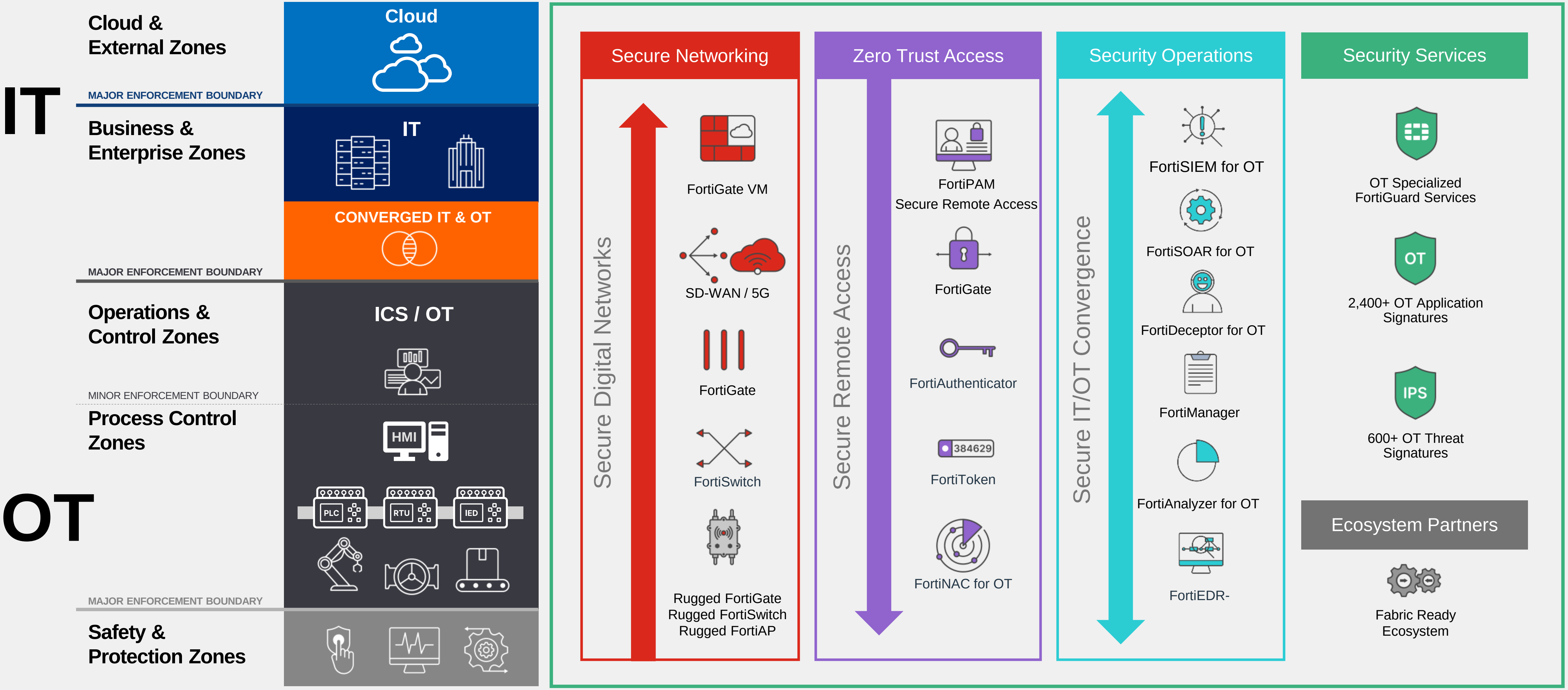
FORTINET

# Lösungen und Strategien zur Absicherung von OT Anlagen

Andreas Troger

Systems Engineer

# Fortinet’s OT Aware Security Fabric



IT

Cloud & External Zones

MAJOR ENFORCEMENT BOUNDARY

Business & Enterprise Zones

MAJOR ENFORCEMENT BOUNDARY

Operations & Control Zones

MINOR ENFORCEMENT BOUNDARY

Process Control Zones

OT

MAJOR ENFORCEMENT BOUNDARY

Safety & Protection Zones

Cloud

IT

CONVERGED IT & OT

ICS / OT

## Secure Networking

Secure Digital Networks

- FortiGate VM
- SD-WAN / 5G
- FortiGate
- FortiSwitch
- Rugged FortiGate
- Rugged FortiSwitch
- Rugged FortiAP

## Zero Trust Access

Secure Remote Access

- FortiPAM Secure Remote Access
- FortiGate
- FortiAuthenticator
- FortiToken
- FortiNAC for OT

## Security Operations

Secure IT/OT Convergence

- FortiSIEM for OT
- FortiSOAR for OT
- FortiDeceptor for OT
- FortiManager
- FortiAnalyzer for OT
- FortiEDR-

## Security Services

- OT Specialized FortiGuard Services
- 2,400+ OT Application Signatures
- 600+ OT Threat Signatures

## Ecosystem Partners

- Fabric Ready Ecosystem

# Network Segmentation

Restricted Data Flow – FR5 (IEC 62443)

As IT and OT converge, the air gap is no longer the first line of defense in restricting data flow.  How can Fortinet address the segmentation required for reducing exposure and the spread within an ICS environment?

