(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 697 20 351 T2** 2004.02.19

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 825 748 B1**
(21) Deutsches Aktenzeichen: **697 20 351.4**
(96) Europäisches Aktenzeichen: **97 304 968.7**
(96) Europäischer Anmeldetag: **08.07.1997**
(97) Erstveröffentlichung durch das EPA: **25.02.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **02.04.2003**
(47) Veröffentlichungstag im Patentblatt: **19.02.2004**

(51) Int Cl.[7]: **H04L 29/06**
H04L 29/12

(30) Unionspriorität:
679466 **15.07.1996** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
AT & T Corp., New York, N.Y., US

(74) Vertreter:
derzeit kein Vertreter bestellt

(72) Erfinder:
Bellovin, Steven Michael, Westfield, New Jersey 07090, US; Cheswick, Wiliam Robert, Bernardsville, New Jersey 07924, US

(54) Bezeichnung: **Verfahren und Vorrichtung zum Begrenzen des Zugriffes an privater Information in Domänennamensystemen durch Umleitung von Abfrageanforderungen**

Anmerkung: Innerhalb von neun Monaten nach der Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents kann jedermann beim Europäischen Patentamt gegen das erteilte europäische Patent Einspruch einlegen. Der Einspruch ist schriftlich einzureichen und zu begründen. Er gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist (Art. 99 (1) Europäisches Patentübereinkommen).

Die Übersetzung ist gemäß Artikel II § 3 Abs. 1 IntPatÜG 1991 vom Patentinhaber eingereicht worden. Sie wurde vom Deutschen Patent- und Markenamt inhaltlich nicht geprüft.

Beschreibung

HINTERGRUND DER ERFINDUNG

1. GEBIET DER ERFINDUNG

[0001] Diese Erfindung betriff das Einschränken eines Zugriffs auf private Information in Domänennamen-Systemen.

2. BESCHREIBUNG DES VERWANDTEN SACHSTANDS

[0002] Viele Vertriebs- bzw. Verteilungssysteme weisen in dem Vertriebs- bzw. Verteilungssystem Namen durch ein hierarchisches Benennungsverfahren zu, welches als Domänennamen bekannt ist. Verteilungssysteme, die Domänennamen verwenden, werden als Domänennamen-Systeme (Domain Name Systems, DNSs) bezeichnet. Ein Domänenname ist eine Sequenz von Domänennamen, die durch Punkte getrennt sind. Z. B. ist research.att.com ein Domänenname. Com ist ein Domänenname einer oberen Ebene (Top Level) einer Domäne einer oberen Ebene, att ist ein Domänenname einer zweiten Ebene (Second Level) einer Domäne einer zweiten Ebene und research ist ein Domänenname einer dritten Ebene einer Domäne einer dritten Ebene. Eine Einrichtung (Device) in einer Domäne wird durch den Namen der Einrichtung, die dem Domänennamen folgt, gekennzeichnet. Somit weist eine Einrichtung, die mit "Server" gekennzeichnet ist, in der research.att.com-Domäne den Namen server.research.att.com auf. Ein Einrichtungsname wird ebenfalls als ein Domänenname bezeichnet.

[0003] Während Domänennamen ein Verteilungssystem in einer logischen und hierarchischen Weise aufteilen, werden Nachrichten zwischen Einrichtungen des DNS durch Identifizieren von Einrichtungen unter Verwendung von IP-Adressen transferiert. IP-Adressen sind 32-Bit-Zahlen, die als vier 8-Bitwerte getrennt durch Punkte, wie 191.192.193.2, ausgedrückt werden. IP-Adressen enthalten Informationen, wie eine Netz-ID einer Einrichtungsnetzverbindung und eine Einrichtungs-ID. Die IP-Adressen werden durch eine Adressenautorität zugewiesen. Die Adressen werden in Blöcken autoritätssteuernden Adressenservern zugewiesen.

[0004] Ferner beziehen sich die IP-Adressen ebenfalls in einer hierarchischen Weise aufeinander. Jedoch beziehen sich die Domänennamenhierarchie und die IP-Adressenhierarchie nicht direkt aufeinander. Während einige Namenserver auch Adressenserver sind, müssen Namen- und Adressenserver nicht die gleiche Einrichtung sein. Somit ist es möglich, dass ein Server eine Autorität (Berechtigung) zum Auflösen eines Domänennamens in eine entsprechende IP-Adresse einer Einrichtung aufweist, der Server mit dem gleichen Namen aber nicht in der Lage sein kann, die IP-Adresse zu dem entsprechenden Domänermamen der gleichen Einrichtung aufzulösen. Somit folgt eine Auflösung von IP-Adressen zu Domänennamen einem ähnlichen Prozess wie der Auflösung von Domänennamen in IP-Adressen, außer dass andere Server daran beteiligt sein können.

[0005] Weil IP-Adressen numerisch sind und im Gegensatz zu einem Domänennamen ohne Zusammenhang zu der logischen und hierarchischen Organisation des DNS zugewiesen werden, werden Domänennamen im Allgemeinen in Befehlen für Funktionen für Datentransfer verwendet. Somit identifiziert ein Datentransferbefehl die Empfangseinrichtung durch deren Domänennamen. Jedoch muss der Domänenname in eine entsprechende IP-Adresse übersetzt werden, bevor der Datentransfer auftreten kann.

[0006] Domänennamen werden durch Prozess Autoritätseinrichtungen, die als Namenserver bezeichnet werden, verwaltet. Namenserver überietzen Domänennamen in entsprechende IP-Adressen und umgekehrt. Wenn eine erste Einrichtung eine Nachricht an eine zweite Einrichtung, die nur durch ihren Domänennamen bekannt ist, transferieren möchte, muss die erste Einrichtung einen Namenserver befragen, um die entsprechende IP-Adresse zu dem bekannten Domänennamen der zweiten Einrichtung zu ermitteln.

[0007] Wegen der potentiell großen Anzahl von IP-Adressen-Beüagungsaufforderungen, die die Effizienz des DNS stark verringern kann, sind viele Verfahren implementiert worden, um die Arbeitslast der Namensserver und den zugehörigen Netzverkehr zu verringern. Während diese Verfahren die Effizienz des DNS verbessern, führen sie jedoch auch Möglichkeiten ein, dass nicht autorisierte Aktivitäten einen nicht genehmigten bzw. nicht autorisierten Zugriff auf Information, die zu einer Domäne privat ist, oder ein Login in private Maschinen erhalten. Somit besteht eine Notwendigkeit für einen eingeschrärikten Zugriff auf private Information innerhalb eines DNS.

ZUSAMMENFASSUNG DER ERFINDUNG

[0008] Wie in "Firewalls and Internet Security" von W. R. Cheswick und S. R. Bellovin, April 1994, Addison-Wesley Publishing Company, offenbart, erhält ein Eindringling einen Zugriff auf Information, die zu einer Domäne privat ist, indem der Vorteil des Domänennamen-Auflösungsprozesses genutzt wird, der von DNSs verwendet wird. Weil Befehle für Funktionen, beispielsweise Datentransfers, Domänennamen verwenden, um

Zieleinrichtungen zu spezifizieren, müssen die Domänennamen in IP-Adressen übersetzt (aufgelöst) werden, bevor ein Datentransfer auftreten kann. Der Eindringling nutzt in vorteilhafter Weise den Prozess zum Auflösen von Domänennamen in IP-Adressen, um einen Zugriff auf private Information zu erhalten. Insbesondere übergibt der Eindringling zerstörte IP-Adressen und/oder Domänennamen an eine Zieldomäne, so dass normale Namenauflösungen die IP-Adresse der Einrichtung des Eindringlings anstelle einer beabsichtigten Zieleinrichtung erzeugt.

