HIRSCHMANN
A BELDEN BRAND

HOPF
PARTNER | SOLUTIONS | COMPONENTS

White Paper

WP00019HE

Firewall-Technologie für die industrielle Cyber-Sicherheit verständlich gemacht

Prof. Dr. Tobias Heer, Future Technologies, Hirschmann Automation and Control GmbH

Dr. Oliver Kleineberg, Advanced Development, Hirschmann Automation and Control GmbH

Jeff Lund, Senior Director Product Line Management, Belden Inc.

Inhaltsverzeichnis

Be certain.
Belden.

Einleitung

Firewalls sind ein unverzichtbarer Baustein für die Netzwerksicherheit. Da in industriellen Anlagen zunehmend Ethernet-Infrastrukturen eingesetzt und an unternehmensweite IT-Systeme angebunden werden, sind Firewalls zu einer zentralen Komponenten geworden, um die Sicherheit des Netzwerks, eine höhere Widerstandsfähigkeit und Anlagenzuverlässigkeit zu gewährleisten. Firewalls sind jedoch keine Geräte, mit denen sich sämtliche Bedrohungsszenarien verhindern lassen, sondern sie werden in verschiedenen Ausprägungen mit einer Reihe unterschiedlicher Funktionen und Technologien angeboten, um vielfältige Aufgaben im Rahmen einer umfassenden Sicherheitsarchitektur zu übernehmen. Es gibt Firewalls, die für den Einsatz in der klassischen IT konzipiert sind, und Firewalls für industrielle Anwendungen. Diese White Paper stellt die verschiedenen Arten der industriellen Firewalls vor und beschreibt, wo und wie sie integriert werden können, um die Sicherheit und Zuverlässigkeit industrieller Anlagen zu verbessern.

Firewalls: eine zentrale Komponente für die Netzwerksicherheit

Moderne Sicherheitskonzepte folgen einem ganzheitlichen Ansatz, in dem nicht nur die Technologie, sondern auch die Prozesse und das Personal berücksichtigt werden. Deshalb gelten Firewalls schon lange nicht mehr als ausreichende bzw. einzige Maßnahme für den Schutz industrieller Netzwerke und Anlagen. Dennoch bilden Firewalls auch weiterhin die Kernelemente, um Netzwerke zu segmentieren und sind somit ein essentieller Bestandteil jeder Sicherheitsstrategie[1].

Der Begriff Firewall wird inzwischen jedoch sehr weit gefasst und deshalb für verschiedenste Technologien mit unterschiedlichen Methoden und Zielsetzungen verwendet. Beispiele dafür sind Stateless (zustandslose) und Stateful (zustandsbehaftete) Firewalls, transparente Firewalls, Firewalls auf verschiedenen Ebenen der Netzwerk-Referenzarchitekturen, Firewalls mit Deep Packet Inspection oder Firewalls mit Intrusion-Detection-Funktionalität. Dazu kommen noch weitere Methoden, mit denen der Netzwerkverkehr eingeschränkt werden kann wie etwa Access-Control-Listen. Deshalb stehen die Anlagenplaner vor der Frage, welche Firewall für ihre Zwecke die richtige ist.

Generelle Funktionen einer Firewall

Firewalls sind Geräte, die Netzwerke oder Teilnehmer wie Industrie-PCs, Steuerungen, Kameras etc. vor unbefugtem Zugriff schützen, indem sie Netzwerkverkehr zu oder von diesen Teilnehmern verhindern. Dabei kann man grob zwischen Host-Firewalls und Netzwerk-Firewalls unterscheiden. Erstere werden auf einem Rechner (Host) installiert oder bereits vom Betriebssystem als Softwarefunktion bereitgestellt. Beispiele dafür sind die Windows-Systemfirewall oder die mit den meisten Linux-Systemen bereits mitgelieferte IPtables und Netfilter Firewall.

Im Gegensatz dazu sind Netzwerk-Firewalls speziell für die Funktion als Firewall entwickelt worden und werden nicht auf einem PC, sondern im Netzwerk installiert. Diese Netzwerk- oder Hardware-Firewalls sind wichtige Elemente in industriellen Anlagen, insbesondere wenn diese mit weiteren Netzwerken (z. B. Büronetzwerken) verbunden werden oder die kabelgebundene Datenübertragung mit Funktechnologien kombiniert wird. In diesen Fällen richtet eine Netzwerk-Firewall an der Grenze des Netzwerks eine erste Verteidigungslinie gegen Angriffe ein und lässt nur erwünschten Datenverkehr in das Netz hinein und aus diesem heraus.

Die technische Grundfunktion jeder Firewall ist das Filtern von Paketen. Dabei wird jedes empfangene Paket geprüft und entschieden, ob es einem für den Netzwerkverkehr erwünschten bzw. unerwünschten Muster entspricht. Danach filtert und verwirft die Firewall die dem Muster entsprechenden bzw. nicht entsprechenden Pakete. Eine Firewall an der Netzwerkgrenze kann beispielsweise Regeln beinhalten wie „Der Aufbau einer Kommunikationsverbindung darf von innerhalb des Netzwerkes nur zu einem bestimmten Server erfolgen“ oder „Von außerhalb des Netzwerkes sind nur die Login-PCs für die Fernwartung erreichbar und keine weiteren Geräte“. Eine Firewall, die einen Produktionsbereich einer Fabrik schützt, kann möglicherweise Regeln für Industrieprotokolle wie Modbus/TCP haben, beispielsweise „Schreibbefehle für das ModBus/TCP-Protokoll, Coil 56, sind nur vom Wartungsterminal aus erlaubt“.

Da netzwerkbasierte Firewalls von großer Bedeutung für Industrieanlagen sind, werden sie im Mittelpunkt der folgenden Betrachtungen stehen. Wo kommen diese Firewalls in heutigen Sicherheitskonzepten zum Einsatz?

