(19) Deutsches Patent- und Markenamt

(10) **DE 10 2012 109 212 B4** 2023.02.09

(12) # Patentschrift

(21) Aktenzeichen: **10 2012 109 212.5**
(22) Anmeldetag: **28.09.2012**
(43) Offenlegungstag: **28.03.2013**
(45) Veröffentlichungstag der Patenterteilung: **09.02.2023**

(51) Int Cl.: ***H04L 43/00*** (2022.01)
H04L 65/00 (2022.01)
H04L 67/00 (2022.01)
H04L 69/00 (2022.01)
H04L 9/40 (2022.01)

(30) Unionspriorität:
61/540,219 **28.09.2011** **US**

(73) Patentinhaber:
Fisher-Rosemount Systems, Inc., Round Rock, Tex., US

(74) Vertreter:
Meissner Bolte Patentanwälte Rechtsanwälte Partnerschaft mbB, 80538 München, DE

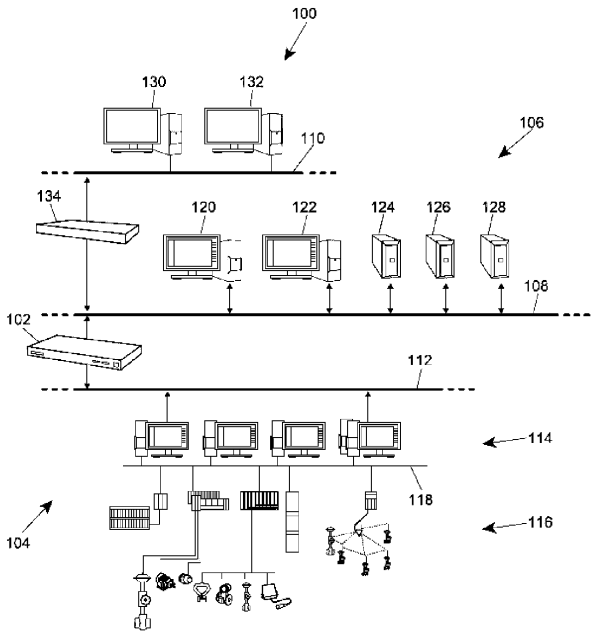
(72) Erfinder:
Huba, Robert Kent, Georgetown, Tex., US; Schleiss, Duncan, Austin, Tex., US; Law, Gary, Georgetown, Tex., US

(56) Ermittelter Stand der Technik:

DE	**10 2006 056 566**	**B3**
US	**2003 / 0 028 806**	**A1**
US	**2009 / 0 254 985**	**A1**

(54) Bezeichnung: **Methoden, Vorrichtung und Herstellungsprodukte zur Bereitstellung von Firewalls für Prozesssteuerungssysteme**

(57) Hauptanspruch: Ein Verfahren, das Folgendes umfasst:
Analysierung einer Netzkommunikation zur Ermittlung eines ersten Diensts, einer Adresse in Verbindung mit dem ersten Dienst innerhalb eines gesicherten Teils eines Netzwerks und einer Untermenge von Ports, die von dem ersten Dienst verwendet wird, wobei die Netzkommunikation aus dem gesicherten Teil des Netzwerks stammt und an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks übertragen werden soll; und
Speicherung eines Identifikators des ersten Diensts, der Adresse, und der Untermenge von Ports, wenn die Netzkommunikation den Identifikator, die Adresse, und eine Untermenge von Ports umfasst.



Beschreibung

BEREICH DER OFFENLEGUNG

[0001] Die vorliegende Offenlegung bezieht sich im Allgemeinen auf Prozesssteuerungssysteme und insbesondere auf Methoden, Vorrichtungen und Herstellungsprodukte zur Bereitstellung von Firewalls für Prozesssteuerungssysteme.

HINTERGRUND

[0002] Prozesssteuerungssysteme, wie sie beispielsweise in chemischen, Öl- oder sonstigen Verfahren eingesetzt werden, umfassen typischerweise eine oder mehr Process Controller und Eingabe-/Ausgabe-Vorrichtungen (E/A), die datentechnisch mit mindestens einem Host oder einer Bediener-Arbeitsstation und an ein oder mehr Feldvorrichtungen per analogen, digitalen oder analog-digitalen Datenlbussen verbunden sind. Die Feldvorrichtungen, die beispielsweise Ventile, Ventilpositionierer, Schalter und Transmitter (z.B. Temperatur-Druck- und Durchflusssensoren) sein können, führen Prozesssteuerungsfunktionen im Rahmen des Verfahrens aus, wie beispielsweise die Öffnung oder Schließung von Ventilen, und ein Messen der Prozesssteuerungsparameter. Dabei empfangen die Process Controller Signale, welche die von den Feldvorrichtungen vorgenommenen Prozess-Messungen erkennen lassen. Sie verarbeiten diese Informationen zur Ausführung einer Steuerroutine und zur Erzeugung von Steuersignalen, die über Datenbusse oder sonstige Verbindungen an die Feldvorrichtungen zur Steuerung des Arbeitsablaufs des Prozesses geschickt werden. Auf diese Art und Weise können die Process Controller die Steuerungsstrategien über die Datenbusse und/oder sonstige Verbindungen ausführen und koordinieren und somit die Feldvorrichtungen datentechnisch verbinden.

[0003] Die von den Feldvorrichtungen und den Controllern stammenden Prozessinformationen können für eine oder mehrere Anwendungen verfügbar gemacht werden (z.B., Software-Routinen, Programme, usw.), welche von der Bediener-Arbeitsstation ausgeführt werden (z.B. ein prozessor-basiertes System), um einem Bediener die Ausführung der gewünschten Funktionen in Bezug auf das Verfahren zu ermöglichen, wie beispielsweise das Ansehen des laufenden Prozesszustands (z.B. über eine grafische Benutzeroberfläche), eine Bewertung des Prozesses, eine Änderung des Arbeitsablaufs des Prozesses (z.B. über ein visuelles Objektdiagramm), usw. Viele Prozesssteuerungssysteme umfassen auch eine oder mehrere Anwendungsstationen. Diese Anwendungsstationen werden typischerweise mit Hilfe eines Personalcomputers, einer Arbeitsstation, o.ä. umgesetzt, die datentechnisch mit den Controllern, Bediener-Arbeitsstationen und sonstigen Systemen innerhalb des Prozesssteuerungssystems über ein lokales Datennetz (LAN) verbunden sind. Jede Anwendungsstation kann eine grafische Benutzerschnittstelle umfassen, die die Prozesssteuerungsinformationen samt der Werte der Prozessvariablen, der Werte der mit dem Prozess verbundenen Qualitätsparameter, die Prozessfehlererkennungsangaben und/oder Prozessstatusinformationen anzeigen.

[0004] Aus der DE 10 2006 056 566 B3 ist ein Industrienetzwerk sowie ein Verfahren zum Aufbau einer Datenverbindung mit einem mobilen Endgerät, insbesondere zum Bereitstellen eines Servicezugangs in einem Industrienetzwerk, bekannt. In dem Verfahren wird das mobile Endgerät bei einer Registrierungseinheit für einen bestimmten Zeitraum registriert, wenn das mobile Endgerät an einen nicht frei zugänglichen Netzwerk-Registrierungspunkt angeschlossen wird. Dabei werden nach der Registrierung Parameter an das mobile Endgerät übertragen, die Zertifikate für den Zugriff auf Ressourcen des Industrienetzwerkes, Datenblätter eingesetzter Geräte und Diagnosedaten aufweisen. Anschließend wird eine Datenverbindung zwischen dem mobilen Endgerät und dem Industrienetzwerk aufgebaut, wenn das mobile Endgerät innerhalb des bestimmten Zeitraumes bei einem frei zugänglichen Netzwerk-Zugangspunkt angeschlossen wird und bei der Registrierungseinheit registriert ist.

[0005] Die US 2009 / 0 254 985 A1 zeigt eine Schnittstellenvorrichtung für eine geschützte Arbeitsstation oder einen geschützten Host. Die Schnittstellenvorrichtung weist eine Netzwerkschnittstelle auf, die so konfiguriert ist, dass sie mit einem Netzwerk verbunden werden kann, in dem Daten zwischen einer Anzahl von Hosts ausgetauscht werden. Dabei weist die Netzwerkschnittstelle eine erste Netzwerkadresse auf, die einem Guard-Steuerport der Schnittstelle entspricht, und eine zweite Netzwerkadresse, die einem Guard-Datenport entspricht.

[0006] Ferner weist die Schnittstellenvorrichtung einen Transport-Guard auf, der Daten, welche an die zweite Netzwerkadresse adressiert sind, vom Guard-Datenport der Netzwerkschnittstelle an eine Hostschnittstelle des Transport-Guards weiterleitet. Ferner leitet der Transport-Guard ausgehende Daten an der Hostschnittstelle an den Guard-Datenport der Netzwerkschnittstelle weiter, entsprechend einer Sicherheitskonfiguration, die von einer Steuerkomponente des Transport-Guards ausgegebenen wird.

[0007] Aus der US 2003 / 0 028 806 A1 ist ein Verfahren und eine Firewall zur Sicherung einer Kommunikationssitzung über ein Paketdatennetzwerk bekannt. Das Verfahren umfasst die folgenden Schritte: Empfangen eines Signals, das eine einem

ersten Endgerät zugeordnete Portnummer enthält; Empfangen von Datenpaketen von einem zweiten Endgerät zur Übertragung an das erste Endgerät; und Übertragen der Datenpakete an das erste Endgerät, wobei die Datenpakete die dem ersten Endgerät zugeordnete Portnummer identifizieren.

ZUSAMMENFASSUNG

[0008] Es werden Methoden, Vorrichtungen und Herstellungsprodukte zur Bereitstellung von Firewalls für Prozesssteuerungssysteme offengelegt. Die Methoden umfassen zum Beispiel die Analyse einer Netzkommunikation zur Ermittlung eines ersten Diensts, einer Adresse, die mit dem ersten Dienst innerhalb eines gesichterten Teils eines Netzwerk verbunden ist, und einem Untermenge von Ports, die von dem ersten Dienst verwendet werden, wobei die Netzkommunikation aus dem gesichterten Teil des Netzwerks stammt und auf eine Zieladresse übertragen werden soll, die sich außerhalb des geschützten Teils des Netzwerks befindet, und wobei ein Identifikator des ersten Diensts, die Adresse und die Untermenge der Ports gespeichert wird, wenn die Netzkommunikation den Identifikator, die Adresse und die Untermenge der Ports enthält.

[0009] In bestimmten beispielhaften Methoden wird weiterhin eine zweite von außerhalb des gesicherten Teils des Netzwerks empfangene Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und der Untermenge der Ports verglichen. Gewisse dieser beispielhaften Methoden umfassen die Weiterleitung der zweiten Netzkommunikation an eine Adresse und einen Port, der von der zweiten Netzkommunikation angegeben wurde, wenn die zweite Netzkommunikation mit dem Identifikator des ersten Dienstes, der Adresse und einem Port in der Untermenge der Ports übereinstimmt.

[0010] Einige Beispiele umfassen weiterhin die Weiterleitung der zweiten Netzkommunikation an eine Adresse und einen Port, der von der zweiten Netzkommunikation angegeben wurde, wenn die zweite Netzkommunikation mit der Adresse und einem Port in der Untermenge der Ports und nicht mitdem Identifikator übereinstimmt, wobei sich auf mindestens eine der Schwellwertzeiten für die erste Netzkommunikation oder ein Ping-Flag gestützt wird. Dieserart beispielhafte Methoden umfassen weiterhin die Einstellung des Ping-Flag auf der Grundlage der ersten Netzkommunikation.

[0011] Gewisse beispielhafte Methoden umfassen weiterhin das Löschen der zweiten Netzkommunikation, wenn die zweite Netzkommunikation nicht mit einer gespeicherten Adresse und einem gespeicherten, dem ersten Dienst entsprechenden Port übereinstimmt. Bestimmte Beispiele umfassen das Löschen des Identifikators des ersten Diensts, der Adresse und der Untermenge der Ports von einer Ablage auf der Grundlage der Schwellwertzeit.

[0012] Eine Beispielvorrichtung umfasst einen Kommunikationsfilter zur Analyse einer Netzkommunikation, die aus einem gesicherten Teil eines Netzwerks stammt und die an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks übertragen werden soll, einen Kommunikationsanalysator zur Ermittlung des ersten Diensts, eine Adresse, die mit dem ersten Dienst innerhalb des gesicherten Teils des Netzwerks und zur Ermittlung einer von dem ersten Dienst verwendeten Untermenge von Ports verbunden ist, und einen Firewall-Ausnahmeerzeuger zur Speicherung eines Identifikators des ersten Diensts, der Adresse und des Untermenge von Ports, wenn die Netzkommunikation den Identifikator, die Adresse und den Untermenge von Ports umfasst.

[0013] In gewissen Beispielen vergleicht der Kommunikationsfilter eine zweite von außerhalb des gesicherten Teils des Netzwerks empfangenen Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und der Untermenge der Ports. In mehreren dieser Beispiele leitet der Kommunikationsfilter die zweite Netzkommunikation an eine Adresse und einen Port weiter, die von der zweiten Netzkommunikation vorgegeben werden, wenn die zweite Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und einem Port in der Untermenge der Ports übereinstimmt.

[0014] In gewissen Beispielen leitet der Kommunikationsfileter die zweite Netzkommunikation an eine Adresse und einen Port weiter, der von der zweiten Netzkommunikation vorgegeben wurde, wenn die zweite Netzkommunikation mit der Adresse und einem Port in der Untermenge der Ports und nicht mit dem Identifikator übereinstimmt, wobei sich auf mindestens eine der Schwellwertzeiten für die erste Netzkommunikation oder ein Ping-Flag gestützt wird. In bestimmten Beispielvorrichtungen ermittelt der Kommunikationsanalysator einen Wert für das Ping-Flag auf der Grundlage der ersten Netzkommunikation, und der Firewall-Ausnahmeerzeuger muss den Wert des Ping-Flag auf der Grundlage der ersten Netzkommunikation abspeichern.