[0009] Die Erfindung verhindert, dass der Eindringling einen Zugriff auf private Information einer Domäne erhält, indem jegliche Möglichkeit beseitigt wird, dass eine Einrichtung innerhalb der Domäne private Information von einer Einrichtung, die extern zu der Domäne ist, empfängt. Insbesondere stellt die Erfindung eine DNS-Proxy-Einrichtung bereit, die eine Umschaltfunktion ausführt.

[0010] Die Umschaltfunktion empfangt Anfrageauffordezungen nach Domänennamenauflösungen von Einrichtungen innerhalb der Domäne und leitet irgendwelche Aufforderungen nach Domänennamen oder IP-Adressen von Einrichtungen innerhalb der Domäne an eine andere Einrichtung innerhalb der Domäne, beispielsweise einen Namenserver, um. Sämtliche Aufforderungen nach Information, die nicht privat für die Domäne sind, werden an die Zieleinrichtung, die extern zu der Domäne ist, weitergeleitet.

[0011] Insbesondere stellt ein erster Aspekt der Erfindung ein Untersystem in einem DNS bereit, das einen Zugriff auf private Information einer ersten Domäne einschränkt. Das Untersystem umfasst eine Umschalteinrichtung. Die Umschalteinrichtung empfängt sämtliche Aufforderungen nach Information von der ersten Domäne und leitet eine Aufforderung nach privater Information an Autoritätsquellen für die private Information in der ersten Domäne um. In einer ersten Ausführungsform werden sämtliche Aufforderungen, die an Einrichtungen in der zweiten Domäne gerichtet sind, nach Information, die nicht privat ist, an die Einrichtungen in der zweiten Domäne transferiert. Andere Aspekte und Merkmale der Erfindung sind in den übrigen Ansprüchen aufgeführt.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0012] Die Erfindung wird ausführlich unter Bezugnahme auf die beiliegenden Zeichnungen beschrieben, in denen die gleichen Bezugszeichen gleiche Elemente bezeichnen. In den Zeichnungen zeigen:

[0013] **Fig.** 1 ein Blockdiagramm eines Verteilungssystems;

[0014] **Fig.** 2 ein Diagramm, das eine Hierarchie von Domänennamen zeigt;

[0015] **Fig.** 3 ein Diagramm von hierarchischen Domänennamen, die in Domänen aufgetrennt sind;

[0016] **Fig.** 4 ein Diagramm der Domänen der **Fig.** 3 mit Einrichtungen, die IP-Adressen aufweisen;

[0017] **Fig.** 5 ein Diagramm einer Domäne, die Einrichtungen mit entsprechenden IP-Adressen aufweist;

[0018] **Fig.** 6 ein Diagramm der Domäne der **Fig.** 5 mit Einrichtungen, die miteinander und mit Einrichtungen außerhalb der Domäne kommunizieren;

[0019] **Fig.** 7 ein Diagramm der Domäne, die in **Fig.** 6 gezeigt ist, mit einer Firewall;

[0020] **Fig.** 8 ein Diagramm einer Umschalteinrichtung;

[0021] **Fig.** 9 ein Diagramm einer Filteningseinrichtung;

[0022] **Fig.** 10 ein Diagramm einer Domäne mit einer DNS-Proxy-Einrichtung;

[0023] **Fig.** 11 ein Diagramm einer Domäne mit einer DNS-Proxy-Einrichtung, die in eine Firewall eingebaut ist;

[0024] **Fig.** 12 ein Flussdiagramm eines Prozesses für die Umschalteinrichtung; und

[0025] **Fig.** 13 ein Flussdiagramm für einen Prozess der Filterungseinrichtung.

AUSFÜHRLICHE BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0026] **Fig.** 1 zeigt eine physikalische Verbindung für ein Verteilungssystem **20** mit einem Netz **10** und Einrichtungen **102**, **104** und **106**. Das Verteilungssystem **20** kann als ein Domänennamensystem (Domain Name System, DNS) **30** organisiert sein, wie in **Fig.** 2 gezeigt.

[0027] Das DNS **30** weist eine Wurzel **100** auf, die die Autorität der höchsten Ebene für Domänennamen in dem DNS **30** hält. Die Wurzel (root) kann Domänennamen wie edu, com und gov, die Ausbildungsinstitutionen, kommerzielle Institutionen bzw. Regierungsinstitutionen darstellen, zuweisen. Jede von diesen Domänen kann weiter in andere Domänen unterteilt werden, wie purdue.edu, att.com und nrl.gov. Die Wurzel **100** kann eine Namenautorität für Domänen an andere Einrichtungen delegieren, die als Autorisierungsnamenserver (Authoritative Name Servers) bekannt sind. Z. B. kann die Domäne att.com der AT&T Corp. gehören und kann von dieser gesteuert bzw. kontrolliert werden. Die AT&T Corp. kann Einrichtungen bestimmen, um Autorisierungsnamenserver zu sein, die eine Autorität (Genehmigung) aufweisen, Namen innerhalb der att.com-Domäne zuzuweisen und zu verwalten. Somit kann das gesamte DNS **30** in eine Vielzahl von Domänen aufgeteilt werden, wobei die benennende Autorität in jeder Domäne in Autorisieningsnamenserver dieser Domäne liegt.

[0028] Autorisierungsnamenserver können ihre Namenautorität an noch andere Server innerhalb ihrer Domäne delegieren. Z. B. kann die att.com-Domäne eine Einrichtung, die server.att.com genannt wird, als einen Au-

torisierungsnamen aufweisen, der eine Autorität für Domänennamen unter att.com aufweist. Att.com kann eine Unterdomäne aufweisen, die als research.att.com bezeichnet wird, und server.att.com kann die Namenautorität für die research.att.com-Unterdomäne an eine Einrichtung delegieren, die server.research.att.com genannt wird. Unterdomänen werden ebenfalls als Domänen bezeichnet. Somit weist server.research.att.com eine Namenautorität für Einrichtungsnamen in der research.att.com-Domäne, wie wsl.research.att.com für die Einrichtung **102** und ws2.research.att.com für die Einrichtung **104**, auf.

[0029] Server.buzbiz.com kann ein Autorisierungsnamenserver für die buzbiz.com-Domäne sein. Die buzbiz.com-Domäne kann eine Einrichtung wie eine Einrichtung **106** mit dem Namen intzu.buzbiz.com enthalten.

[0030] **Fig.** 3 zeigt das in die Domänen purdue.edu **202**, att.com **204**, buzbiz.com **206**, nrl.gov 208 und Wurzel **210** aufgeteilte DNS **30**. Die Wurzeldomäne **101** ist so dargestellt, dass sie die Domänen edu, com und gov enthält. Die Domänen edu, com und gov können durch den Wurzelnamenserver **100** an andere Autorisierungsnamenserver delegiert werden. Jedoch behält in diesem Fall ein einzelner Namenserver, Wurzel (root) **100**, die Autorität für Domänen edu, com und gov.

[0031] Wie voranstehend diskutiert, werden Daten zwischen den Einrichtungen **102**, **104** und **106** in dem DNS **30** durch Verwenden von IP-Adressen transferiert. **Fig.** 4 zeigt die IP-Adressen der Einrichtungen **102**, **104** und **106**. Um Daten von der Einrichtung **106** an die Einrichtung **102** zu transferieren, muss die Einrichtung **106** 192.193.194.1 als die Ziel-IP-Adresse spezifizieren.

[0032] Jede Einrichtung in dem DNS **30** weist wenigstens eine IP-Adresse auf. Wie in **Fig.** 5 gezeigt, umfasst die Domäne **204** Einrichtungen **102**, **104**, **I08** und **110**. Jede der obigen Einrichtungen weist einen Domänennamen und eine IP-Adresse auf. Server.research.att.com ist der Name der Einrichtung **110** mit der IP-Adresse von 192.203.194.3 und server.research.att.com ist ein Autorisierungsnamenserver für die research.att.com-Domäne **210**. Die research.att.com-Domäne **210** umfasst Einrichtungen **102** und **104** mit IP-Adressen **192**.193.194.1 bzw. 192.193.194.2.