Firewalls im industriellen Umfeld: Einsatzgebiete und Anforderungen

Firewalls sind wichtige Bausteine heutiger Sicherheitskonzepte. An verschiedenen Punkten des Netzwerks werden unterschiedliche Firewalls eingesetzt, um im Zuge einer Defense-in-Depth-Strategie[2] eine Reihe andersartiger Schutzmechanismen zur Verfügung zu stellen. Firewalls können die Verbindung zwischen einem Unternehmensnetzwerk und dem industriellen Netzwerk schützen, um Angriffe externer Hacker zu verhindern. Andere Firewalls können innerhalb eines Netzwerks Geräte voneinander trennen oder nur eine spezifizierte Kommunikation zwischen ihnen erlauben, um nicht nur gegen böswillige Angriffen zu schützen, sondern auch vor Geräte- und Bedienfehlern. Dieses Konzept einer präzisen Einschränkung der Kommunikation zwischen Teilnehmern eines internen Netzwerks und der Segmentierung verschiedener Netzwerkbereiche wird als Zones and Conduits (Zonen und Leitungen) bezeichnet. Zones und Conduits sind ein zentraler Baustein des internationalen Standards IEC 62443 und ein wichtiges Element einer Defense-in-Depth-Sicherheitsstrategie.

Das ist, im Gegensatz zu lediglich einem Schutzmechanismus wie etwa einer einzelnen Firewall, eine Strategie der gestaffelten Verteidigung durch mehrere Sicherheitsebenen. Der Grund, warum Zones und Conduits und Defense-in-Depth so gut harmonieren, liegt darin, dass sich die wesentlichen Elemente dieser beiden Strategien ergänzen.

Zum einen werden durch Defense-in-Depth Angriffe auf Netzwerke durch mehrere, gestaffelte Sicherheitsebenen erschwert, das heißt, eine Angreifer muss verschiedene Hürden überwinden und nicht nur ein einzelnes Hindernis. Zum anderen fügen die Segmentierung eines Netzwerks in mehrere Kommunikationszonen und die Implementierung eines Need-to-Communicate-Ansatzes (Kommunikationsnotwendigkeit) gemäß Zones und Conduits zwangläufig weitere Sicherheitsebenen hinzu, die für den Fall, dass ein Bereich durch einen Angreifer gefährdet wird, einen höheren Schutz des Netzwerks gewährleisten. Denn dann ist nur der Bereich, zu dem der Angreifer Zugriff erlangt hat, betroffen, während das übrige Netzwerk geschützt bleibt. Und da die Mehrzahl der Cyber-Vorfälle aus Gerätefehlern, fehlerhafter Software, menschlichen Fehlern oder Schadware resultieren, erhöht Zones und Conduits die Zuverlässigkeit der Anlagen, indem verhindert wird, dass sich Vorfälle in einer Zone auf andere ausbreiten.

Die Strategien Defense-in-Depth und Zones und Conduits sind nicht neu. Sie wurden beispielsweise schon beim Bau von Burgen berücksichtigt. Denn besonders gefährdete Bereiche waren auch besonders geschützt, etwa durch Wassergräben, mehrere Mauern und Türme. Außerdem wurden manche Bereiche einer Burg mit bewachten Zugängen wie Tore, Zugbrücken und eiserne Fallgitter voneinander getrennt, um es Angreifern so schwer wie möglich zu machen.

In Kommunikationsnetzwerken entspricht die Segmentierung von mehreren angebundenen Geräten in Zones und Conduits den Toren. Dieses Verfahren sollte zusammen mit einer gestaffelten Verteidigung gemäß Defense-in-Depth eingesetzt werden, da Tore ohne Mauern nutzlos sind. Um diese Best Practices (bewährte Vorgehensweisen) in Kommunikationsnetzwerke zu implementieren, werden zahlreiche Firewalls an verschiedenen Punkten des Netzwerks eingesetzt.

Firewalls an Netzwerkgrenzen

Firewalls spielen bei der Segmentierung von Netzwerken verschiedene Rollen. Mit ihnen kann beispielsweise das Netzwerk eines Unternehmens vor Bedrohungen von außen geschützt werden. In diesem Fall ist die Rundum-Absicherung die Domäne von IT-Firewall-Lösungen, die im Rechenzentrum eines Unternehmens platziert werden. Firewalls können aber ebenso dazu verwendet werden, um Netzwerke gegeneinander zu schützen, etwa um das Unternehmensnetzwerk vom Produktionsnetzwerk zu trennen.

Firewalls in einer kleinen Zelle oder einer Außenstelle

Industrielle Firewalls mit Router-Funktionen sind ideal geeignet für kleinere Außenstellen. So lassen sich etwa Verteilerstationen oder entfernte Arbeitsplätze über ein Funknetz mit der übrigen Steuerungsinfrastruktur eines Unternehmens verbinden. Die Firewall überwacht dabei den Datenverkehr aus und in das lokale Netzwerk der Außenstelle. Da eine solche Firewall den Übergang vom unternehmenseigenen Netzwerk (die Außenstelle) hin zu einem fremden Netzwerk (ein Provider-Netzwerk oder das Internet) darstellt, muss sie über sämtliche Möglichkeiten zur Filterung der Pakete wie auch des Verkehrs zwischen verschiedenen Netzwerken verfügen (siehe Abb. 1). Eine solche Firewall wird als IP Firewall bezeichnet, da sie den Verkehr des Internet Protokolls (IP) überwacht. Weil diese Firewalls oft sehr nahe an den eigentlichen Anlagen installiert werden, muss darauf geachtet werden, dass sie industriegerecht, also robust sind. Erweiterte Temperaturbereiche und/oder Zulassungen für spezielle Einsatzgebiete (z. B. Energieversorgung, Gefahrenbereiche und Transportwesen) sind maßgebliche Kriterien.