[0015] In gewissen Beispielen umfasst mindestens die erste oder zweite Netzkommunikation eine verteilte Objektmodellkommunikation für Komponenten. Bestimmte Beispielvorrichtungen umfassen weiterhin eine Speicherungsvorrichtung, einen Firewall-Ausnahmeerzeuger zur Speicherung des Identifikators, der Adresse und einer Untermenge an Ports in der Speicherungsvorrichtung.

[0016] Ein beispielhaftes computerlesbares Speicherungsmedium umfasst computerlesbare Anweisungen, welche nach der Bearbeitung durch einen

Prozessor bewirken, dass der Prozessor eine Netzkommunikation zur Ermittlung eines ersten Diensts, einer Adresse, die mit dem ersten Service innerhalb eines gesicherten Teils eines Netzwerks verbunden ist, und einer von dem ersten Dienst verwendeten Untermenge von Ports analysiert, wobei die Netzkommunikation aus dem gesicherten Teil des Netzwerks stammt und auf eine Zieladresse außerhalb des Netzwerks übertragen und ein Identifikator des ersten Diensts, die Adresse und die Untermenge der Ports gespeichert werden soll, wenn die Netzkommunikation einen Identifikator, die Adresse und die Untermenge der Ports umfasst.

Figurenliste

Fig. 1 zeigt eine Prozesssteuerungsumgebung samt einer beispielhaften Firewall an.

Fig. 2 zeigt eine grafische Beispielbenutzerschnittstelle an, die zur Konfiguration der beispielhaften Firewall von **Fig. 1** benutzt werden kann.

Fig. 3 und **Fig. 4** veranschaulichen jeweils eine schematische Ansicht und ein Ablaufdiagramm für eine beispielhafte Art und Weise oder einen Beispielprozess, in dem DCOM-Kommunikationen von der beispielhaften Firewall von **Fig. 1** bearbeitet werden können.

Fig. 5 ist ein ausführlichereres Blockdiagramm der beispielhaften Firewall von **Fig. 1**.

Fig. 6 ist ein Ablaufdiagramm, das eine Beispielmethode zur Ausführung der Firewall von **Fig. 1** und **Fig. 5** zur dynamischen Erstellung einer Ausnahme für einen Dienst darstellt.

Fig. 7 ist ein Ablaufdiagramm, das eine Beispielmethode zur Ausführung der Firewall von **Fig. 1** und **Fig. 5** darstellt, um Kommunikationen wahlweise für einen Dienst zu gestatten, der zu einem gesichterten Teil eines Netzwerks geführt werden soll.

Fig. 8 ist ein Ablaufdiagramm, dass eine Beispielmethode zur Ausführung der Firewall von **Fig. 1** und **Fig. 5** zur Verwaltung dynamischer Ausnahmen für Dienste darstellt.

Fig. 9 ist ein Blockdiagramm einer beispielhaften Abwicklungsplattform, die die Anweisungen von **Fig. 4** und **Fig. 6** - **Fig. 8** zur Ausführung der Firewall von **Fig. 1** und/oder 5 ausführen kann.

AUSFÜHRLICHE BESCHREIBUNG

[0017] Obwohl im Folgenden beispielhafte Methoden, Vorrichtungen und Herstellungsprodukte beschrieben werden, die unter anderen Komponenten Software und/oder Firmware umfassen, die auf Hardware ausgeführt werden, sollte man beachten, dass diese Beispiele nur der Veranschaulichung dienen und nicht als einschränkend angesehen werden dürfen. So wird beispielsweise in Erwägung gezogen, dass die Hardware-, Software- und Firmwarekomponenten gänzlich oder teilweise in der Hardware oder ausschließlich in der Software oder in beliebigen Kominationen aus Hardware und Software enthalten sind. Während im Folgenden beispielhafte Methoden, Vorrichtungen und Herstellungsprodukte beschrieben werden, werden Personen mit durchschnittlichen Kenntnissen also ohne Weiteres zu schätzen wissen, dass die gelieferten Beispiele nicht die einzige Art und Weise zur Umsetzung dieser Methoden, Vorrichtungen und Herstellungsprodukte darstellen.

[0018] Firewalls werden gemeinhin zur Gewährleistung der Sicherheit für Kommunikationsnetzwerke eingesetzt. Sie können zur Verhinderung eines unbefugten Zugriffs auf ein Kommunikationsnetzwerk von aus einem anderen Netzwerk und/oder einer anderen Vorrichtung stammenden Kommunikationen verwendet werden. Typischerweise befindet sich eine Firewall physisch oder logisch in einer Stelle, die das zu schützende Netzwerk oder ein Netzwerk mit einer relativ hohen Sicherheitsstufe mit einem anderen Netzwerk mit einer relativ niedrigen Sicherheitsstufe verbindet. Bestimmte Systeme oder Netzwerke haben mehrere Sicherheitsstufen und können daher mehrere Firewalls und/oder sonstige Sicherheitsvorrichtungen umfassen. Üblicherweise können die mehrfachen Sicherheitsstufen in diesen komplexeren Systemen oder Netzwerken als verschiedene Schichten oder Zonen einer erhöhten Sicherheit angesehen werden. Während die Sicherheit für jede nachfolgende Schicht, Zone oder Stufe erhöht wird, nehmen die Einschränkungen, die damit in Zusammenhang stehen, welche Einheiten mit der nächsthöheren Sicherheitsschicht, Zone oder Stufe kommunizieren dürfen, zu, und die Anzahl der Einheiten, denen eine Kommunikation gestattet wird, nimmt üblicherweise ab.

[0019] Mehrzweckfirewalls, die üblicherweise in Unternehmensinformationstechnologie (IT) Netzwerken eingesetzt werden, sind äußerst komplexe Vorrichtungen und bedürfen einer signifikanten IT-Erfahrung für eine sachgemäße Installation, Konfiguration und Pflege. So verwenden diese Mehrzweckfirewalls zum Beispiel Kommunikationsregeln als eine Sicherheitsvorrichtung zur Bestimmung davon, welche Kommunikationen unbefugt sind, und aus diesem Grund blockiert werden müssen. Genauer gesagt wird jedes Kommunikationspaket, dass die Firewall durchdringen möchte (d.h., das versucht, sich von einer niedrigereren Sicherheitsstufe auf einer Seite der Firewall auf die höhere, von der Firewall geschützten Sicherheitsstufe zu begeben) angesichts der in der Firewall festgelegten Regeln abgefragt und bewertet. Alle Pakete, die diesen Regeln für Kommunikationspakete, denen ein Durchgang durch

die Firewall gestattet wird, nicht nachkommen, werden verworfen und blockiert.

[0020] Die von diesen Mehrzweckfirewalls eingesetzten Regeln werden für jede Anwendung, jeden Computer oder sonstige Vorrichtung, die auf Anwendungen, Computer und/oder Vorrichtungen auf der sicheren Seite der Firewall zugreifen sollen, empirisch entwickelt. Diese Regelentwicklung, die als ein Bestandteil des FirewallKonfigurationsvorgangs angesehen werden kann, kann von hochqualifiziertem IT-Personal und/oder anderen Menschen mit maßgeblichen Erfahrungen im Bereich Networking und Datenanalyse ausgeführt werden. Der Regelentwicklungsvorgang umfasst häufig die Überwachung des Kommunikationsverkehrs in einem unbeschränkten Betriebsmodus zur Festlegung der Charakteristika jeder autorisierten Kommunikation und die darauffolgende Erstellung entsprechender Regeln für den Gebrauch seitens der Firewall, welche dazu führen, dass nur diese autorisierten Kommunikationen durch die Firewall gehen dürfen. Allgemeiner ausgedrückt, versucht der Entwicklungsvorgang für Regeln einen Fingerabdruck eines authentifizierenden Merkmals zu erhalten oder diesen zu entwickeln, der in einer Regel für jede befugte Kommunikationsart zusammengefasst wird, und diese Fingerabdrücke oder authentifizierenden Merkmale zur Abfrage und Blockierung unbefugter Kommunikationen zu benutzen.

[0021] Während der weiter oben angegebene Regelentwicklungsprozess eine beträchtliche Flexibilität liefert, welche dazu führt, dass Mehrzweckfirewalls in praktisch jedem Netzwerktyp, System oder jeder Anwendung angewendet werden können, ist ein erhebliches Fachkönnen erforderlich, damit eine unsachgemäße Konfiguration der Firewall vermieden wird (z.B., eine sachgemäße Entwicklung der Regeln). Die unsachgemäße Konfiguration der Firewall kann in manchen Fällen dazu führen, dass Unbefugte auf das von der Firewall geschützte Netzwerk zugreifen und/oder dass Kommunikationen blockiert werden. Des Weiteren wird die von Mehrzweckfirewalls gelieferte Anpassungsfähigkeit bzw. Einsatzflexibilität in gezielteren Anwendungen nicht benötigt, bei denen eine Sonderzweck-Firewall u.U. eingesetzt wird.

[0022] Im Fall von Prozesssteuerungssystemen führt der Einsatz von Mehrzweckfirewalls, die einen Schutz zwischen beispielsweise einem Prozesssteuerungssystemnetz und Netzwerken, die eher allgemeinen Zwecken in einer mit dem Prozesssteuerungssystem verbundenen Anlage bzw. Unternehmen dienen, zu den weiter oben im Zusammenhang mit Mehrzweckfirewalls aufgeführten Schwierigkeiten. Überdies verschlimmern sich diese Probleme in Prozesssteuerungsumgebungen, da diese Mehrzweckfirewalls oft von IT- oder sonstigem außerhalb der Prozessbereiche befindlichem Personal gepflegt werden (z.B. per Fernbedienung) und daher nicht wie erforderlich zur Verfügung stehen, um die zeitkritischen Prozesse des Prozesssteuerungssystems zu pflegen.

[0023] Demzufolge liefern die hier beschriebenen Beispielmethoden, Vorrichtung und Herstellungsprodukte eine Sonderzweck-Firewall zum Einsatz in Prozesssteuerungssystemen oder -umgebungen. Im engeren Sinne machen die hier beschriebenen Firewalls die Entwicklung von Regeln zur Konfiguration der Firewalls in der weiter oben beschriebenen Art und Weise in Zusammenhang mit den Mehrzweckfirewalls überflüssig. Stattdessen enthalten die Firewalls (z.B. in einem Datenspeicher) eine Auflistung von Anwendungen samt Informationen, die zur Einrichtung von Kommunikationsverbindungen zwischen den Anwendungen und Geräten verwendet werden, die typischerweise in einem Prozesssteuerungssystem oder einer Anlage verteilt sind. Die in den Anwendungen der Auflistung enthaltenen Informationen umfassen Informationen, welche die Kommunikationen für jede befugte Kommunikationsart (z.B. Regeln) unter anderen Daten charakterisieren.

[0024] In gewissen Beispielen kann der Konfigurationsvorgang eine grafische Benutzeroberfläche umfassen, auf der eine grafische und/oder textliche Liste (z.B. eine Dropdown-Liste) der zur Verfügung stehenden Anwendungen dargestellt ist, wobei jede davon einer bestimmten Kommunikationsverbindung zwischen den Anwendungen, Rechnern und/oder Geräten auf der der Firewall gegenüberliegenden Seite entspricht. Zur Konfiguration der Firewall wählt der Anwender einfach eine oder mehr der Anwendungen aus (z.B. mit einer Maus oder sonstigem Zeigegerät), woraufhin die Firewall in Erwiderung darauf die mit der bzw. den ausgewählten Anwendung(en) verbundenen Regeln instanziiert. Die grafische Benutzeroberfläche kann verschiedene Auswahlen anbieten, die mit verschiedenen Verbindungsarten verbunden sind, wie beispielsweise ausgehende und eingehende Verbindungen, Intrusion Prävention und Scanschutz. Noch darüber hinaus kann die grafische Benutzeroberfläche für jede Auswahlanwendung dem Anwender die Festlegung ermöglichen, dass die mit der ausgewählten Anwendung verbundenen Kommunikationen aufzuzeichnen sind und/oder dass die ausgewählten Anwendungen (samt ihrer Regeln) nach einer festgelegten Zeit ungültig werden sollen (z.B. nach einer zeitbedingten autorisierten Verbindung).

[0025] Die Liste der Anwendungen kann in der Firewall vorbestückt werden (z.B. zum Herstellungszeitpunkt) und kann später auf die Firewall zum Beispiel über ein geschütztes an die Firewall angeschlossenes Kommunikationsnetzwerk, über eine Konfigurationsstation, über ein Handgerät, usw. heruntergela-

den werden. Des Weiteren können die hier beschriebenen beispielhaften Firewalls dem Anwender die Erstellung von Anwendungen ermöglichen, die der Anwendungsliste hinzugefügt werden können. Diese zusätzlichen Anwendungen können hinzugefügt werden, indem Regeln wie weiter oben in Verbindung mit den Mehrzweckfirewalls beschrieben entwickelt werden, die dann in die Firewall geladen werden, um diese hinzugefügten Anwendungen zusammen mit den vorbestückten Anwendungen über die grafische Benutzeroberfläche darzustellen.