FortiGate

FortiSwitch

FortiAP

FortiNAC

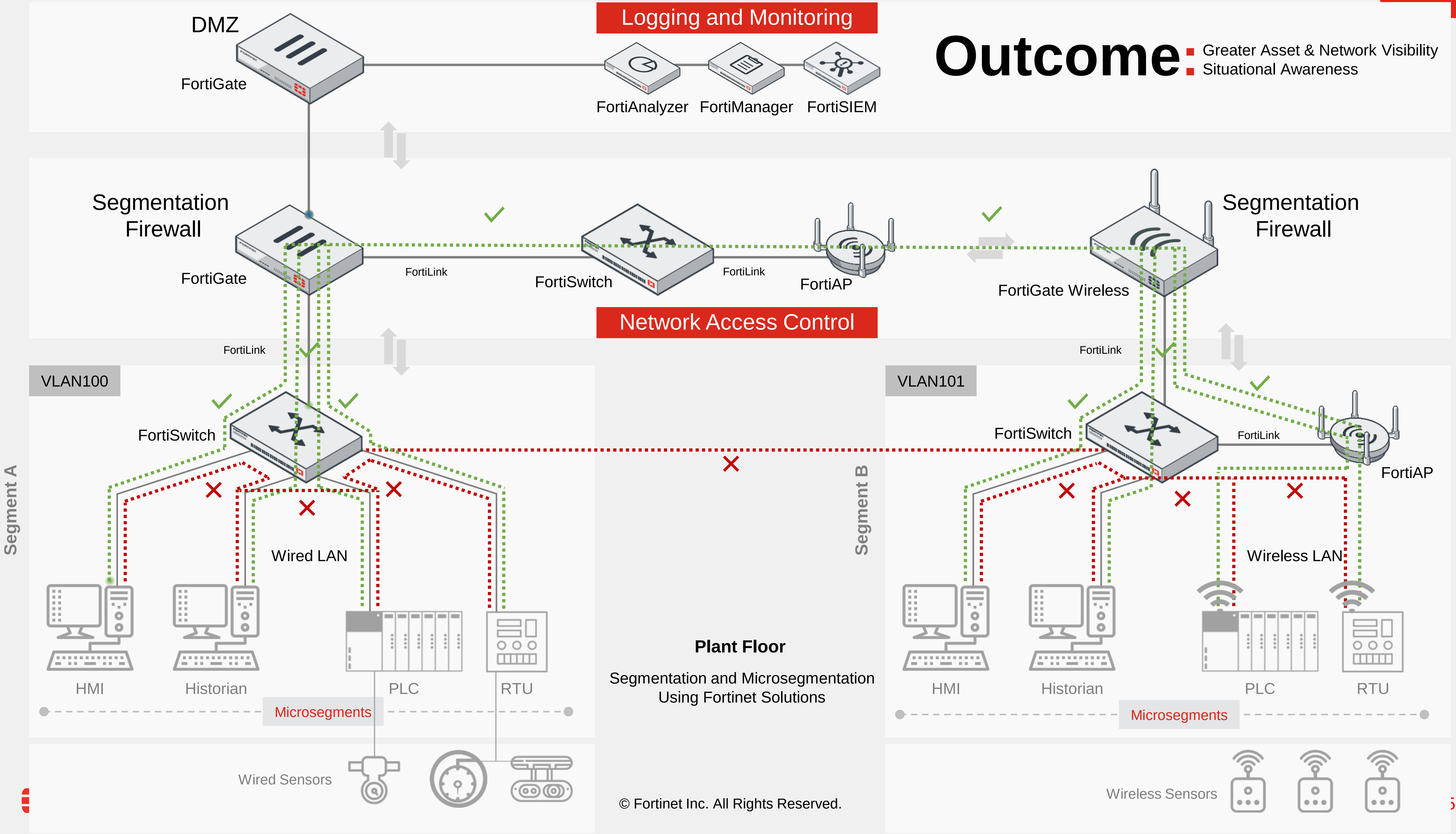
# Restricted Data Flow [FR5]

Foundational Requirement 5

- *„[…] asset owners need to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information.“*
- Network Segmentation
  - IT and OT
  - Edge computing and cloud analytics
- Primary most common activity
  - Segment off non-control system networks
- Reduce exposure of ICS network (ingress) and spread from ICS network (egress)

# Outcome:

- Greater Asset & Network Visibility
- Situational Awareness



# Fortinet Solution Offering for ICS/OT

## FortiGate and FortiSwitch Rugged with FortiAP Outdoor

COMMON CRITERIA CERTIFIED EAL4+ · ICSA labs · ICSA labs · ICSA labs · ICSA labs · ICSA labs · FIPS VALIDATED 140-2 · IEC 61850-3 IEEE 1613

### Ruggedized Design

Fan-less and use of robust components ensure reliable operation in harsh industrial environments.