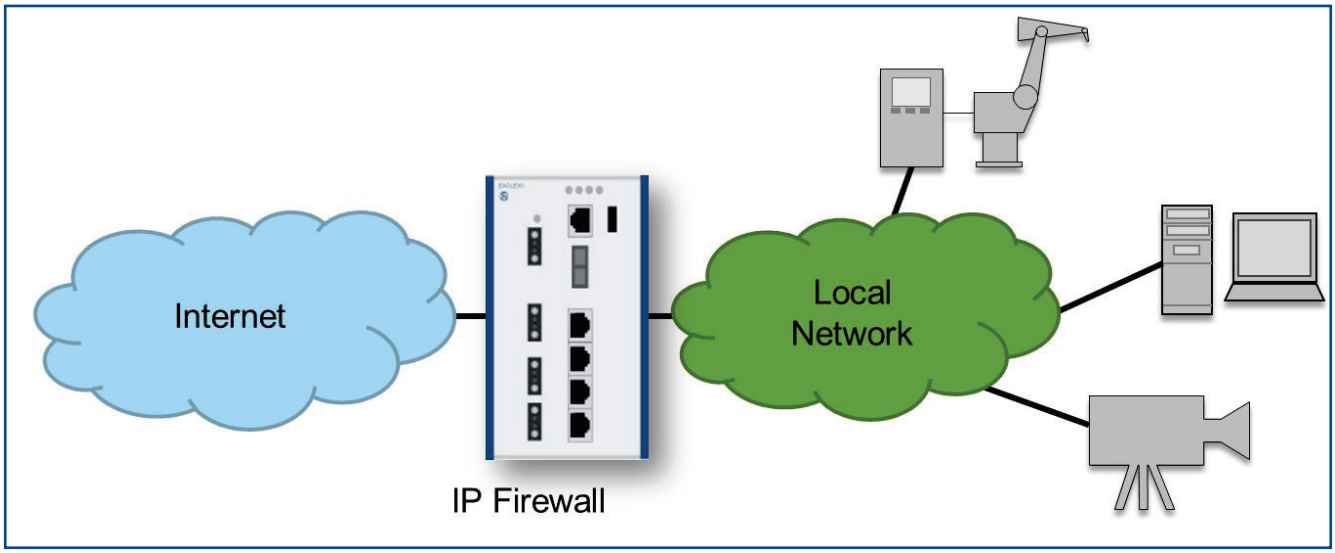


Abb. 1: Firewall zwischen dem Internet und dem lokalen Unternehmensnetzwerk

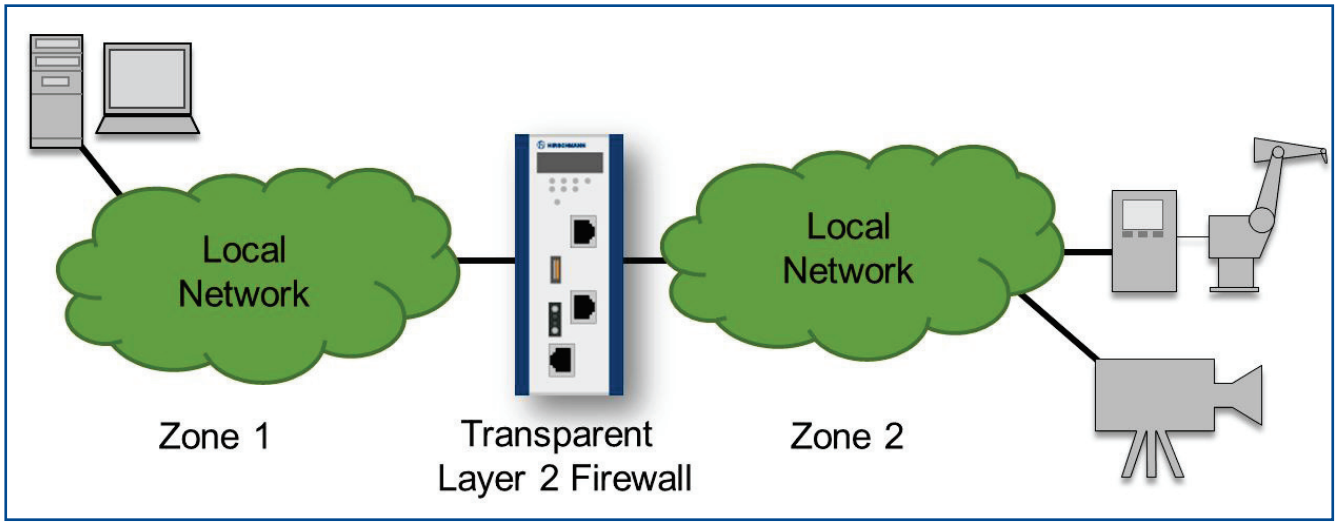


Abb. 2: Firewall innerhalb eines lokalen Netzwerks

Firewalls auf der Feldebene

Es reicht selten aus, nur die äußeren Grenzen des Netzwerkes gegen Angreifer zu schützen. Denn viele Bedrohungen entstehen innerhalb eines Netzwerks. Das zeigen auch Studien aus der Industrie, die belegen, dass die meisten Cyber-Vorfälle nicht aus externen Angriffen resultieren, sondern aus Software-, Geräte- und Bedienfehlern. In einem vernetzten Steuerungssystem können sich Fehler schnell über das gesamte System ausbreiten, wenn nicht Vorkehrungen getroffen werden, um sie zu isolieren und einzudämmen. Deshalb ist eine effektive Cyber-Sicherheits-Strategie nicht nur für die Datensicherheit wichtig, sondern ebenso für die Sicherheit und Zuverlässigkeit der Anlagen.