[0026] Die hier beschriebenen beispielhaften Firewalls verarbeiten auch Distributed Component Object Model (DCOM) Kommunikationen, ohne dabei nicht verwendete Ports in der Firewall öffnen und freilegen zu müssen. Bei Mehrzweckfirewalls können DCOM-Kommunikationen in herkömmlicher Art und Weise behandelt werden, was eine gewisse Anzahl an Ports in der Firewall offen lässt, um einen dynamischen Portzuteilungsvorgang (anstelle eines permanenten Portzuteilungsvorgangs) zu ermöglichen, was zur Erstellung einer normalen DCOM-Verbindung gehört. Anders gesagt, kann die Mehrzweckfirewall Regeln für den Umgang mit DCOM-Kommunikationen umfassen, die Ports dynamisch zuteilen, welche in der Firewall für diesen Zweck offengelassen wurden. Jedoch legt das Offenlassen einer Anzahl von Ports für diesen Zweck diese Ports frei, sodass sie womöglich für einen unbefugten Zugriff durch die Firewall durch verwendet werden könnten.

[0027] Im Gegensatz zu der bekannten weiter oben beschriebenen Methode zur Bearbeitung von DCOM-Kommunikationen in einer Firewall können die hier beschriebenen beispielhaften Firewalls automatisch erkennen, wenn eine DCOM-Kommunikation durch die Firewall hergestellt wird und dynamisch einen vorgegebenen Port öffnen und diesen nach Abschluss der Kommunikation schließen. Auf diese Art und Weise werden mehrere Ports in der Firewall für eine spätere dynamische Zuteilung nicht offen gelassen, wie dies der Fall mit der weiter oben beschriebenen bekannten Methode der Fall ist. Dadurch liefern die hier beschriebenen beispielhaften Firewalls ein wesentlich sichereres System.

[0028] Wenn wir uns jetzt **Fig. 1** ansehen, umfasst die Prozesssteuerungsumgebung 100 die hier beschriebene beispielhafte Firewall 102. Die beispielhafte Firewall 102 fügt Kommunikationen zwischen dem Prozessbereich oder Stufe 104 und der Anlagen- oder Unternehmensstufe 106 der Prozesssteuerungsumgebung 100 ein. Genauer gesagt blockiert die beispielhafte Firewall 102 nicht autorisierte Kommunikationen, die über die Netzwerke mit einer relativ niedrigeren Sicherheitsstufe 108 und 110 an die Firewall 102 übermittelt wurden, und die für das Netzwerk mit einer relativ höheren Sicherheitsstufe 112 bestimmt sind, das mit Prozessstufe 104 verbunden ist. Die Netzwerke mit einer niedrigeren Sicherheitsstufe 108 und 110 können dem Unternehmensnetzwerk 110 auf der niedrigsten Sicherheitsstufe, dem Anlagennetzwerk 108 auf der höchsten Sicherheitsstufe und dem Prozesssteuerungsnetzwerk 112 auf der höchsten Sicherheitsstufe entsprechen.

[0029] Die Prozessstufe 104 kann eine oder mehr Workstations oder Anwendungsstationen 114 umfassen, die datentechnisch mit den Kontrollern, den Ein-/Ausgabevorrichtungen und den Feldvorrichtungen 116 durch das lokale Datennetz 118 verbunden sind, das diesen Vorrichtungen zugeordnet wurde. Die Anlagen- oder Unternehmensstufe 106 umfasst eine oder mehrere Workstations mit überwachtem Zugriff 120 und 122, und einen oder mehrere Server 124, 126 und 128, die verschiedene Datendienste ausführen (z.B. Historian-Dienste, Antivirus-Dienste, Software-Patch-Dienste, usw.). Die Anlagen- oder Unternehmensstufe 106 kann auch die Workstations der Unternehmensstufe 130 und 132 umfassen, die Buchhaltungsfunktionen, Unternehmensintegrationsfunktionen, usw. ausführen. Des Weiteren kann die Mehrzweckfirewall 134 die Kommunikationen zwischen den Workstations der Unternehmensstufe 130 und 132 und dem Netzwerk einfügen, das mit den Workstations mit überwachtem Zugriff 120 und 122 und den Servern 124, 126 und 128 verbunden ist.

[0030] Somit umfasst die beispielhafte Prozesssteuerungsumgebung 100 in **Fig. 1** drei Sicherheitsstufen, wobei die niedrigste Sicherheitsstufe den Workstations der Unternehmensstufe 130 und 132, die nächsthöhere Sicherheitsstufe den Workstations 120 und 122 mit überwachtem Zugriff und den Servern 124, 126 und 128, und die höchste Sicherheitsstufe dem Prozessbereich 104 entspricht. Gemäß der Lehre dieser Offenlegung liefert die beispielhafte Firewall 102 die weiter oben beschriebene Funktionalität, die in Zusammenhang mit **Fig. 2** - **Fig. 8** weiter unten noch ausführlicher beschrieben wird. Obwohl die beispielhafte Firewall 102 in Zusammenhang mit der Prozesssteuerungsumgebung 100 von **Fig. 1** beschrieben wurde, kann die beispielhafte Firewall 102 außerdem noch in allgemeinerer Art und Weise auf andere vorhandene oder später entwickelte Prozesssteuerungsumgebungen angewendet werden.

[0031] **Fig. 2** beschreibt die beispielhafte grafische Benutzeroberfläche 200, die zur Konfiguration der beispielhaften Firewall 102 von **Fig. 1** benutzt werden kann. Im engeren Sinne kann die beispielhafte grafische Benutzeroberfläche 200 durch die ausführenden Anweisungen, den Code oder die Software, die in einem Datenspeicher (nicht dargestellt) der Firewall 102 gespeichert sind, über eine Prozessoreinheit oder einen Prozessor der Firewall 102

erzeugt werden. In einem Beispiel kann ein Rechner (z.B. ein Laptop, ein Handgerät, usw.) mit der Firewall 102 verbunden werden (z.B. durch eine festverdrahtete Verbindung, drahtlos, usw.), um dem Anwender eine Ansicht der grafischen beispielhaften Benutzeroberfläche 200 zu ermöglichen. Wahlweise oder zusätzlich kann der Anwender die Benutzeroberfläche 200 durch eine oder mehrere der Computergeräte aktivieren und ansehen, die in **Fig. 1** dargestellt sind, wie beispielsweise Workstations 120, 122, 130 und/oder 132 und/oder Anwendungsstationen 114.

[0032] In jedem Fall ermöglicht die beispielhafte grafische Benutzeroberfläche 200 dem Anwender die Auswahl einer oder mehrerer Anwendungen 202 per Pulldown-Liste oder -Menü 204. Jede der verfügbaren Anwendungen 202 entspricht einer autorisierten Kommunikationsverbindung und einer zu Grunde liegenden Regel oder einem unterliegenden Regelwerk, das von der Firewall 102 zu benutzen ist, um den jeweiligen autorisierten Kommunikationen die Durchquerung der Firewall 102 zu gestatten. Die Anwendungen 202 können in der Firewall 102 zum Herstellungszeitpunkt oder allen anderen Zeitpunkten vor der Konfiguration der Firewall 102 vorbestückt oder gespeichert werden. Des Weiteren kann der Anwender eine oder mehrere der Anwendungen 202 in der Pulldown-Liste 204 nach der Entwicklung der Regeln unter Einsatz der bekannten Methoden hinzugefügt werden.

[0033] Die grafische Beispielsschnittstelle 200 umfasst ebenfalls das Protokoll-Ankreuzkästchen 206, das der Anwender verwenden kann, um die Protokollierung ausgewählter Verbindungen oder Anwendungen 202 zu bewirken. Des Weiteren kann die grafische Benutzerschnittstelle 200 das Ankreuzkästchen zur Aktivierung 208 enthalten, dass der Anwender auswählen kann, um ausgewählte Anwendungen zu aktivieren, und auch das „Verfall"-Ankreuzkästchen 210, das ausgewählt werden kann, um zu bewirken, dass eine oder mehrere der ausgewählten Anwendungen (z.B. Regeln) 202 nach einer vorgegebenen (z.B. vom Anwender festgelegten) Zeit deaktiviert wird bzw. werden.

[0034] **Fig. 3** stellt die schematische Ansicht 300 dar und **Fig. 4** ist ein Ablaufdiagramm, das eine beispielhafte Art und Weise bzw. einen beispielhaften Prozess darstellt, mittels dessen DCOM-Kommunikationen von der beispielhaften Firewall 102 von **Fig. 1** bearbeitet werden. In Bezug auf **Fig. 3** und **Fig. 4** wird der Netzwerkadministrator 302 zunächst datentechnisch mit der Firewall 102 (**Fig. 1**) verbunden, um die Firewall 102 zu konfigurieren, um einen Zugriff zu dem internen oder Hochsicherheitsnetzwerk 304 oder dem geschützten Teil eines Netzwerks von einem externen, relativ weniger geschützten Netzwerk 306 oder der Außenseite eines geschützten Teils eines Netzwerks aus durch einen spezifischen Port der Firewall 102 (Block 400) zu gewähren.

[0035] Der mit dem hochgeschützten internen Netzwerk 304 verbundene Server 308 schickt die Kommunikation 309 durch die Firewall 102 an einen externen Rechner 310, der an das externe, weniger geschützte Netzwerk 306 (Block 402) angeschlossen ist. Diese Kommunikation 309 enthält Informationen für den externen Rechner 310, welche den Computer 310 anweisen, den Port zu benutzen, der in Block 400 für Kommunikationen mit dem internen Netz 304 und insbesondere dem Server 308 vorgegeben ist. Nebenbei parst die Firewall 102 diese Kommunikation 309 und bewirkt auf der Grundlage der von der geparsten Kommunikation 309 entnommenen Informationen, dass die Firewall 102 Kommunikationen zwischen dem externen Netzwerk 306 und dem internen Netzwerk 304 durch die temporäre Verbindung auf dem vorgegebenen Port (Block 404) vorübergehend erlaubt. Genauer ausgedrückt, kann das Parsing der Kommunikation 309 bei dem Block 404 eine automatische Festlegung mit sich ziehen, dass die angeforderte Kommunikation eine DCOM-Kommunikation ist.

[0036] Der externe Rechner 310 verbindet dann den Server 308 über den vorgegebenen Port und fordert 312 eine Verbindung mit einem DCOM-Dienst innerhalb des Servers 308 (Block 406) an. Die Firewall 102 genehmigt dann die Verbindung und der externe Rechner 310 und der Server 308 können somit DCOM-Kommunikationen 314 durch die Firewall 102 (Block 406) austauschen.

[0037] Das Beispiel von **Fig. 3** und **Fig. 4** stellt lediglich eine Art und Weise dar, in der die beispielhafte Firewall 102 verwendet werden kann, um DCOM-Kommunikationen zwischen einem geschützten oder höher geschützen und einem relativ wenig geschützten Netzwerk einzurichten, ohne eine Vielzahl an Ports der Firewall 102 zu öffnen oder freizugeben haben. Infolgedessen kann die Firewall im Vergleich zu den bekannten Mehrzweckfirewalls eine maßgeblich höhere Stufe der Netzsicherheit bieten. Ausführlichere Beispiele zur Sicherung eines Netzwerks mit der Firewall 102 werden weiter unten beschrieben.

[0038] **Fig. 5** ist ein ausführlicheres Blockdiagramm der beispielhaften Firewall 102 von **Fig. 1**. Die beispielhafte Firewall 102 von **Fig. 5** kann beispielsweise zur Sicherung eines Teils eines Netzwerks benutzt werden (z.B. des Netzwerks mit einer höheren Sicherheitsstufe 112) in Bezug auf einen anderen Teil eines Netzes (z.B. die Netzwerke mit einer niedrigeren Sicherheitsstufe 108, 110).

[0039] Die beispielhafte Firewall 102 von **Fig. 5** umfasst den Kommunikationsfilter 502, den Kommunikationsanalysator 504, den Firewall-Ausnahmeerzeuger 506 und die Speicherungsvorrichtung 508.

[0040] Der beispielhafte Kommunikationsfilter 502 von **Fig. 5** empfängt die Kommunikationen von einem gesicherten Teil des Netzwerks (z.B. den Anwendungsstationen 114, Feldvorrichtungen 116, usw.), die an Zieladressen außerhalb des gesicherten Teils des Netzwerks zu übertragen sind. Die beispielhaften Kommunikationsfilter 502 empfangen auch Kommunikationen von sich außerhalb des gesicherten Teils des Netzwerks befindlichen Geräten, die an Zieladressen innerhalb des gesicherten Teils des Netzwerks übertragen werden sollen. In gewissen Beispielen umfassen die die Firewall 102 durchquerenden Kommunikationen DCOM-Kommunikationen und/oder Kommunikationen, die mit den Diensten und/oder Programmfernaufrufen verbunden sind.

[0041] Zum Schutz des gesicherten Teils des Netzwerks analysiert der beispielhafte Kommunikationsfilter 502 die Netzkommunikationen zwischen dem gesicherten Teil und den Ressourcen, die sich außerhalb des gesicherten Teils befinden, um festzulegen, ob diese Kommunikationen wünschenswert sind. In gewissen Beispielen genehmigt die Firewall 102 dynamisch die Übertragung von Kommunikationen (z.B. DCOM-Kommunikationen) an gesicherte Teile des Netzwerks von Ressourcen aus, die sich außerhalb des gesicherten Abschnitts befinden, damit gewünschte Dienste ermöglicht werden, ohne dabei das gesicherte Netz irgendwelchen Angriffen auf ungenutzte Kommunikationsports auszusetzen.

[0042] Zur dynamischen Autorisierung der Kommunikationen analysiert der beispielhafte Kommunikationsfilter 502 eine aus einem gesicherten Teil des Netzes stammende Netzkommunikation, die an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks übertragen werden soll (z.B., die Kommunikation 309 in **Fig. 3**). Der beispielhafte Kommunikationsanalysator 504 parst die Kommunikation, damit ein mit der Kommunikation verbundener Dienst ermittelt werden kann (z.B. ein universeller Schnittstellen-Identifikator eines DCOM-Diensts) sowie auch die Adresse einer Vorrichtung innerhalb des gesicherten Netzwerks auf der Grundlage der Kommunikation (z.B. eine IP-Adresse, an die dynamisch eine autorisierte Kommunikation bzw. Kommunikationen, die von der außenliegenden Seite des gesicherten Teils des Netzwerks empfangen wurden, zu übertragen sind) und ein Untermenge von Ports, die für die dynamisch autorisierte(n) Kommunikatione(n) geöffnet werden soll.