### Consolidated Security Architecture

FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products.

### Ease of Management

Allows rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

## FortiGate Rugged Series

**FGR-70F 3G/4G**
SoC4-powered, security and VPN gateway with compact, fanless design and embedded 3G/4G/LTE

**FGR-70F**
SoC4-powered, security and  VPN gateway with compact, fanless design

**FGR-60F 3G/4G**
SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

**FGR-60F**
SoC4-powered, security and VPN gateway

## FortiGate Features

- Security (IPS, FW, OT traffic monitor)
- Encryption (GRE, VXLAN, IPSEC)
- Connectivity (Proxy, VLANs, IPv6.)
- Advance features (SD-WAN)
- Central authentication (LDAP, RADIUS, etc.)
- Microsegmentation
- DLP
- Wi-Fi
- Antivirus
- DNS Filter
- Web Filtering
- IPSEC VPN
- SSL VPN – Client/Clientless
- SSL Inspection
- Packet capture triggered by IPS
- Virtual Domains (VDOM)
- Transparent or Proxy (Man in the middle)

## FortiSwitch Rugged, FortiAP Outdoor Series

**FSR-424F-POE and FSR-112D-POE**
Mean time between failure >25 years. Gigabit and M-Gig Ethernet. Next-Generation 802.3bt PoE++  DIN-rail and rack mount options. Zero-touch Deployment, Entry-Level NAC,  Microsegmentation. Supports: Precision Time Protocol IEEE1588v2, HSR/PRP to implement zero-loss redundancy, meets power substations requirements IEEE1613 / IEC 61850-3

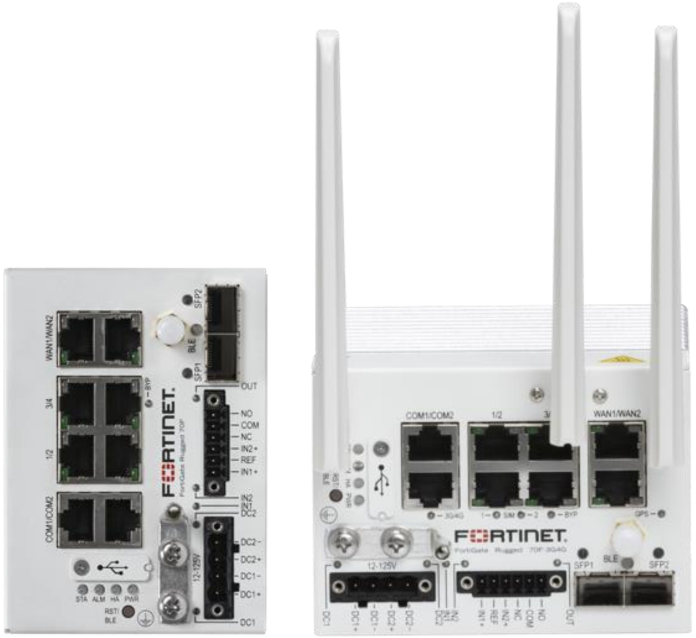
**FortiAP Outdoor 234F**
Internal Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

**FortiAP Outdoor 432F**
External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

# FortiGate Rugged 70F / 70F 3G4G with Digital I/O

Digitial I/O: Automation actions triggered by physical devices, ex. Key Switch for VPN On/Off

## Product Information



## Key Differentiators

- ASIC-based NGFW/ NGIPS
- Secure SD-WAN
- Specialized IPS for ICS/OT
- 3rd party integrations

## Industry Compliance

IEC 61850-3 IEEE 1613

EN 50155

COMMON CRITERIA CERTIFIED EAL4+

FIPS VALIDATED 140-2

## Key Benefits

**Ruggedized NGFW**
comply with industrial requirements and certifications to ensure reliable operations in harsh conditions

**Optimal User Experience**
ASIC-based processor for high-speed NGFW/ NGIPS performance

**Cost-effective**
compact design with integrated networking, security, wireless, and secure SD-WAN features

**Centralized Visibility**
support for unified logging, reporting, and management for centralized control over security operations

