Joint Solution Brief

Fortinet FortiGate NGFW and Radiflow iSID

Utilize the FortiGate firewall to protect your OT assets, through automatic creation and enforcement of firewall rules, with full visibility of all OT assets, protocols and connections

Industrial cyber security is one of the core features of transitioning OT infrastructures to Industry 4.0 levels.

The following dynamics are having a dramatic affect 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 IoT 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) network, in terms of OT asset type and function and the different interconnected business processes that make up the industrial operation.

HIGHLIGHTS

- 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 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

Leveraging Fortinet's open API's between Fortinet's Fortigate Next Generation Firewall and Radiflow's iSID Industrial Threat Detection System delivers simplicity and operational optimization ensuring security threat vectors are detected and remediated, ensuring industrial processes occur as prescribed.

iSID's network overview dashboard

FEATURES OF THE JOINT SOLUTION

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 cyber-security 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 (for example, 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.

radiflow FORTINET

The joint solution between the FortiGate NGFW (Next Generation Firewall) and Radiflow's iSID not only equips the FortiGate firewall with a clear model of all assets, asset types, protocols and ports on the network, it also provides the criticality of each asset. This enables configuring rules for otherwise undetected assets, as well as rules that much better comply with the security needs of the industrial operator.

QUICK & SIMPLE SETUP

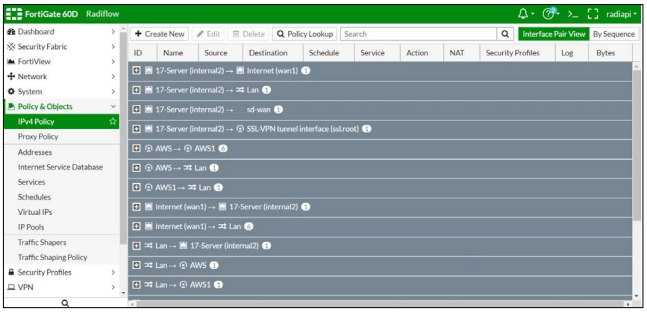
Linking between iSID and FortiGate and configuring firewall rules for different asset types is quick and easy - simply enter the identifiers of the FortiGate firewall (Name, IP address, Port and API token, source interface and destination interface), hit enter, and you're done.

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.

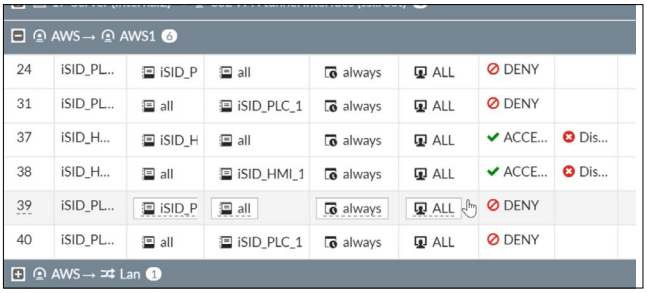
Once iSID connects to Fortigate and its underlying OT network, it detects all of the assets on the network via passive monitoring, along with their status (Active/Inactive), type, name, and IP and MAC addresses.

Depending on the organization's OT environment, iSID is able to conclude the business process each asset belongs to and assigns a severity (criticality level for that asset; these definitions can be changed manually).

The list of iSID's 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.



FortiGate's Policies Dashboard



Configuration of communications permissions in FortiGate for iSID-detected devices

ABOUT FORTINET

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 450,000 customers trust Fortinet to protect their businesses. More at www.fortinet.com

ABOUT RADIFLOW

Radiflow is a leading provider of industrial cyber security solutions for critical business operations. Our comprehensive portfolio of cybersecurity solutions empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent threat management for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment. The Radiflow team consists of professionals from diverse backgrounds, from veterans of military cyber and communications units to former employees of leading players in the industry. Founded in 2009, Radiflow' first solutions were launched in late 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at www.radiflow.com.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

DACH:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

www.radiflow.com | info@radiflow.com