[0033] Weil jede Einrichtung in dem DNS **30** einen Domänennamen und eine IP-Adresse aufweist, können zwei Übersetzungstabellen konstruiert werden, siehe z. B. die nachstehende Tabelle 1 und die Tabelle 2. Die Tabelle 1 mit Domänennamen weist für jeden Domänennamen eine entsprechende IP-Adresse auf und die Tabelle 2 mit IP-Adressen weist für jede IP-Adresse einen entsprechenden Domänennamen auf. Wenn die Tabelle 1 nach dem Domänennamen sortiert wird und die Tabelle 2 nach den IP-Adressen sortiert wird, kann die Tabelle 1 verwendet werden, um schnell die IP-Adresse für einen Domänennamen zu bestimmen und die Tabelle 2 kann verwendet werden, um schnell den Domänennamen für eine IP-Adresse zu bestimmen. Jeder Namenserver enthält Tabellen, die der Tabelle 1 und der Tabelle 2 entsprechen, für sämtliche Einrichtungen, für die er eine Namenautorität aufweist. Weil Autorisierungsnamenserver diese Information enthalten, senden andere Einrichtungen get-address(Adresse-holen)- und get-name-(Namen-holen)-Aufforderungen an die Autorisierungsnamenserver, um IP-Adressen von Domänennamen bzw. Domänennamen von IP-Adressen unter deren Autorirät bereitzustellen.

Tabelle 1

att.com	128.129.130.1
research.att.com	192.203.194.3
ws1.research.att.com	192.193.194.1
ws2.research.att.com	192.193.194.2

Tabelle 2

128.129.130.1	att.com
192.193.194.1	ws1.research.att.com
192.193.194.2	ws2.research.att.com
192.203.194.3	research.att.com

[0034] Wenn eine erste Einrichtung einen Befehl zum Senden von Daten an eine zweite Einrichtung, die durch ihren Domänennamen bekannt ist, empfängt, sendet die erste Einrichtung eine Anfageaufforderung an einen Autorisierungsnamenserver der zweiten Einrichtung für die IP-Adresse der zweiten Einrichtung. Der Autorisierungsnamenserver gibt entweder die angeforderte Information zurück oder, wenn die Namenautorität delegiert worden ist, gibt der Autorisierungsnamenserver den Namen eines anderen Autorisierungsnamenserven zurück, der die Information aufweist. Nach Ermitteln der IP-Adresse baut die erste Einrichtung die IP-Adresse in eine Nachricht ein, die die Daten enthält, und sendet die Nachricht an die zweite Einrichtung.

[0035] Nicht alle Namenserver haben eine Namenautorität. Manchmal enthalten Dateiserver Domänennamen und IP-Adressen, so dass Einrichtungen, die zu den Dateiservern lokal sind, einen einfachen Zugriff auf Namen von anderen lokalen Einrichtungen erhalten können. Diese Dateiserver werden auch als Namenserver oder Auflöser zum Auflösen von Domänennamen mit IP-Adressen und umgekehrt bezeichnet.

[0036] Wenn ein Namenserver (autorisierend oder nicht autorisierend) eine IP-Adresse, die durch den Namenserver nicht bekannt ist, weiterleitet, wird die IP-Adresse auch in dem Cachespeicher des Namenserver als eine Ressourcenaufzeichnung für eine zukünftige Auflösung des gleichen Domänennamens gespeichert.

Somit können Autorisierungsnameaserver auch IP-Adressen und entsprechende Domäneanamen sammeln, um eine effiziente Auflösung von Domänennamen in IP-Adressen und umgekehrt zu erleichtern. Somit werden Autorisieivngsnamenserver (Authoritative Name Server) auch als Auflöser (Resolver) zum Auflösen von Domänennamen bezeichnet.

[0037] In einem weiteren Versuch zum Verbessern der Effizienz des DNS **30** leiten Namenserver oft "zusätzliche Information", wie IP-Adressen von anderen im Zusammenhang stehenden Einrichtungen und deren Domänennamen durch Anhängen der zusätzlichen Information an Anfrageaufforderungsantworten weiter. Auflöser empfangen und speichern die zusätzliche Information in den Cachespeichern für zukünftige Adressenauflösungen.

[0038] **Fig.** 6 zeigt, dass die Domäne **204** ferner Auflöser **112** und **114** umfasst. Die Einrichtungen **102** und **104** senden Anfrageaufforderungen an Auflöser **112** und **114** über Kommunikationsleitungen **302** bzw. **308**, um Domänennamen in IP-Adressen aufzulösen. Die Auflöser **112** und **114** sind physikalisch jeweils nahe zu den Einrichtungen **102** und **104** angeordnet. Z. B. können die Auflöser **112** und **114** auf dem gleichen LAN oder in einem einzelnen Gebäude eng mit den Einrichtungen **102** bzw. **104** verbunden sein.

[0039] Somit kann eine Adressenauflösung, die von den Einrichtungen **102** und **I04** benötigt wird, ohne irgendeinen Netzverkehr über lokale LAN-Verbindungen hinaus ausgeführt werden.

[0040] Wenn jedoch die Auflöser **112** und **114** Domänennamen durch Empfangen von IP-Adressen, die nicht von einer Autorisierungsquelle erhalten werden, auflösen, werden die IP-Adressen an der anfragenden Einrichtung nicht als autorisierend empfangen. Oft entscheidet die anfragende Einrichtung, die IP-Adresse trotzdem zu verwenden, weil sich das DNS **30** im Allgemeinen nicht so schnell ändert.

[0041] Das DNS **30** verändert sich, weil z. B. Maschinen hinzugefügt, bewegt oder entfernt werden. In dieser dynamischen Situation umfasst jede der Ressourcenaufzeichnungen ein Lebensdauerfeld (Time-to-Live Feld), das die Lebensdauer jeder Ressourcenaufzeichnung andeutet. Die Auflöser **112** und **114** löschen Ressourcenaufzeichnungen periodisch, wenn der Lebensdauerwert der Ressourcenaufzeichnungen abläuft. Die Lebensdauerwerte werden von dem Namenserver gesetzt, der eine Autorisierung für die Inhalte der Ressourcenaufzeichnung, wie der IP-Adresse, aufweist.

[0042] Wie voranstehend diskutiert kann att.com eine Domäne sein, die der AT&T Corp. gehört und von dieser gesteuert bzw. kontrolliert wird. Somit sind sämtliche Einrichtungen, die von der AT&T Corp. gesteuert werden, innerhalb der att.com-Domäne. Die AT&T Corp. kann die Einrichtungen in der att.com-Domäne an Orte verteilen, die physikalisch getrennt voneinander sind. Z. B. kann die Einrichtung **102** und der Auflöser **112** an einem Ort angeordnet sein und die Einrichtung **104** und der Auflöser **114** können an einem anderen Ort angeordnet sein. Die Kommunikationspfade **302**, **304** und **308** stellen eine Interkommunikation zwischen Einrichtungen innerhalb der att.com-Domäne dar, obwohl ein Kommunikationspfad **304** zwischen zwei geographisch getrennten Orten vorhanden ist. Kommunikationspfade **310** und **312** stellen Kommunikationspfade zwischen den Auflösern **112** und **114** innerhalb der att.com-Domäne und Einrichtung von anderen Domänen dar.

