Fortinet FortiGate Rugged Firewall Positioning

Fortinet positioning in Rockwell Automation System Security Architectures

Introduction

Industrial Automation and Control System (IACS) networks are generally designed with openness as a primary consideration. This openness can be defined as a lack of security or lack of network boundaries and segmentation. In either case, it facilitates the needs and requirements of the ICS and its related technologies and products by providing the impression of easy deployment and maintenance. Openness can lead to many architectural and design constraints such as a lack of ICS hardening, lack of ability to scale, and general application performance impacts.

The focus of this white paper is to highlight the need for the deployment of Industrial Firewalls which, as a part of a holistic industrial security practice, helps to harden ICS networks and create smaller, function based, zones of trust. The degree of hardening depends upon many factors, including but not limited to, corporate standards, application requirements, industry security standards, regulatory compliance, and overall risk tolerances identified through proper threat modeling and risk assessments.

Industrial Firewalls provide restriction and inspection of traffic flows through the ICS and create boundaries within the generally open ICS networks. For networks that contain legacy devices, industrial firewalls may be used to provide mitigation for devices with potential threat vectors that cannot be patched. As with most security tools, industrial firewalls require monitoring to realize their full potential. Industrial firewalls available through the Rockwell Automation PartnerNetwork™ program, such as the FortiGate Rugged FGR-70F, can be deployed and managed locally or centrally.

Rockwell Automation and Fortinet Partnership

The Fortinet FortiGate Next-Generation Firewall (NGFW) is the world's most deployed network security solution.[1] FortiGate delivers unparalleled AI-powered security performance and threat intelligence, along with full visibility and security. Fortinet has a strong track record protecting critical infrastructure, and ruggedized FortiGate NGFWs are built to secure sites with extreme heat, cold, vibration, and electrical interference.

- Fortinet and Rockwell Automation can provide powerful cybersecurity protection to global customers through the convergence of advanced networking and security capabilities.
- The differences between operational technology and information technology environments mean that ICS systems often face different cybersecurity risks and a unique threat landscape that requires security solutions tailored to their challenges.
- Fortinet has years of experience securing OT environments with solutions that can help connected organizations protect, consolidate, and scale their security.

[1] IDC Worldwide Security Appliance Tracker, December 2022 (based on unit shipments of UTM appliances)

FortiGate Rugged 70F (FGR-70F)

While traditional security solutions are designed and intended for the world of offices and corporations, the FortiGate Rugged Series offers an industrially hardened, all-in-one security appliance that delivers specialized threat protection to help secure critical industrial and control networks against malicious attacks.

FortiGate FGR-70F Specifications

	FortiGate Rugged 70F	FortiGate Rugged 70F-3G4G
Interfaces and Modules		
GE RJ45 Interfaces	6	
Bypass GE RJ45 Port Pair	PORT3 and PORT4	
Dedicated GE SFP Slots	2	
GE RJ45/SFP Shared Media Pairs	No	
Serial Interface	1 RJ45	
USB (Client / Server)	1	
Cellular Modem	No	3G / 4G LTE, GPS
RJ45 Console Ports	1	
Bluetooth Low Energy (BLE)	Yes	
Trusted Platform Module (TPM)	Yes	
Digital I/O Module (DIO)	Yes	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets)	8/8/8 Gbps	
Firewall Latency (64 byte, UDP)	6.71 µs	
Firewall Throughput (Packet per Second)	12 Mpps	
Concurrent Sessions (TCP)	1 Million	
New Sessions/Sec (TCP)	35,000	
Firewall Policies	5,000	

IPsec VPN Throughput (512 byte)	6.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	500	
SSL-VPN Throughput	450 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum)	100	
SSL Inspection Throughput	500 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS)	380	
SSL Inspection Concurrent Session (IPS, avg. HTTPS)	90,000	
Application Control Throughput (HTTP 64K)	1.1 Gbps	
High Availability Configurations	Active-Active, Active-Passive, Clustering	
System Performance — Enterprise Traffic Mix		
IPS Throughput	975 Mbps	
NGFW Throughput	950 Mbps	
Threat Protection Throughput	580 Mbps	
Dimensions and Power		
Height x Width x Length (inches)	4.8 x 3.2 x 4.4	
Height x Width x Length (mm)	122 x 80.5 x 111	
Weight (maximum)	2.87 lbs. (1.3 kg)	
Form Factor	DIN-rail	
Antennae (Height x Width)	-	205 mm x 25 mm
IP Rating	IP40	
Power Consumption (Maximum / Average)	16 W /18 W	
Current (Maximum)	12V DC / 1.5A	
Heat Dissipation (Maximum)	62 BTU/h	

Operating Environment and Certifications	
Operating Temperature	-40°–167°F (-40°–75°C)
Storage Temperature	-40°–167°F (-40°–75°C)
Humidity	5–95% non-condensing
Operating Altitude	Up to 10 000 ft (3048 m)

