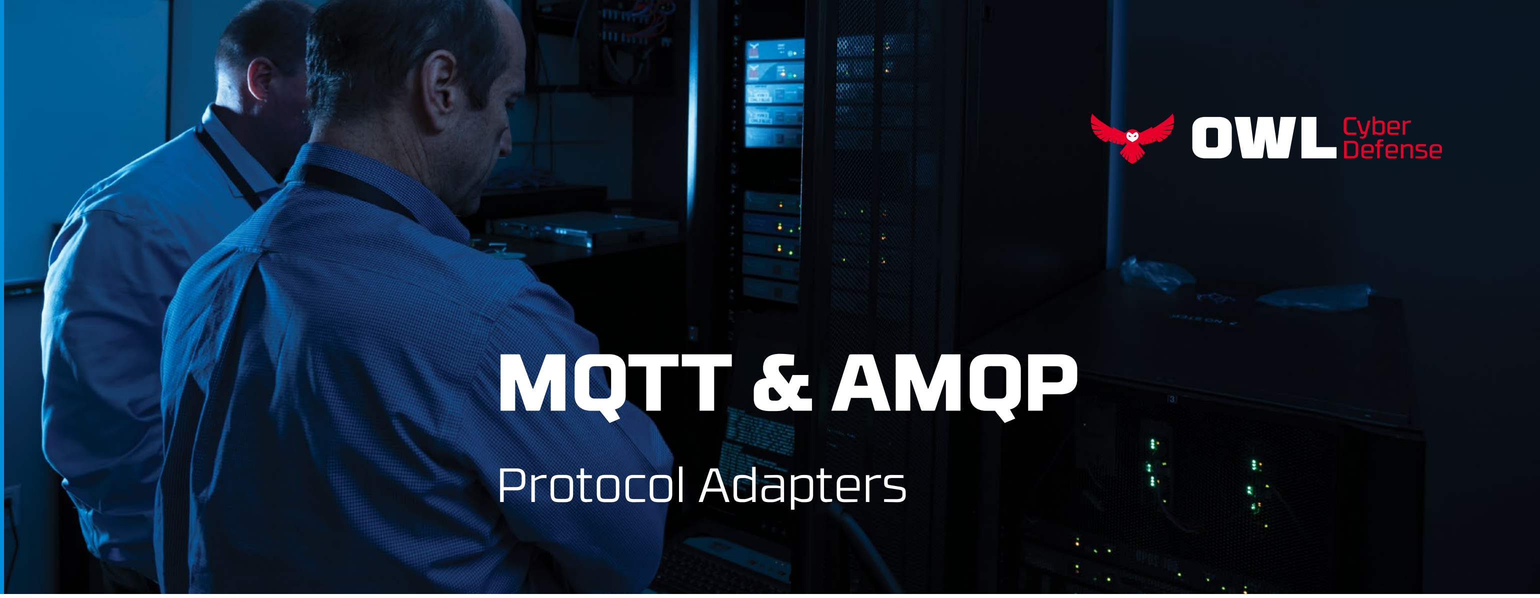
DATA SHEET



OWL Cyber Defense

MQTT & AMQP

Protocol Adapters

AT-A-GLANCE

- MQTT and AMQP are the most widely used protocol adapters for moving IIoT data to the cloud
- Secure, one-way transfers of MQTT and AMQP messages
- Protects IIoT and OT assets and enables secure cloud connectivity
- Seamless integration with Owl data diodes

ABOUT THE PROTOCOLS

MQTT

- Developed for constrained environments on low throughput networks
- Supports client to server (broker) architectures
- Publish and subscribe communication method
- Delivers messages in real-time and stores messages when clients are offline

AMQP

- Supports client to broker or client to server architectures
- Publish and subscribe and response or request communication methods
- Advanced messaging services

Secure Transfer of MQTT & AMQP Messages

As demands rise for connected systems and cloud connectivity, industrial organizations are leveraging two of the most widely used protocols for cloud-based data, MQ Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP). MQTT and AMQP provide open communications, however once communications are open, they need to be secured. Owl has developed Protocol Adapters that allow MQTT and AMQP two-way traffic to be sent over secure, one-way data diodes. The proxies allow Owl's hardware-enforced data diodes to securely transfer MQTT and AMQP traffic across the Operational Technology (OT) network boundary to the cloud, corporate data centers, Security Operations Centers (SOC), remote monitoring centers, or anywhere, with no risk of threats entering back into the source network. The MQTT and AMQP Protocol Adapters combined with a data diode, integrate with Amazon Web Services (AWS), AZURE, and other common private clouds, while maintaining the confidentiality, integrity, and availability of OT systems and MQTT and AMQP messages.