[0043] Der beispielhafte Kommunikationsanalysator 504 kann zweckdienlicherweise das Vorhandensein dieser Informationen in der geparsten Netzkommunikation erkennen, indem er einen Marker in den Nutzdaten der Kommunikation ermittelt (z.B. einen Marker-String). Sollte kein Marker vorhanden sein, kann der Kommunikationsanalysator 504 die Suche in der Kommunikation einstellen. Andererseits kann im Falle eines Vorhandenseins eines Markers der beispielhafte Firewall-Ausnahmeerzeuger 506 den Dienst-Identifikator (z.B. die UID) sowie auch die Adresse und den Port bzw. die Ports von der Netzkommunikation extrahieren. Der beispielhafte Firewall-Ausnahmeerzeuger 506 speichert den Dienst-Identifikator, die Adresse und den Port bzw. die Ports als eine Ausnahme in der Ausnahmeliste 510 ab, die in der Speicherungsvorrichtung 508 gespeichert ist. In gewissen Beispielen bestimmt der Firewall-Ausnahmeerzeuger 506, ob ein Ping-Flag oder eine Variable einen ersten Wert hat (z.B. aktiviert, deaktiviert). Das Ping-Flag kann zur Aktivierung weiterer Dienste verwendet werden, die auf der Grundlage der Netzkommunikation autorisiert werden (z.B. für Dienste in Bezug auf einen dynamisch autorisierten Dienst).

[0044] Während die Ausnahme weiterhin genehmigt bleibt, empfängt die beispielhafte Firewall 102 eine oder mehr Netzkommunikationen von außerhalb des gesicherten Teils des Netzes, deren Zieladresse sich in dem gesicherten Teil des Netzwerks befindet (z.B. die Kommunikationen 312, 314 von **Fig. 3**). Der beispielhafte Kommunikationsfilter 502 vergleicht die Netzkommunikation mit dem Dienst-Identifikator bzw. den Dienst-Identifikatoren, der bzw. den Adresse(n) und dem bzw. den Port(s) in den Einträgen in der Ausnahmeliste 510 (z.B. in dem Speicher 508) zur Ermittlung einer Übereinstimmung. Sollte eine solche vorhanden sein, leitet der beispielhafte Kommunikationsfilter 502 die Kommunikation weiter.

[0045] Sollte der Kommunikationsfilter 502 festlegen, dass die Kommunikation mit einer Ausnahme in der Adresse und dem Port bzw. den Ports übereinstimmt, jedoch nicht mit einem Dienst-Identifikator, bestimmt der beispielhafte Kommunikationsfilter 502, ob eine Master-Verbindung immer noch aktiv ist (d.h., ob die Kommunikation 309 unterbrochen oder abgetrennt wurde). Falls die Master-Verbindung noch aktiv sein sollte, kann der beispielhafte Kommunikationsfilter 502 die Kommunikation an das Gerät weiterleiten. Andererseits, kann der beispielhafte Kommunikationsfilter 502 festlegen, ob das Ping-Flag aktiviert ist, sollte die Master-Verbindung inaktiv sein. Der beispielhafte Kommunikationsfilter 502 kann die Kommunikation an die Vorrichtung weiterleiten, falls das Ping-Flag deaktiviert sein sollte. Im Falle einer inaktiven Master-Verbindung und einem aktivierten Ping-Flag wird der Kommunkiationsfilter 502 jedoch die Kommunikation filtern oder löschen.

[0046] Die Beispielkomponenten und Funktionen der beispielhaften Firewall 102 von **Fig. 5** sind weiter oben beschrieben. Die beispielhafte Firewall 102 kann ebenfalls sonstige Firewallfunktionen ausführen, wie beispielsweise normale Firewall-Funktionsweisen. Diese Funktionen werden nicht erörtert, um eine Verunklarung der Beispiele zu vermeiden. Darüber hinaus können die beispielhaften Firewalls 102 als Software-Firewalls in einer Rechnervorrichtung in einem Netzwerk zum Schutz der Rechnervorrichtung eingesetzt werden, während die beispielhaften Firewalls 102 von **Fig. 1** - **Fig. 5** als eine separate Firewall beschrieben werden.

[0047] Obwohl eine beispielshafte Anwendungsart der Firewall 102 von **Fig. 1** in **Fig. 5** veranschaulicht wurde, können eine oder mehrere der in **Fig. 5**. dargestellten Elemente, Prozesse und/oder Vorrichtungen kombiniert, aufgeteilt, neu angeordnet, ausgelassen, beseitigt und/oder auf andere Art und Weise eingesetzt werden. Des Weiteren können der beispielhafte Kommunikationsfilter 502, der beispielhafte Kommunikationsanalysator 504, der beispielhafte Firewall-Ausnahmeerzeuger 506, die beispielhafte Speicherungsvorrichtung 508 und/oder allgemeiner ausgedrückt, die beispielhafte Firewall 102 von **Fig. 1** und/oder 5 von Hardware, Software, Firmware und/oder beliebigen Kombinationen von Hardware, Software und/oder Firmware eingesetzt werden. So kann zum Beispiel der beispielhafte Kommunikationsfilter 502, der beispielhafte Kommunikationsanalysator 504, der beispielhafte Firewall-Ausnahmeerzeuger 506, die beispielhafte Speicherungvorrichtung 508 und/oder allgemeiner ausgedrückt, die beispielhafte Firewall 102 von einer oder mehreren Schaltungen, programmierbaren Prozessoren, anwenderspezifisch-integrierten Schaltungen (ASCIs), programmierbaren Logik-Schaltungen (PDLs) und/oder programmierbaren Logik-Feldschaltungen (FPLDs), usw. eingesetzt werden. Wenn einer der Vorrichtungs- oder Systemansprüche dieses Patents so ausgelegt wird, dass sie lediglich eine Software und/oder Firmwareanwendung abdecken, so wird mindestens einer der beispielhaften Kommunikationsfilter 502, der beispielhaften Kommunikationsanalysatoren 504, der beispielhaften Firewall-Ausnahmeerzeuger 506, und/oder der beispielhaften Speicherungsvorrichtung 508 hiermit ausdrücklich so definiert, dass sie ein konkretes computerlesbares Speichermedium, wie beispielsweise einen Datenspeicher, eine DVD, CD, Blu-ray, usw. umfassen, welche die Software und/oder Firmware speichert. Sogar noch darüber hinaus kann die beispielhafte Firewall 102 von **Fig. 1** und/oder 5 ein oder mehrere Elemente, Prozesse und/oder Vorrichtungen zusätzlich zu, oder anstelle von denen in **Fig. 5** veranschaulichten umfassen, und/oder mehr als eine aller beliebigen oder aller der dargestellten Elemente, Prozesse und Vorrichtungen umfassen.

[0048] Die Ablaufdiagramme, die die Beispielmethoden zur Umsetzung der Firewall 102 von **Fig. 1** und/oder 5 darstellen, werden in **Fig. 4** und **Fig. 6** - **Fig. 8** angezeigt. In diesen Beispielen können die Methoden unter Einsatz der maschinenlesbaren Anweisungen umgesetzt werden, die ein Programm bzw. Programme zur Ausführung seitens eines Prozessors umfassen, wie beispielsweise der Prozessor 912, der in der beispielhaften Abwicklungsplattform 900 dargestellt ist und weiter unten in Zusammenhang mit **Fig. 9** erörtert wird. Das Programm kann bzw. die Programme können in einer Software enthalten sein, die auf einem konkreten computerlesbaren Datenmedium wie beispielsweise einer CD-ROM, einer Floppy Disk, einer Festplatte, einer DVD, einer Blu-ray Disk oder einem mit Prozessor 912 verbundenen Datenspeicher gespeichert sind, wobei jedoch das gesamte Programm und/oder Teile davon alternativ von einer Vorrichtung ausgeführt werden kann bzw. können, die nicht der Prozessor 912 ist und/oder in einer Firmware oder dedizierten Hardware enthalten ist. Des Weiteren können viele sonstige Methoden zur Umsetzung der Firewall 102 wahlweise benutzt werden, obwohl die Beispielprogramme in Bezug auf die Flowchart beschrieben werden, die in **Fig. 5** und **Fig. 6** - **Fig. 8** veranschaulicht sind. So können beispielsweise die Ausführungsbefehle der Blöcke geändert werden und/oder einige der beschriebenen Blöcke geändert, entfernt oder zusammengelegt werden.

[0049] Wie weiter oben erwähnt, können die Beispielprozesse von **Fig. 4** und **Fig. 6** - **Fig. 8** mit Hilfe der verschlüsselten Anweisungen (z.B. computerlesbare Anweisungen) umgesetzt werden, die auf einem konkreten computerlesbaren Datenmedium, wie beispielsweise einem Festplattenlaufwerk, einem Flash-Speicher, einem schreibgeschützten Speicher (ROM), einer Compact-Disk (CD), einer DVD, einem Cache, einem RAM-Speicher und/oder sonstigem Speichermedium gespeichert werden, auf dem Informationen für beliebige Zeiträume gespeichert werden (z.B. für längere Zeiträume, auf Dauer, nur kurz, für ein zeitweises Buffering, und/oder zum Caching von Informationen). Der hier verwendete Ausdruck konkretes computerlesbares Datenmedium wird ausdrücklich so definiert, dass er sämtliche Arten der computerlesbaren Speicherung umfasst und alle sich verbreitenden Signale ausschließt. Des Weiteren bzw. wahlweise können die Beispielprozesse von **Fig. 4** und **Fig. 6** - **Fig. 8** unter Einsatz verschlüsselter Anweisungen (z.B. computerlesbarer Anweisungen) umgesetzt werden, in einem nichttransitorischen computerlesbaren Datenmedium, wie beispielsweise einem Festplattenlaufwerk, einem Flash-Speicher, einem schreibgeschützten Speicher, einer Compact-Disk, einer DVD, einem Cache, einem RAM-Speicher und/oder sonstigen Datenspeichermedien gespeichert werden, in denen die Informationen für eine beliebige

Zeitdauer gespeichert werden (z.B. für längere Zeiträume, auf Dauer, nur kurz, für ein zeitweises Buffering, und/oder zum Caching von Informationen). Der hier verwendete Begriff nicht-transitorisches computerlesbares Datenmedium wird ausdrücklich so definiert, dass er jede Art von computerlesbaren Datenspeichern umfasst und sich verbreitende Signale ausschließt. Der hier verwendete Ausdruck „mindestens“ wird als ein Übergangsausdruck in einem Oberbegriff eines Anspruchs verwendet und ist genauso offen wie der Ausdruck „umfasst“. Daher kann ein Anspruch, der „mindestens“ als Übergangsbegriff in seinem Oberbegriff verwendet, zusätzliche Elemente zu denen umfassen, die ausdrücklich in dem Anspruch aufgeführt sind.

[0050] **Fig. 6** ist ein Ablaufdiagramm, auf dem eine Beispielmethode 600 zur Umsetzung der Firewall 102 von **Fig. 1** und **Fig. 5** zur dynamischen Erstellung einer Ausnahme für einen Dienst dargestellt ist. Die Beispielmethode 600 kann dann ausgeführt werden, wenn die Firewall 102 eine Netzkommunikation von einer Vorrichtung innerhalb eines gesicherten Teils eines Netzwerks empfängt (z.B., das Netzwerk 112 von **Fig. 1**), das für eine Vorrichtung außerhalb des gesicherten Teils des Netzwerks bestimmt ist.

[0051] Die Beispielmethode 600 beginnt mit der Analyse (z.B. via dem Kommunikationsfilter 502 von **Fig. 5**) der Netzkommunikation von dem gesicherten Teil des Netzwerks, die für eine Adresse oder Vorrichtung außerhalb des gesicherten Teils des Netzwerks bestimmt ist (Block 602). Der beispielhafte Kommunikationsanalysator 504 legt fest, ob ein Marker in der Netzkommunikation (Block 604) vorliegt. Sollte ein Marker anwesend sein (Block 604), ermittelt der beispielhafte Firewall-Ausnahmeerzeuger 506 eine UID für einen Dienst, eine Adresse (z.B. eine IP-Adresse des Servers 308 von **Fig. 3**) und den Port bzw. die Ports des Servers 308 der Netzkommunikation (Block 606). Der beispielhafte Firewall-Ausnahmeerzeuger 506 speichert die UID, die Adresse und den Port bzw. die Ports ab (z.B. in der Ausnahmeliste 510 in der Speicherungsvorrichtung 508 von **Fig. 5**) (Block 608). In dem Beispiel von **Fig. 6** speichert der Firewall-Ausnahmeerzeuger 506 ebenfalls einen Ping-Flag-Wert (Block 610) ab. Dies stellt dann die Beendigung der Beispielmethode 600 dar.

[0052] **Fig. 7** ist ein Ablaufdiagramm, das eine Beispielmethode 700 zur Umsetzung der Firewall 102 von **Fig. 1** und **Fig. 5** darstellt, um wahlweise Kommunikationen für einen Dienst zu gestatten, der an einen gesicherten Teil eines Netzwerks weitergeleitet werden soll. Die Beispielmethode 700 kann durch die beispielhafte Firewall 102 dann ausgeführt werden, wenn beispielsweise eine Kommunikation zur Übertragung an den gesicherten Teil eines Netzwerks empfangen wurde (z.B. die Kommunikationen 312, 314 von **Fig. 3**).

