Enabling Secure One-way Cloud Data Transfers with MQTT

Summary

INDUSTRY

Cloud Services
IoT Security

CHALLENGES

Distributed, cloud-connected IoT assets in an increasingly threat-rich environment require one-way transfer of two-way MQTT protocol

SOLUTION

OPDS data diodes & MQTT protocol adapter

BENEFITS

Isolates IoT assets and enables secure one-way transfer of MQTT data transfer to cloud services / hosting provider

Cybersecurity Challenge

Critical infrastructure and industrial organizations continue the push to digitize operations and employ connected devices into the "Internet of Things" (IoT) at a time when advanced, persistent threats (APT) against these industries are rising at an unprecedented pace. While the convergence of digital assets with cloud computing can provide numerous benefits to efficiency, productivity, and reliability, every additional connected asset also represents a potential access point for bad actors. While data diodes have been used to secure IoT assets using industrial protocols, there remains the challenge of supporting data transfers between the devices and the cloud, using inherently two-way cloud-based protocols, such as MQTT.

OWL MQTT PROTOCOL ADAPTER USE CASES

- One-way transfer to Cloud Services
- One-way transfer to Internal Broker within the business/IT network
- One-way transfer to External Broker, such as HiveMQ
- One-way transfer to Remote Client
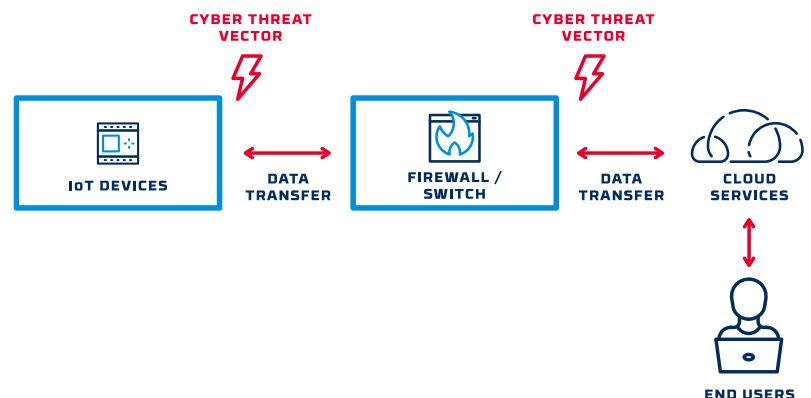
Before Architecture

Solution

MQTT Protocol Adapter paired with Owl data diodes provides secure, one-way transfers of MQTT messages while proxies maintain simultaneous two-way communications. Hardware-enforced separation of source and destination networks ensures security for IoT assets and no shared routing or device information between domains. Can be used with or without cloud-based or external brokers and integrates with all common cloud service providers including AWS and MS Azure.
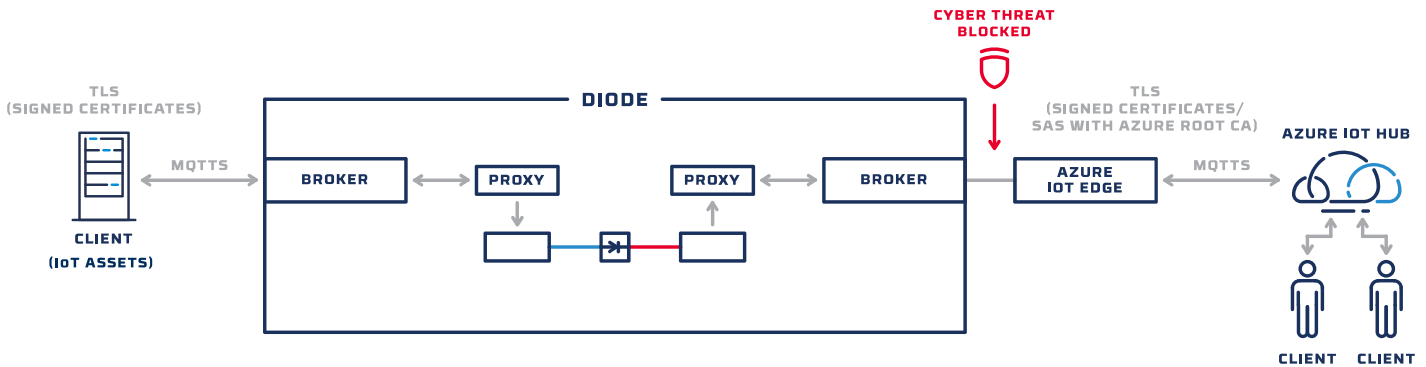
After Architecture

Results

- Securely connect IoT assets to Azure, AWS, and other popular cloud service providers
- Effective network segmentation and one-way flow ensures absolute elimination of inbound cyber threats
- Can be integrated with cloud-based or external brokers, including Mosquitto, HiveMQ, and Ignition
- Supports TLS communication - MQTTS can be used on both sides of the data diode

Case Study

A global manufacturer of powder-based manufacturing systems wanted to remotely monitor and optimize the performance of their machinery. They used an edge gateway to transform the Modbus protocol of their machinery to MQTT. An Owl data diode with the MQTT Protocol Adapter then subscribed to that data on the operational network and published it for an Azure IoT Hub in the network DMZ. The Hub then sent that data to Microsoft Azure IoT analytics applications in the cloud.

1 Messages published to Topic Queues hosted on MQTT Broker

2 Topic Messages consumed by Owl MQTT Protocol adapter and passed across the diode

3

4 Messages received across the diode and re-produced by Owl MQTT Protocol Adapter

5 Messages published to respective Topic Queue by Owl MQTT Protocol Adapter

OWL Cyber Defense

Owl Cyber Defense cross domain, data diode, and portable media solutions provide hardened network security checkpoints for hardened threat prevention and secure data availability. For over 20 years, Owl's unmatched expertise, products, and services have been trusted by clients in government, defense, critical infrastructure, and commercial organizations around the world.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com