MQTT Protocol Adapter

MQTT is a lightweight messaging protocol that utilizes publish and subscribe operations to exchange data between clients and a server, also known as a broker. MQTT was designed for lightweight devices, like mobile devices and embedded systems, operating on minimum network throughput. Developed specifically for Machine to Machine (M2M) and Industrial Internet of Things (IIOT) environments, the MQTT Protocol Adapter paired with Owl data diodes provides a secure, hardware-enforced transfer of MQTT messages across network boundaries. Although MQTT is inherently a two-way communication protocol, data diodes create an air gap at the network boundary to provide secure, one-way transfers of MQTT messages, physically preventing threats from entering back into the IIoT or OT network. The MQTT Protocol Adapter securely transfers MQTT messages, in real-time, through a data diode to verified subscribers.

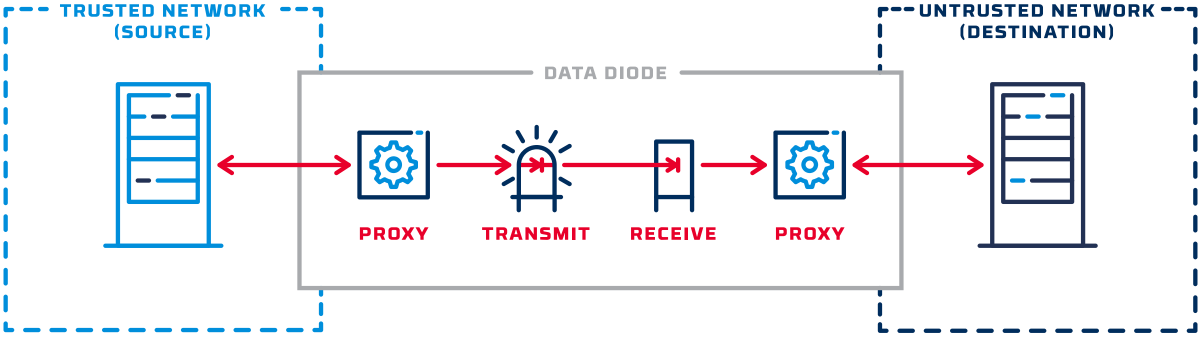
AMQP Protocol Adapter

AMQP is an open standard application layer protocol adapter for message-oriented middleware. The AMQP Protocol Adapter, paired with data diodes, provides a secure, hardware-enforced, one-way transfer of AMQP messages across network boundaries to a range of destination delivery points. The AMQP Protocol Adapter seamlessly integrates with data diodes placed between IIoT networks and the cloud to securely transfer messages to untrusted destinations.

One-Way In A Two-Way World

A successful one-way data transfer of MQTT and AMQP messages requires meeting the expectations of a two-way world. MQTT and AMQP are inherently two-way connections. A majority of network traffic involves some sort of acknowledgment or two-way connection in order to function. The “secret sauce” of data diodes paired with MQTT and AMQP is in providing a one-way transfer, with a true separation between source and destination networks, while maintaining simultaneous two-way communications with both the source network and the destination network to avoid disruption. This is accomplished through using proxies that run on each side of a data diode.

The send side proxy communicates with the source network, acknowledging the receipt of packets before extracting the payload, and then sending it across the data diode. On the receive side, the proxy receives the payload, builds a new packet around it using the original protocol, and sends the data on its way over the two-way protocol. In this way, MQTT and AMQP achieve a one-way transfer in the middle of two, two-way exchanges. This protocol termination also means data diodes protect network privacy by removing all source network routing and IP information when performing a one-way data transfer of MQTT or AMQP messages.



Brokers and Encryption

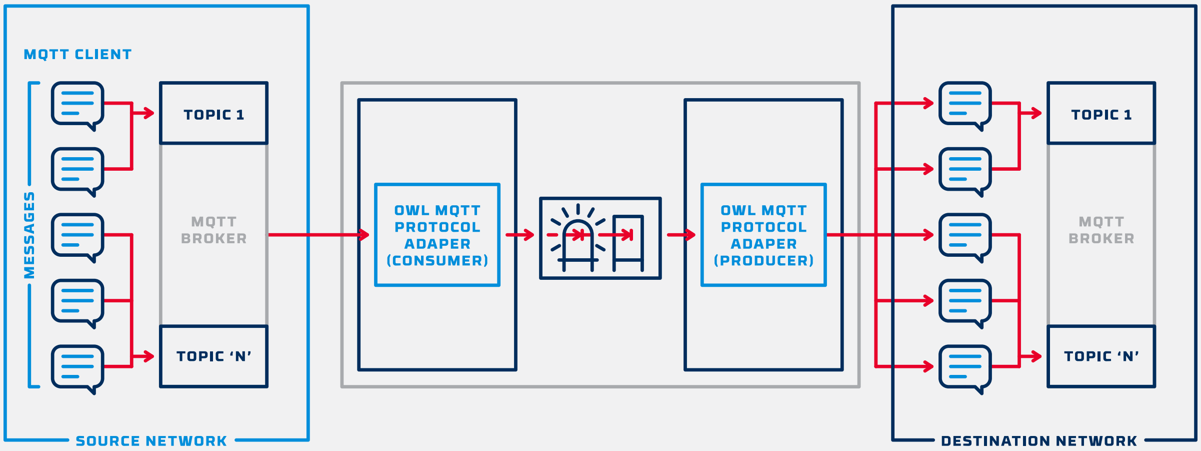
MQTT and AMQP require the use of a central broker to deliver messages. The role of a broker is to receive all messages, filter all messages based on topic, determine who is subscribed to each message, and deliver those messages to subscribed clients. The broker acts as a middle-man and all messages must pass through them to reach their destination. Most MQTT and AMQP brokers allow the use of Transport Layer Security (TLS) to encrypt MQTT communications to the cloud or end destination. The Owl MQTT and AMQP Protocol Adapters supports TLS communication to cloud based or external brokers. The Protocol Adapter works with commonly used products like Mosquitto, Ignition (Spark Plug B), and HiveMQ for MQTT as well as RabbitMQ for AMQP.