[0043] Weil Information innerhalb der att.com-Domäne für die AT&T Corp. wertvoll sein kann, besteht ein großes Interesse, die Information, die für att.com als privat angesehen wird, vor einem nicht autorisierten Zugriff zu schützen. Eine private Information einer Domäne ist Infotmation, die etwas über diese Domäne beschreibt. Die Autorität zum Ändern der privaten Information liegt innerhalb der Domäne. Z. B. sind IP-Adressen und Domänennamen private Information innerhalb der Domäne.

[0044] Einrichtungen wie eine Firewall **402**, wie in **Fig.** 7 gezeigt, sind installiert, um Datentransfers in die Domäne **204** hinein und davon heraus zu steuern. Kommunikationspfade **310** und **312** gehen durch die Firewall **402**, bevor sie Einrichtungen innerhalb der Domäne **204** durch eine Kommunikationsleitung **316** erreichen. Die Firewall **402** verhindert einen nicht autorisierten Transfer von privater Information aus der Domäne **204** heraus und weist Aufforderungen von Einrichtungen, die zu der Domäne **204** extern sind, nach Information, die für die Domäne **204** privat ist, ab.

[0045] Jedoch verhindern einige herkömmliche Firewalls einen Zugriff auf private Information, die indirekt durch Ausnutzen von Namenauflösungsverfahren erhalten werden, die von Domänennamensystemen wie DNS **30** verwendet werden, nicht. Insbesondere kann der Prozess, mit dem Domänennamen in die entsprechenden IP-Adressen aufgelöst werden, durch ein oder mehrere Verfahren ausgenutzt werden. Einige von diesen Verfahren werden nachstehend beispielhaft erläutert.

[0046] Für den Zweck der folgenden Beispiele sein angenommen, dass ein Eindringling eine Zieleinrichtung, einen Benutzernamen zur persönlichen Identifikation und eine Einrichtung, der die Zieleinrichtung vertraut, so dass ein Kennwort für die vertraute Einrichtung zum Login an der Zieleinrichtung nicht erforderlich ist, identifiziert hat. Der Eindringling kann Zieleinrichtungen aus Posmachrichten (Mail-Nachrichten) oder Nachrichtenartikeln identifizieren. Sobald die Zieleinrichtung Identifiziert ist, kann der Eindringling standardmäßige Dienste wie ein einfaches Netzverwaltungsprotokoll (Simple Network Management Protocol, SNMP) verwenden, um die Zieleinrichtung zu untersuchen, um andere Einrichtungen zu entdecken, die mir der Zieleinrichtung verbunden sind. Zusätzlich stellen Dienste wie "Finger" ("finger") eine persönliche Information entweder über einen individuellen Benutzer oder andere Benutzer, die auf einem System eingeloggt haben, bereit. Ferner zeigen

Mail-Anfangsblöcke oft den Namen eines Dateiservers, der ein offensichtlicher Absender der Mail ist, und den Namen der tatsächlichen Einrichtung, die die Quelle der Mail ist, was typischerweise der Name einer Arbeitsstation (Work Station) ist, an. Im Allgemeinen kommunizieren Dateiserver und Work Stations, die von dem Dateiserver bedient werden, ohne die Verwendung von Passwörtern (Kennwörtern). Somit kann der Eindringling sämtliche benötigte Information unter Verwendung von standardmäßigen verfügbaren Diensten ermitteln.

[0047] Unter der Annahme, dass der Eindringling eine Kontrolle über einen legitimierten Namenserver wie intzu.buzbiz.com in der buzbiz.com-Domäne hat, weist der Eindringling die Fähigkeit auf, irgendwelche Dateien in intzu.buzbiz.com zu modifizieren. Wenn der Eindringling wsl.research.att.com als ein Ziel identifizien hat und auch ws2.research.att.com als eine Einrichtung identifiziert hat, der wsl.research.att.com vertraut, dann kann der Eindringling die Übersetzungstabelle, ähnlich wie Tabelle 2, die zum Umwandeln von IP-Adressen in entsprechende Domänennamen verwendet wird, modifizieren, so dass die IP-Adresse von intzu.buzbiz.com (201.202.203.1) dem Domänennamen ws2.research.att.com entspricht. Nach Modifizieren der Übersetzungstabelle versucht der Eindringling dann an wsl.research.att.com als eine vertraute Einrichtung unter Verwendung einer r-Login-Prozedur (rlogin) und unter Bereitstellung von 201.202.203.1 als die IP-Adresse von ws2.research.att.com einzuloggen.

[0048] Nach Empfangen der r-Login-Aufforderung führt wsl.research.att.com eine get-name-(Namenholen)-Aufforderung für die IP-Adresse 201.202.203.1 aus, um den entsprechenden Domänennamen zu ermitteln. Die get-name-Aufforderung wird schließlich an intzu.buzbiz.com gelenkt, weil intru.buzbiz.com der Autorisierungsadressenserver für die 201.202.203.1-IP-Adresse ist und die Tabelle zum Umwandeln von 201.202.203.1 in ihren entsprechenden Domänennamen aufweist. Weil jedoch die Tabelle modifiziert worden ist, um anstelle von intzu.buzbiz.com ws2.research.att.com im Ansprechen auf eine get-name-Aufforderung für die IP-Adresse 201.202.203.1 auszugeben, wird der fehlerhafte Domänennamen von ws2.research.att.com zurückgegeben. Somit empfängt wsl.research.att.com ws2.research.att.com als den Domänennamen der Einrichtung, die der r-Login-Aufforderung entspricht. Da ws2.research.att.com eine vertraute Maschine ist, akzeptiert wsl.research.att.com die r-Login-Aufforderung und erlaubt dem Eindringling an wsl.research.att.com einzuloggen. Demzufolge erwirbt der Eindringling einen Zugang bzw. Zugriff auf die gesamte private Information, die innerhalb von wsl.research.att.com erhältlich ist.

[0049] Eine andere Technik zum Ermitteln eines nicht autorisierten Zugriffs auf private Information besteht dann, den Cachespeicher eines Auflösers, beispielsweise des Auflösers **112**, zu vergiften bzw. zu verwirren. Unter der Annahme, dass der Eindringling wsl.research.att.com als ein Ziel identifiziert hat, leitet der Eindringling durch verschiedene Verfahren wsl.research.att.com ab, um intru.buzbiz.com nach Information zu befragen. Wsl.research.att.com sendet eine get-address-(Adresse-holen)-Aufforderung an den Auflöser **112** zum Ermitteln der IP-Adresse der eindringenden Einrichtung intru.buzbiz.com. Da der Auflöser **112** keinerlei Information bezüglich intzu.buzbiz.com aufweist, gibt er eine get-address-Aufforderung an einen Namenserver nach intru.buzbiz.com, was in diesem Fall intzu.buzbiz.com selbst ist, aus. Intru-buzbiz.com gibt die angeforderte IP-Adresse zurück, hängt aber zusätzliche Information an, die anzeigt, dass die IP-Adresse von ws2.research.att.com zu der IP-Adresse 201.202.203.1, anstelle zu der rechtmäßigen IP-Adresse 192.193.194.2, gehört. Der Eindringling setzt eine sehr kurze Lebensdauer für die zusätzliche Information, so dass der Auflöser **1I2** die zerstörte Ressourcenaufzeichnung sofort nachdem der Eindringling den nicht autorisierten Zugriff beendet, löschen wird. Der Auflöser akzeptiert die Antwort von intzu.buzbiz.com und gibt, wie voranstehend diskutiert, die IP-Adresse für intzu.buzbiz.com in seinen Cache sowie die falsche IP-Adresse **201**.202.203.1 für ws2.research.att.com ein. Somit wird der Cachespeicher des Auflösen **112** mit der falschen IP-Adresse für ws2.research.att.com vergiftet bzw. verstellt.