## Product Literature

Datasheet, Quickstart Guide

# FortiGuard OT Security Service

## IPS Application Control Signatures – ICS/OT Protocols

- Allen-Bradley DF-1 →
- **Allen-Bradley PCCC →**
- **Beckhoff AMS →**
- **BSAP**
- BACnet →
- CC-Link →
- CN/IP CEA-852 →
- CoAP →
- DDSI-RTPS
- Digi ADDP →
- Digi RealPort (Net C/X)
- Digi RealPort (Net C/X) DNP3 ⇶
- Direct Message Profile →
- DLMS/COSEM(IEC62056) →
- DNP3 →
- ECHONET Lite →
- ECOM100
- ELCOM 90 →
- Emerson DeltaV
- Emerson ROC
- Ether-S-Bus →
- Ether-S-I/O →
- EtherCAT →
- Ethernet POWERLINK
- EtherNet/IP-CIP →
- FactorySuite NMXSVC
- FL-NET →
- GE EGD
- GE SRTP →
- Hart IP →
- IEC 60870-5-104 ⇶
- IEC 60870-6 (ICCP/TASE.2) →
- IEC 61850 →
- IEC 61850-90-5 R-GOOSE
- IEC 61850-90-5 R-SV
- IEEE 1278.2 DIS →
- IEEE C37.118 Synchrophasor →
- KNXnet/IP (EIBnet/IP) →
- LonTalk IEC14908-1 CNP →
- Mitsubishi MELSEC →
- MMS →
- Modbus TCP/IP ⇶
- Moxa Modbus RTU →
- Moxa UDP Device Discovery
- MTConnect
- Niagara Fox
- oBIX
- **OCPP →**
- Omron FINS →
- OPC AE →
- OPC Common →
- OPC DA →
- OPC DA Automation
- OPC HDA →
- OPC HDA Automation →
- OPC UA →
- OpenADR →
- OSIsoft Asset Framework
- OSISoft PI
- Profinet CBA →
- Profinet IO →
- Rockwell FactoryTalk View SE
- **Rockwell FactoryTalk ViewPoint**
- Schneider UMAS →
- **SECS-II/GEM →**
- **Siemens OCG ATCS →**
- Siemens LOGO →
- Siemens S7 →
- Siemens S7 1200 →
- Siemens S7 Plus →
- Siemens SIMATIC CAMP →
- STANAG 4406 Military Messaging
- STANAG 5066
- Triconex TSAA →
- TriStation →
- Veeder-Root ATG
- Vnet/IP
- **WITS0**

