SOLUTION BRIEF

Fortinet and Radiflow Joint Security Solution

A Broad, Integrated, and Automated Solution to Protect OT Assets, Through Automatic Creation and Enforcement of Firewall Rules, with Full Visibility of Devices, Protocols, and Connections

Executive Summary

Fortinet and Radiflow have partnered to deliver an integrated solution that includes the Fortinet Fortigate next-generation firewall (NGFW) and Radiflow's iSID (Industrial Threat Protection). Radiflow's iSID equips the FortiGate firewall with a clear model of all assets, asset types, protocols, and ports on the network and also provides the criticality of each asset. This enables configuring rules for otherwise undetected assets and rules that much better comply with the security needs of the industrial operator.

Overview

Industrial cybersecurity is one of the core features of transitioning operational technology (OT) infrastructures to Industry 4.0.

The following dynamics are having a dramatic effect to protect the growing attack surface and enable the business to remain highly competitive:

- The growing push for businesses to reduce OPEX by converging the IT and OT environments
- Interconnectivity between the enterprise and its business partners and customers
- The introduction of hundreds of thousands of Industrial Internet-of-Things (IIoT) devices and the dramatic increase in communication protocols
- Increasing complexity of the enterprise as organizations adopt digital transformation and the exposure of various digital entities to both external and internal threats

These trends and the ensuing challenges they introduce require contextualizing the cyber-securing of industrial (IACS) networks, in terms of OT asset type and function and the different interconnected business processes that make up the industrial operation.

Leveraging Fortinet open application programming interfaces (APIs) between the Fortinet FortiGate NGFW and Radiflow's iSID Industrial Threat Detection System delivers simplicity and operational optimization, ensuring that security threat vectors are detected and remediated and that industrial processes occur as prescribed.

Joint Solution Benefits

- Add industrial context and detection rules to your FortiGate firewall functionality, with detailed OT asset information and alerting prioritization
- Instant detection of new assets on the OT network with integration between the FortiGate firewall and the Radiflow iSID threat detection system
- Full visibility of the OT network, drillable down to each asset's details and vulnerabilities
- Leverage your investment: By integrating Radiflow's iSID, your FortiGate firewall is able to expand its protection to the OT network

FORTINET Fabric-Ready

Joint Solution Description

Firewall policy rules, which define the firewall behavior when faced with a set of conditions (e.g., "block all external communications to an IP address"), are the foundation of any industrial cybersecurity system.

However, without a clear picture of the network—which asset is located at each IP address (e.g., PLC, RTU, HMI), which business process the asset belongs to, and the criticality level of the business process (e.g., a PLC belonging to a high-pressure turbine would have a higher criticality score than the same device controlling the manufacturing floor lighting)—it would be very hard to set rules that reflect the actual nature of the industrial facility's operations.

Linking between iSID and FortiGate and configuring firewall rules for different asset types is quick and easy—all it takes is entering the identifiers of the FortiGate firewall (name, IP address, port and API token, source interface, and destination interface). Then, for each available asset type (HMI, PLC, Server, Router, Historian, OPC Server, and Engineering Station), the user is able to select a behavior: None, Block, and Allow.

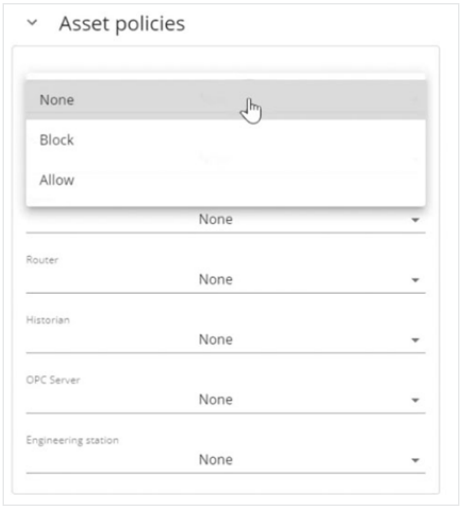
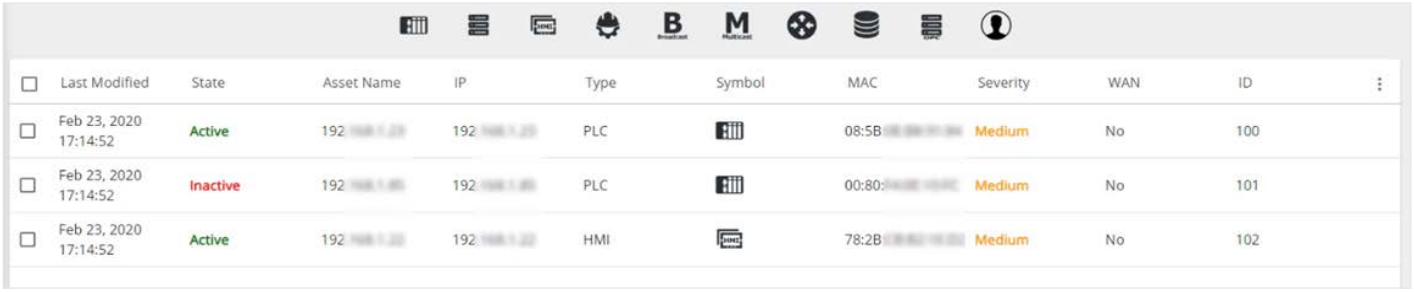


Figure 1: Configuring asset policies for the FortiGate firewall in iSID.

Once iSID connects to FortiGate and its underlying OT network, it detects all of the assets on the network via passive monitoring, along with their status (active/inactive), type, name, and IP and MAC addresses. Depending on the OT environment, iSID concludes the business process each asset belongs to and assigns a severity (criticality level for that asset; these definitions can be changed manually).



