mistakes

Warning

Segmentation pitfalls to avoid:

- **VLANs without firewalls:** VLANs alone don't filter traffic
- **Overly permissive rules:** "Allow any" defeats the purpose
- **Dual-homed systems:** Workstations bridging zones
- **Forgotten connections:** Vendor modems, cellular gateways
- **No monitoring:** Segmentation without visibility
- **Static rules:** Never reviewed or updated

7 Validation and Maintenance

7.1 Testing Segmentation

- **Network scanning:** Verify only expected hosts reachable
- **Rule review:** Audit firewall rules regularly
- **Traffic analysis:** Confirm actual flows match policy
- **Penetration testing:** Validate segmentation effectiveness

7.2 Ongoing Maintenance

- **Change management:** Document and approve all rule changes
- **Regular audits:** Quarterly review of firewall rules
- **Asset inventory:** Keep zone assignments current
- **Incident integration:** Update rules based on lessons learned

8 Further Reading

Standards

- **IEC 62443-3-2** – Security Risk Assessment and Zone/Conduit Design
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Network Segmentation Fact Sheet
  https://www.cisa.gov/resources-tools/resources