**70+**

OT Protocols

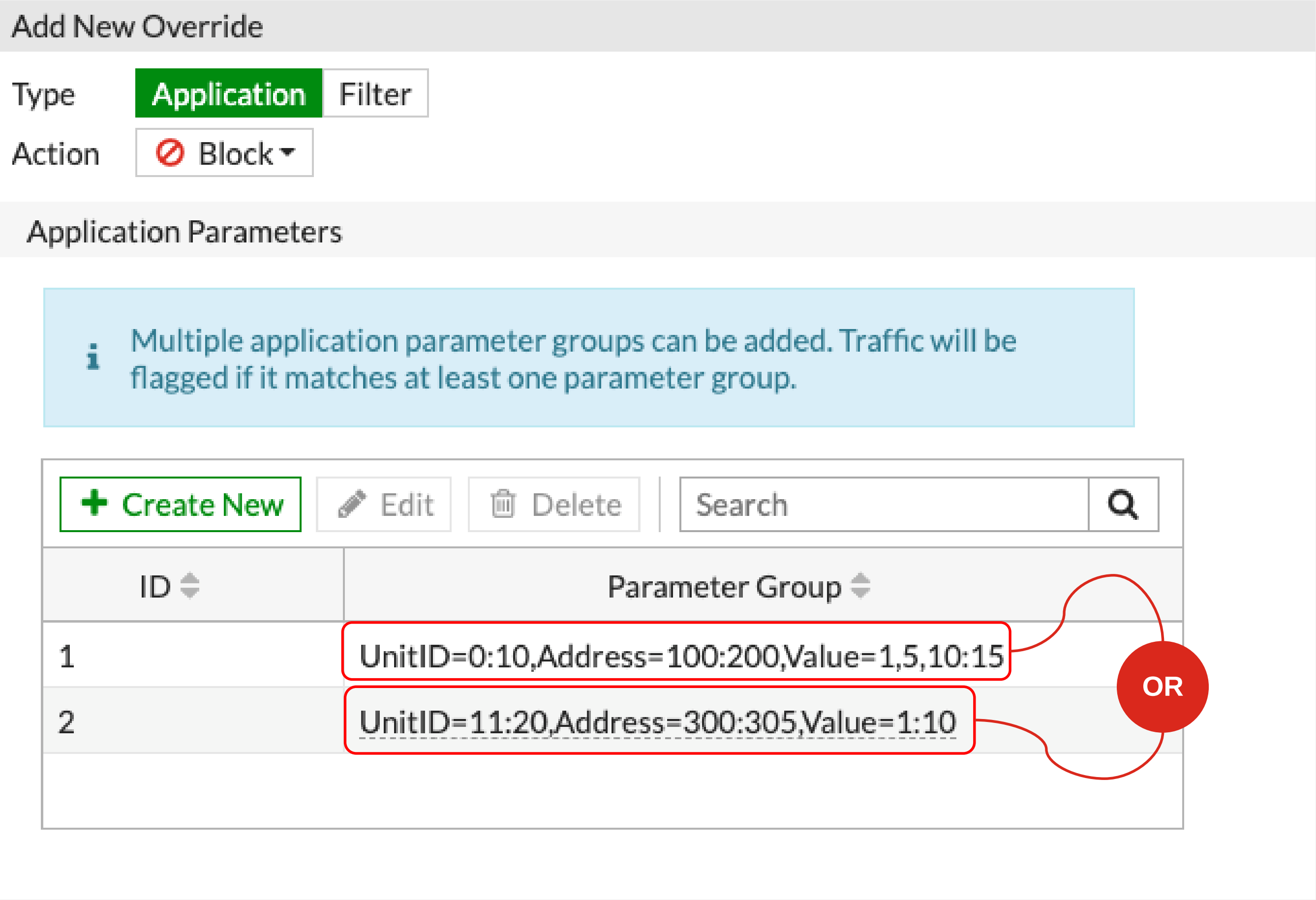
**Recent additions/ updates**

→ message layer policy ⇶ message and parameter policy (FortiOS v6.4 and above)

FortiGuard Industrial Security Service provides broader coverage for Industrial Control System and Operational Technology applications and protocols through Application Control (AppCtrl) and IPS signatures. **For up to date list of supported signatures, please visit fortiguard.com.**

**Entire list:** https://www.fortiguard.com/appcontrol?category=Industrial **Submit new (signature) request:** https://www.fortiguard.com/learnmore#is