[0050] Danach führt intrv.buzbiz.com ein Login an ws l.research.att.com unter Verwendung von 201.202.203.1 als die IP-Adresse aus. Wenn wsl.research.att.com einen get-name-(Name-holen)-Befehl ausführt, gibt der Auflöser **112** ws2.research.att.com auf Grundlage der Information in seinem verstellten Cache zurück. wsl.research.att.com lässt dann die r-Login-Aufforderung von dem Eindringling zu, weil ws2.research.att.com eine vertraute Einrichtung ist. Weil dann die kurze Lebensdauer der Ressourcenaufzeichnung für die falsche IP-Adresse abläuft, löscht der Auflöser **112** die Ressourcenaufzeichnung, wobei jeglicher Nachweis der Eindringung gelöscht wird. Somit hat der Eindringling wiederum erfolgreich einen Zugriff auf sämtliche private Information innerhalb von wsl.research.att.com erfolgreich erhalten.

[0051] Der Eindringling ist nicht auf die Verwendung der r-Login-Prozedur, wie voranstehend beschrieben, eingeschränkt. Sobald die zerstörte bzw. falsche oder gefälschte IP-Adresse von dem Auflöser **112** oder wsl.research.att.com akzeptiert wird, kann der Eindringling z. B. wählen, jegliche Nachrichten abzufangen, die von wsl.research.att.com an ws2.research.att.com gesendet werden. Das Abfangen ist möglich, weil der Auflöser **112** anstelle der IP-Adresse von ws2.research.att.com die IP-Adresse zurückgibt, die intru.buzbir.com entspricht. Nach Empfangen der Ausgänge von wsl.research.att.com, vorgesehen für ws2.research.att.com, kann der Eindringling die Daten an ws2.research.att.com weiterleiten, so dass die Kommunikation zwischen wsl.research.att.com und ws2.research.att.com fortgesetzt wird ohne Modifikation. Somit kann der Eindringling private Information wie Passwörter abfangen, wobei nur eine geringe Möglichkeit besteht, dass er entdeckt

wird.

[0052] Der nicht autorisierte Zugriff auf private Information von dem Eindringling, wie voranstehend beschrieben, wird erreicht, weil Einrichtungen innerhalb der Domäne **204** eine IP-Adresse von anderen Einrichtungen in der Domäne **204** von einer unzuverlässigen Quelle, die extern zu der Domäne **204** ist, empfangen. Die vorliegende Erfindung verhindert, dass falsche private Information wie IP-Adressen eine Domäne betreten, indem verhindert wird, dass Kommunikationen auftreten, wie nachstehend diskutiert.

1) Die Erfindung verhindert, dass eine Einrichtung von innerhalb einer Domäne private Information von einer Einrichtung anfordert, die extern zu der Domäne ist. Wie in **Fig.** 8 gezeigt, empfangt eine Umschalteinrichtung **500** Anfragen **510** von get-name-(Name-holen)- oder get-address-(Adresseholen)-Aufforderungen. Die Umschalteinrichtung **500** durchsucht die Inhalte jeder Aufforderung und jegliche Aufforderung nach Namen oder IP-Adressen von Einrichtungen innerhalb der Domäne **204** wird an einen Namenserver, der zu der Domäne **204** intern ist, als umgeleitete Aufforderungen **514** umgeleitet. Aufforderungen nach Namen oder IP-Adressen von Einrichtungen außerhalb der Domäne **204** werden an den geeigneten Namenserver, der zu der Domäne **204** extern ist, als weitergeleitete Aufforderungen **512** weitergeleitet.

2) Eine Filtereinrichtung verhindert, dass private Information in die Domäne von einer unzuverlässigen Quelle, die extern zu der Domäne ist, eindringt. Die Filtereinrichtung filtert sämtliche private Information, die von Einrichtungen bereitgestellt werden, die extern zu der Domäne sind, heraus.

[0053] Wie in **Fig.** 9 gezeigt, empfangt die Filtereinrichtung **502** Nachrichten **520** von Einrichtungen, die zu der Domäne **204** extern sind. Die Filtereinrichtung **502** untersucht die empfangenen Nachrichten **520** nach irgendeiner Information, die für die Domäne **204** privat ist, beispielsweise nach IP-Adressen und Domänennamen, und löscht die private Information von den Nachrichten. Dann werden die gefilterten Nachrichten **522** an die Zieleinrichtungen in der Domäne **204** weitergeleitet.

[0054] **Fig.** 10 zeigt, dass die Domäne **204** eine DNS-Proxy-Einrichtung **404** einschließt. Der DNS-Proxy **404** führt die Umschalt- und Filterungsfunktionen, die voranstehend beschrieben wurden, aus. In dieser Ausführungsform werden die Einrichtungen innerhalb der Domäne **204** modifiziert, um sämtliche Anfragen an den DNS-Proxy **404** zu richten. Der DNS-Proxy **404** untersucht sämtliche Anfrageaufforderungen von Einrichtungen in der Domäne **204** und trennt Aufforderungen nach Information, die für die Domäne **204** privat ist, und Aufforderungen nach anderer Information. Aufforderungen von privater Information werden an Namenserver innerhalb der Domäne **204** umgeleitet, beispielsweise an server.att.com und server.research.att.com. Anfragen nach anderer Information als privater Information werden an die Firewall **402** durch einen Kommunikationspfad **328** weitergeleitet, der wiederum die Aufforderung an externe Quellen durch einen Kommunikationspfad **316** weiterleitet.

[0055] Die in **Fig.** 10 gezeigte Ausführungsform erfordert eine Modifikation der Software von Einrichtungen wie Auflöser **112** und **114** und der Einrichtung **116**, um Anfrageaufforderungen anstelle an einen geeigneten Namenserver, der extern zu der Domäne **204** ist, an den DMS-Proxy **404** umzuleiten. Die Einrichtung **116** ist nicht ein Namenserver, sondern weist die Fälhigkeit auf, mit externen Quellen direkt durch den Komunikationspfad **322** zu kommunizieren. Diese Ausführungsform leitet die Kommunikationspfade **318**, **320** und **322** an den DNS-Proxy **404** um.

[0056] Information, die von externen Quellen durch den Kommunikationspfad **330** empfangen wird, wird von dem DNS-Proxy **404** gefiltert. Der DNS-Proxy **404** untersucht sämtliche Information, die in die Domäne **204** eintritt, und filtert jegliche Information heraus, die für die Domäne **204** privat ist, beispielsweise IP-Adressen von Einrichtungen innerhalb der Domäne **204**. Die private Information, die in der Information enthalten ist, die von den externen Quellen zugeführt wird, wird gelöscht, bevor die Information an die Zieleinrichtung innerhalb der Domäne **204** weitergeleitet wird. Somit werden jegliche Versuche, falsche IP-Adressen an richtige Antworten auf Anfrageaufforderungen anzuhängen, beseitigt.

[0057] Information, die von den externen Quellen durch den Kommunikationspfad **330** empfangen wird, kann ebenfalls wegen lokaler Sicherheitsverwaltungsstrategien gelöscht oder modifiziert werden. Wenn z. B. die Information, die von den externen Quellen empfangen wird, Verweise (Pointer) auf Namenserver außerhalb der Domäne **204** einschließt, müssen die Verweise gelöscht werden, bevor die Information an eine Zieleinrichtung innerhalb der Domäne **204** weitergeleitet wird. Ansonsten können Einrichtungen innerhalb der Domäne **204** versuchen, diese Namenserver direkt ohne die Intervention des DNS-Proxy **404** zu kontaktieren. Im Gegensatz dazu können Verweise auf Namenserver innerhalb der Domäne **204** in die Information eingefügt werden, die von externen Quellen empfangen wird, so dass weitere Namen- oder Adressen-Anfragen intern zu der Domäne **204** direkt aufgelöst werden können, nämlich ohne die Hilfe des DNS-Proxys **404**.

