datenblatt

mGuard
opc inspector

Die intelligente Absicherung von OPC Classic

OPC Classic und Firewalls

OPC ist einer der am weitesten verbreiteten Standards in der industriellen Automatisierungswelt, um die Anforderungen des universellen Datenzugriffs zu bewältigen. Als OLE for Process Control entwickelt, wird es nun zumeist als OPC Classic bezeichnet.

OPC Classic wird von einer breiten Palette von Industrie- und Businessanwendungen, wie zum Beispiel HMI-Workstations, SPS-Steuerungen und Prozessleitsystemen, aber auch von Unternehmensdatenbanken und weiteren geschäftsorientierten Systemen unterstützt.

Das grundsätzliche Konzept von OPC Classic, keine festen TCP-Port Nummern zu nutzen, sondern innerhalb der ersten geöffneten Verbindung neue Portnummern auszuhandeln führt dazu, dass zwischengeschaltete Firewalls deshalb nur mit weit geöffneten Toren eingesetzt werden können und somit praktisch keine Wirksamkeit erzielen. Zudem führen die innerhalb der OPC-Verbindung kommunizierten IP Adressen von Client und Server dazu, dass konventionelles NAT Routing (Network Address Translation) nicht eingesetzt werden kann. Dieser Problematik begegnet der *mGuard OPC Inspector* durch den Einsatz einer Deep Packet Inspection für OPC Classic.

Deep Packet Inspection für OPC Classic

Mit Deep Packet Inspection schaut der mGuard wörtlich tief in die übermittelten Pakete, analysiert und verändert diese gegebenenfalls. Dabei kann konfiguriert werden, dass über den OPC Classic Port 135 ausschließlich OPC Pakete gesendet werden dürfen. Die innerhalb der ersten geöffneten Verbindung ausgehandelten TCP-Ports werden zudem zuverlässig erkannt und für OPC Pakete geöffnet. Werden über diese Ports innerhalb eines konfigurierbaren Timeouts keine OPC Pakete versendet, werden diese wieder geschlossen. Natürlich kann mit granularen Firewall-Regeln exakt definiert werden, welche Clients mit welchen Servern per OPC kommunizieren dürfen. Durch dieses Connection Tracking entsteht Sicherheit auf höchstem Niveau!

Defense in Depth

Angreifer nutzen verschiedene Wege, um Zugang zu Produktionsanlagen zu erlangen. Stuxnet hat beispielsweise gezeigt, dass Angriffe mittels kompromittierter USB Sticks auch aus dem Inneren von Anlagen möglich sind. Abhilfe schafft hierbei die Anwendung des auf ISA-99 basierenden „Defense in Depth“ Konzepts. Es basiert auf der netzwerktechnischen Segmentierung von Anlagen und der dezentralen Absicherung dieser einzelnen Segmente. Dank des *mGuard OPC Inspector* kann dieses Konzept nun auch in Anlagen, in denen OPC Classic Verwendung findet, umgesetzt werden.

Segmentierung durch NAT

Und für eine individuelle Segmentierung von OPC-basierenden Netzen ermöglicht die intelligente Deep Packet Inspection des *mGuard OPC Inspector* als Weltneuheit sogar die Verwendung von NAT-Verfahren wie Masquerading oder 1:1 NAT.

