Industrial Firewalls

Network Security Controls for OT Environments

OT Security Learning Series

Document 307 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Firewalls are fundamental security controls that enforce network segmentation by controlling traffic between zones. In OT environments, firewalls must balance security requirements with operational constraints including real-time performance, protocol support, and high availability demands that differ significantly from IT deployments.

Information

This document covers firewall technologies for OT environments, including types, deployment architectures, OT-specific requirements, and configuration best practices. Understanding industrial firewall capabilities and limitations is essential for effective network segmentation.

2 Firewall Types

2.1 Technology Overview

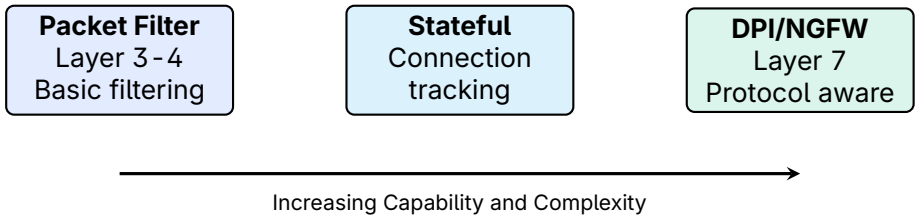

Figure 1: Firewall technology spectrum

2.2 Comparison

Type	Capabilities	OT Advantage	Limitation
Packet Filter	IP/port filtering	Low latency, simple	No state tracking
Stateful	Connection tracking	Blocks unsolicited traffic	Limited protocol insight
Application-Aware	Protocol validation	Detects protocol abuse	Requires protocol support
NGFW/DPI	Deep inspection, IPS	Content inspection	Higher latency, complexity

Table 1: Firewall type comparison

2.3 Deep Packet Inspection for OT

DPI-capable firewalls can inspect OT protocol content:

- **Modbus:** Validate function codes, register addresses
- **DNP3:** Inspect object types, function codes

- **OPC UA:** Validate service requests, node access
- **EtherNet/IP:** Inspect CIP services and objects
- **S7comm:** Monitor read/write operations to PLCs

Warning

DPI for OT protocols requires specific protocol support. Not all firewalls support all industrial protocols. Verify protocol coverage before deployment.

3 OT-Specific Requirements

3.1 Operational Constraints

Requirement	Description
Low latency	Control loops require predictable, minimal delay
High availability	Process cannot tolerate firewall failures
Protocol support	Must understand OT protocols for effective filtering
Environmental	May need ruggedized hardware for plant floor
Long lifecycle	Must remain supportable for 10-20 years
Deterministic behavior	Consistent performance under all conditions

Table 2: OT firewall requirements

3.2 Performance Considerations

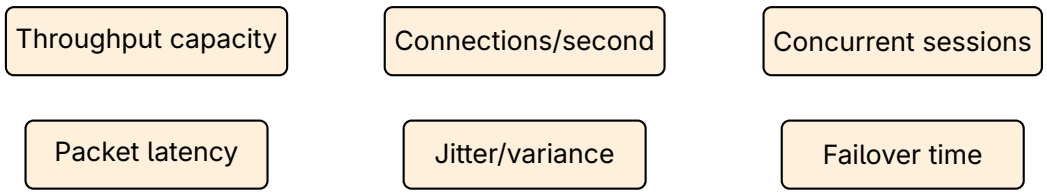

Figure 2: Key performance metrics for OT firewalls

Tip

For time-critical control traffic, measure latency under load conditions, not just rated throughput. A firewall meeting bandwidth requirements may still introduce unacceptable latency for real-time protocols.

3.3 High Availability

OT firewalls typically require redundant deployment:

- **Active/Passive:** Standby unit takes over on failure
- **Active/Active:** Load sharing with automatic failover

- **Bypass mode:** Fail-open option for critical paths (use cautiously)
- **Stateful failover:** Sessions maintained during switchover

Critical

Fail-open bypass modes maintain availability but eliminate security protection. Use only where safety or process requirements absolutely demand it, and implement compensating controls.

4 Deployment Architectures

4.1 Zone Boundary Protection

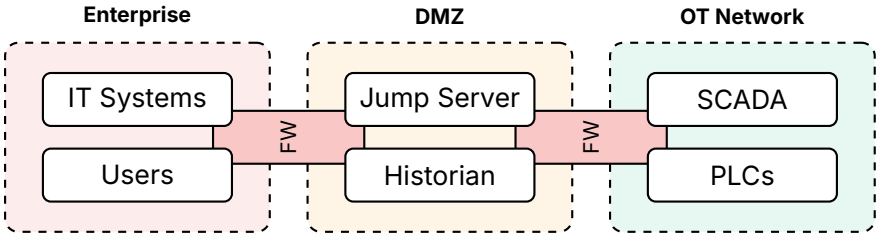

Figure 3: Firewall placement at zone boundaries

4.2 Cell/Area Protection

Within OT networks, firewalls can isolate individual cells:

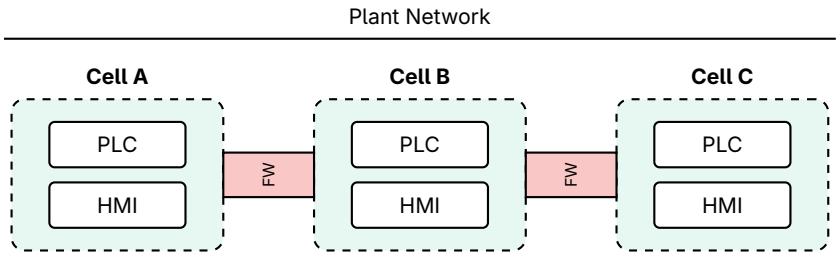

Figure 4: Cell-level firewall segmentation

4.3 Deployment Considerations

Location	Purpose	Typical Rules
IT/OT boundary	Isolate enterprise from OT	Strict allow-list, limited services
DMZ boundaries	Control data exchange	Specific app flows, no direct IT-OT
Cell perimeter	Contain lateral movement	Inter-cell traffic restrictions
Remote access	Secure external connections	VPN termination, MFA enforcement

Table 3: Firewall deployment locations and purposes

5 Configuration Best Practices

5.1 Rule Design Principles

- **Default Deny:** Block all traffic not explicitly permitted
- **Least Privilege:** Allow only required protocols and ports
- **Specificity:** Use specific IPs, not broad subnets where possible
- **Direction Awareness:** Consider which side initiates connections
- **Documentation:** Document business justification for each rule

5.2 Rule Structure Example

#	Source	Dest	Service	Action	Purpose
1	Historian	PLCs	Modbus/502	Allow	Data collection
2	Eng WS	PLCs	S7/102	Allow	Programming
3	Jump Host	HMIs	RDP/3389	Allow	Remote admin
99	Any	Any	Any	Deny	Default deny

Table 4: Example firewall rule structure

5.3 OT Protocol Rules

Key Point

Recommendation: For OT protocols, define rules at the application level where possible. Instead of just allowing TCP/502, use DPI rules that restrict specific Modbus function codes to authorized operations.

5.4 Change Management

Firewall rule changes require careful process:

1. Request with business justification
2. Security review and approval
3. Test in non-production if possible
4. Implement during maintenance window
5. Verify functionality and logging
6. Document change and update diagrams

6 Common Mistakes

Mistake	Impact
Any-to-any rules	Defeats purpose of segmentation
Disabled logging	No visibility into blocked or allowed traffic
Unused rules accumulation	Increases attack surface, complicates audits
No rule review process	Rules become stale, overly permissive
Bypassing for troubleshooting	Temporary bypasses become permanent
Single point of failure	Firewall failure impacts production
Ignoring outbound rules	Misses data exfiltration, C2 traffic

Table 5: Common firewall configuration mistakes

7 Monitoring and Maintenance

7.1 Logging Requirements

Essential logs to collect and monitor:

- **Denied connections:** Potential attacks or misconfigurations
- **Allowed connections:** Baseline for anomaly detection
- **Configuration changes:** Audit trail for compliance
- **Administrative access:** Who accessed the firewall
- **System health:** CPU, memory, session counts

7.2 Regular Review

- **Rule audit:** Quarterly review for unused or overly broad rules
- **Firmware updates:** Apply security patches during maintenance windows
- **Policy compliance:** Verify configuration matches security policy

- **Performance review:** Ensure capacity meets current demands

8 Summary

Key Takeaways

- **Technology Selection:** Choose firewall type based on required protocol visibility—DPI for OT protocol inspection, stateful for basic segmentation
- **OT Requirements:** Prioritize low latency, high availability, and OT protocol support over IT-centric features
- **Deployment:** Place firewalls at zone boundaries (IT/OT, DMZ) and consider cell-level segmentation for critical areas
- **Default Deny:** Start with deny-all and add specific allow rules with documented justification
- **High Availability:** Deploy redundant firewalls for production environments; avoid fail-open modes where possible
- **Change Control:** Implement formal change management for all rule modifications
- **Monitoring:** Enable logging, review regularly, and integrate with security monitoring

9 Further Reading

Standards and Guidelines

- **IEC 62443-3-3** – System Security Requirements and Levels
  https://webstore.iec.ch/publication/7033
- **NIST SP 800-82 Rev 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA** – Industrial Control Systems Security
  https://www.cisa.gov/topics/industrial-control-systems
- **SANS ICS** – Industrial Control Systems Security
  https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials

Books

- Knapp, Eric D. – *Industrial Network Security* (Syngress)
- Stouffer et al. – *Guide to ICS Security* (NIST)

Part of the OT Security Learning Series