SOLUTION BRIEF

Securing Open Platform Communications in OT Environments with FortiGate Next-generation Firewalls

Executive Summary

Open Platform Communications (OPC) is an interoperability standard used widely in operational technology (OT)/industrial control system (ICS) environments. Sectors such as manufacturing, utilities, energy, and building automation rely on OPC standards to address the demands of universal data access. As such, OPC must be secured, especially given that OT organizations are increasingly attractive targets for hackers. However, traditional firewalls have difficulty understanding OPC.

Fortinet FortiGate next-generation firewalls (NGFWs) are not only able to understand OPC but they also provide granular control of more than 250 standard OPC functions. Additionally, the FortiGate application control feature supports more than 30 different OT/ICS protocols.

OPC Background

Originally referred to as Object Linking and Embedding (OLE) for Process Control, this protocol is now known as OPC. This communication standard is used for secure and reliable data communication in Industrial Automation and Control System (IACS) environments. The original implementation of this open standard is called OPC Classic or Legacy OPC.

OPC Classic is restricted to Microsoft Windows and is typically deployed using a client-server architecture. In a Microsoft Windows network environment, OPC Classic uses Microsoft Distributed Component Object Model (DCOM) technology and offers Data Access (DA), Historical Data Access (HDA), and Alarms and Events (AE) services. Microsoft DCOM is a network-oriented version of the Component Object Model (COM) standard that is based on OLE technology. This is commonly used for communication between software components in a typical Microsoft Windows network environment.

OPC UA Differentiator

OPC UA does not rely on DCOM technology, enabling it to work on any software platform, including Microsoft Windows, Linux, Unix, macOS, or Android. This allows OPC UA to scale from embedded systems to massive cloud deployments. **FortiGate network firewalls natively support OPC UA.**

There is a newer OPC release known as Open Platform Communications Unified Architecture (OPC UA). This version is platform independent and is based on service-oriented architecture. OPC UA integrates all the functionality of the individual OPC Classic specifications into one extensible framework and offers built-in security. It is also compatible with OPC Classic.

OPC Classic Deployment

A typical deployment of OPC Classic includes an OPC server, OPC client, sensors, and actuators. Sensors and actuators control field devices such as valves, fans, and pumps. Oftentimes, programmable logic controllers (PLCs) or intelligent electronic devices (IEDs) are added to ICS environments that talk to sensors to enable advanced automation.

The field devices communicate to the IEDs via serial communications, which send the signaling and telemetry data to the OPC server. Once the IEDs receive the communication, it is then translated to IP-based protocols. The OPC server acts as the central repository and data store of all the information from the field and makes it available to OPC clients upon request.

The client-server communication within OPC Classic environments is based on Microsoft DCOM and relies on Microsoft Remote Procedure Call (MS RPC). This allocates dynamic communication ports between OPC servers and clients.

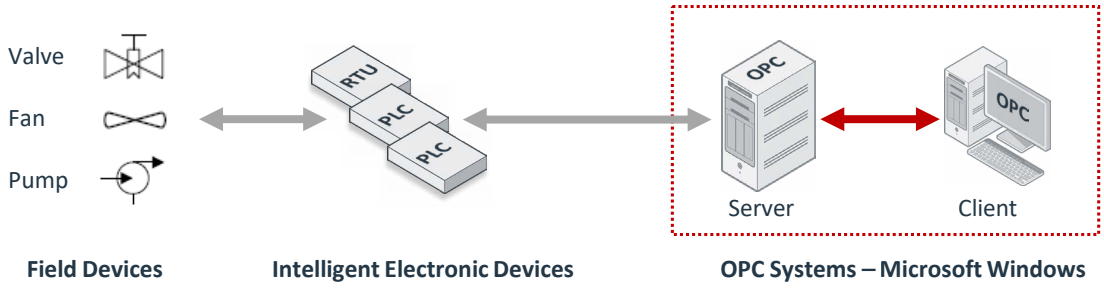

Figure 1: Typical OPC Classic deployment.

Challenges of Securing OPC

Since OPC Classic communication relies on MS RPC, the network firewall must be aware of the dynamic ports created by the OPC server and allow communications though those ports, while restricting other ports. Further, the firewall needs to be able to interpret OPC to distinguish it from other Microsoft Windows network communication sessions between the same client-server network.

FortiGate Secures OPC

FortiGate NGFWs run on the Fortinet proprietary operating system FortiOS. FortiOS has built-in support for handling dynamic ports over network communication channels using session helper technology. FortiOS uses session helpers to analyze traffic, specifically the data in the network packet bodies, and adjust the firewall to allow appropriate packets through the firewall.

FortiOS also includes application control technology that not only understands OPC Classic communication, but it also provides granular control over standard OPC Classic functions for complete control over these communications. For example, an OT network administrator could create a firewall policy that only allows OPC commands to start or stop a specific pump, and disallows OPC commands that increase or decrease speed.

The following is a standard OPC Classic scenario. Based on the defined security policy on FortiGate for the OPC server and client, the firewall will allow OPC client communication with the OPC server. Then, using session helpers for MS RPC, it efficiently manages the access control for the dynamic ports created by the OPC server. This allows communication only on the required network ports between the OPC server and client while restricting any other communication ports. The session helpers ensure that the broad range of network communication ports that are usually required by DCOM to function properly are not arbitrarily opened on the firewall.

Using in-depth knowledge of standard OPC Classic functions, the application control feature further analyzes the established communication session and checks to ensure the session is a genuine OPC. If the session is not a genuine OPC, the communication between the server and client is blocked.

On FortiGate network firewalls, both the OPC Classic and OPC UA security functionality are not limited to application control policies. Security controls such as intrusion prevention system (IPS) policies are included to identify any malicious network traffic hidden inside the OPC stream and respond accordingly.

Fortinet Secures OT Environments

Fortinet offers comprehensive security for the entire OT environment, not just OPC. By integrating OT security solutions with proven threat protection for IT environments, the entire network is protected, from the data center, to the network perimeter, to the cloud.

The Fortinet Security Fabric delivers visibility, control, and fast, automated response to threats, while provisioning built-in support for industry standards in an OT environment. Reduced complexity and cost further contribute to make Fortinet the ideal security partner for OT environments.

January 23, 2020 6:47 AM

519922-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\OT Solution Brief\sb-FA-securing-an-open-platform-commmunications-in-ot-environments