Somit können Firewalls zu einem Rundumschutz gegen unbeabsichtigte Fehler beitragen, indem sie die Kommunikation zwischen verschiedenen Zonen eines lokalen Netzwerks einschränken (siehe Abb. 2). Das erfordert jedoch eine Firewall, die für dieses Einsatzszenario maßgeschneidert ist. Soll die Kommunikation von außerhalb einer Anlage nur mit einem einzelnen Gerät möglich sein, sollte die Firewall diese Verbindung gezielt zulassen und alle anderen Kommunikationsversuche verhindern.

Die Anforderungen an den Einsatz einer Firewall innerhalb eines Netzwerks unterscheiden sich von denen zwischen Netzwerken. Auf der Ethernet-Ebene ist eine transparente Layer-2-Firewall erforderlich und keine IP-Firewall. Das Hauptmerkmal einer transparenten Layer-2- Firewall zeigt Abb. 3. Diese Firewall bietet Filterfunktionen für die lokale Kommunikation, die normalerweise in der Ethernet-Schicht bzw. dem Layer 2 des Department of Defense (DoD) oder des ISO-OSI-Schichtenmodells passieren.

Dagegen registrieren reine Layer-3-Firewalls in der Regel keinen Layer-2-Verkehr. Deshalb sind Layer-2-Firewalls gegenüber den höheren Protokollschichten transparent, bieten aber eine wichtige Sicherheitsfunktion für lokale Netzwerke.

Angesichts des Umstandes, dass diese Firewalls gewöhnlich auf der Feldebene eingesetzt werden, müssen die Anwendungsgegebenheiten (Temperatur, Vibration und andere Umgebungsfaktoren) sowie die erforderlichen Zulassungen beachtet werden. Das drückt sich nicht nur in deutlichen funktionalen Unterschieden im Vergleich zu klassischen IT-Firewalls aus, sondern auch in einem anderen Erscheinungsbild, anderen Abmessungen und Gehäusen, einer anderen Kühlung (normalerweise ist nur eine passive Kühlung möglich) sowie in der unterstützten Medien- und Transceiver-Technologie.

Firewalls eines WLAN

Auch die Kommunikation von drahtlosen zu kabelgebundenen Netzwerken lässt sich durch Firewalls schützen. Wenn ein Client mit einem WLAN (Wireless Local Area Network) verbunden ist, kann er grundsätzlich mit allen anderen Geräten des gleichen Netzwerks direkt kommunizieren. Somit kann ein Angreifer eine erfolgreiche Attacke auf einen Client auf beliebig viele mit dem Ethernet-Netzwerk verbundene Geräte ausweiten. Das lässt sich verhindern, indem die Weiterleitung von Nachrichten zwischen WLAN-Clients am WLAN-Access-Point durch eine Firewall eingeschränkt wird. Beispielsweise kann die Kommunikation eines Tablets, das via WLAN mit einem Gerät verbunden ist, so begrenzt werden, dass es nur auf die Daten der Benutzerschnittstelle, jedoch nicht auf weitere Subsysteme oder andere verbundene Geräte zugreifen kann. Deshalb bieten alle industriellen WLAN-Access-Points von Hirschmann wie etwa die BAT-Familie eine Firewall-Funktionalität. Hierzu muss die Firewall direkt auf dem Access Point implementiert sein. Außerdem müssen diese Geräte rauen Umgebungsbedingungen standhalten, da sie direkt im Feld eingesetzt werden.

Sicherheit in anderen Netzwerkinfrastrukturen

Im Zuge von Defense-in-Depth ist es darüber hinaus sinnvoll, die Kommunikation auch an jedem anderen Punkt eines Netzwerks auf die gewünschten Kommunikationsmuster und -beziehungen zu begrenzen. Da Firewalls jedoch negative Auswirkungen auf die Übertragungslatenz (Kommunikationsverzögerung) und den Netzwerkdurchsatz haben können, ist der Einsatz einer dedizierten Firewall nicht in allen Teilen des Netzwerks möglich. In diesem Fall lässt sich der Schutz des internen Netzwerks über hochwertige Switches und Router mit leistungsfähigen zustandslosen Filterregeln, die im folgenden Abschnitt beschrieben werden, realisieren. Diese Regeln werden üblicherweise nicht als Firewall-Regeln, sondern als Access Control Lists (ACL) bezeichnet. ACLs bieten sich immer dann an, wenn innerhalb eines Netzwerks schnell gefiltert werden muss.

