SOLUTION BRIEF

Security für Open Platform Communications in OT-Umgebungen mit FortiGate Next Generation Firewalls

Zusammenfassung

Open Platform Communications (OPC) ist ein Interoperabilitätsstandard, der in Umgebungen mit Betriebstechnologie (OT) und industrieller Steuerungstechnik (ICS) weitverbreitet ist. OPC-Standards dienen z. B. in der Fertigung, Versorgung, Energiewirtschaft und Gebäude-Automation zum Datenaustausch zwischen unterschiedlichsten Systemen. Dieser universelle Datenzugriff muss geschützt werden, zumal heute noch ein anderer Faktor hinzukommt: OT-Unternehmen sind ein zunehmend beliebtes Angriffsziel von Hackern, lassen sich aber schlecht mit herkömmlichen Firewalls schützen, die mit OPC ihre Schwierigkeiten haben.

Fortinet FortiGate Next Generation Firewalls (NGFWs) verstehen OPC, bieten eine granulare Kontrolle über mehr als 250 OPC-Standardfunktionen und unterstützen dank der integrierten Application Control über 30 verschiedene OT/ICS-Protokolle.

Wissenswertes über OPC

Ursprünglich als „Object Linking and Embedding (OLE) for Process Control“ bezeichnet, wurde dieses Protokoll später in „Open Plattform Communications (OPC)“ umbenannt. OPC ist der Kommunikationsstandard für den sicheren, zuverlässigen Datenaustausch in Umgebungen mit industrieller Automatisierungs- und Steuerungstechnik – kurz IACS (Industrial Automation and Control System). Die ursprüngliche Implementierung dieses offenen Standards wird als OPC Classic oder Legacy OPC bezeichnet.

OPC Classic ist auf Microsoft Windows beschränkt und wird normalerweise mit einer Client-Server-Architektur implementiert. In einem Windows-Netzwerk verwendet OPC Classic die DCOM-Technologie (Microsoft Distributed Component Object Model) und stellt Dienste wie Data Access (DA), Historical Data Access (HDA) sowie Dienste für Alarme und Ereignisse (AE) bereit. Microsoft DCOM ist eine netzwerkorientierte Version des COM-Standards (Component Object Model), der auf der OLE-Technologie basiert. Diese dient in einem typischen Windows-Netzwerk für den Datenaustausch zwischen Software-Komponenten.

Unterschied zu OPC UA

OPC UA ist nicht auf die DCOM-Technologie angewiesen und funktioniert mit jedem Betriebssystem, einschließlich Microsoft Windows, Linux, Unix, MacOS und Android. OPC UA lässt sich deshalb sehr gut von Embedded-Systemen bis hin zu großen Cloud-Implementierungen skalieren. **FortiGate Netzwerk-Firewalls bieten eine native Unterstützung von OPC UA.**

Die neuere OPC-Version – bekannt als „Open Platform Communications Unified Architecture (OPC UA)“ – ist plattformunabhängig und basiert auf einer dienstorientierten Architektur. OPC UA integriert alle Funktionen der einzelnen OPC Classic-Spezifikationen in einem erweiterbaren Framework, bietet eine integrierte Security und ist zu OPC Classic kompatibel.

Implementierung von OPC Classic

Eine typische Implementierung von OPC Classic umfasst einen OPC-Server, einen OPC-Client sowie Sensoren und Aktoren. Die Sensoren und Aktoren steuern Feldgeräte wie Ventile, Ventilatoren und Pumpen. Häufig werden ICS-Umgebungen mit speicherprogrammierbaren Steuerungen (SPS) oder intelligenten elektronischen Geräten (IED) erweitert, die mit Sensoren kommunizieren und so eine umfassendere Automatisierung ermöglichen.

Die Feldgeräte kommunizieren über die serielle Kommunikation mit den IEDs, die die Signalisierungs- und Telemetriedaten an den OPC-Server senden. Die IEDs übersetzen dafür die eingehende Kommunikation in IP-basierte Protokolle. Der OPC-Server fungiert als zentrales Repository, speichert sämtliche Feldinformationen und stellt sie OPC-Clients auf Anfrage zur Verfügung.

Die Client-Server-Kommunikation in OPC Classic-Umgebungen basiert auf Microsoft DCOM mit Microsoft Remote Procedure Call (MS RPC). Hiermit werden dynamische Kommunikationsschnittstellen zwischen OPC-Servern und -Clients zugewiesen.