[0058] Ferner kann Information wie Aufzeichnungen des Austauschs von elektronischer Post (Electronic Mail), die von den externen Quellen empfangen werden, modifiziert werden, um nach außen gerichtete elektronische Mail an eine Erfassungseinrichtung (nicht gezeigt) innerhalb der Domäne **204** umzuleiten, um eine Log-Aufzeichnung zu führen. Die Log-Aufzeichnung stellt zusätzliche Information bereit, um den Schutz von privater Information innerhalb der Domäne **204** zu unterstützen.

[0059] **Fig.** 11 zeigt, dass der DNS-Proxy **404** in die Firewall **402** eingebaut ist. In dieser Ausführungsform müssen keinerlei Programme der Einrichtungen innerhalb der Domäne **204** modifiziert werden. Sämtliche Anfrageaufforderungen werden weiter an externe Quellen durch Kommunikationspfade **310**, **3l2** und **322** gerichtet. Jedoch schaltet der DNS-Proxy innerhalb der Firewall **402** sämtliche Anfrageaufforderungen nach privater Information der Domäne **204** beispielsweise entweder an server.att.com oder server.research.att.com durch Kommunikationspfade **324** bzw. 326. Information, die von externen Quellen durch Kommunikationspfade **322** eingegeben wird, wird gefiltert, um irgendwelche private Information zu löschen, bevor sie an die Zieleinrichtungen innerhalb der Domäne **204** weitergeleitet wird.
[0060] **Fig.** 12 zeigt einen Prozess des DNS-Proxy **404**, der die Umschaltfunktion ausführt. Im Schritt **S1000** empfängt der DNS-Proxy **404** Anfrageaufforderungen, die an Einrichtungen extern zu der Domäne **204** gerichtet sind, und geht zum Schritt **S1002**. Im Schritt **1002** untersucht der DNS-Proxy **404** jede Anfrageaufforderung, um zu bestimmen, ob von den Einrichtungen, die extern zu der Domäne **204** sind, private Information abgerufen wird. Dann geht der DNS-Proxy **404** zum Schritt **S1004**. Im Schritt **S1004** geht der DNS-Proxy **404** zum Schritt **S1006**, wenn private Information angefordert wurde; ansonsten geht der DNS-Proxy **404** zum Schritt **S1010**.
[0061] Im Schritt **S1006** trennt der DNS-Proxy **404** Anfragen nach privater Information der Domäne **204** von Anfragen nach Information, die für die Domäne **204** nicht privat ist. Dann geht der DNS-Proxy **404** zum Shritt **S1008**. Im Shritt **S1008** leitet der DNS-Proxy **404** sämtliche Aufforderungen nach privater Information an eine Einrichtung innerhalb der Domäne **204**, beispielsweise an einen Namenserver der Domäne **204**. Dann geht der DNS-Proxy zum Shritt **S1010**.
[0062] Im Shritt **S1010** leitet der DNS-Proxy **404** sämtliche Aufforderungen nach Information, die für die Domäne **204** nicht privat ist, an die Einrichtung, die zu der Domäne **204** extern ist. Dann geht der DNS-Proxy **404** zum Schritt **S1012** und beendet den Prozess.
[0063] **Fig.** 13 zeigt den Prozess des DNS-Proxy **404** zum Filtern einer Kommunikation, die von einer Einrichtung empfangen wird, die extern zu der Domäne **204** ist. Im Schritt **S2000** empfängt der DNS-Proxy **404** die Kommunikation von der externen Einrichtung und geht zum Schritt **S2002**. In **S2002** untersucht der DNS-Proxy **404** die Kommunikation nach privater Information und geht zum Shritt **S2004**. Im Schritt **S2004** geht der DNS-Proxy **404** zum Shritt **52006**, wenn eine private Information in der Kommunikation von der externen Einrichtung entdeckt wurde, ansonsten geht der DNS-Proxy **404** zum Schritt **S2008**.
[0064] Im Schritt **S2006** filtert der DNS-Proxy **404** die Kommunikation durch Entfernen von sämtlicher privater Information von der Kommunikation und geht zum Schritt S2008. Im Schritt **S2008** leitet der DNS-Proxy **404** die gefilterte Kommunikation an die Zieleinrichtung innerhalb der Domäne **204**, geht zum Schritt **S2010** und beendet den Prozess.
[0065] Während diese Erfindung im Zusamenhang mit spezifischen Ausführungsformen davon beschrieben worden ist, ist offensichtlich, dass Durchschnittsfachleuten in dem technischen Gebiet viele Alternativen, Modifikationen und Variationen ersichtlich sein werden. Demzufolge sind die bevorzugten Ausführungsformen der Erfindung, wie hier aufgeführt, dafür vorgesehen, um illustrativ und nicht einschränkend zu sein. Verschiedene Änderungen können an den voranstehend beschriebenen bevorzugten Ausführungsformen durchgeführt werden, ohne von dem Umfang der Erfindungen, wie in den folgenden Ansprüchen definiert, abzuweichen.

Patentansprüche

1. Untersystem für ein Domänennamensystem, welches einen Zugriff auf private Information einer ersten Domäne (**204**) einschränkt, wobei die erste Domäne mit einer zweiten Domäne gekoppelt ist, wobei das Untersystem umfasst:
eine Schalteinrichtung (**404**), die dafür ausgelegt ist, um eine Kommunikation von einer ersten Einrichtung (**112**, **114**, **116**) der ersten Domäne (**204**) zu empfangen, wobei die Schalteinrichtung dafür ausgelegt ist, um zu untersuchen, ob die Kommunikation eine erste Aufforderung nach privater Information der ersten Domäne, gerichtet an eine Einrichtung der zweiten Domäne, einschließt, wobei die Schalteinrichtung (**404**) dafür ausgelegt ist, um die erste Aufforderung nach der privaten Information der ersten Domäne an eine zweite Einrichtung (**108**, **110**) in der ersten Domäne umzuleiten, wenn die Kommunikation die erste Aufforderung nach privater Information der ersten Domäne einschließt.

2. Untersystem nach Anspruch i, wobei die Kommunikation eine zweite Aufforderung nach Information, die nicht private Information der ersten Einrichtung (**204**) ist, einschließt, wobei die Schalteinrichtung dafür ausgelegt ist, um die zweite Aufforderung an die Einrichtung der zweiten Domäne weiterzuleiten.

3. Untersystem nach Anspruch 1, wobei die zweite Einrichtung (**108**, **110**) ein Namenserver der ersten Domäne ist.

4. Untersystem nach Anspruch 1, wobei die private Information der ersten Domäne ein Domänenname einer Einrichtung in der ersten Domäne (**204**) und/oder eine IP-Adresse der Einrichtung in der ersten Domäne ist.

5. Untersystem nach Anspruch 1, wobei die erste Domäne eine Vielzahl von Einrichtungen (**112**, **114**, **116**) umfasst, wobei die Vielzahl von Einrichtungen modifiziert sind, um sämtliche Kommunikation mit der zweiten Domäne an die Schalteinrichtung (**404**) zu richten.

6. Untersystem nach Anspruch 1, wobei die erste Einrichtung ein Namenserver oder ein Auflöser ist, wobei Aufforderungen nach Information von anderen Einrichtungen in der ersten Domäne als der ersten Einrichtung in der Verwendung an die erste Einrichtung gerichtet werden.

7. Untersystem nach Anspruch 1, wobei die Schalteinrichtung (**404**) Teil einer Firewall (**402**) der ersten Domäne ist.

8. Untersystem nach Anspruch 1, wobei die zweite Einrichtung (**108**, **110**) in der ersten Domäne in der Lage ist, die private Information der ersten Domäne bereitzustellen.