[0053] Die Beispielmethoden 700 werden eingeleitet, indem eine Netzkommunikation (z.B. via einem Kommunikationsfilter 502 von **Fig. 5**) analysiert wird, welche von außerhalb eines gesicherten Teils eines Netzwerks empfangen wurde (Block 702). Der beispielhafte Kommunikationsfilter 502 bestimmt eine Zieladresse und einen Port bzw. mehrere Ports für die Netzkommunikation (Block 704).

[0054] Der beispielhafte Kommunikationsfilter 502 bestimmt, ob die Netzkommunikation mit einer Adresse und einem Port bzw. mehreren Ports übereinstimmt, die der Adresse in einer Ausnahmliste entsprechen (z.B. die Ausnahmeliste 510 von **Fig. 5**) (Block 706). Der Kommunikationsfilter 502 löscht die Netzkommunikation (Block 716), wenn die Netzkommunikation mit keinen Adressen und entsprechendem Port bzw. entsprechenden Ports in der Ausnahmeliste 510 (Block 706) übereinstimmt.

[0055] Andererseits bestimmt der beispielhafte Kommunikationsfilter 502, ob die Netzkommunikation mit dem Dienst-Identifikator (z.B. der UID) in der Ausnahmeliste 510 und dem bzw. den Port(s) übereinstimmt, wenn der Kommunikationsfilter 502 bestimmen sollte, dass die Netzkommunikation nicht mit einer Adresse und dem entsprechenden Port bzw. den entsprechenden Ports übereinstimmt. Falls die Netzkommunikation mit dem Service-Identifikator (Block 708) übereinstimmt, leitet der beispielhafte Kommunikationsfilter 502 die Netzkommunikation an die Adresse und den Port bzw. die Ports innerhalb des gesicherten Teils des Netzwerks weiter (Block 714).

[0056] Falls die Netzkommunikation mit einer Adresse und einem entsprechenden Port bzw. entsprechenden Ports jedoch nicht mit dem Dienst-Identifikator (Block 708) übereinstimmen sollte, bestimmt der beispielhafte Kommunikationsfilter 502, ob eine Master-Verbindung für die Netzkommunikation aktiv ist (Block 710). Die Master-Verbindung kann die Netzkommunikation sein, von dem die Übereinstimmungsausnahme in der Ausnahmeliste 510 abgeleitet wurde (z.B. die Netzkommunikation 309 für die Kommunikationen 312, 314 von **Fig. 3**). Falls die Master-Verbindung aktiv sein sollte (Block 710), kann der beispielhafte Kommunikationsfilter 502 die Netzkommunikation (Block 714) weiterleiten. Falls die Master-Verbindung nicht aktiv sein sollte (Block 710), bestimmt der beispielhafte Kommunikationsfilter 502, ob das Ping-Flag für die Master-Verbindung aktiviert wurde (Block 712). So kann der Kommunikationsfilter 502 beispielsweise die Ausnahmeliste 510 darauf prüfen, ob der Eintrag der Adresse oder dem Port bzw. den Ports entspricht, um einen Wert des Ping-Flags oder der Variable fest-

zulegen. Der beispielhafte Kommunikationsfilter 502 filtert oder löscht die Netzkommunikation, falls das Ping-Flag für die Master-Verbindung aktiviert wurde (Block 712). Andernfalls leitet der beispielhafte Kommunikationsfilter 502 im Falle eines deaktivierten Ping-Flags (Block 712) die Netzkommunikation an die Adresse und den Port bzw. die Ports an den gesicherten Teil des Netzwerks (Block 714) weiter.

[0057] Nach der Weiterleitung der Netzkommunikation (Block 714) oder der Löschung der Netzkommunikation (Block 716), kann die Beispielmethode 700 unter Umständen beendet werden.

[0058] **Fig. 8** ist ein Ablaufdiagramm, das eine Beispielmethode 800 zur Umsetzung der Firewall 102 von **Fig. 1** und **Fig. 5** zur Verwaltung der dynamischen Ausnahmen für Dienste darstellt. Die Beispielmethode 800 von **Fig. 8** kann regelmäßig oder auch aperiodisch, auf Anforderung, als Reaktion auf ein Ereignis und/oder zu jeder anderen Zeit zur Verwaltung dynamischer Ausnahmen ausgeführt werden.

[0059] Der beispielhafte Firewall-Ausnahmeerzeuger 506 von **Fig. 5** wählt eine Eingabe in der Ausnahmeliste 510 aus (z.B., in der Datenspeicher-Vorrichtung 508) (Block 802). Der beispielhafte Firewall-Ausnahmeerzeuger 506 bestimmt, ob die ausgewählte Eingabe in der Ausnahmeliste 510 für eine gewisse Schwellwertzeit (Block 804) vorhanden war. Die Schwellwertzeit kann empirisch bestimmt, von einer Richtlinie und/oder von einem Administrator des gesicherten Teils des Netzwerks eingestellt werden. Falls die ausgewählte Eingabe in der Ausnahmeliste 510 für die Schwellwertzeit (Block 804) vorhanden gewesen sein sollte, löscht der beispielhafte Firewall-Ausnahmeerzeuger 506 die Eingabe von der Ausnahmeliste (Block 806). Das Löschen der Ausnahmeeingabe kann die Sicherheit in dem gesicherten Teil des Netzwerks erhöhen, indem die Anzahl an offenen, jedoch nicht verwendeten Ports in der Firewall 102 verringert wird. Falls die ausgewählte Eingabe weniger lang als die Schwellwertzeit (Block 804) oder nach Löschen der Eingabe (Block 806) vorhanden war, kann die Beispielmethode 800 u.U. enden. In gewissen Beispielen iteriert der Firewall-Ausnahmeerzeuger 506 die Methode 800 für jede der Eingaben in der Ausnahmeliste 510.

[0060] **Fig. 9** ist das Blockdiagram einer beispielhaften Abwicklungsplattform 900, die die Anweisungen von **Fig. 4** und **Fig. 6** - **Fig. 8** zur Umsetzung der Firewall 102 von **Fig. 1** und/oder 5 ausführen kann. Die Abwicklungsplattform 900 kann beispielsweise eine Firewall-Anwendung, ein Server, ein Personal Computer oder eine beliebige sonstige Computervorrichtung oder Internet-Anwendung sein.

[0061] Die Abwicklungsplattform 900 des aktuellen Beispiels umfasst den Prozessor 912. Der Prozessor 912 kann beispielsweise von einem oder mehreren Mikroprozessoren oder Kontrollern von jeder beliebigen Familie oder jedem beliebigen Hersteller ausgeführt werden.

[0062] Der Prozessor 912 umfasst einen lokalen Speicher 913 (z.B., ein Cache) und steht in Verbindung mit einem Hauptspeicher und zwar einschließlich eines flüchtigen Speichers 914 und eines nichtflüchtigen Speichers 916 via einem Datenbus 918. Der flüchtige Speicher 914 kann mittels eines Synchronen Dynamischen Arbeitsspeichers (SDRAM), Dynamischen Arbeitsspeichers (DRAM), RAMBUS Dynamischen Arbeitsspeichers (RDRAM) und/oder beliebigen sonstigen Arten einer Arbeitsspeichervorrichtung ausgeführt werden. Der nichtflüchtige Speicher 916 kann durch einen Flash-Speicher und/oder beliebige andere Speichervorrichtungen ausgeführt werden. Der Zugriff auf den Hauptspeicher 914, 916 wird von einem Speichercontroller gesteuert.

[0063] Die Abwicklungsplattform 900 umfasst ebenfalls die Schnittstellenschaltung 920. Diese Schnittstellenschaltung 920 kann von jeder beliebigen Art an Schnittstellensstandard, wie beispielsweise einer Ethernet-Schnittstelle, eines universellen seriellen Busses (USB) und/oder einer PCI-Express-Schnittstelle ausgeführt werden.

[0064] Eine oder mehrere Eingabegeräte 922 sind mit der Schnittstellenschaltung 920 verbunden. Die Eingabegerät(e) 922 erlauben dem Anwender die Eingabe von Daten und Befehlen in den Prozessor 912. Die Eingabegerät(e) können beispielsweise für eine Tastatur, eine Maus, einen Berührungsbildschirm, ein Trackpad, einen Trackball, Isopoint und/oder ein Spracherkennungssystem zur Anwendung gebracht werden.

[0065] Mit der Schnittstellenschaltung 920 werden ebenfalls eine oder mehrere Ausgabevorrichtung(en) 924 verbunden. Die Ausgabevorrichtungen 924 können beispielsweise durch Anzeigegeräte (z.B., eine Flüssigkristallanzeige, eine Bildschirmröhrenanzeige (CRT), usw.) angewendet werden. Die Schnittstellenschaltung 920 umfasst daher typischerweise eine Grafik-Driver-Karte.

[0066] Des Weiteren umfasst die Schnittstellenschaltung 920 eine Kommunikationsvorrichtung, wie beispielsweise eine Modem- oder Netzwerk-Schnittstellenkarte, um einen Datenaustausch mit externen Rechnern über ein Netzwerk 926 (z.B., einen Ethernetanschluss, eine Digital Subscriber Line (DSL), eine Telefonleitung, ein Koaxialkabel, ein Zellulartelefonsystem, usw.) zu ermöglichen.

[0067] Die Abwicklungsplattform 900 umfasst ebenfalls eine oder mehrere Massendatenspeichervorrichtung(en) 928 zur Speicherung von Software und

Daten. Beispiele dieser Massendatenspeichervorrichtung(en) 928 umfassen Diskettenlaufwerke, Festplattenlaufwerke, Kompakt-Diskettenlaufwerke und DVD-Laufwerke. Die Massendatenspeichervorrichtung 928 kann die Beispielsdatenspeichervorrichtung 508 von **Fig. 5** ausführen.

[0068] Verschlüsselte Anweisungen 932 zur Ausführung der Methoden von **Fig. 4** und **Fig. 6** - **Fig. 8** können in der Massendatenspeichervorrichtung 928, in dem flüchtigen Speicher 914, in dem nicht-flüchtigen Speicher 916 und/oder auf einem abnehmbaren Datenspeichermedium, wie beispielsweise einer CD oder DVD gespeichert werden.

[0069] Obwohl bestimmte Beispielmethoden, Vorrichtungen und Herstellungsprodukte nicht hier beschrieben wurden, ist der Deckungsumfang dieses Patents nicht darauf beschränkt; vielmehr deckt dieses Patent sämtliche Methoden, Vorrichtungen und Herstellungsprodukte, die billigerweise in den Umfang der Ansprüche dieses Patents fallen.

Patentansprüche

1. Ein Verfahren, das Folgendes umfasst:
Analysierung einer Netzkommunikation zur Ermittlung eines ersten Diensts, einer Adresse in Verbindung mit dem ersten Dienst innerhalb eines gesicherten Teils eines Netzwerks und einer Untermenge von Ports, die von dem ersten Dienst verwendet wird, wobei die Netzkommunikation aus dem gesicherten Teil des Netzwerks stammt und an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks übertragen werden soll; und
Speicherung eines Identifikators des ersten Diensts, der Adresse, und der Untermenge von Ports, wenn die Netzkommunikation den Identifikator, die Adresse, und eine Untermenge von Ports umfasst.

2. Ein Verfahren, wie in Anspruch 1 definiert, das weiterhin ein Vergleichen einer zweiten von außerhalb des gesicherten Teils des Netzwerks empfangenen Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und der Untermenge von Ports umfasst.

3. Ein Verfahren, wie in Anspruch 2 definiert, das weiterhin eine Weiterleitung der zweiten Netzkommunikation an eine Adresse und einen Port umfasst, welche von der zweitem Netzkommunikation bestimmt wurde, wenn die zweite Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und einem Port in der Untermenge der Ports übereinstimmt.

4. Ein Verfahren, wie in einem der Ansprüche 2 oder 3 definiert, das weiterhin die Weiterleitung einer zweiten Netzkommunikation an eine Adresse und einen Port umfasst, der von der zweiten Netzkommunikation bestimmt wurde, wenn die zweite Netzkommunikation mit der Adresse und einem Port in der Untermenge der Ports übereinstimmt und nicht mit dem Identifikator übereinstimmt und zwar auf der Grundlage von mindestens einer der Schwellwertzeiten für die erste Netzkommunikation oder eines Ping-Flag.

5. Ein Verfahren, wie in Anspruch 4 definiert, das weiterhin eine Einstellung des Ping-Flag auf der Grundlage der ersten Netzkommunikation umfasst.

6. Ein Verfahren, wie in einem der Ansprüche 2 bis 5 definiert, das weiterhin das Löschen der zweiten Netzkommunikation umfasst, wenn die zweite Netzkommunikation nicht mit einer gespeicherten Adresse und einem gespeicherten Port übereinstimmt, der einem erstem Dienst entspricht.

7. Ein Verfahren, wie in einem der Ansprüche 1 bis 6 definiert, das weiterhin ein Löschen des Identifikators des ersten Diensts, der Adresse und des Untermenge von Ports von einem Datenspeicher auf der Grundlage einer Schwellwertzeit umfasst.

8. Eine Vorrichtung, die folgendes umfasst:
einen Kommunikationsfilter zur Analysierung einer Netzkommunikation, welche von innerhalb eines gesicherten Teils eines Netzwerks herrührt und an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks übertragen werden soll;
einen Kommunikationsanalysator zur Ermittlung eines ersten Diensts, eines Identifikators des ersten Dienstes, einer Adresse, die mit dem ersten Dienst innerhalb des gesicherten Teil des Netzwerks verbunden ist, sowie auch der Ermittlung einer Untermenge von Ports, die von dem ersten Dienst verwendet wird; und
einen Firewall-Ausnahmeerzeuger zur Speicherung des Identifikators des ersten Diensts, der Adresse und der Untermenge von Ports, wenn die Netzkommunikation den Identifikator, die Adresse und die Untermenge von Ports umfasst.