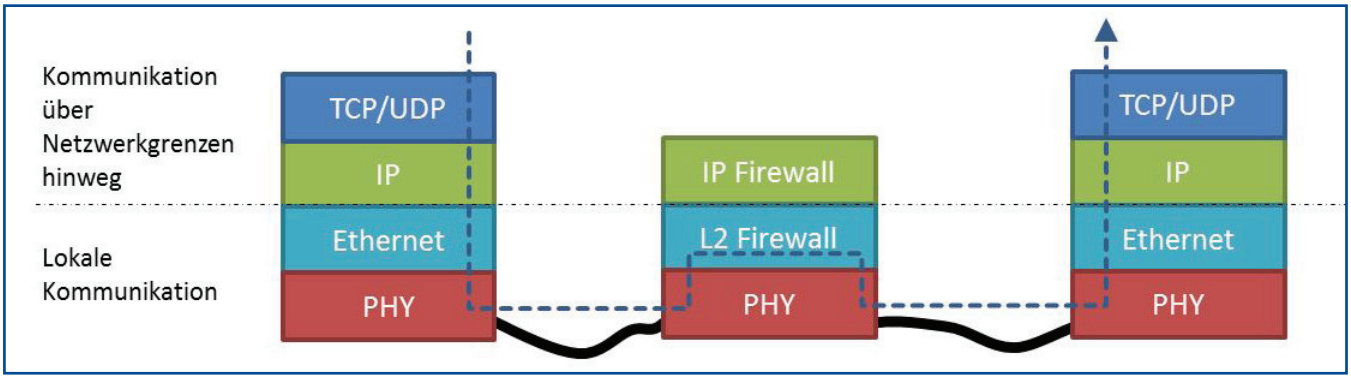


Abb. 3: Transparente Layer-2-Firewall

Unterschiede bei der Filterung

Die Umgebung und die Platzierung innerhalb des Netzwerks sind nicht die einzigen Faktoren, die die Anforderungen an eine Firewall bestimmen. Unterschiedliche Einsatzszenarien erfordern auch unterschiedliche Filtermechanismen. Deshalb ist es wichtig zu unterscheiden, wie tief eine Firewall die Kommunikation zwischen den jeweiligen Geräten überwachen kann. Entsprechende Lösungen sind in verschiedenen Ausführungen erhältlich. Das Spektrum reicht von Firewalls, die nur eine einfache Mustererkennung auf Paketen (sogenannte Signaturen) durchführen können, bis hin zu Firewalls, die auch die Funktionen und Verfahren industrieller Protokolle „verstehen" und so gezielt einzelne Kommunikationsmuster unterbinden können.

Die gleichzeitige Kombination unterschiedlicher Sicherheitsmerkmale wie etwa Firewall-Mechanismen kann bei der Umsetzung eines Defense-in-Depth-Konzepts für zusätzliche Sicherheit sorgen. Für ein solches Konzept diverser Abwehrmaßnahmen liefern wiederum die mittelalterlichen Baumeister die Inspiration: In Burgen und anderen Verteidigungsanlagen wurden oft hohe Mauern mit weiteren Vorkehrungen kombiniert, beispielsweise einem Wassergraben. Um beide Hindernisse zu überwinden, mussten die Angreifer eine wesentlich ausgefeiltere Strategie entwickeln.

Auch in modernen Kommunikations-netzwerken ist es sinnvoll, unterschiedliche Firewall-Mechanismen einzusetzen und diese in einem Defense-in-Depth-Konzept miteinander oder mit zusätzlichen Sicherheitsmechanismen zu kombinieren.

Die folgenden Filtermechanismen sind allgemein bekannt:

Stateless Firewalls

Kommunikationsbeziehungen zwischen Geräten können sich in verschiedenen Phasen bzw. Zuständen (States) befinden. Zum Beispiel wird in einer ersten Phase die Kommunikationsbeziehung aufgebaut. In einer zweiten Phase wird dann aktiv kommuniziert und in einer dritten Phase die Verbindung wieder beendet. Ein Protokoll, das dieses Verfahren einsetzt, ist etwa das Transmission Control Protocol (TCP), das oft zusammen mit dem Internet Protocol (IP) zu TCP/IP kombiniert wird.

Stateless (zutandslose) Firewalls[3] können, wie der Name schon ausdrückt, weder auf den Zustand einer Kommunikationsverbindung reagieren noch die verschiedenen Phasen unterscheiden. Deshalb lässt sich mit stateless Firewalls nur festgelegen, welche Geräte oder Anwendungen miteinander kommunizieren dürfen, jedoch nicht überwachen, ob die Teilnehmer gemäß der normalen Verfahren miteinander kommunizieren. Insbesondere können solche Firewalls keine Angriffe, die aus einem ungewöhnlichen Protokollverhalten resultieren, erkennen und verhindern. Dadurch sind besonders verwundbare Industriegeräte mit minimalem eigenen Schutz beispielsweise der Gefahr sogenannter Denial-of-Service-Attacken ausgesetzt, bei denen die Kommunikationsschnittstelle dieser Geräte vorsätzlich mit Datenverkehr geflutet und mit falschen oder fehlerhaften Kommunikationsanforderungen überlastet wird.

Stateful Firewalls

Im Gegensatz zu Stateless Firewalls können Stateful (zustandsbezogene) Firewalls den Kommunikationsverlauf der Teilnehmer überwachen und die gespeicherten Informationen, etwa zum Aufbau und der Beendigung der Verbindung, als Grundlage für die Paketfilterung verwenden. So lassen sich auch Angriffe, die über bereits bestehende Verbindungen versucht werden, erkennen und verhindern. Ebenso können Angriffe unterbunden werden, die bewusst einen fehlerhaften Verbindungsaufbau verwenden, um Systeme zu überlasten.

Deep Packet Inspection

Deep Packet Inspection ist eine Erweiterung der Stateful Packet Inspection. Stateful Firewalls untersuchen normalerweise nur den am Anfang eines Pakets stehenden Header, da dieser alle Informationen enthält, die die Firewall braucht, um den Kommunikationszustand wie etwa die Sequenznummern und die Kommunikations-Flags des TCP zu ermitteln und zu überwachen. Deep Packet Inspection geht einen Schritt weiter und ermöglicht es, über den Header hinaus auch die Nutzlast (z. B. der Steuerungsprotokolle von Industrieanwendungen) eines Pakets zu untersuchen. So können auch hoch spezialisierte Angriffsmuster, die tief in den Kommunikationsströmen versteckt sind, entdeckt werden.

Um ein „gutes" Paket von einem bösartigen Paket bzw. bösartiger Nutzlast unterscheiden zu können, muss die Firewall allerdings das jeweilige Kommunikationsprotokoll „verstehen". Deshalb werden Deep Packet Inspection Firewalls oft als zusätzliche Komponenten einer Stateful Packet Inspection Firewall eingesetzt, und zwar nur für bestimmte Protokolle und Einsatzszenarien - etwa Industrieprotokolle.

Eine Deep Packet Inspection Firewall bietet durch einen oft sehr individuell und fein abgestuften konfigurierbaren Regelsatz ein hohes Maß an Sicherheit, erfordert aber mehr Rechenleistung. Außerdem muss eine spezielle Konfigurationsschnittstelle vorhanden sein, um die Firewall-Regeln festzulegen. Leistungsfähige Produkte verfügen jedoch über integrierte Tools, mit denen sich dieser Prozess einfach und schnell durchführen lässt.

