# Mehr Sicherheit durch Verinselung

**Steuerungen über ein Sicherheitsgateway ins Intranet einbinden**

**Ob in der Haus- und Gebäudeautomation oder im industriellen Umfeld, die Einbindung von Automatisierungseinrichtungen in ein bereits existierendes Intranet bietet viele Vorzüge, aber eben auch viele nicht zu unterschätzende Gefahren. Einem Teil dieser Gefahren kann man bereits wirkungsvoll am Übergang zwischen Inter- und Intranet entgegentreten, bei anderen wiederum bedarf es eines gezielteren Herangehens.**

Die Wiesemann und Theis GmbH (W&T) ist ein in Wuppertal beheimatetes und nach den Firmengründern benanntes Technologieunternehmen. Ein Blick auf das Produktportfolio des Unternehmens macht schnell deutlich, dass hier, ausgehend vom Wissen um die Techniken des Internets eine neue Generation von Automatisierungslösungen angeboten wird. Internettechnologien werden nicht in existierende Produkte „nachgerüstet", sondern diese Lösungen werden ausgehend von Netzwerk- und Web-Techniken entwickelt. Die Internettechnologien sind also Basis der Produkte. Beispielhaft hierfür sind die unter der Produktbezeichnung Web-IO angebotenen Automatisierungslösungen. Zum Produktangebot des Unternehmens gehören weiter diverse Schnittstellen zur Anbindung von Sensorik sowie Netzwerktechnik. Aktuell hat das Unternehmen sein Portfolio um zwei Produkte ergänzt, die dazu beitragen, die mit dem Intranet/Internet verbundenen Systeme vor unerlaubten Zugriffen über das Netz zu schützen.

## Verinselung als Konzept

Obwohl beide Geräte für grundsätzlich unterschiedliche Aufgabenbereiche konzipiert sind, liegt beiden Geräten der Grundgedanke der Abtrennung der schutzbedürftigeren Komponente vom übrigen Netz zugrunde (Bild 1). Diese von den Entwicklern „Verinselung" genannte Vorgehensweise basiert letztlich auf der auch ansonsten aus unterschiedlichen Beweggründen angewandten Praxis der Segmentierung von Netzen. Während es ansonsten vorzugsweise darum geht eigene Netzsegmente für die unterschiedlichen Bereiche (Verwaltung, Entwicklung und Produktion) eines Unternehmens zu bilden, sind diese Geräte vor allem zur Anbindung einzelner Endgeräte mit einem höheren Schutzbedarf konzipiert. Gleiches gilt auch für Komponenten, die wegen der darauf installierten Software (z. B. ältere Technik) einer höheren Gefährdung ausgesetzt sind. Durch diese Vorgehensweise können die Maßnahmen zur Erhöhung der Sicherheit wesentlich gezielter erfolgen. Die Geräte sind schon wegen der Bauform als Reiheneinbaugeräte vor allem für den Einsatz im industriellen Umfeld konzipiert, gleichwohl ist ein Einsatz in der Medizintechnik sowie der Haus- und Gebäudeautomation ebenso denkbar.

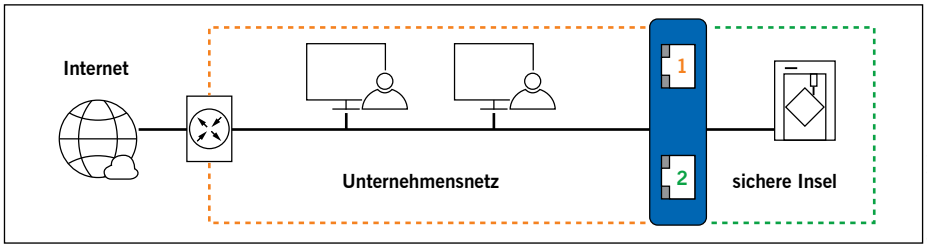
**Autor**
Dr.-Ing. Horst Möbus ist als Honorardozent und Fachautor tätig, Groß Düben.