# Logical Operator Between Parameter Groups



Add New Override

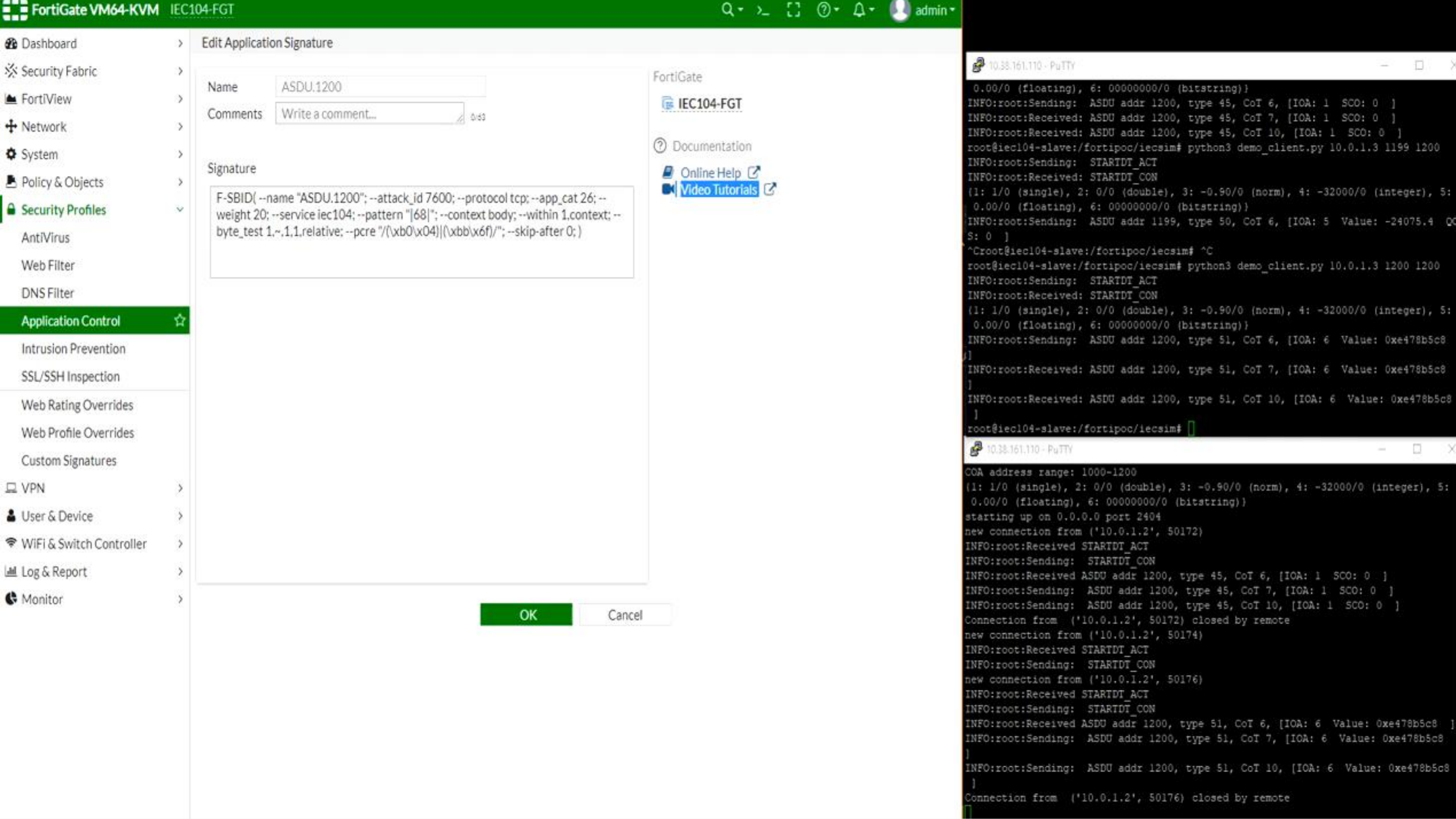
Type: [✓ Application] Filter

Action: Block

Application Parameters

Multiple application parameter groups can be added. Traffic will be flagged if it matches at least one parameter group.

| ID | Parameter Group |
|---|---|
| 1 | UnitID=0:10,Address=100:200,Value=1,5,10:15 |
| 2 | UnitID=11:20,Address=300:305,Value=1:10 |



