Security Gateway for Automated Micro-Segmentation and VPN Encryption in Industrial Legacy Systems

Sabrina Kaniewski*, Lukas Bechtel*, Pascal Kneisel*, Michael Menth†, Tobias Heer*
*Esslingen University of Applied Sciences, Germany,
{sabrina.kaniewski, lukas.bechtel, paknit01, tobias.heer}@hs-esslingen.de
†Chair of Communication Networks University of Tuebingen, Germany, menth@uni-tuebingen.de

***Abstract*—In today's industrial networks, secure communication among participants is crucial. Security measures commonly employed in IT networks, e.g., network segmentation and Virtual Private Networks (VPN), prevent unauthorized access by restricting communication flows within logical segments and ensure data confidentiality by encryption, respectively. In industrial networks, however, security measures are often not used due to legacy devices lacking the required capabilities to implement them. Thus, maintaining network security is particularly difficult. In this work, we take up the concept of retrofitting security measures using a security gateway. The gateway is placed in front of a legacy device and takes over tasks such as micro-segmentation and VPN encryption. A resulting challenge is the derivation of appropriate micro-segments and VPN tunnels. We address this challenge using heuristics based on observed network traffic. We demonstrate the feasibility of the approach through a Proof-of-Concept (PoC). The proposed semi-automated approach allows for retrofitting of security measures, thereby ensuring a seamless migration from the existing to a more secure infrastructure and contributing to the secure integration of legacy devices.**

***Index Terms*—Network Security, Segmentation, Brownfield, Legacy Devices, Retrofit, Migration**

I. Introduction

Secure communication among networked devices is a critical requirement in today's industrial networks [1]. Commonly employed security measures in IT networks include segmentation and Virtual Private Networks (VPNs). Segmentation partitions networks into logical segments to restrict communication flows. Segments can range from groups of devices to fine-grained partitions at the level of individual devices or applications, i.e., *micro-segmentation*, and are typically implemented by firewalls. Encryption mechanisms, such as *VPNs*, protect insecure communication and ensure data confidentiality.

Industrial networks, such as those found in industrial plants or factory automation systems, have long operational lifetimes, strict compliance requirements, and slow adoption of new technologies. As a result, many older devices, which we refer to as *legacy devices*, remain in use. Legacy devices, e.g., Programmable Logic Controllers (PLCs), often communicate without encryption and authentication and lack access control mechanisms. These devices further lack the required computational capacities for such security measures and often cannot be retrofitted due to missing manufacturer support or standardization efforts [2]. This lack of built-in security measures allows an attacker to intercept and tamper with traffic, which can have a major impact on security.

This work has been funded by the BMWK under support code 16KN084434 Collaborative Project ESP, in part by the Federal States Program "FH-Personal" (FKZ: 03FHP115), funded by the BMBF and MWK Baden-Württemberg, and by the Deutsche Forschungsgemeinschaft (DFG) Project-ID 528745080 - FIP 68. The authors alone are responsible for the content of the paper.

Fig. 1: Security gateway implementing various security measures to securely integrate a legacy device into the network.

In this work, we present an approach to retrofit legacy devices with micro-segmentation and VPN encryption through a security gateway. A dedicated security gateway is placed directly upstream of each legacy device, cf. Figure 1. The gateway implements various security measures, including micro-segmentation (firewalling), authentication (802.1X), and encryption (VPN), to segment the network and secure communication of the legacy device to the network. The identification of appropriate micro-segments and VPN tunnels, however, is challenging. In particular, due to the traffic volume within a network, it is a labor-intensive and error-prone process if done manually. To automate the respective processes, we analyze network traffic and break it down into logical relations, deriving rules for micro-segmentation and VPN tunnel configurations accordingly. Overall, we aim to address the following challenges **C1-C3**:

- **C1** Identify communication relations to derive appropriate micro-segments.
- **C2** Allow for the encryption of insecure communication flows through VPN tunnels.
- **C3** Automate the respective configuration processes.

We provide a Proof-of-Concept (PoC) that addresses these challenges and demonstrates the secure integration of legacy devices. We contribute (i) open-source code for automated traffic analysis, segmentation, and VPN configuration, and (ii) a set of heuristics that guide the identification of insecure communication flows, supporting a practical adoption and migration towards secure industrial networks. The code and artifacts are available at https://github.com/hs-esslingen-it-security/hses-legacy-microsegmentation-vpn.