Da sie nicht nur für die Kommunikations-beziehungen zwischen Geräten einen fein abgestuften Schutz bieten, sondern auch Steuerungsprotokolle "verstehen" und nur bestimmte Kommunikationsarten zulassen, sind Deep Packet Inspection Firewalls ideal geeignet, um die Leitungen zwischen verschiedenen industriellen Zonen zu sichern. Wenn diese Firewalls an bestimmten Punkten innerhalb des Netzwerks gezielt eingesetzt werden, lässt sich die industrielle Kommunikation deutlich besser schützen.

Manchmal wird der Begriff Deep Paket Inspection auch für einen sehr speziellen Sicherheitsmechanismus verwendet, der eher für den Einsatz einer Signaturdatenbank implementiert wurde als zur vollständigen Dekodierung des Anwendungsprotokolls. Signaturdaten bieten eine völlig andere Art des Schutzes. Sie überprüfen die Bits eines Pakets mit zahlreichen Signaturen, um eine Reihe zuvor identifizierter Schwachstellen zu identifizieren und zu blockieren. Dadurch helfen Signaturdaten zwar gegen bekannte Schwachstellen, bieten aber weder einen umfassenden Schutz vor bösartigen Paketen auf der DPI-Protokollschicht noch ermöglichen sie es, den Nachrichtenfluss so zu konfigurieren, dass nur noch für den Betrieb der jeweiligen Anlagen plausible Nachrichten erlaubt sind.

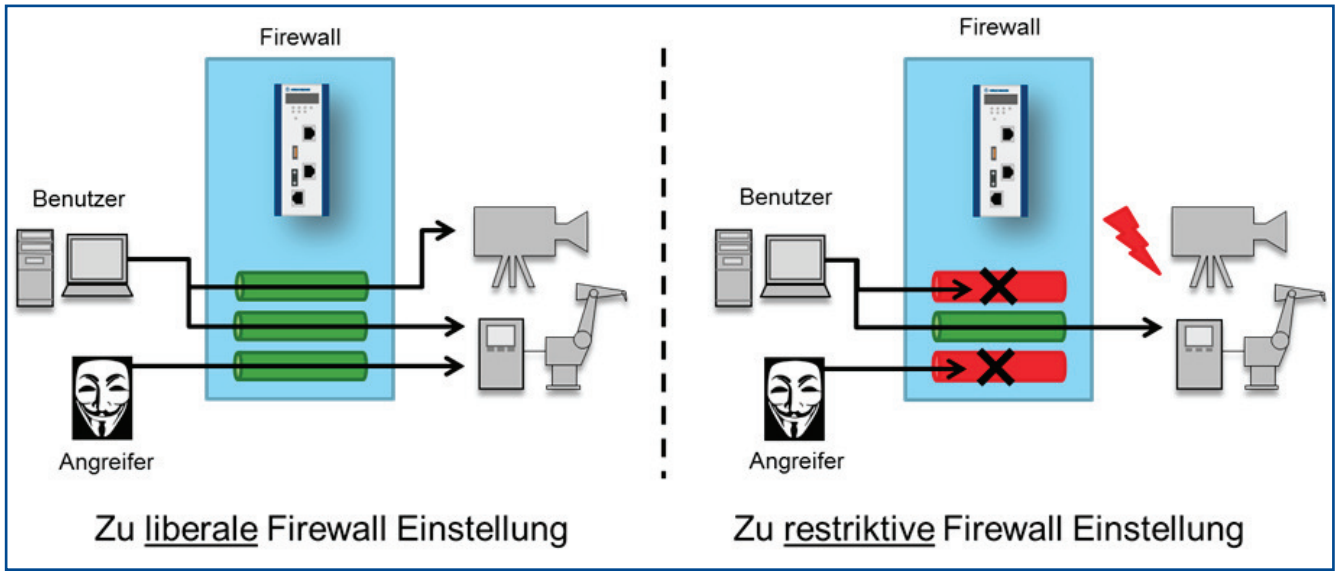


Abb. 4: Die Integration einer Firewall in ein bestehendes Industrienetzwerk kann zu Regeln führen. die zu tolerant oder zu restriktiv konfiguriert sind.

Management von Firewalls

Genauso wie es beim Anwendungsgebiet und der Leistungsfähigkeit des Paketfilters Unterschiede gibt, gibt es auch Unterschiede bei den weiteren Funktionen einer Firewall. So kann der Bedienungskomfort darüber entscheiden, ob eine Firewall eine praktikable Lösung bietet oder eher ein Hindernis für die Umsetzung einer Sicherheitsstrategie darstellt. Das lässt sich an zwei typischen Managementaufgaben verdeutlichen: a) der Einbindung einer neuen Firewall in ein bestehendes Industrienetzwerk und b) der Verwaltung mehrerer Firewalls mit Netzwerkmanagement-Tools.

Lernende Firewalls

Die Einbindung einer neuen Firewall in ein bestehendes Industrienetzwerk kann sich schwierig gestalten, denn in der Regel gibt es eine Vielzahl von Kommunikationsbeziehungen, die nur in den seltensten Fällen komplett und korrekt erfasst und dokumentiert sind. Da die Hauptfunktion einer Firewall darin besteht, unbekannten Netzwerkverkehr zu unterbinden, ist die anfängliche Konfiguration besonders schwierig und für den sicheren Betrieb einer Anlage entscheidend. Wird die Firewall zu tolerant konfiguriert, kann der Steuerungs- und Überwachungsverkehr der Anlage zwar problemlos passieren, jedoch stellt sie dann weder ein großes Hindernis für Angreifer dar noch bietet sie Schutz vor sich falsch verhaltenden Geräten oder Schadware.

Wird die Firewall dagegen zu restriktiv konfiguriert, blockiert sie zwar die Kommunikation eines Angreifers, behindert jedoch auch den regulären Verkehr der Anlage, so dass diese nicht mehr in allen Situationen fehlerfrei funktioniert, was zu Standzeiten und erhöhten Wartungskosten führen kann.