## Gerätetechnik

Die angebotenen Geräte sind bezüglich der Handhabung und der möglich Einsatzbereiche recht unterschiedlich (Tabelle 1). Während die Microwall Gigabit wegen ihrer Konfigurierbarkeit in etwa als das „Schweizer Taschenmesser" angesehen werden kann, ist die Fix Defined Firewall eher ein perfekt auf lediglich einen Anwendungszweck zugeschnittenes Gerät (Bild 2).

**Tabelle 1 Technische Angaben (Auswahl)**

| | Microwall Gigabit | Fix Defined Firewall |
|---|---|---|
| Bauform | Reiheneinbaugerät | Reiheneinbaugerät |
| Schnittstellen | 2 x Ethernet 100/1000BaseT<br>-Autosensing/Auto-MDIX<br>RJ45 | 2 x Ethernet 100BaseT<br>-Autosensing/Auto-MDIX<br>RJ45 |
| Funktionalität | frei konfigurierbar<br>Betriebsarten<br>– Standard-Router<br>– NAT-Router<br>Whitelist-basierter Paketfilter | nicht konfigurierbar<br>Plug&Play-Lösung<br>Datenverkehr nur in einer Richtung möglich |



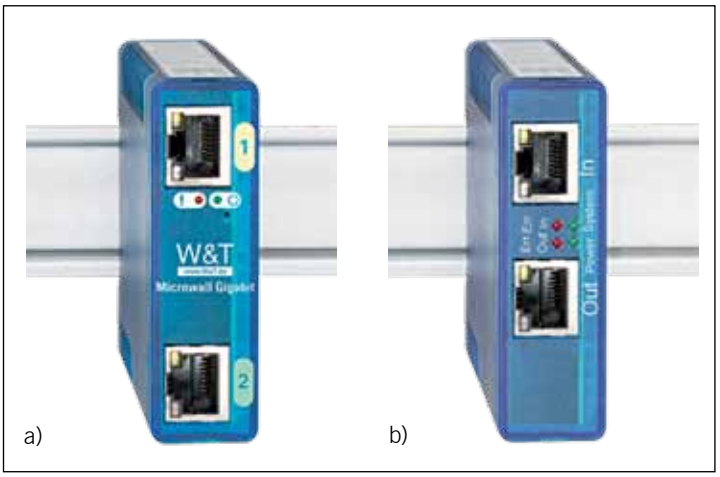

Quelle: W&T/ep P. Richter

**1 Mehr Sicherheit durch Verinselung**

## Sicherheitsgateway

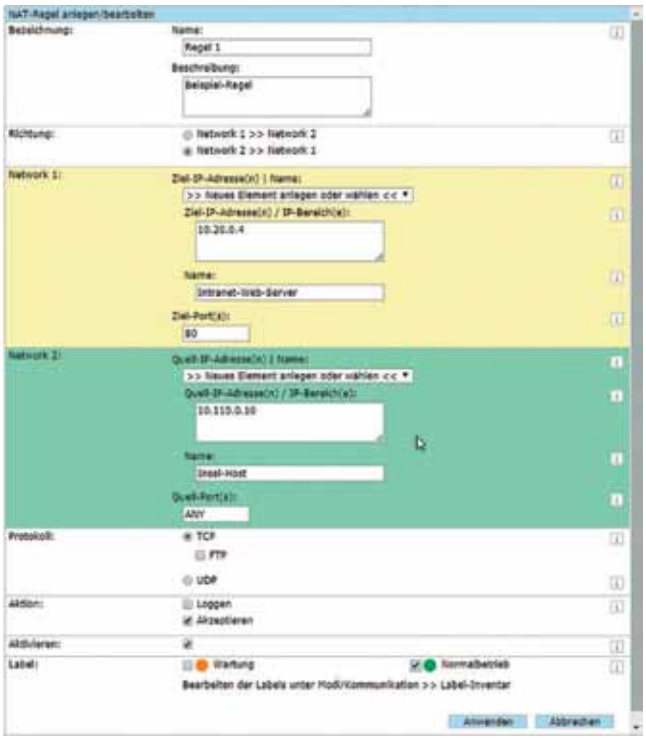
Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten zur Gewährleistung einer sicheren Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei vor allem die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen und die Kontrolle der übertragenen Daten. Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs Firewall soll verdeutlichen, dass zur Absicherung von Netzübergängen heute nicht mehr ein einzelnes Gerät verwendet wird, sondern eine Menge von Rechnern und deren Konzeption, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs.