9. Eine Vorrichtung, wie in Anspruch 8 definiert, wobei der Kommunikationsfilter eine zweite von außerhalb des gesicherten Teils des Netzwerks empfangene Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse, und der Untermenge von Ports vergleichen soll.

10. Eine Vorrichtung, wie in Anspruch 9 definiert, wobei der Kommunikationsfilter die zweite Netzkommunikation an eine Adresse und einen Port weiterleiten soll, welche von der zweiten Netzkommunikation bestimmt wird, wenn die zweite Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und einem Port in der Untermenge von Ports übereinstimmt.

11. Eine Vorrichtung, wie in einem der Ansprüche 9 oder 10 definiert, wobei der Kommunikationsfilter die zweite Netzkommunikation an eine Adresse und einen Port weiterleitet, der von der zweiten Netzkommunikation festgelegt wurde, wenn die zweite Netzkommunikation mit der Adresse und einem Port in der Untermenge von Ports übereinstimmt und nicht mit dem Identifikator übereinstimmt und zwar auf der Grundlage von mindestens einer der Schwellwertzeiten für die erste Netzkommunikation oder eines Ping-Flag.

12. Eine Vorrichtung, wie in Anspruch 11 definiert, wobei der Kommunikationsanalysator einen Wert für das Ping-Flag auf der Grundlage der ersten Netzkommunikation ermitteln soll, und der Firewall-Ausnahmeerzeuger den Wert des Ping-Flag auf der Grundlage der ersten Netzkommunikation abspeichem soll.

13. Eine Vorrichtung, wie in einem der Ansprüche 9 bis 12 definiert, wobei mindestens eine der ersten oder zweiten Netzkommunikation eine verteilte Component Object Model Kommunikation ist.

14. Eine Vorrichtung, wie in einem der Ansprüche 8 bis 13 definiert, die weiterhin eine Datenspeicher-Vorrichtung, den Firewall-Ausnahmeerzeuger zur Speicherung des Identifikators, der Adresse und der Untermenge von Ports in der Datenspeicher-Vorrichtung abspeichern soll.

15. Ein computerlesbares Datenspeichermedium, das computerlesbare Anweisungen umfasst, die nach deren Ausführung durch einen Prozessor bewirken, dass der Prozessor mindestens:
eine Netzkommunikation analysiert zur Ermittlung eines ersten Diensts, einer mit dem erstem Dienst innerhalb eines gesicherten Teil eines Netzwerks verbundenen Adresse und einer von dem ersten Dienst verwendeten Untermenge von Ports, wobei die Netzkommunikation von innerhalb des gesicherten Teil des Netzwerks herrührt und an eine Zieladresse außerhalb des gesicherten Teils des Netzwerks zu übertragen ist; und
die Speicherung eines Identifikators des ersten Diensts, der Adresse und die Untermenge von Ports, wenn die Netzkommunikation den Identifikator, die Adresse und die Untermenge von Ports umfasst.

16. Ein Datenspeichermedium, wie in Anspruch 15 definiert, wobei die Anweisungen weiterhin bewirken, dass der Prozessor die zweite von außerhalb des gesicherten Teils des Netzwerks empfangene Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und der Untermenge von Ports vergleicht.

17. Ein Datenspeichermedium, wie in Anspruch 16 definiert, wobei die Anweisungen weiterhin bewirken, dass der Prozessor die zweite Netzkommunikation an eine Adresse und einen Port weiterleitet, der von der zweiten Netzkommunikation festgelegt wurde, wenn die zweite Netzkommunikation mit dem Identifikator des ersten Diensts, der Adresse und einem Port in der Untermenge von Ports übereinstimmt.

18. Ein Datenspeichermedium, wie in einem der Ansprüche 16 oder 17 definiert, wobei die Anweisungen weiterhin bewirken, dass der Prozessor die zweite Netzkommunikation an eine Adresse und einen Port weiterleitet, der von der zweiten Netzkommunikation festgelegt wurde, wenn die zweite Netzkommunikation mit der Adresse und einem Port in der Untermenge von Ports übereinstimmt und nicht mit dem Identifikator übereinstimmt, und zwar auf der Grundlage von mindestens einer der Schwellwertzeiten für die erste Netzkommunikation oder eines Ping-Flag.

19. Ein Datenspeichermedium, wie in einem der Ansprüche 16 bis 18 definiert, wobei die Anweisungen weiterhin bewirken, dass der Prozessor die zweite Netzkommunikation löscht, wenn die zweite Netzkommunikation nicht mit einer gespeicherten Adresse und einem gespeicherten Port übereinstimmt, die dem ersten Dienst entsprechen.

20. Ein Datenspeichermedium, wie in einem der Ansprüche 15 bis 19 definiert, wobei die Anweisungen weiterhin bewirken, dass der Prozessor den Identifikator des ersten Diensts, die Adresse und die Untermenge von Ports von einem Datenspeicher auf der Grundlage einer Schwellwertzeit löscht.

Es folgen 9 Seiten Zeichnungen

Anhängende Zeichnungen

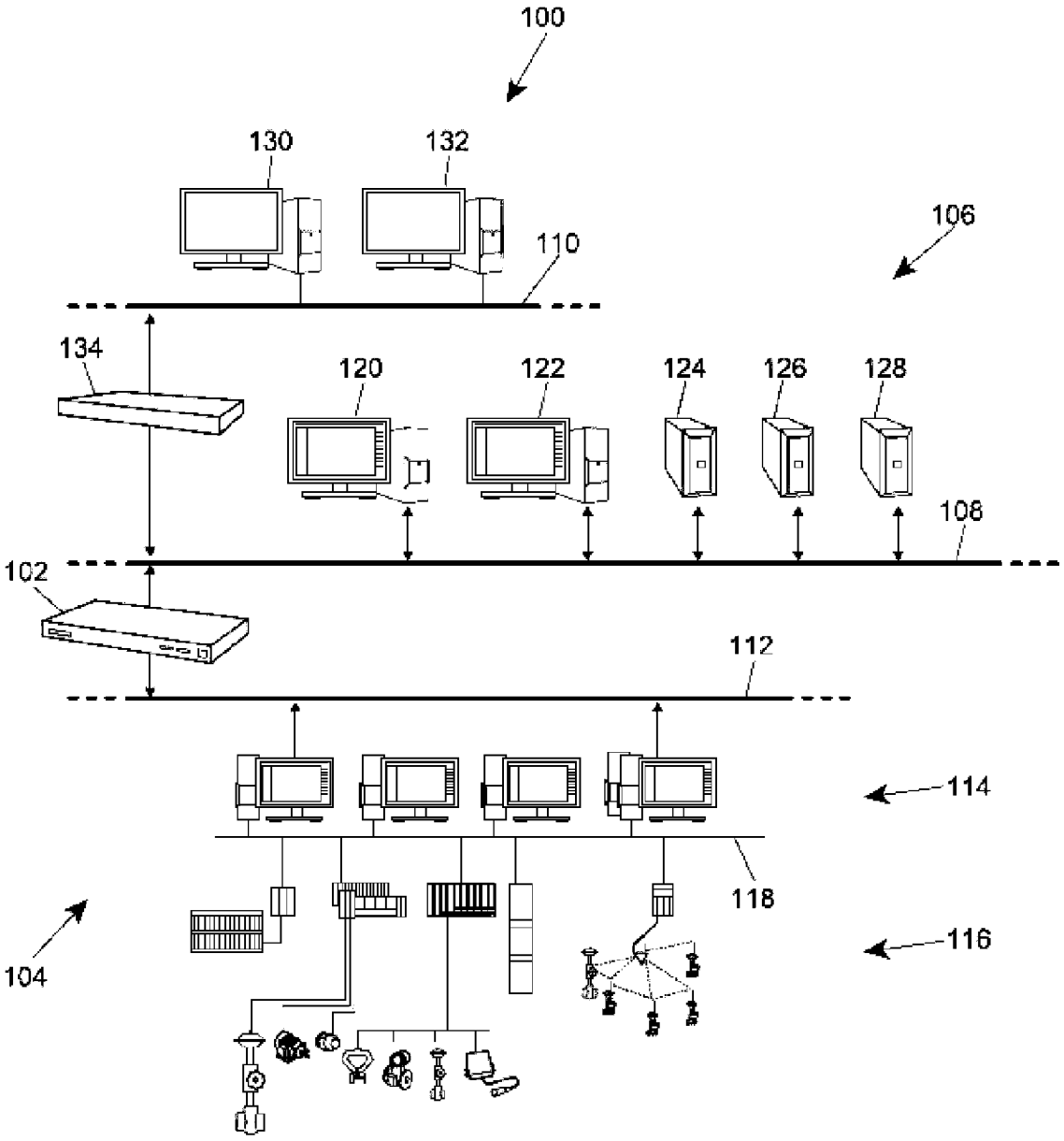


FIG. 1

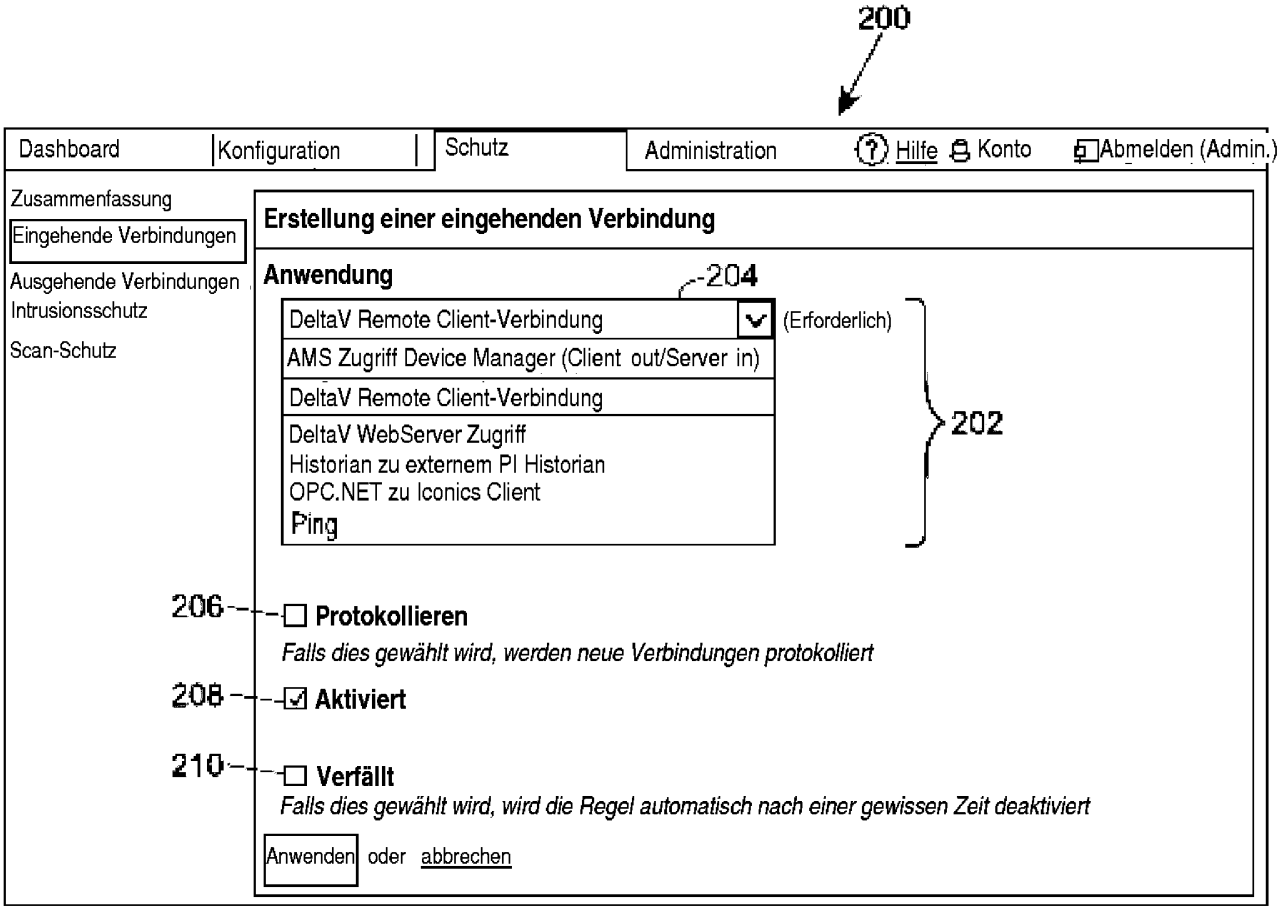

200
Dashboard
Konfiguration
Schutz
Administration
Hilfe
Konto
Abmelden (Admin.)
Zusammenfassung
Eingehende Verbindungen
Ausgehende Verbindungen
Intrusionsschutz
Scan-Schutz
Erstellung einer eingehenden Verbindung
Anwendung
204
DeltaV Remote Client-Verbindung
(Erforderlich)
AMS Zugriff Device Manager (Client out/Server in)
DeltaV Remote Client-Verbindung
DeltaV WebServer Zugriff
Historian zu externem PI Historian
OPC.NET zu Iconics Client
Ping
202
206
Protokollieren
Falls dies gewählt wird, werden neue Verbindungen protokolliert
208
Aktiviert
210
Verfällt
Falls dies gewählt wird, wird die Regel automatisch nach einer gewissen Zeit deaktiviert
Anwenden
oder
abbrechen