Edit Application Signature

Name: ASDU.1200

Comments: Write a comment... 0/63

Signature

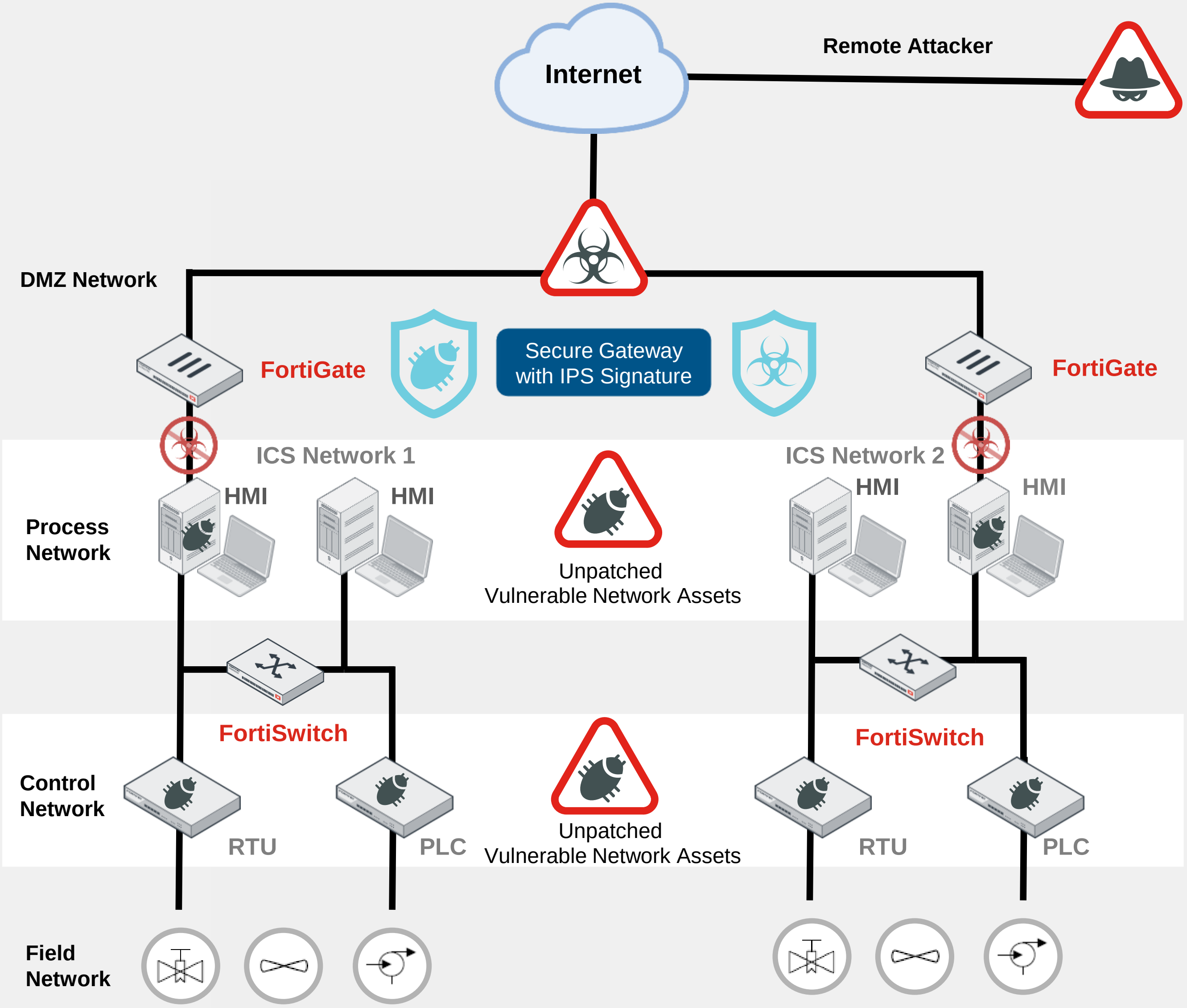
```
F-SBID( --name "ASDU.1200"; --attack_id 7600; --protocol tcp; --app_cat 26; --weight 20; --service iec104; --pattern "|68|"; --context body; --within 1,context; --byte_test 1,~,1,1,relative; --pcre "/(\xb0\x04)|(\xbb\x6f)/"; --skip-after 0; )
```

```
 0.00/0 (floating), 6: 00000000/0 (bitstring)}
INFO:root:Sending:  ASDU addr 1200, type 45, CoT 6, [IOA: 1  SCO: 0  ]
INFO:root:Received: ASDU addr 1200, type 45, CoT 7, [IOA: 1  SCO: 0  ]
INFO:root:Received: ASDU addr 1200, type 45, CoT 10, [IOA: 1  SCO: 0  ]
root@iec104-slave:/fortipoc/iecsim# python3 demo_client.py 10.0.1.3 1199 1200
INFO:root:Sending:  STARTDT_ACT
INFO:root:Received: STARTDT_CON
{1: 1/0 (single), 2: 0/0 (double), 3: -0.90/0 (norm), 4: -32000/0 (integer), 5:
 0.00/0 (floating), 6: 00000000/0 (bitstring)}
INFO:root:Sending:  ASDU addr 1199, type 50, CoT 6, [IOA: 5  Value: -24075.4  QO
S: 0  ]
^Croot@iec104-slave:/fortipoc/iecsim# ^C
root@iec104-slave:/fortipoc/iecsim# python3 demo_client.py 10.0.1.3 1200 1200
INFO:root:Sending:  STARTDT_ACT
INFO:root:Received: STARTDT_CON
{1: 1/0 (single), 2: 0/0 (double), 3: -0.90/0 (norm), 4: -32000/0 (integer), 5:
 0.00/0 (floating), 6: 00000000/0 (bitstring)}
INFO:root:Sending:  ASDU addr 1200, type 51, CoT 6, [IOA: 6  Value: 0xe478b5c8
]
INFO:root:Received: ASDU addr 1200, type 51, CoT 7, [IOA: 6  Value: 0xe478b5c8
]
INFO:root:Received: ASDU addr 1200, type 51, CoT 10, [IOA: 6  Value: 0xe478b5c8
 ]
root@iec104-slave:/fortipoc/iecsim#
```

```
COA address range: 1000-1200
{1: 1/0 (single), 2: 0/0 (double), 3: -0.90/0 (norm), 4: -32000/0 (integer), 5:
 0.00/0 (floating), 6: 00000000/0 (bitstring)}
starting up on 0.0.0.0 port 2404
new connection from ('10.0.1.2', 50172)
INFO:root:Received STARTDT_ACT
INFO:root:Sending:  STARTDT_CON
INFO:root:Received ASDU addr 1200, type 45, CoT 6, [IOA: 1  SCO: 0  ]
INFO:root:Sending:  ASDU addr 1200, type 45, CoT 7, [IOA: 1  SCO: 0  ]
INFO:root:Sending:  ASDU addr 1200, type 45, CoT 10, [IOA: 1  SCO: 0  ]
Connection from  ('10.0.1.2', 50172) closed by remote
new connection from ('10.0.1.2', 50174)
INFO:root:Received STARTDT_ACT
INFO:root:Sending:  STARTDT_CON
new connection from ('10.0.1.2', 50176)
INFO:root:Received STARTDT_ACT
INFO:root:Sending:  STARTDT_CON
INFO:root:Received ASDU addr 1200, type 51, CoT 6, [IOA: 6  Value: 0xe478b5c8  ]
INFO:root:Sending:  ASDU addr 1200, type 51, CoT 7, [IOA: 6  Value: 0xe478b5c8
]
INFO:root:Sending:  ASDU addr 1200, type 51, CoT 10, [IOA: 6  Value: 0xe478b5c8
 ]
Connection from  ('10.0.1.2', 50176) closed by remote
```

# FortiGuard Virtual Patching – with FOS 7.4 Auto!

**Virtual patching or vulnerability shielding** — acts as **compensatory security measure against threats** that **have potential to exploit known or unknown vulnerabilities**. Virtual patching works by implementing layers of security controls that **intercept and prevent an exploit from compromising the vulnerable assets** connected on the network(s).