Quelle: BSI-Leitfaden „Integration und IT-Revision von Netzübergängen"




Quelle: W&T

**2 Zwei Geräte – ein Konzept**
a) Microwall Gigabit – Router mit konfigurierbarem Paketfilter
b) Fix Defined Firewall – Einbahnstraße für Datenpakete



Quelle: W&T

**3 Erfassungsmaske zur Anlage der Filterregeln**

## Microwall Gigabit – Router mit konfigurierbarem Paketfilter

Das unter der Bezeichnung Microwall Gigabit angebotene Gerät ist bezüglich der Funktion ein Router und kann wahlweise als Standard- oder als NAT-Router eingesetzt werden.
Die Betriebsart Standard-Router erfordert eine Intergration der über das Gerät eingebundenen Endgeräte in das Routing-Konzept des Intranets. Bei der Betriebsart NAT-Router sind alle angeschlossenen Endgeräte unter einer einzigen Intranet-IP erreichbar.
Für die Inbetriebnahme kann das Tool Wutility von der Website des Unternehmens heruntergeladen werden. Hiermit können zunächst die Netzwerkbasisparameter

- IP-Adresse
- Subnetzmaske
- Gateway-Adresse
- DNS-Server

eingestellt werden. Für die weitere Konfiguration kann auf ein Standard Web-Based-Management (WBM) zugegriffen werden, so dass auch eine Fernkonfiguration möglich ist. Zur Sicherheit erfolgt die Kommunikation hierbei ausschließlich verschlüsselt per HTTPS.
Die Anlage des Regelwerks für den Paketfilter erfolgt für jede Betriebsart (Standard- oder NAT-Router) gesondert. Durch Zuordnung eines Labels (z. B. Normalbetrieb oder Wartung) zu den erstellten Filterregeln können zeitlich unterschiedliche Anforderungen bezüglich der Filterung der Datenpakete realisiert werden. Der Anlage der Filteregeln liegt das **Whitelist-Prinzip** zugrunde, es ist also **alles verboten was nicht ausdrücklich erlaubt ist.** Die Anlage der Filteregeln erfolgt in einer überaus übersichtlichen und damit gut verständlichen Erfassungsmaske (Bild 3). Hierzu trägt sowohl die farbliche Kennzeichnung der Eingabebereiche als auch die konsequent schrittweise Vorgehensweise bei. Beginnend mit der Vergabe einer Bezeichnung für die anzulegende Regel muss zunächst festgelegt werden für welche Richtung die Regel gelten soll. Danach erfolgt die Festlegung der Filteregeln für Quelle und Ziel anhand der Adressierungsinformationen

- IP-Adresse(n) und
- Port-Nummer(n)

sowie der Angabe des Transportprotokolls (TCP oder UDP). Bei TCP kann noch eine weitere Einschränkung auf das File Transfer Protocol (FTP) erfolgen. Die Anlage der Filterregeln schließt mit deren Aktivierung, Angaben zu Aktionen und der Zuordnung zu einem Label. Über Info-Buttons können Information/Ausfüllhinweise zu den einzelnen Feldern aufgerufen werden.

## Fix Defined Firewall – Einbahnstraße für Datenpakete

Dieses Gerät folgt zwar ebenfalls dem Konzept der Verinselung, aber in einer völlig anderen Weise. Die Fix Defined Firewall wird komplett konfiguriert ausgeliefert und ist damit „Plug&Play“ installierbar – ohne Netzwerkkenntnisse. Die Funktion des Gerätes lässt sich in einem Satz beschreiben: In einer Richtung können ausnahmslos alle Datenpakete passieren und in der Gegenrichtung kommt kein Datenpaket durch. Damit ist zwar der Einsatzbereich dieses Gerätes deutlich abgegrenzt, aber dort wo genau das nötig ist, erfüllt es diese Anforderung vollumfänglich. Seitens des Herstellers wird diesbezüglich der Anschluss eines Netzwerksniffers genannt. Es sind aber auch Einsatzmöglichkeiten im Rahmen von IoT- und I4.0-Projekten (Stichwort: Daten sammeln) denkbar. Hier sind zwar keine Netzwerkkenntnisse zur Installation nötig, wohl aber im Vorfeld bei der Geräteauswahl und Bestimmung der Einsatzbereiche.