FIG. 2

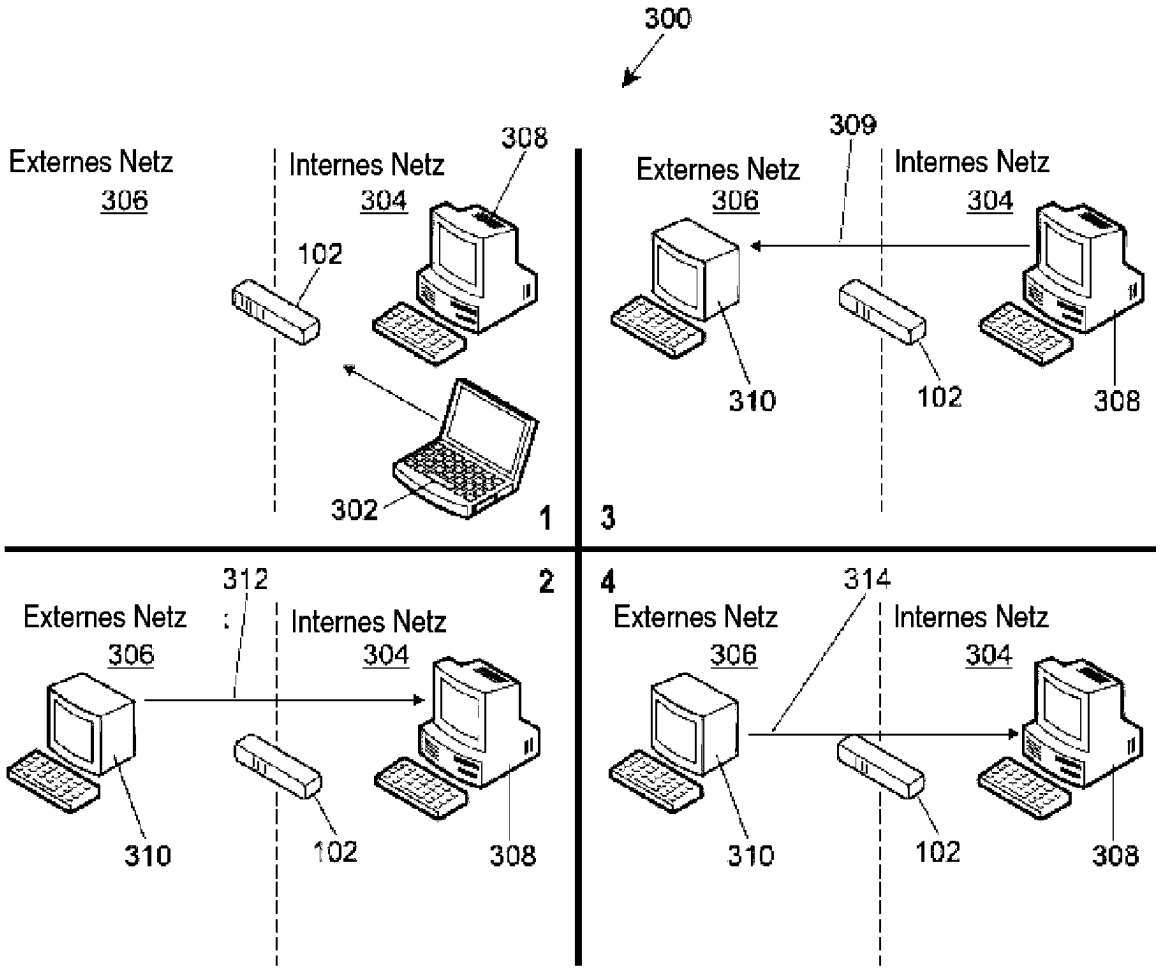

300
Externes Netz
306
Internes Netz
304
308
102
302
1
309
Externes Netz
306
Internes Netz
304
310
102
308
3
312
2
Externes Netz
306
Internes Netz
304
310
102
308
314
4
Externes Netz
306
Internes Netz
304
310
102
308

FIG. 3

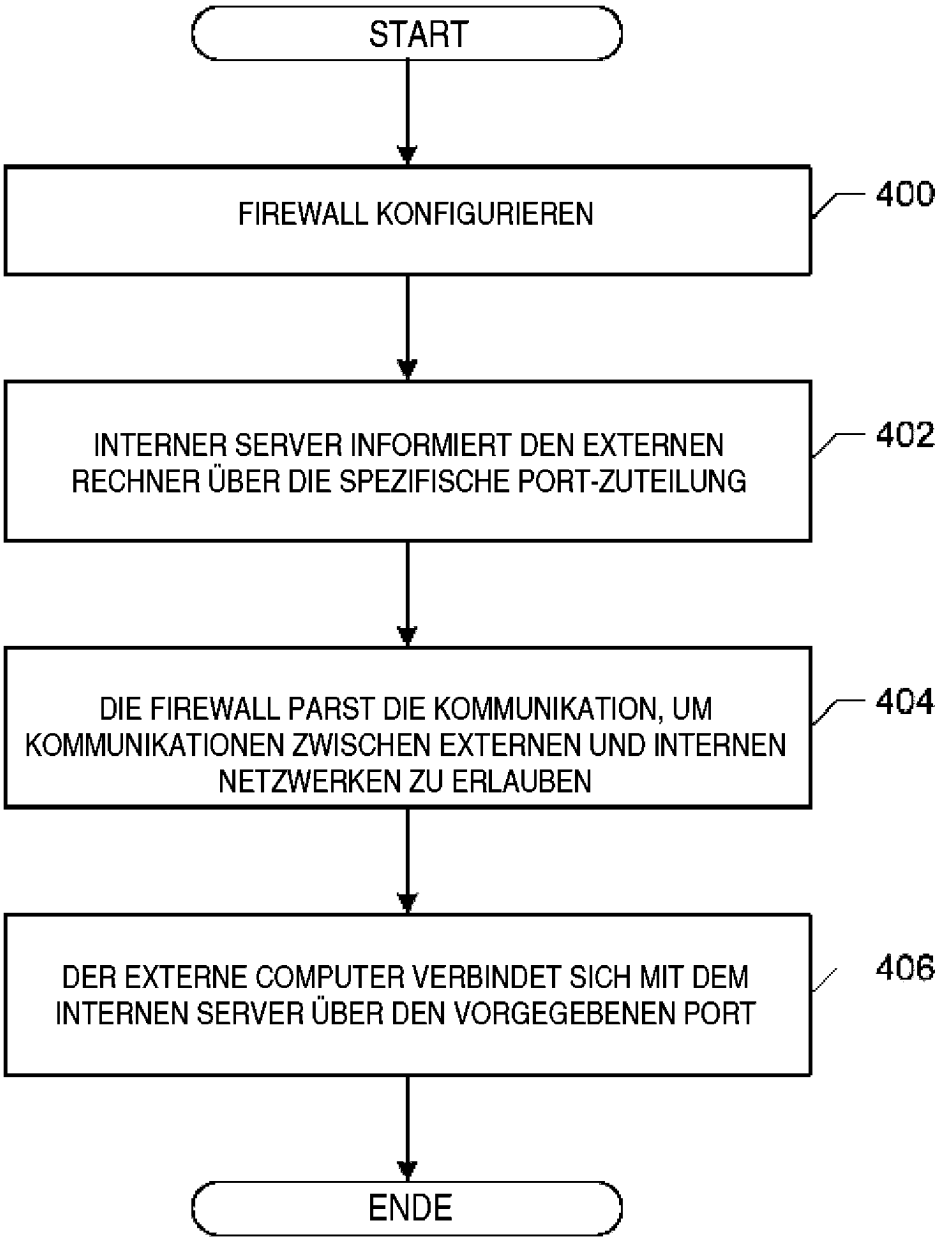

START
FIREWALL KONFIGURIEREN
400
INTERNER SERVER INFORMIERT DEN EXTERNEN RECHNER ÜBER DIE SPEZIFISCHE PORT-ZUTEILUNG
402
DIE FIREWALL PARST DIE KOMMUNIKATION, UM KOMMUNIKATIONEN ZWISCHEN EXTERNEN UND INTERNEN NETZWERKEN ZU ERLAUBEN
404
DER EXTERNE COMPUTER VERBINDET SICH MIT DEM INTERNEN SERVER ÜBER DEN VORGEGEBENEN PORT
406
ENDE

FIG. 4

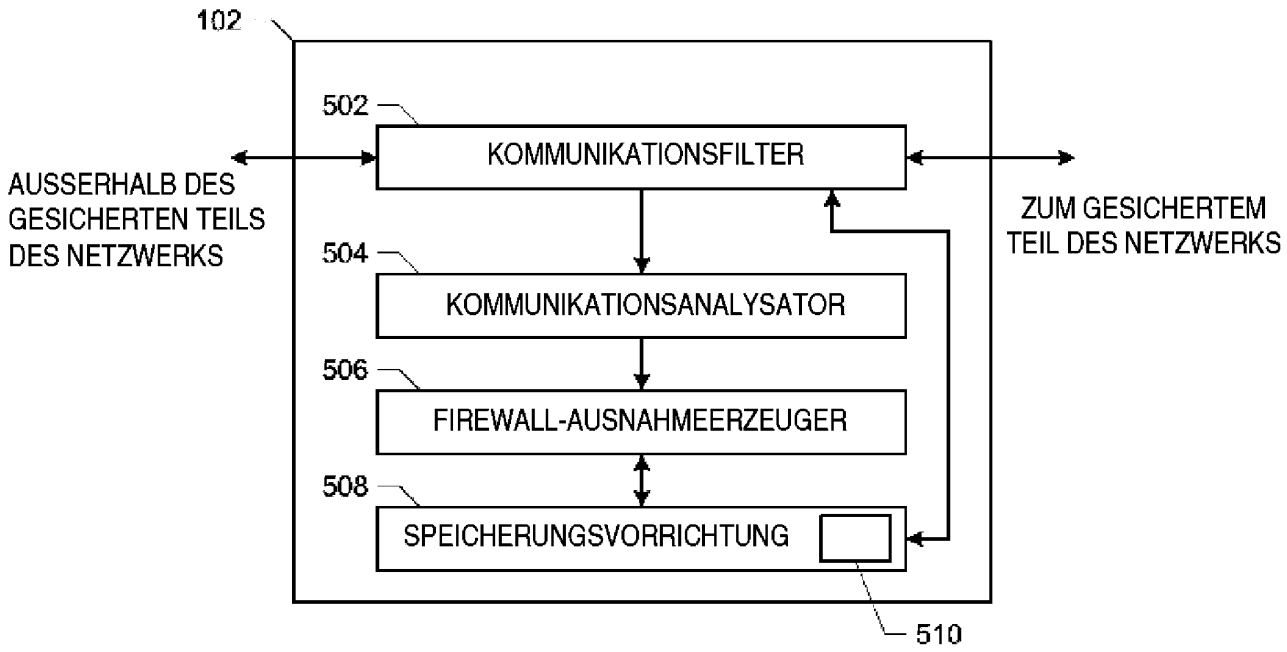

102
502
KOMMUNIKATIONSFILTER
AUSSERHALB DES GESICHERTEN TEILS DES NETZWERKS
ZUM GESICHERTEM TEIL DES NETZWERKS
504
KOMMUNIKATIONSANALYSATOR
506
FIREWALL-AUSNAHMEERZEUGER
508
SPEICHERUNGSVORRICHTUNG
510

FIG. 5

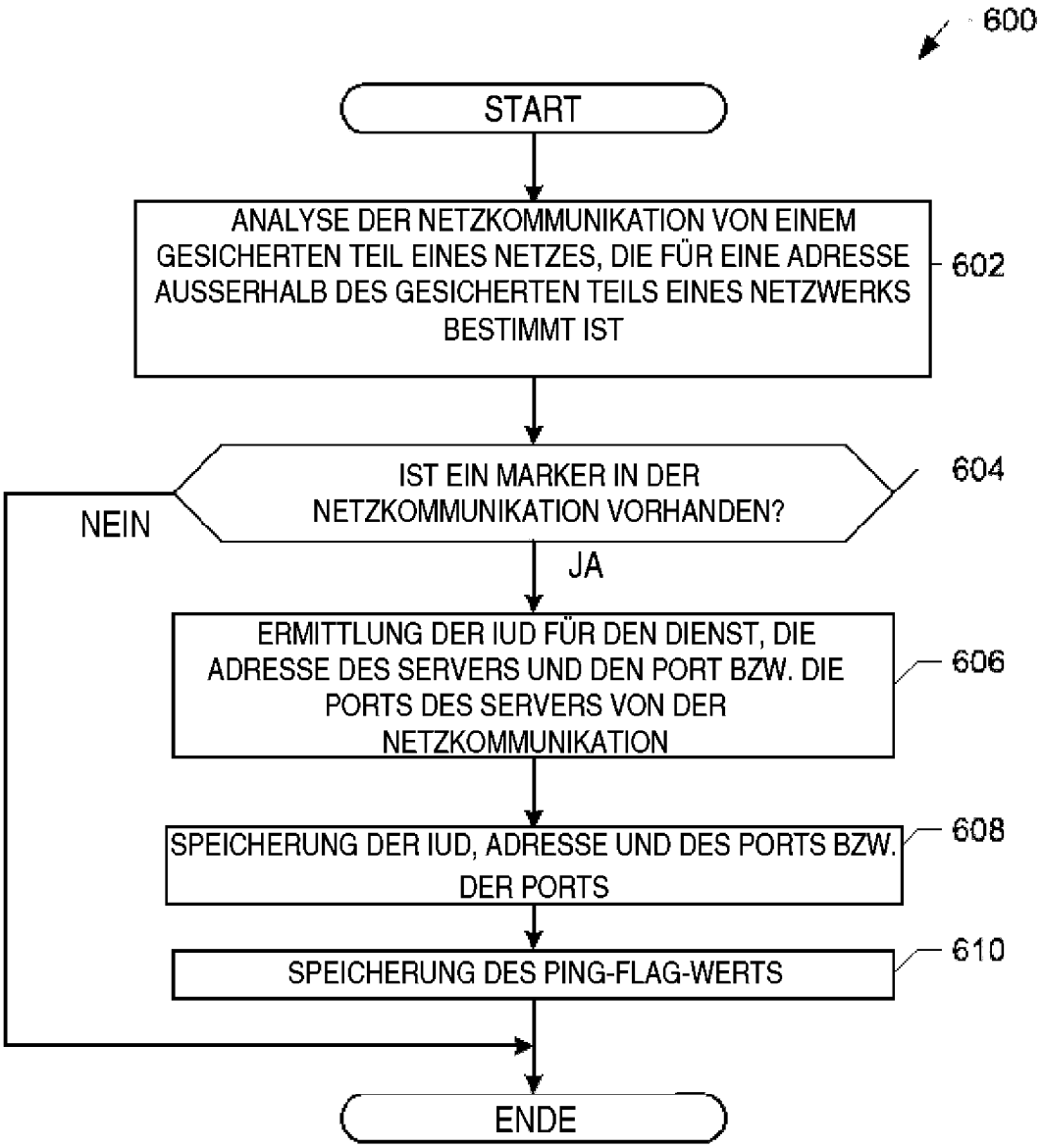

600
START
ANALYSE DER NETZKOMMUNIKATION VON EINEM GESICHERTEN TEIL EINES NETZES, DIE FÜR EINE ADRESSE AUSSERHALB DES GESICHERTEN TEILS EINES NETZWERKS BESTIMMT IST
602
IST EIN MARKER IN DER NETZKOMMUNIKATION VORHANDEN?
604
NEIN
JA
ERMITTLUNG DER IUD FÜR DEN DIENST, DIE ADRESSE DES SERVERS UND DEN PORT BZW. DIE PORTS DES SERVERS VON DER NETZKOMMUNIKATION
606
SPEICHERUNG DER IUD, ADRESSE UND DES PORTS BZW. DER PORTS
608
SPEICHERUNG DES PING-FLAG-WERTS
610
ENDE