Um nur den gewünschten Verkehr zuzulassen und zugleich den nicht gewünschten zu unterbinden, muss die Firewall korrekt konfiguriert werden. Ohne eine komplette Sicht auf alle Kommunikationsbeziehungen wird die Integration einer Firewall in ein bestehendes Netzwerk daher zu einer Zitterpartie (siehe Abb. 4).

Deshalb unterstützen hochwertige industrielle Firewalls das Personal bei der Inbetriebnahme mit speziellen Analysemodi. Durch diese Modi (z. B. Firewall Learning Mode oder Test Mode) kann die Firewall die Kommunikationsbeziehungen in einem Netzwerk während einer Lernphase analysieren. In dieser Phase zeichnet sie alle Kommunikationsbeziehungen auf, ohne eine von ihnen zu beschränken. Anhand der analysierten Verbindungen kann ein Administrator schnell und einfach die gewünschten bzw. unerwünschten Kommunikationsbeziehungen erkennen und die Firewall (semi-)automatisch exakt konfigurieren. Das spart Zeit und ermöglicht es, eine funktionierende und sichere Konfiguration zu finden, ohne Ausfälle und Fehlfunktionen zu riskieren. Die Dauer der Lernphase sollte allerdings frei wählbar sein, da die Firewall in dieser Zeit alle Kommunikationsbeziehungen registrieren muss. Insbesondere bei sporadischen Vorgängen wie etwa regelmäßigen Wartungen sollte eine angemessene Dauer gewählt werden.

Management mehrerer Firewalls

Der Einsatz mehrere Firewalls zur Isolierung verschiedener Maschinen und Anlagenteile ist ein wichtiger Aspekt der Defense-in-Depth-Strategie. Denn wenn ein Angreifer die erste Hürde genommen hat und in ein Netzwerk eingedrungen ist, können zusätzliche Firewalls mit spezifischeren Regeln verhindern, dass er in weitere und sensitivere Bereiche vordringt.

Der Einsatz von IP-Firewalls und transparenten Layer-2 Firewalls bedingt jedoch, dass mehrere Geräte konfiguriert und verwaltet werden müssen. Ohne ein leistungsfähiges Management-Tool zur einfachen (Massen-)Konfiguration von Firewalls kann dies bei Änderungen der Netzwerkinfrastruktur jedoch sehr aufwändig sein. Deshalb ist es wichtig, dass sich die Firewalls zentral verwalten und überwachen lassen.

Mit effektiven Management-Tools (z. B. Industrial HiVision) können Standardkonfigurationen schnell auf neu installierten Firewalls implementiert und massenhafte Konfigurationsänderungen auch entsprechend den Änderungen der Netzwerkinfrastruktur durchgeführt werden. Ein Beispiel für Letzteres kann ein neuer Logserver sein, der für alle Geräte im Produktionsnetzwerk erreichbar sein soll. Müssen alle Firewalls einzeln konfiguriert werden, so müssen auch die IP-Adresse und der Port des Logservers auf ihnen einzeln gesetzt werden, was zeitaufwändig und fehleranfällig ist. Durch Massenkonfiguration mittels eines Netzwerkmanagement-Tools kann diese Aufgabe für alle Firewalls zuverlässig und gleichzeitig durchgeführt werden.

Verfügbarkeit der vorgestellten Technologien

Belden bietet mit seinen Marken Hirschmann, Tofino Security und GarrettCom Produkte für umfassende Firewall-Lösungen. Die Vielfältigkeit dieser Lösungen verdeutlicht Tabelle 1. Je nach Anwendungsszenario verfügen die Firewalls über unterschiedliche Eigenschaften.

Die EAGLE20/30-Firewall-Familie verfügt sowohl über eine Stateful IP Firewall und hardwarebeschleunigte ACL-Filter-Regeln als auch einen Industrieprotokoll-spezifischen DPI-Filter für Deep Packet Inspection. Die EAGLE-One-Geräte sind transparente Layer-2-Firewalls für den Einsatz innerhalb eines lokalen Netzwerks. Beide EAGLE-Produkte besitzen einen Firewall Learning Mode, um Regeln aus dem beobachteten Netzwerkverkehr abzuleiten. Tofino DPI ist eine transparente Layer-2-Firewall mit einem auf industrielle Anwendungen zugeschnittenen Benutzer-Interface sowie umfangreichen Möglichkeiten für die Deep Packet Inspection verschiedener gängiger Industrie-Protokolle. Die sicheren Router Magnum 5RX und 10 RX von GarrettCom bieten eine integrierte Stateful Firewall sowie VPN-Sicherheit (Virtual Private Network). Die WLAN-Access-Points von Hirschmann haben eine integrierte Stateful-Layer-2- und IP-Firewall. Viele Belden-Produkte mit Firewall lassen sich mit der Management-Software Industrial HiVision einfach überwachen und konfigurieren. Zahlreiche Hirschmann-Switches bieten darüber hinaus die Möglichkeit, hoch leistungsfähige ACL-Filterregeln zu konfigurieren, um das Netzwerk durchgängig gegen Angreifer zu schützen.

Zusammenfassung

Auch wenn moderne Sicherheitskonzepte weit mehr beinhalten als Firewalls, sind diese immer noch ein zentrales Element, ohne die kein Sicherheitskonzept auskommen kann. Denn für die Umsetzung wichtiger Grundsätze internationaler Standards und Best Practices (bewährter Vorgehensweisen) wie Defense-in-Depth und Zones und Conduits sind Firewalls unverzichtbar.

Firewalls bestehen jedoch nicht aus einem einzigen Gerätetyp, sondern einer Reihe von Geräten mit unterschiedlichen technischen Eigenschaften, Hardware-Funktionen und Ausstattungsmerkmalen sowie gesetzlichen Bestimmungen und industriellen Zulassungen für die jeweiligen Umgebungen und Anwendungen, in denen sie eingesetzt werden können und für die sie optimal geeignet sind.