II. System and Threat Model

This work targets industrial *brownfield networks*, characterized by a heterogeneous mix of devices with and without

Accepted for publication in Proceedings of *30th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Porto, Portugal, September 9-12, 2025.

security measures. Legacy devices, with their lack of built-in security mechanisms, expose the network to a broad attack surface. Communication-related attacks are particularly critical in these environments, where insecure protocols remain prevalent, e.g., Modbus [3] or EtherNet/IP [4], and engineering and diagnosis protocols such as SNMP [5] or syslog [6]. We assume an attacker with access to the local network capable of performing the following attacks:

- *Unauthorized Access*: Access by unauthorized entities or lateral movement within the network.
- *Eavesdropping:* Interception of unencrypted communication to gain access to sensitive process data.
- *Tampering:* Injection of communication to alter device behavior or disrupt operations.

To mitigate these attacks, we propose dedicated security gateways. Each legacy device is paired with a gateway that retrofits critical security measures, e.g., 802.1X authentication and encryption, cf. Figure 1. We emphasize a strict *one-to-one association* between each gateway and its dedicated legacy device to ensure an unambiguous representation and secure integration. For the scope of this work, the gateway itself is assumed to be tamper-resistant, i.e., physical safeguards and mechanisms to detect unauthorized access or modifications. Further, the inherently insecure link between the gateway and the legacy device is protected using compensating tamper detection and monitoring mechanisms (e.g., link-down detection and IP-ID monitoring [7]), ensuring that any attempt to compromise the integrity of the communication is detectable.

III. Concept

In this work, we focus on the firewall and VPN functionalities of the gateway, which enforce micro-segmentation and encrypted communication, respectively. A key challenge lies in deriving suitable micro-segments and VPN tunnels that reflect the communication relations in the network. To address this challenge, we propose a semi-automated, traffic analysis-driven approach. The approach follows three main steps, as visualized in Figure 2: (a) Analyzing network traffic to identify communication relations; based on these relations, (b) deriving appropriate rules for micro-segmentation, and (c) VPN tunnel configurations. We detail these steps in the following.

A. Communication Relations

Communication in industrial networks is typically static and well-defined; for example, controllers continuously exchange measurements with a fixed set of sensors and actuators using Ethernet or IP-based protocols. Capturing and understanding these relations is crucial for migrating to segmented networks without disrupting operations. However, the traffic volume within the network is often too large for manual analysis.

To automate the identification of communication relations, we analyze traffic captures using heuristics and extract logical relations. Specifically, we use aggregated flows and their features [8]. IP flows, for example, are characterized by 5-tuples of source IP, destination IP, source port, destination port, and protocol. From well-known protocol-port combinations, we further infer industrial application-layer protocols. For example, EtherNet/IP uses UDP port 2222 or TCP port 44818, cf. Table I. We also consider flow statistics for packet counts (source-to-destination and vice versa) to capture directionality. Bidirectional flows reflect, e.g., cyclic command–response exchanges, while unidirectional flows reflect event- or alert-driven communication. These distinctions are critical for generating appropriate segmentation rules.

While traffic captures form the foundation of our analysis, they are inherently incomplete, as engineering-related or infrequent event-based traffic, such as SNMP traps, may not be captured, even during extended observation periods. Nevertheless, by aggregating who communicates with whom, over which protocols and ports, and in which direction, we capture communication relations that reflect the operational structure of the network. This serves as the initial basis for deriving micro-segmentation rules and VPN tunnel configurations. The aggregated data also provides insights into communication volume and frequency, indicating expected behavior. For example, how frequently a firewall rule is expected to be activated during normal operation.

B. Micro-Segmentation

Industrial networks are typically structured into hierarchical layers, e.g., the field layer containing sensors and actuators and the control layer containing controllers and workstations. While layers may be separated by routers or sometimes firewalls, communication within a layer is often unrestricted. As a result, an attacker can easily move within the layer once a single device is compromised, e.g., to spread malware. More fine-grained segmentation of the network reduces the attack surface and, hence, enhances security. However, such segmentation is highly restrictive and may block legitimate communication, requiring a well-prepared configuration.