9. Verfahren zum Betrieb eines Untersystems in einem Domänennamensystem zum Einschränken eines Zugriffs auf eine private Information einer ersten Domäne (**204**), wobei die erste Domäne (**204**) mit einer zweiten Domäne gekoppelt ist, wobei das Verfahren die folgenden Schritte umfasst:
Empfangen (**S1000**) einer Kommunikation von einer ersten Einrichtung (**112**, **114**, **116**) der ersten Domäne, die an eine Einrichtung der zweiten Domäne gerichtet wird, wobei die Kommunikation eine erste Aufforderung nach privater Information der ersten Domäne einschließt; und
Umleiten (**S1008**) der ersten Aufforderung nach der privaten Information der ersten Domäne an eine zweite Einrichtung (**108**, **110**) der ersten Domäne.

10. Verfahren nach Anspruch 9, ferner umfassend die folgenden Schritte:
Weiterleiten (**S1010**) einer zweiten Aufforderung der Kommunikation von der ersten Einrichtung an die Einrichtung der zweiten Domäne, wobei die zweite Aufforderung Information anfordert, die für die erste Domäne nicht privat ist.

11. Verfahren nach Anspruch 9, wobei die zweite Einrichtung (**108**, **110**) ein Namenserver der ersten Domäne ist.

12. Verfahren nach Anspruch 9, wobei die private Information ein Domänenname und/oder eine IP-Adresse der ersten Domäne ist.

13. Vorrichtung zur Verwendung in einem Domänennamensystem, wobei die Vorrichtung umfasst:
eine Schalteinrichtung (**404**), die dafür ausgelegt ist, um eine Kommunikation von einer ersten Einrichtung (**112**, **114**, **116**) einer ersten Domäne (**204**) zu empfangen, wobei die Schalteinrichtung dafür ausgelegt ist, um zu untersuchen, ob die Kommunikation eine erste Aufforderung nach privater Information der ersten Domäne (**204**) umfasst, und an eine Einrichtung einer zweiten Domäne gerichtet ist, wobei die Schalteinrichtung dafür ausgelegt ist, um die erste Aufforderung nach privater Information der ersten Domäne an eine zweite Einrichtung (**108**, **110**) in der ersten Domäne umzuleiten, wenn die Kommunikation die erste Aufforderung nach privater Information der ersten Domäne einschließt.

14. Vorrichtung nach Anspruch 13, wobei die Kommunikation eine zweite Aufforderung nach Information einschließt, die nicht private Information der ersten Domäne (**204**) ist, wobei die Schalteinrichtung (**404**) dafür ausgelegt ist, um die zweite Aufforderung an die Einrichtung der zweiten Domäne weiterzuleiten.

15. Vorrichtung nach Anspruch 13, wobei die zweite Einrichtung (**108**, **110**) ein Namenserver der ersten Domäne ist.

16. Vorrichtung nach Anspruch 13, wobei die private Information der ersten Domäne ein Domänenname einer Einrichtung in der ersten Domäne und/oder eine IP-Adresse der Einrichtung in der ersten Domäne ist.

17. Vorrichtung nach Anspruch 13, wobei die Schalteinrichtung (**404**) Teil einer Firewall (**402**) der ersten Domäne (**204**) ist.

18. Verfahren zum Betrieb einer Vorrichtung in einem Domänennamensystem zum Einschränken eines

Zugriffs auf private Information einer ersten Domäne (**204**), wobei die erste Domäne (**204**) mit einer zweiten Domäne gekoppelt ist, wobei das Verfahren die folgenden Shritte umfasst:
Empfangen (**S1000**) einer Kommunikation von einer ersten Einrichtung (**112**, **114**, **116**) der ersten Domäne, die an eine Einrichtung der zweiten Domäne gerichtet wird, wobei die Kommunikation eine erste Aufforderung nach privater Information der ersten Domäne einschließt; und
Umleiten (**S1008**) der ersten Aufforderung nach privater Information der ersten Domäne an eine zweite Einrichtung (**108**, **110**) der ersten Domäne.

19. Verfahren nach Anspruch 18, ferner umfassend den folgenden Schritt:
Weiterleiten einer zweiten Aufforderung der Kommunikation von der ersten Einrichtung (**112**, **114**, **116**) an die Einrichtung der zweiten Domäne, wobei die zweite Aufforderung Information anfordert, die für die erste Domäne nicht privat ist.

20. Verfahren nach Anspruch **18**, wobei die zweite Einrichtung ein Namenserver der ersten Domäne ist.

21. Verfahren nach Anspruch 18, wobei die prvate Information der ersten Domäne ein Domänenname und/oder eine IP-Adresse der ersten Domäne ist.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