Stratix 5950 and FortiGate Rugged FGR-70F

The Allen-Bradley Stratix 5950 security appliance combines several enhanced security functions into a single appliance to help protect your industrial automation infrastructure. As part of the Rockwell Automation security offering, the Stratix 5950 builds on common network security technologies from traditional firewalls to help provide enhanced access control, threat detection, and application visibility in your Industrial Control System (ICS). The Stratix 5950 has begun its transition to End of Life and Discontinuation. Due to this lifecycle change, the Fortinet offering has been brought into the Rockwell Automation Technology Partner Program. Overall, the two offerings are comparable and are expected to meet applicable requirements to help protect the industrial automation infrastructure.

Stratix 5950

FortiGate FGR-70F

Stratix 5950 and FortiGate Rugged FGR-70F Technical Comparison

Below is a high-level comparison of the technical specifications of the Stratix 5950 and FGR-70F.

	FGR-70F	Stratix 5950
Total GE Ports	8	4
GE RJ45	6	4 / 2 for SFP model
Hardware Bypass Pairs	1	2 / 1 for SFP model
Dedicated GE SFP Slots	2	0 / 2 for SFP model
Console Port	Yes	
IPv4 Firewall Throughput (1518** / 512 / 64 byte UDP packets)	8 Gbps	2 Gbps
Firewall Latency (64 byte, UDP)	6.71 µs	17.71 µs
Firewall Throughput (Packets Per Second)	12 Mpps	186 Kpps
Concurrent Sessions (TCP)	1 M	50,000
New Sessions/Second (TCP)	35,000	2,700
IPsec VPN Throughput (512 byte)	6.5 Gbps	1 Gbps
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active/standby failover
CIP Inspection	Yes	
Height x Width x Length (mm)	122 x 80.5 x 111	129 x 106 x 159
Form Factor	DIN-rail	
Operating Temperature	-40…+75 °C (-40…+167 °F)	-40…+60 °C (-40…+140 °F)

System Security Architectures

Integrating IACS with enterprise-level systems enables better visibility and collaboration, which helps improve efficiency, production, and profitability. But greater connectivity also exposes control systems to additional cybersecurity risks. Availability is the most crucial aspect of a secure IACS. To meet the needs of industrial environments, Rockwell Automation aligns their PlantPAx systems with the international standard ISA-99/IEC 62443-3-3. This standard is designed specifically for Industrial Automation and Control Systems and defines procedures and requirements to implement secure systems. ISA-99/IEC 62443 is based on seven foundational requirements that cover a defense-in-depth approach. These foundational requirements are:

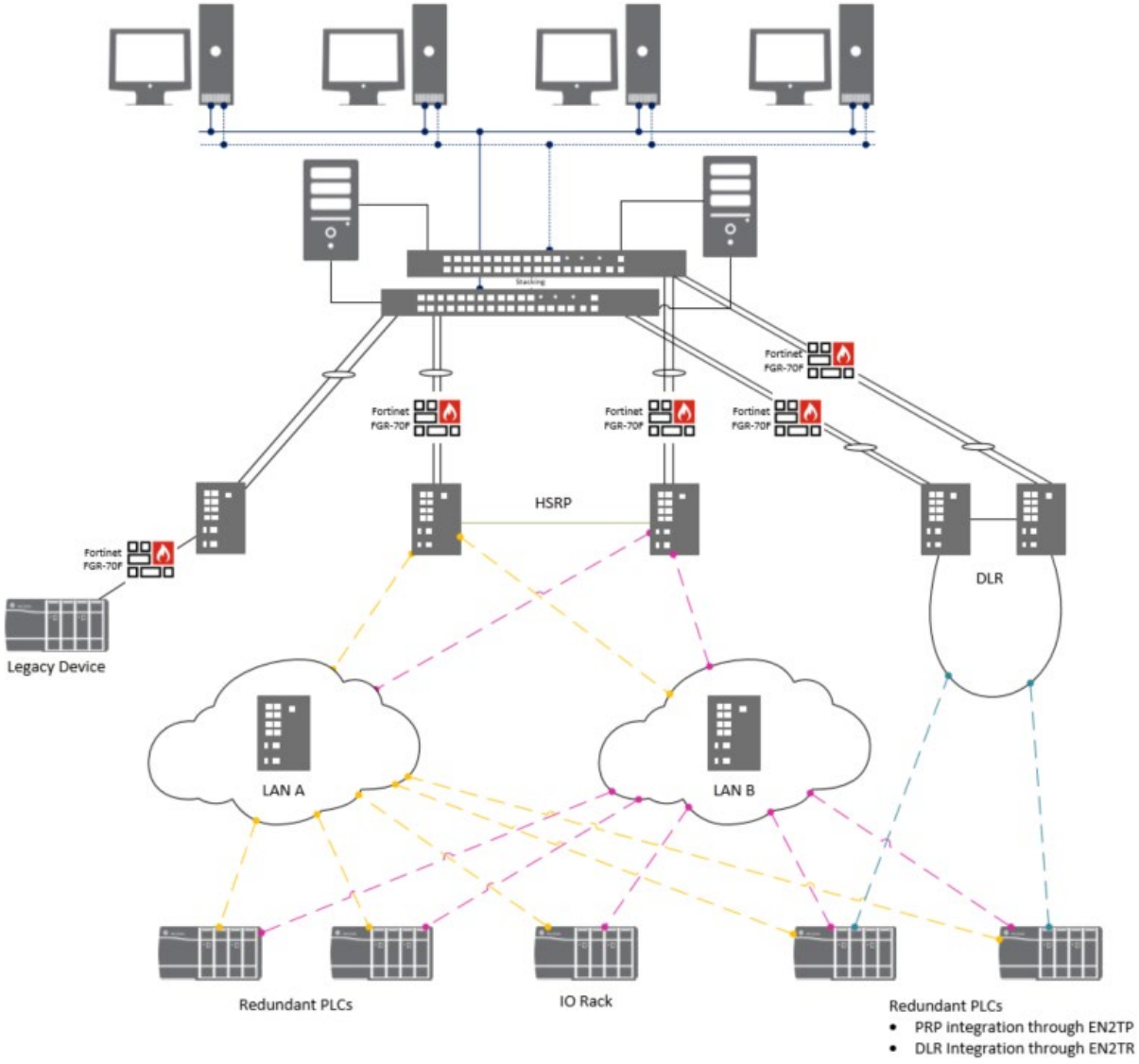
- FR1: Identification and authentication control (IAC)
- FR2: Use control (UC)
- FR3: System integrity (SI)
- FR4: Data confidentiality (DC)
- FR5: Restricted data flow (RDF)
- FR6: Timely response to events (TRE)
- FR7: Resource availability (RA)