We implement micro-segmentation at the gateway using firewall rules. Every legacy device is placed in its own micro-segment, where the firewall blocks or allows communication

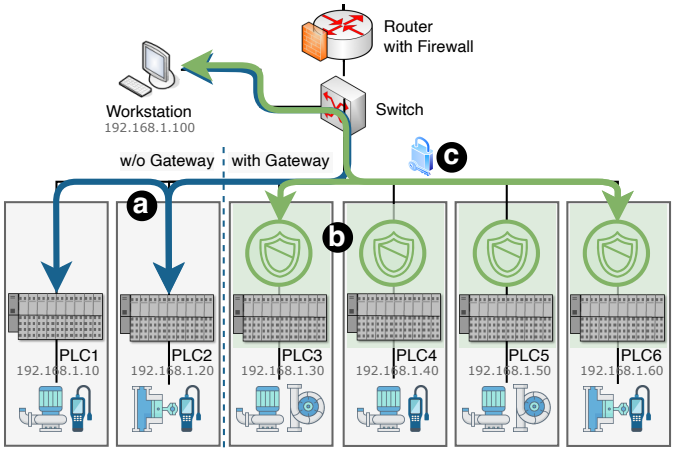

Fig. 2: Example infrastructure implementing the presented approach: (a) identify communication relations, derive and configure appropriate (b) micro-segments and (c) VPN tunnels.

TABLE I: Example flows and segmentation rules of (1) device- and (2) application-level granularity for **PLC6**, cf. Figure 2.

	src ip	dst ip	src port	dst port	protocol	bidirectional	**Firewall rule parameters** (chain `FORWARD`, action `ACCEPT`)
(1)	192.168.1.30	**192.168.1.60**	2222	2222	UDP	False	`-s 192.168.1.30 -d 192.168.1.60`
(2)	192.168.1.100	**192.168.1.60**	49859	44818	TCP	True	`-p tcp -s 192.168.1.100 -d 192.168.1.60 --dport 44818` `-p tcp -s 192.168.1.60 -d 192.168.1.100 --sport 44818`

between segments based on defined rules. To define appropriate rules, we convert the characteristics of identified relations into `iptables` rules that describe the permitted traffic for each micro-segment. These rules can follow different segmentation granularities, i.e., device or application level. For device-level segmentation, we block or allow communication at the device level, making decisions based on source and destination IP, cf. Table I (1). For application-level segmentation, we further consider the specific protocol and application port, making decisions more granular, cf. Table I (2). In each case, the firewall allows only explicitly specified traffic.

One limitation in defining firewall rules based on observed traffic is the incompleteness of network captures. Critical but infrequent communication could be unintentionally blocked by the firewall. To address this limitation, we implement a log-and-review approach. We place a `LOG` rule before the final default `DROP` rule. This rule logs any traffic that does not match an existing firewall rule and sends it to a central controller, allowing administrators to review and add rules for additional devices or applications. This approach results in a semi-automated workflow: The initial rules are generated automatically from observed traffic, while exceptions are handled manually through log review and ruleset refinement. Further, the identification of communication relations can be re-triggered, supporting adaptation of the ruleset in response to dynamic communication patterns and operational requirements.

C. VPN Encryption

Many legacy industrial communication protocols, such as Modbus and EtherNet/IP, lack built-in authentication and encryption. Although secure extensions for these protocols exist, their adoption remains limited. Communication using such insecure protocols can be eavesdropped on or otherwise tampered with. To enhance security, particularly in mission-critical infrastructures, such communication should be encrypted.

To retrofit encryption, we employ commonly used VPN technologies, such as WireGuard [9], at the gateway. For WireGuard, VPN tunnel configurations consist of two main components: interface and peer. The interface specifies the local IP address, private key, and listening port; the peer defines the public key of the remote endpoint, allowed IP ranges, and the endpoint address. Based on the identified communication relations and the selected segmentation granularity, a legacy device may be assigned one or more VPN tunnels, each corresponding to a specific communication partner or application. Regarding communication relations, we support both unicast (1:1) and multicast/broadcast communication (1:many). All communication patterns are ultimately mapped to point-to-point VPN tunnels. Hence, the mesh of VPN tunnels enables many:many communication. In the case of multicast and broadcast communication, the gateway routes the traffic into the respective VPN tunnels, which terminate at another gateway or device able to implement VPNs (cf. Figure 2).