Last Modified	State	Asset Name	IP	Type	Symbol	MAC	Severity	WAN	ID
Feb 23, 2020 17:14:52	Active	192	192	PLC		08:5B	Medium	No	100
Feb 23, 2020 17:14:52	Inactive	192	192	PLC		00:80:	Medium	No	101
Feb 23, 2020 17:14:52	Active	192	192	HMI		78:2B	Medium	No	102

Figure 2: List of networked assets as detected by iSID.

The list of newly detected assets automatically syncs with FortiGate, where the firewall rules can be further tweaked to determine the firewall rules for incoming and outgoing traffic, for each asset.

Components of the Joint Solution

Radiflow iSID Industrial Threat Detection & Analysis System

Radiflow's iSID Detection & Analysis Platform provides proactive cybersecurity for critical infrastructures through non-intrusive monitoring of distributed production networks for changes in topology and behavior.

iSID's multiple security engines offer capabilities pertaining to the specific type of network activity: modeling and visibility of OT and IT devices, protocols and sessions; detection of threats and attacks; policy monitoring and validation of operational parameters; rules-based maintenance management; and networked device management.

iSID employs Radiflow's iSAP Smart Collectors, installed at distributed networks' remote sites, to collect, compress (to prevent network overload), and send over GRE all LAN traffic from the local switch, using port mirroring to a centrally installed iSID over VPN tunnels.

iSID allows for different modes of deployment, allowing organizations to optimize their cybersecurity expenditure: on-site at the industrial (ICS/SCADA-based) facility; at the operator's central monitoring location; or at an MSSP's security operations center (SOC) using the iCEN management platform for multiple instances of iSID.

Key Benefits of the Joint Solution

1. Automatic remediation: FortiGate NGFW policy rules are automatically enforced upon detection of new assets trying to connect to the OT network by iSID. This prevents relying on manual procedures for updating firewall rules for newly connected devices.
2. Contextual asset information: Operators are able to leverage iSID's contextual OT asset information for enhanced enforcement of FortiGate policy rules in OT networks, allowing for greater flexibility during scheduled maintenance and provisioning.
3. End-to-end protection: The combination of iSID and FortiGate provides comprehensive and proactive protection across IT, OT, and IoT networks, and secures all inter-network communication to prevent cross-transmission of malware.
4. Complex industrial networks

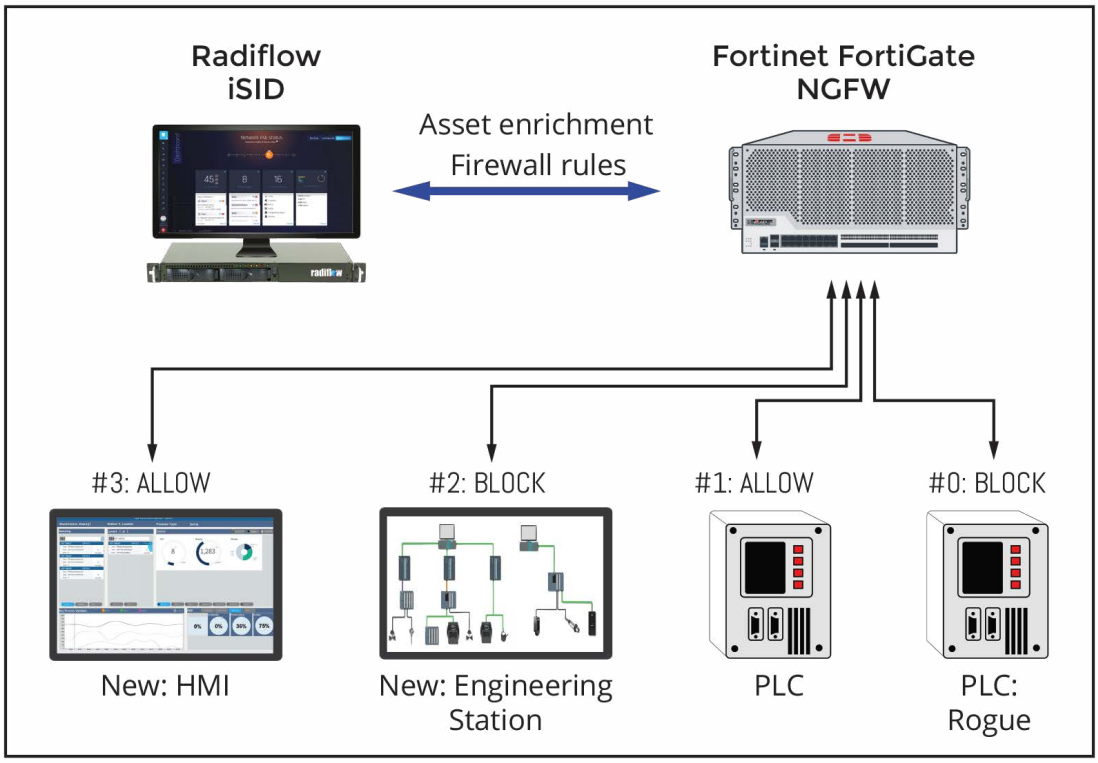


Figure 3: Automatic implementation of enhanced firewall rules in FortiGate using rich asset information from iSID.

June 30, 2020 8:31 AM

D:\Fortinet\Solution Briefs\Grey Solution Brief\Radiflow Security Solution\sb-fortinet-and-radiflow-security-solution-V1-6302020

716455-0-0-EN