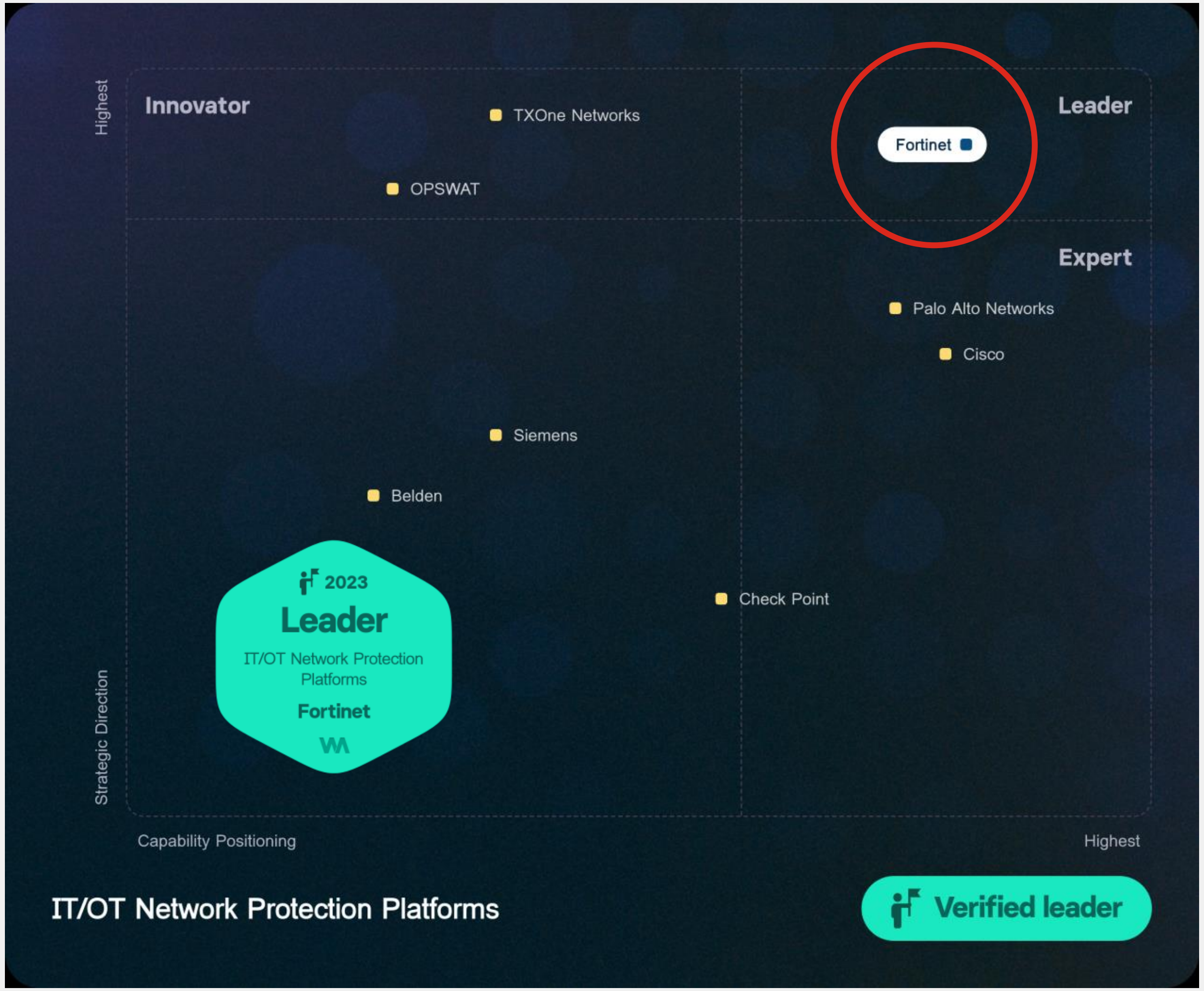


# Fortinet Is the Sole Leader in the IT/OT Security Platforms Navigator 2023

Fortinet OT Aware Fabric identified as a **Navigator Leader** for two consecutive years

*“Fortinet is a leading IT and OT cybersecurity solutions provider to the industrial and critical infrastructure sectors, with a high customer base and strong coverage of all industrial verticals.”*

Westlands Advisory, Industrial Cybersecurity Outlook 2023-2030



FORTINET®