IV. Proof-of-Concept

To validate the feasibility of the presented approach, we present a PoC consisting of the implementation and evaluation setup that incorporates the steps of communication relations analysis, micro-segmentation, and VPN encryption described above. With the PoC, we aim to address the discussed challenges: **C1** identifying relations to derive appropriate micro-segments, **C2** enabling encryption through VPN tunnels, and **C3** automating these processes.

The PoC is based on the Secure Water Treatment (SWaT) testbed [10], a physical industrial testbed designed for security research, covering different devices in the scope of considered legacy devices. We use a Docker-based network to replicate a simplified version of the SWaT infrastructure, consisting of PLC1 to PLC6, a workstation, and a dedicated security gateway for each PLC (cf. Figure 2). The analysis is based on a SWaT traffic capture of 50000 packets in the absence of attacks. The PLCs and workstation communicate using EtherNet/IP.

Figure 3 illustrates the workflow of the PoC. We use NFStream [8], a Python-based network analytics framework, to extract communication flows from captured traffic. NFStream aggregates flows, extracts statistical features, and allows plugin-based extension for protocol classification. Based on the aggregated flows, we derive communication relations to generate `iptables` firewall rules for micro-segmentation (**C1**). For VPN encryption, we use WireGuard [9], selected for its performance and simplicity [11]. We derive VPN tunnels following the identified insecure communication relations (**C2**). Configurations and required routing rules are generated automatically through triggered scripts on the gateways (**C3**). Overall, 68 different communication flows were captured, from which we derived 6 micro-segments (one for each PLC-gateway association) and 12 VPN interface configurations for communication between the respective gateways.

We validate segmentation and VPN enforcement within the Docker-based environment. To verify segmentation, we replay and inspect captured SWaT traffic using `tcpreplay` and `tcpdump`, respectively. To verify encryption, we manually inspect network traffic. First, we replay the original traffic

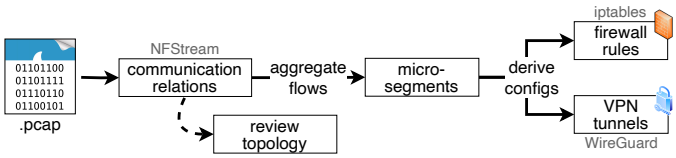

Fig. 3: PoC components and workflow.

capture to ensure that segmentation did not disrupt existing communication. Then, we inject traffic that was not present in the original trace, e.g., PLC6 initiating communication with PLC5. This additional traffic simulates both malicious activity (an attacker attempting to manipulate operations) and legitimate, previously not captured communication to validate the log-and-review approach. The verification confirms that only permitted inter-segment communication is successful and encrypted. Any communication outside of the specified relations is logged for review by an administrator, who determines whether it is valid or invalid. In both cases, this communication is correctly detected, resulting in either the successful blocking of unauthorized communication or the refinement of policies.

Deploying the presented concept mitigates the attacks outlined in Section II. Using VPN tunnels prevents eavesdropping of traffic, while micro-segmentation limits unauthorized access, injection of communication, and lateral movement. Application-level segmentation increases security by strictly limiting communication, but introduces more firewall rules and processing overhead. Device-level segmentation reduces complexity but permits broader communication, increasing the risk of unauthorized access.

The presented concept is generally applicable to legacy systems and supports any device that communicates over IP- or Ethernet-based protocols. It can be implemented in either hardware or software. This implementation detail has an impact on latency and jitter that could affect real-time performance. In addition, by default, we use VPN tunnels for all identified relations using insecure protocols, e.g., EtherNet/IP, Modbus, or SNMPv1. Administrators can override this behavior to disable encryption for cases where a VPN setup is not feasible or performance constraints are too restrictive. For example, in remote plant deployments, encryption may be enforced for communication between field devices and a remote control center, while local traffic within the plant remains unencrypted to reduce latency and computational overhead.

V. Related Work

In this section, we review related works on security gateway approaches with a particular focus on brownfield environments. Unlike greenfield approaches that introduce new technologies or protocols, brownfield approaches emphasize non-intrusive solutions to integrate security into existing infrastructures.

Using gateways for retrofits in industrial networks has been proposed in earlier works such as Priller et al. [12], but with limited focus on securing legacy systems. Khan et al. use gateways to secure communication with cloud-based systems with VPN tunnels [13] and enhance endpoint security using message encryption [14]. Frauenschläger and Mottok [15] implement security gateways with TLS and firewall functionality to secure communication paths.