USE CASE

MQTT Protocol Adapter

The MQ Client sends an MQTT message to a third-party broker. The source broker then sends the message, or a group of bundled messages, to the source diode IP and the Owl MQ Proxy (Consumer) sends the proxied message across the data diode. The Owl MQ Proxy (Producer) rebuilds the MQTT message and forwards it to a destination third-party broker. The Owl MQ Proxy can send messages directly to an internal or external broker.

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



Technical Specifications

SUPPORTED BROKERS

- Ignition (Spark Plug)
- Mosquitto
- Hive MQ

SUPPORTED ON

- OPDS-100
- OPDS-100D
- OPDS-1000
- EPDS

Use Cases

- One-way transfer to Internal Broker within the business network
- One-way transfer to External Broker such as HiveMQ
- One-way transfer to Remote Client
- One-way transfer to Cloud Services

AMQP Protocol Adapter

The Remote Client Producer sends an AMQP message to a third-party broker (most common: RabbitMQ). The source broker consists of an "Exchange" and "Queue". The Exchange receives messages from a Producer and manages which queue the data should be sent to. The Queue then passes the AMQP message to the Owl AMQP Proxy (Consumer) which moves the payload across the data diode. The Owl AMQP Proxy (Producer) rebuilds the AMQP message and forwards it to a destination third-party broker, usually RabbitMQ or CloudAMQP (RabbitMQ as a service).

The RabbitMQ broker can be installed on the data diode. If significant volumes of data are being transferred, a flanking server is recommended.

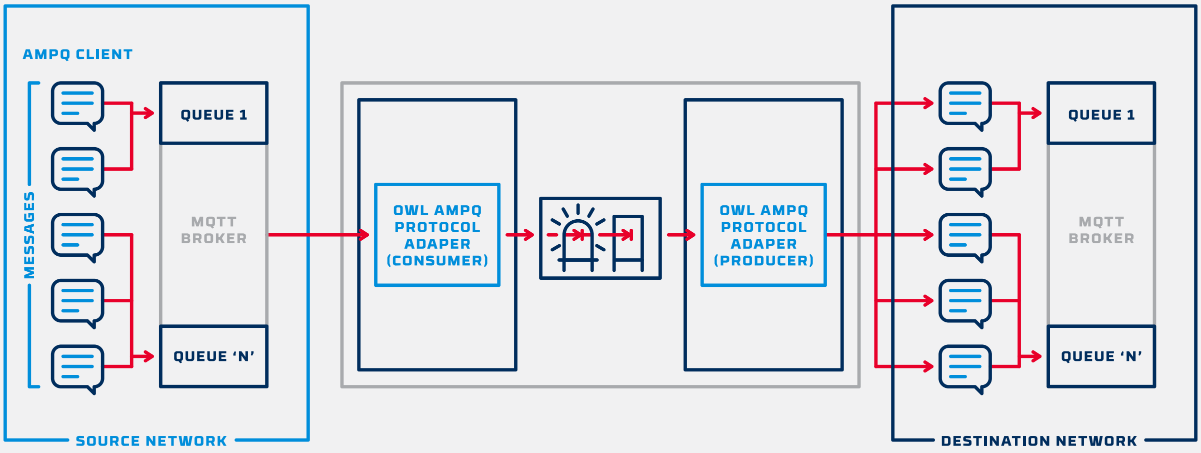
1 → Messages published to Topic Queues hosted on AMPQ Broker

2 → Messages consumed by Owl AMPQ Protocol adapter and sent across the diode

3 →

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

5 Messages published to respective Queue by Owl Protocol Adapter



Technical Specifications

SUPPORTED BROKERS

- RabbitMQ

SUPPORTED ON

- OPDS-100
- OPDS-100D
- OPDS-1000
- EPDS

Use Cases

- One-way transfer to Local Broker such as RabbitMQ within the Business network
- One-way transfer to External Broker
- One-way transfer to Cloud Services

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

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

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com