SecurITy
made in Germany

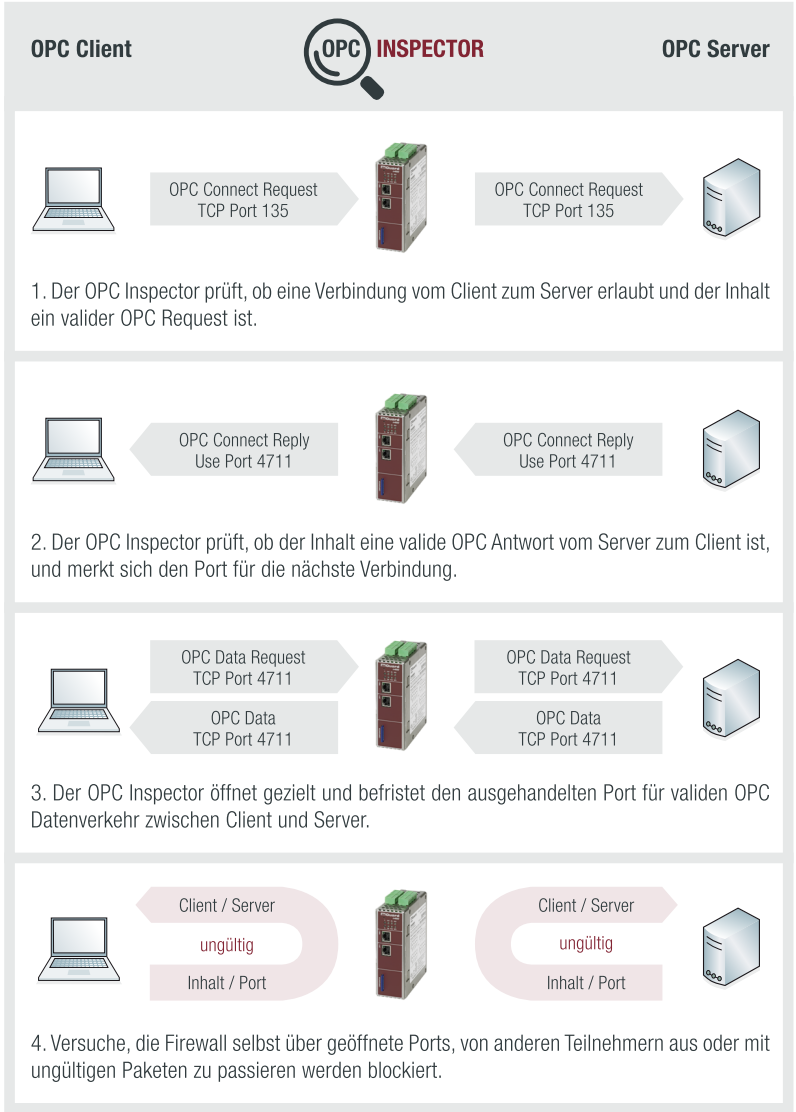

Abbildung: Funktionsweise mGuard OPC Inspector

Available models and order numbers:

mGuard OPC Inspector	SL-106010

Benötigt mGuard Firmware 8.1 oder höher.

Das mGuard Produktportfolio

mGuard Security Appliances werden in mehreren Bauformen für verschiedene Einsatzszenarien angeboten und kombinieren jeweils eine leistungsfähige mGuard Hardware-Plattform mit der bewährten mGuard Firmware. Auf Basis eines gehärteten Embedded Linux Systems sind darin folgende aufeinander abgestimmte Sicherheitskomponenten integriert: eine bidirektionale Stateful Packet Inspection Firewall, ein flexibler NAT-Router, eine IPsec Implementierung für hochsichere Virtual Private Networks (VPNs), QoS Support (Quality of Service) sowie optional ein industrietauglicher Schutz vor Schadsoftware und Support für Hochverfügbarkeitslösungen durch Firewall / VPN-Redundanz.

Vorteile der mGuard Technologie

Sicherheit: mGuard Security Appliances schützen Ihre Systeme, Maschinen und Kommunikationswege mit höchster Sicherheit vor Angriffen und lassen Sie beruhigt schlafen.

Plug-n-Protect: mGuard Security Appliances sind autark und durch den patentierten mGuard Stealth Mode schnell und ohne Rückwirkungen integrierbar. Sie verhalten sich dabei Routing-technisch völlig transparent und verwenden die IP-Adresse des jeweils zu schützenden Systems. Hierdurch sind die Geräte für einen Angreifer nicht zu erkennen und nicht kompromittierbar.

Schnelligkeit: Die exzellenten Durchsatzraten von mGuard Security Appliances ermöglichen Ihnen gesicherte IP-Kommunikation ohne Geschwindigkeitsengpässe.

Aktualität: Neuen sicherheits- und marktgetriebenen Anforderungen werden Sie dank regelmäßigen Upgrades der mGuard Firmware auch künftig problemlos gerecht.

Effizienz: Der optional erhältliche Device Manager erleichtert Ihnen das zentrale Management und den Vorlagen-basierten Roll-out sämtlicher mGuard Geräte.

Über Innominate Security Technologies AG

Innominate, ein Phoenix Contact Unternehmen, ist führender Hersteller von Komponenten und Lösungen für die kontrollierte und gesicherte Kommunikation in industriellen Netzwerken. Kerngeschäftsfelder sind die Absicherung vernetzter industrieller Systeme und die sichere Fernwartung von Maschinen und Anlagen über das Internet. Die Innominate mGuard Netzwerksicherheitsgeräte verfügen über Router, Firewall, Virtual Private Network (VPN) sowie Quality of Service (QoS) Funktionalitäten und unterstützen bei Intrusion Detection und Virenschutz. Ergänzt wird das mGuard Portfolio durch eine hoch skalierbare Device Management Software. Produkte von Innominate werden unter der Marke mGuard von Systemintegratoren sowie über OEM-Partner weltweit vertrieben.

Weitere Informationen finden Sie unter **www.innominate.com.**

Innominate Security Technologies AG | Rudower Chaussee 13 | 12489 Berlin | Deutschland | Tel. +49 30 921028-0 | Fax +49 30 921028-020 | www.innominate.de