Next to academic research, proprietary solutions such as Illumio [16] and Tempered Airwall [17] offer micro-segmentation. Notably, Tempered Airwall uses the Host Identity Protocol [18] to create private overlay networks with encrypted tunnels and trusted cryptographic identities.

Compared to previous work, we present an open-source and semi-automated workflow for brownfield environments that retrofits micro-segmentation and VPN encryption. We also emphasize a one-to-one association between each gateway and legacy device, focusing on a comprehensive integration rather than securing individual communication paths.

VI. Conclusion

We presented a practical approach for securely integrating legacy devices in industrial networks, using dedicated security gateways that enforce micro-segmentation and VPN encryption. We address three key challenges: **C1** identifying appropriate micro-segments, **C2** encrypting insecure protocols via VPNs, and **C3** automating the configuration processes. We contribute an open-source, semi-automated migration workflow that derives communication relations from network traffic captures and generates and deploys corresponding firewall and VPN configurations, with the option for manual review. The PoC based on the SWaT testbed demonstrates its feasibility in real-world industrial networks, mitigating attacks such as unauthorized network access and eavesdropping.

References

[1] *IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*, International Electrotechnical Commission, 2013.

[2] G. M. Køien, "Zero-Trust Principles for Legacy Components 12 Rules for Legacy Devices: An Antidote to Chaos," *Wireless Personal Communications*, vol. 121, no. 2, pp. 1169–1186, 2021.

[3] Modbus Organization, *MODBUS Messaging on TCP/IP Implementation Guide: V1.0b*. Modbus Organization, Oct. 2006.

[4] ODVA, "EtherNet/IP - CIP on Ethernet Technology," Tech. Rep. PUB00138R8, Feb. 2024.

[5] M. Fedor, M. L. Schoffstall, J. R. Davin, and J. D. Case, *RFC 1157: A Simple Network Management Protocol (SNMP)*, May 1990.

[6] R. Gerhards, *RFC 5424: The Syslog Protocol*, Mar. 2009.

[7] S. Kaniewski, L. Bechtel, M. Menth, and T. Heer, "Monitoring IP-ID Behavior for Spoofed IPv4 Traffic Detection," in *IEEE International Conference on Emerging Technologies and Factory Automation*, 2024.

[8] Z. Aouini and A. Pekar, "NFStream: A Flexible Network Data Analysis Framework," *Computer Networks*, vol. 204, p. 108 719, 2022.

[9] J. A. Donenfeld, "WireGuard: Next Generation Kernel Network Tunnel," in *Network and Distributed System Security Symposium*, 2017.

[10] A. P. Mathur and N. O. Tippenhauer, "SWaT: A Water Treatment Testbed for Research and Training on ICS Security," in *International Workshop on Cyber-Physical Systems for Smart Water Networks*, 2016.

[11] L. Osswald, M. Haeberle, and M. Menth, "Performance Comparison of VPN Solutions," in *ITG Workshop on IT Security*, 2020.

[12] P. Priller, A. Aldrian, and T. Ebner, "Case Study: From Legacy to Connectivity Migrating Industrial Devices into the World of Smart Services," in *IEEE International Conference on Emerging Technologies and Factory Automation*, 2014.

[13] R. Khan, K. McLaughlin, B. Kang, D. Laverty, and S. Sezer, "A Seamless Cloud Migration Approach to Secure Distributed Legacy Industrial SCADA Systems," in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference*, 2020.

[14] R. Khan, K. McLaughlin, B. Kang, D. Laverty, and S. Sezer, "A Novel Edge Security Gateway for End-to-End Protection in Industrial Internet of Things," in *IEEE Power & Energy Society General Meeting*, 2021.

[15] T. Frauenschläger and J. Mottok, "Security-Gateway for SCADA-Systems in Critical Infrastructures," in *International Conference on Applied Electronics*, 2022.

[16] *Illumio*. [Online]. Available: https://www.illumio.com/ (visited on May 13, 2025).

[17] *Tempered Airwall*. [Online]. Available: https://www.tempered.io/ (visited on May 13, 2025).

[18] R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, *RFC 7401: Host Identity Protocol Version 2 (HIPv2)*, Apr. 2015.