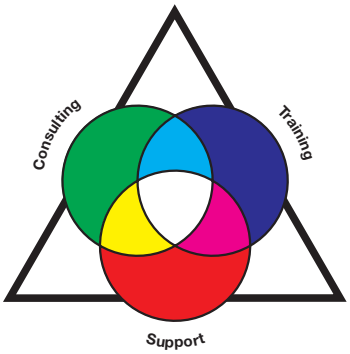
Deshalb kommt der Wahl der richtigen Firewall für die unterschiedlichen Aufgaben in einem industriellen Netzwerk zentrale Bedeutung zu. Um die Effektivität von Firewalls zu erhöhen, müssen Netzwerkarchitekturen den Regeln, die mit den Best Pratices von Zones und Conduits sowie Defense-in-Depth verbunden sind, folgen. Durch die Kombination unterschiedlicher Firewall-Funktionen in eine Gesamtstrategie zum Schutz des Netzwerks und die Positionierung verschiedener Firewall-Arten an den Punkten, wo sie ihre Stärken ausspielen können, ist es möglich, Netzwerke zu realisieren, die auch für künftige Anwendungen größtmögliche Sicherheit gewährleisten.

	Transparente Layer-2-Firewall	Transparente Layer-2-DPI-Firewall	Stateful Layer-3-Firewall	WLAN Access Point mit Firewall	Router mit Firewall
Produktbeispiel	EAGLE One	Tofino Xenon	EAGLE 20/30	OpenBAT	Magnum 10RX Magnum 5RX
Anwendung	Netzwerkgrenze/ internes Netzwerk/ Feldebene	Internes Netzwerk/ Feldebene	Netzwerkgrenze/ internes Netzwerk/ Feldebene	Netzwerkgrenze/ internes Netzwerk/ Feldebene/ WLAN-Schutz	Edge- (5RX) oder Core-Router (10RX)
Produktmerkmale (Auszug)					
Access Control Lists	MAC	MAC	MAC/IP/ TCP/UDP	MAC/IP/ TCP/UDP	MAC/IP/ TCP/UDP
Layer-2-Firewall	✔	✔	-	✔	-
Layer-3-Firewall	✔	-	✔	✔	✔
Deep Packet Inspection	-	Modbus, OPC, Ethernet/IP, DNP3, IEC 60870-5-104	Modbus, OPC	-	-
NAT	✔	-	✔	✔	✔
VPN	✔	-	✔	✔	✔
Router/Router-Redundanz	✔/✔	-	✔/✔	✔/✔	✔/✔
WAN- & WWAN-Schnittstellen	-	-	SHDSL/3G, LTE	3G, LTE (auch IP67-Version)	T1/E1
Ports	2 FE	2 FE	4 FE, 2 GE	2 GE, 2 WLAN	Konfigurierbar mit bis zu 10 GE-Ports (Kupfer oder SFP), 16 T1/E1-Ports oder 32 seriellen Ports.
Firewall Learning/Test Mode	✔	✔	✔	-	-
Konfigurierbar via Industrial HiVision	✔	-	✔	✔	Spezielle Funktionen

Tabelle 1: Vielfältige Firewall-Lösungen

Referenzen

1. National Institute of Standards and Technology NIST, Guide to Industrial Control Systems (ICS) Security, 2011
2. National Institute of Standards and Technology NIST, Guidelines on Firewalls and Firewall Policy, Revision 1, 2009
3. Belden Blog "Cyber Security for Industrial Applications: Defense-in-Depth", http://www.belden.com/blog/industrialethernet/Cyber-Security-for-Industrial-Applications-Defense-in-Depth.cfm



Belden Competence Center

Die zunehmende Komplexität von Kommunikations- und Vernetzungslösungen erhöht auch die Anforderungen in Bezug auf Planung, Implementierung und Wartung dieser Lösungen. Für Nutzer ist es daher entscheidend, auf aktuelles Fachwissen zugreifen zu können. Als verlässlicher Partner für Komplettlösungen bietet Belden unter dem Dach seines „Belden Competence Center" kompetente Beratung, Konzeption, technische Unterstützung sowie Technologie- und Produktschulungsprogramme aus einer Hand. Darüber hinaus bietet Ihnen Belden mit dem weltweit ersten Zertifizierungsprogramm für Industrienetzwerke die passende Qualifikation für jedes Fachgebiet. Aktuelles Herstellerwissen, ein internationales Netzwerk sowie der Zugang zu externen Spezialisten garantieren Ihnen die bestmögliche Unterstützung für Ihre Produkte. Egal, welche Technologie Sie nutzen: Sie können sich auf unsere umfassende Unterstützung verlassen – von der Implementierung bis zur Optimierung jedes einzelnen Aspekts Ihrer täglichen Abläufe.

Über Belden

Belden Inc., ein weltweit führender Anbieter von hochwertigen Signalübertragungslösungen, bietet ein umfassendes Produktportfolio, das auf die Anforderungen unternehmenskritischer Netzwerkinfrastrukturen in den Branchen Industrie- und Gebäudeautomation sowie Broadcast zugeschnitten ist. Mit innovativen Lösungen für die zuverlässige und sichere Übertragung stetig wachsender Datenmengen für Audio- und Videoinformationen, die für moderne Anwendungen benötigt werden, übernimmt Belden eine Schlüsselrolle bei der globalen Veränderung hin zu einer vernetzten Welt. Das Unternehmen mit Hauptsitz in St. Louis, USA, wurde 1902 gegründet und betreibt Fertigungsstätten in Nord- und Südamerika, Europa und Asien.

Für weitere Informationen besuchen Sie uns unter www.belden.com und folgen Sie uns auf: Twitter @BeldenIND.

Telefon: **+49 (0) 7127 /14-1809** **www.beldensolutions.com/hirschmann**