FIG. 6

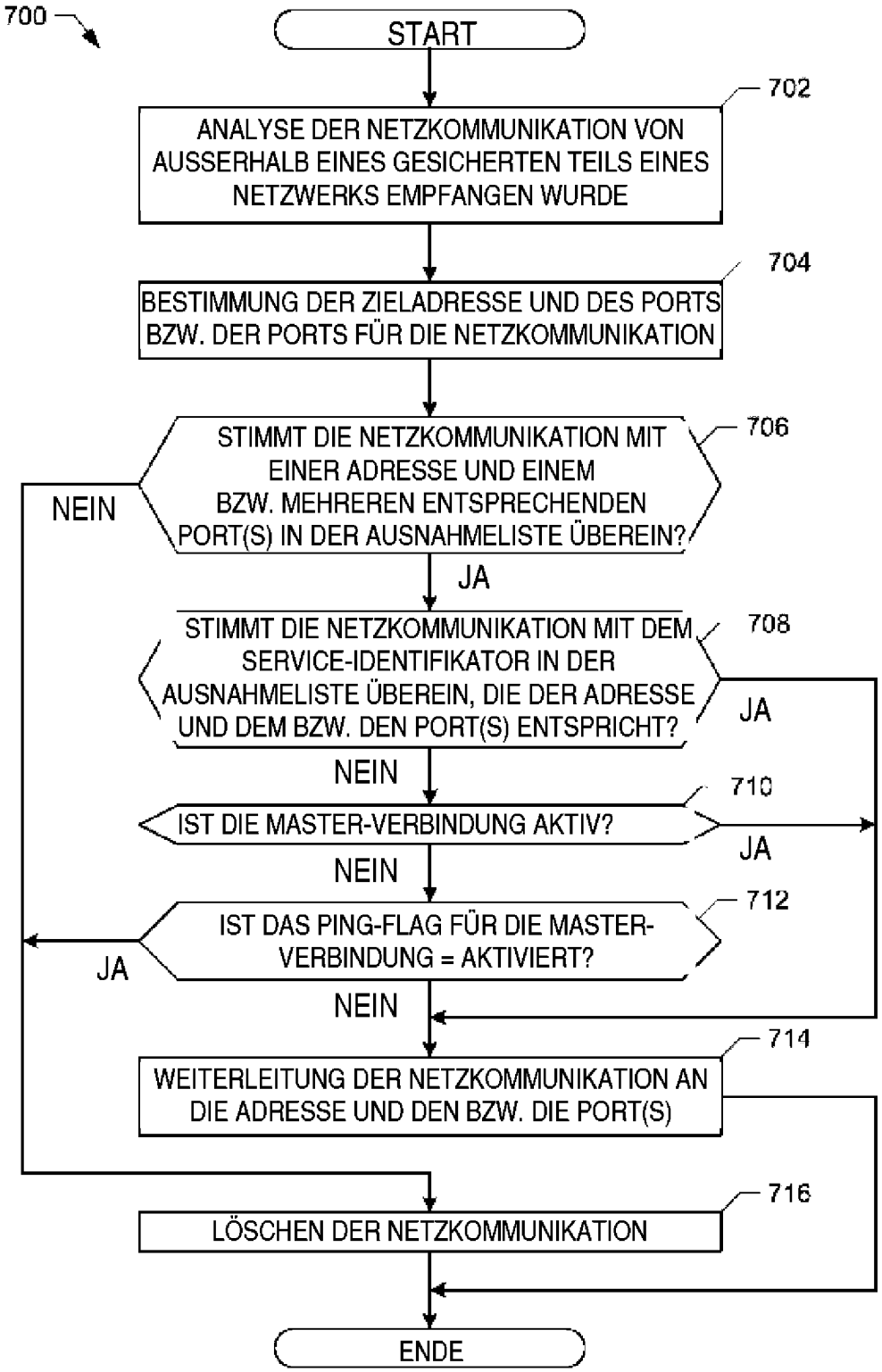

700
START
702
ANALYSE DER NETZKOMMUNIKATION VON AUSSERHALB EINES GESICHERTEN TEILS EINES NETZWERKS EMPFANGEN WURDE
704
BESTIMMUNG DER ZIELADRESSE UND DES PORTS BZW. DER PORTS FÜR DIE NETZKOMMUNIKATION
706
STIMMT DIE NETZKOMMUNIKATION MIT EINER ADRESSE UND EINEM BZW. MEHREREN ENTSPRECHENDEN PORT(S) IN DER AUSNAHMELISTE ÜBEREIN?
NEIN
JA
708
STIMMT DIE NETZKOMMUNIKATION MIT DEM SERVICE-IDENTIFIKATOR IN DER AUSNAHMELISTE ÜBEREIN, DIE DER ADRESSE UND DEM BZW. DEN PORT(S) ENTSPRICHT?
JA
NEIN
710
IST DIE MASTER-VERBINDUNG AKTIV?
JA
NEIN
712
IST DAS PING-FLAG FÜR DIE MASTER-VERBINDUNG = AKTIVIERT?
JA
NEIN
714
WEITERLEITUNG DER NETZKOMMUNIKATION AN DIE ADRESSE UND DEN BZW. DIE PORT(S)
716
LÖSCHEN DER NETZKOMMUNIKATION
ENDE

FIG. 7

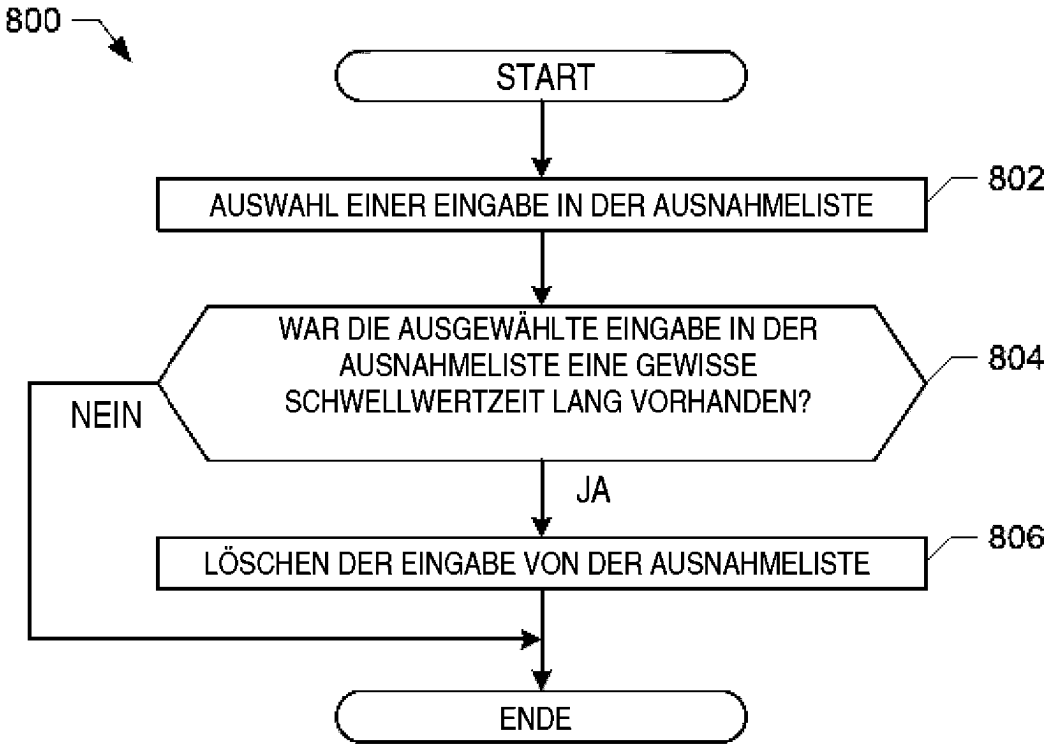

800
START
AUSWAHL EINER EINGABE IN DER AUSNAHMELISTE
802
WAR DIE AUSGEWÄHLTE EINGABE IN DER AUSNAHMELISTE EINE GEWISSE SCHWELLWERTZEIT LANG VORHANDEN?
804
NEIN
JA
LÖSCHEN DER EINGABE VON DER AUSNAHMELISTE
806
ENDE

FIG. 8

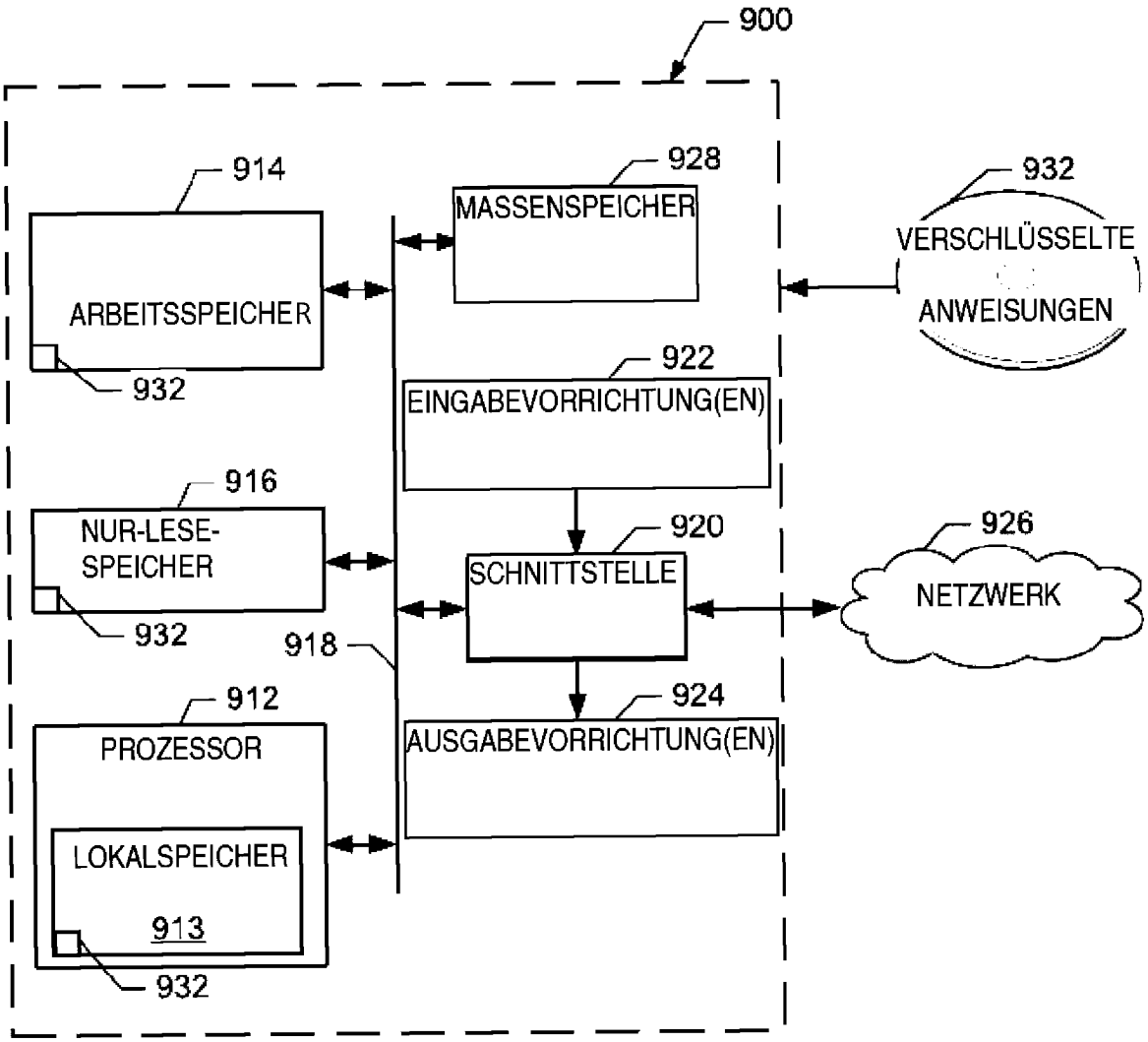


FIG. 9