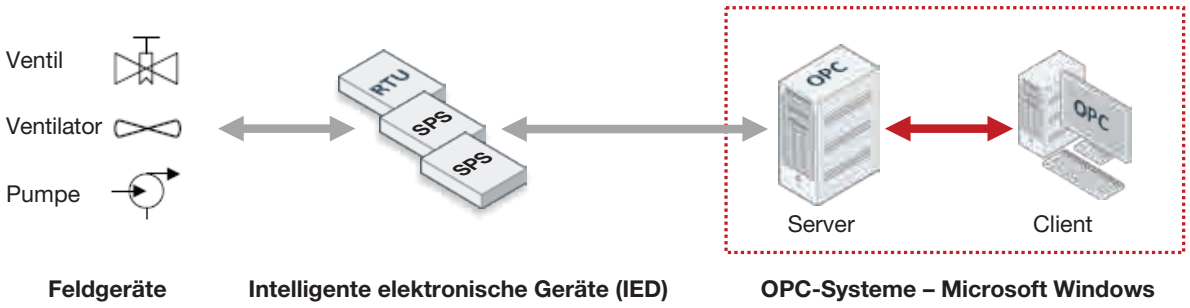

Abbildung 1: Typische Implementierung von OPC Classic

Herausforderungen beim OPC-Schutz

Da der Datenaustausch mit OPC Classic auf MS RPC basiert, muss die Netzwerk-Firewall die dynamischen Ports erkennen können, die der OPC-Server angelegt hat. Die Firewall darf nur die Kommunikation über diese Schnittstellen erlauben, alle anderen Ports sind unzulässig. Auch muss die Firewall OPC interpretieren können, um den OPC-Datenaustausch von anderen Windows-Kommunikationssitzungen im gleichen Client-Server-Netzwerk zu unterscheiden.

OPC-Schutz mit FortiGates

FortiGate NGFWs arbeiten mit dem proprietären Fortinet-Betriebssystem FortiOS. FortiOS bietet mit der Session-Helper-Technologie eine integrierte Unterstützung für dynamische Ports über Netzwerk-Kommunikationskanäle. Zudem verwendet FortiOS Session-Helper, um den Datenverkehr zu analysieren – insbesondere die Daten in Netzwerk-Paketkörpern. Auch lässt sich damit die Firewall so anpassen, dass nur die richtigen Pakete die Firewall passieren dürfen.

FortiOS bietet außerdem eine Application-Control-Technologie, die nicht nur die OPC Classic-Kommunikation versteht, sondern auch eine granulare Kontrolle über die Standardfunktionen von OPC Classic bietet. Netzwerk-Administratoren für Betriebstechnologie erhalten damit vollständige Kontrolle über diesen Datenaustausch. Beispielsweise lässt sich eine Firewall-Richtlinie festlegen, die nur OPC-Befehle zum Starten oder Anhalten einer bestimmten Pumpe zulässt, während OPC-Befehle zur Steuerung der Pumpgeschwindigkeit verboten sind.

Nehmen wir folgendes Standard-Szenario für OPC Classic: In der FortiGate wurden bestimmte Richtlinien festgelegt, nach denen die Firewall die OPC-Client-Kommunikation mit dem OPC-Server zulässt. Dann regelt die Firewall mit Session-Helpern für MS RPC den Zugriff auf die dynamischen Ports, die der OPC-Server erstellt hat. Der Datenaustausch zwischen dem OPC-Server und dem OPC-Client kann so nur über die erforderlichen Netzwerk-Schnittstellen erfolgen – andere Kommunikationsschnittstellen werden blockiert. Session-Helper gewährleisten, dass der große Port-Bereich für die Netzwerk-Kommunikation (der normalerweise notwendig ist, damit DCOM richtig funktioniert) nicht willkürlich bei der Firewall geöffnet wird.

In die Application Control sind umfassende Informationen über OPC Classic-Standardfunktionen integriert. Dies ermöglicht die Analyse bestehender Kommunikationssitzungen und die Überprüfung, ob es sich bei einer Sitzung wirklich um einen OPC-Datenaustausch handelt. Wenn nicht, wird die Kommunikation zwischen Server und Client blockiert.

Bei FortiGate Netzwerk-Firewalls beschränken sich die Security-Funktionen für OPC Classic und OPC UA nicht allein auf Application-Control-Richtlinien. Security-Controls wie IPS-Richtlinien (Intrusion Prevention System) gehören ebenfalls dazu, um jeden im OPC-Datenfluss versteckten bösartigen Netzwerk-Verkehr zu erkennen und abzuwehren.

Fortinet schützt OT-Umgebungen

Fortinet schützt nicht nur OPC, sondern bietet eine umfassende Security für die gesamte OT-Umgebung. Durch die Integration von OT-Security-Lösungen mit einem bewährten Bedrohungsschutz für IT-Umgebungen wird das ganze Netzwerk abgesichert – vom Rechenzentrum und Netzwerk-Rand bis hin zur Cloud.

Die Fortinet Security Fabric bietet Transparenz, Kontrolle und eine schnelle, automatisierte Bedrohungsabwehr mit integrierter Unterstützung der Industriestandards von OT-Umgebungen. Fortinet ist der ideale Security-Partner für den Schutz von Betriebstechnologie, mit dem Unternehmen von geringerer Komplexität und Kostensenkungen profitieren.

FORTINET

www.fortinet.com/de

14. Dezember 2020

519922-0-0-DE