## Netzwerkkenntnisse unerlässlich

Spätestens wenn es um die Schaffung sicherer Netzübergänge [1] oder eben um die Verinselung geht, wird schnell deutlich, dass nur grundlegende Netzwerkkenntnisse nicht mehr genügen. Um IP-Adressen in einem Intranet zu vergeben reichen noch Kenntnisse zum Adressaufbau und zu den zur Verfügung stehenden privat frei nutzbaren Adressbereichen. Aber um einen Paketfilter zu konfigurieren, muss man tiefer in den Adressierungsmechanismus mittels Ports und Protokollen einsteigen. W&T bietet hierzu auf seiner Webseite ein breites und gut aufbereitetes Informationsangebot. Das gilt auch für die Anleitungen zur Inbetriebnahme. Grundlegende und weitestgehend produktneutrale Netzwerkkenntnisse mit einem deutlichen Bezug zur Automatisierungstechnik


Quelle: W&T

**4 Ein gelungenes Grundlagenbuch – auch als PDF-Datei verfügbar**

bietet das als PDF-Datei frei verfügbare Grundlagenbuch „TCP/IP-Handbuch“ von F. Thiel (Bild 4). Die Themenpalette reicht dabei von der physikalischen Übertragung, über die logische Adressierung und den Transportprotokollen, den Anwendungs- und Web-Protokollen, den IoT- und I4.0-Protokollen bis hin zu Aspekten der Daten- und Netzwerksicherheit [2].

## Fazit

Die von W&T angebotenen Geräte sind im besten Sinne des Wortes „praxisgerecht zu Ende gedacht“. Mit dem Wissen um die Technologien des Internets und den Anforderungen der Automatisierungstechnik sind Produkte entstanden, die sowohl den Bedürfnissen der industriellen als auch der handwerklichen Praxis entsprechen. Wegen des vorzüglichen Informationsangebots des Unternehmens und der gelungenen Gestaltung des WBM zur Erstellung von Paketfiltern sind die Produkte auch für die Ausbildung von Meistern, Technikern und Ingenieuren zu empfehlen.

**Literatur**

[1] Möbus, H.: Sichere Netzübergänge (ep-Beitragsreihe).
- Teil 1: Modellvorstellung und Begriffe. ep 73 (2019) 4, LERNEN & KÖNNEN S. 6–7.
- Teil 2: Bausteine von Sicherheitsgateways – Paketfilter. ep 73 (2019) 5, LERNEN & KÖNNEN S. 6–7.
- Teil 3: Bausteine von Sicherheitsgateways – Proxys und NAT. ep 73 (2019) 6, LERNEN & KÖNNEN S. 6–7.
- Teil 4: Virtualisierung und weitere Sicherheitswerkzeuge. ep 73 (2019) 7, LERNEN & KÖNNEN S. 5–7.
- Teil 5: Typische Architekturen und praktische Aspekte. ep 73 (2019) 8, LERNEN & KÖNNEN S. 12–14.

[2] Thiel, F.: TCP/IP-Ethernet: Mach es einfach. Netzwerktechnische Grundlagen. 8. überarbeitete & erweiterte Auflage, Wiesemann & Theis GmbH, Wuppertal 01-2020.