The intent of a certified architecture is to demonstrate security competency, as well as to provide a standard, prescriptive reference design. Industrial firewalls provide compensating countermeasures as a part of some of the above foundational requirements. For additional information on how firewalls can assist in meeting IEC-62443 standards, refer to the System Security Design Guidelines, SECURE-RM001.

Industrial Firewall Network Architectures

With the deployment of most security-related solutions, understanding threat vectors and risk is a crucial part of determining which assets require risk mitigation and the types of risk mitigations to be used. Below in Figure 1, is an architectural example that highlights several common use cases where industrial firewalls may be designed into the network infrastructure. These use cases, while commonly deployed, have not been validated or characterized with Fortinet firewalls to any specific performance requirements.

Fig 1. Industrial Firewall Deployments



Use Cases

▪ Zone Protection and Enforcement

Zones create smaller domains of trust to help protect the IACS network from known and unknown risks in the network. IACS devices are identified and grouped into zones according to a common functionality, physical location, and security requirements. Firewalls can be deployed at traffic ingress and egress locations for a logical zone as pictured in Figure 1. Firewalls are positioned above each zone, where applicable, and would provide inspection and enforcement for any traffic entering or leaving the zone.

▪ Vulnerable and Legacy Devices

Due to several factors, industrial automation devices are not always updated to the latest versions or versions that correct disclosed vulnerabilities. Industrial firewalls can be designed into the network architecture to provide virtual patching via Intrusion Prevention System (IPS) signatures loaded into the industrial firewall, such as the FortiGate Rugged FGR-70F. Fortinet's IPS signature solution combines industry-leading threat intelligence from FortiGuard Labs with FortiGate industrial firewalls to identify the latest threats and prevent them from affecting the device. FortiGuard Labs uses AI and Machine Learning (ML) to analyze billions of events every day. The FortiGuard Labs research team also proactively performs threat research to discover new vulnerabilities and exploitations and produces signatures to identify such threats. These IPS signatures can be delivered to each FortiGate in real time, so that the IPS engine is armed with the latest databases to match the latest threats. Through IPS signatures, an industrial firewall can provide mitigations against known vulnerabilities if a device cannot be updated to a revision providing vulnerability correction.

Summary

The Fortinet rugged firewalls can be positioned within the same network architecture and system security architecture use cases as the Stratix 5950. Customers should evaluate the use cases and performance metrics of the Fortinet rugged products and the Stratix 5950 to understand how the Fortinet products can meet application and security requirements and applicable standards.

Resources

You can read the following for further information:

Fortinet Partner Details | Rockwell Automation

PlantPAx Distributed Control System Configuration and Implementation

System Security Design Guidelines

Blog: Four Common Challenges to DCS Cybersecurity

Blog: It's 10:00 p.m. Do You Know Where Your Data Is?

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication MIGRAT-WP001A-EN-P — October 2023