**ep WEB-TIPP**

Weitere Details zu den vorgestellten Sicherheitsgateways finden Sie auf der Internetseite des Herstellers:
**https://www.wut.de/**

# Digitalisierung mit Single Pair Ethernet (SPE)

**Nächste Generation der Kommunikationsarchitektur**

**Mit der zunehmenden Digitalisierung wird eine Netzwerkinfrastruktur für das Industrial Internet of Things (IIoT) benötigt. Dafür bietet sich das Single Pair Ethernet (SPE) an, das von Experten als die nächste Generation der Kommunikationsarchitektur gesehen wird.**

Ursprünglich für Automotive-Anwendungen entwickelt, verspricht Single Pair Ethernet (SPE) inzwischen nicht weniger als eine durchgängige Verbindung vom Sensor bis zur Cloud. Das Beispiel der Automobilindustrie ist gut auf andere Anwendungen übertragbar. Bereits heute macht bei Fahrzeugen die Verkabelung einen Großteil des Gewichts aus. Sollte das autonome Fahren kommen, benötigen Fahrzeuge noch mehr Sensoren und Verbindungstechnik. Für diese enormen Datenmengen suchte die Branche eine Infrastruktur, die mit möglichst wenig Kabel viel leisten kann: Der Ursprung für SPE.

## Aufwand der Vernetzung wird komplexer

Ähnliches ist für die Industrie und Gebäudeautomation zu erwarten. Denn durch die weltweit steigende Anzahl smarter Endgeräte aufgrund der Digitalisierung wird der Aufwand der Vernetzung zunehmend komplexer. Im Anlagenfeld steigt die Zahl intelligenter Endgeräte, aber nicht der zur Verfügung stehende Platz – ganz im Gegenteil. Da immer mehr Sensorik in die Maschinen und Anlagen eingebunden werden soll, muss die Verkabelung entsprechend industrietauglich, kompakt und einfach aufgebaut sein. Dazu kommen extreme Einsatzorte, wo eine Verkabelung mit kleinem Außendurchmesser, kleinen Biegeradien und geringem Gewicht unabdingbar ist, beispielsweise bei Roboterarmen.
Die Lösung ist ein Ethernet-Standard, der nicht die hohen Datenübertragungsraten der IT-Welt bieten muss, aber dafür große Leitungslängen mit einer kompakten Bauform und einer einfachen und robusten Verkabelung kombiniert: Das Single Pair Ethernet, kurz SPE.
Auch bei der Gebäudeautomatisierung wird der Einsatz von SPE zur Integration von einpaarigem Ethernet in Hierarchie und Struktur heutiger Gebäudeverkabelung diskutiert.
SPE steht für eine durchgängige, skalierbare und deterministische Vernetzung von der Sensorik bis in die Cloud. Und das in praktisch jeder Anwendung, ob in der Industrie, in der Logistik, im Gebäude oder wo auch immer Daten anfallen. Das Konzept dahinter ist eine Erweiterung von Ethernet bis in die Sensorik, also überall dorthin, wo es keine Datenautobahnen, sondern im Wortsinn „Feldwege“ bis in den letzten Winkel des Anlagenfeldes braucht – kompakt, flexibel und mit hoher Reichweite.
Bisherige Lösungen benötigen zwei (Fast Ethernet) beziehungsweise vier Adernpaare (Gigabit Ethernet und höher), während Single Pair Ethernet nur noch ein Adernpaar benötigt. Gleichzeitig kann die Single-Pair-Ethernet-Technologie neben Daten auch Leistung bis zu 60 W an der PSE (Power Source Equipment) zur Verfügung stellen. Damit garantiert sie eine wirtschaftliche, zukunftssichere und durchgängige Vernetzung einer Vielzahl an Endgeräten – von der Geräteschnittstelle bis zur aktiven Vernetzung intelligenter Geräte sowie von der Gebäudetechnik bis zur Sensorik im Feld.
Die physikalischen Eigenschaften und Übertragungsraten werden international von unterschiedlichen Standardisierungsgremien definiert. Diese neuen Varianten des Ethernets stoßen auch in der Automatisierungstechnik auf großes Interesse, denn SPE erfüllt alle Voraussetzungen für die Industriekommunikation im Zeitalter der Digitalisierung. Die Übertragungsraten von 10 Mbit/s bei einer Übertragungslänge von 1 000 m bis hin zu 1 Gbit/s mit einer Übertragungslänge von 40 m bzw. bis 100 m sind selbst für eine anspruchsvolle Sensorik völlig ausreichend. Auch Scanner und Kameras zur Überwachung

**Autorin**
Dipl.-Ing. Silke Lödige ist Referentin Fachpresse bei der Weidmüller Interface, Detmold.