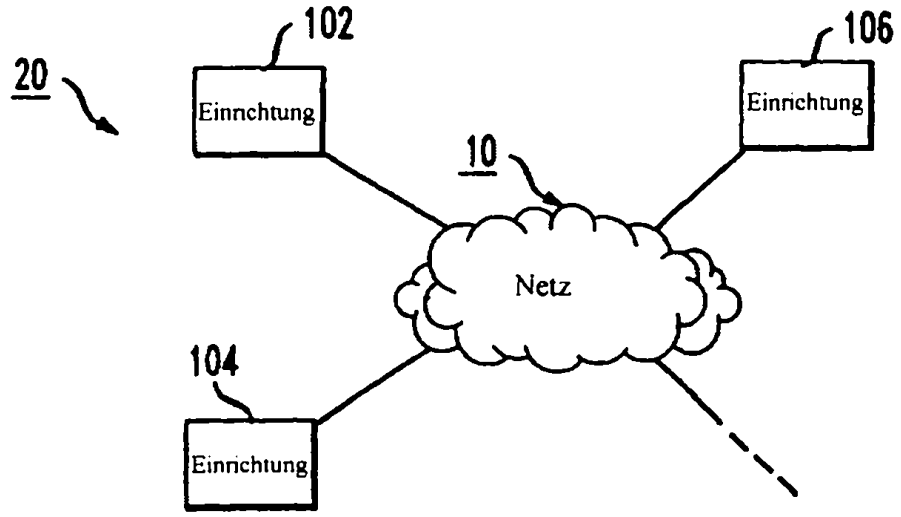


FIG. 2

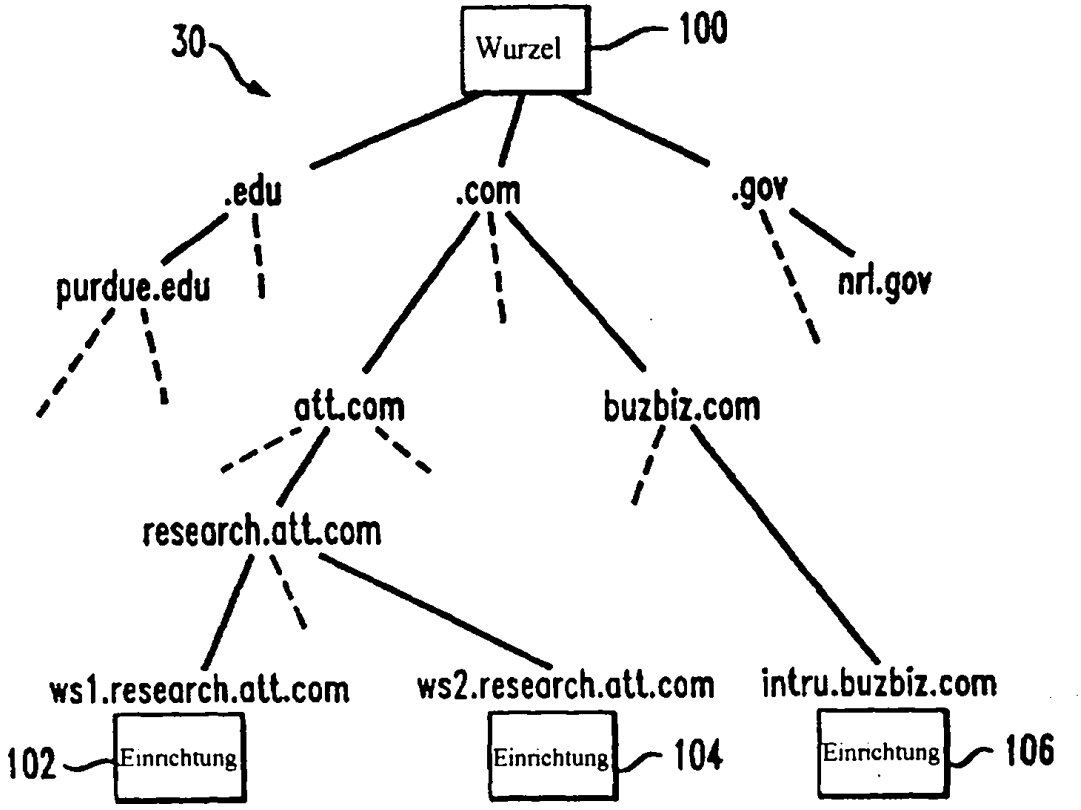


FIG. 3

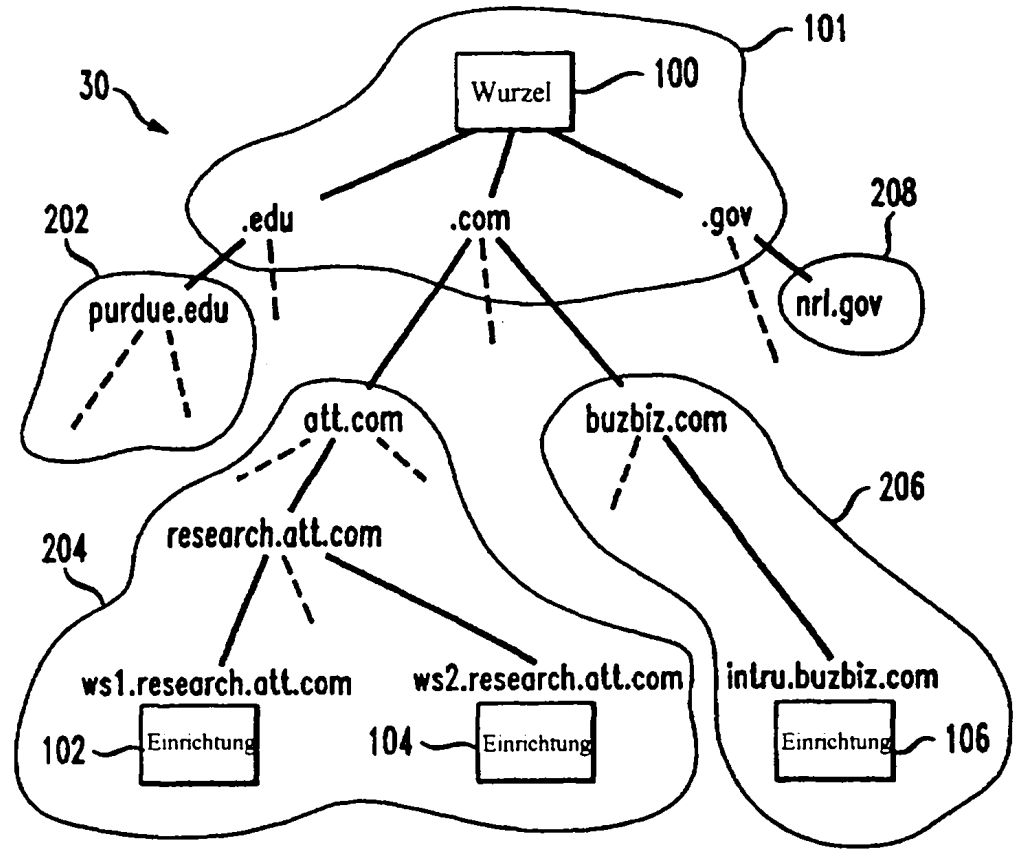

101
30
Wurzel
100
202
.edu
.com
.gov
208
purdue.edu
nrl.gov
att.com
buzbiz.com
206
204
research.att.com
ws1.research.att.com
ws2.research.att.com
intru.buzbiz.com
102
Einrichtung
104
Einrichtung
Einrichtung
106

FIG. 4

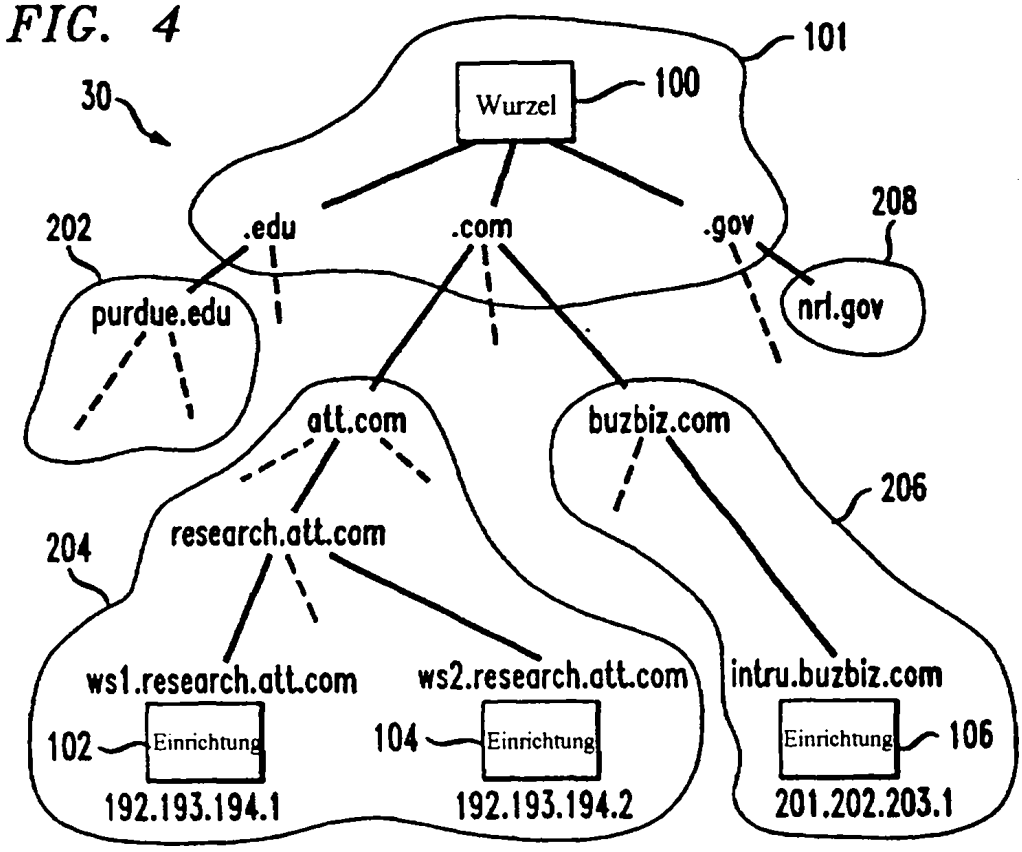

101
30
Wurzel
100
202
.edu
.com
.gov
208
purdue.edu
nrl.gov
att.com
buzbiz.com
206
204
research.att.com
ws1.research.att.com
ws2.research.att.com
intru.buzbiz.com
102
Einrichtung
104
Einrichtung
Einrichtung
106
192.193.194.1
192.193.194.2
201.202.203.1

FIG. 5

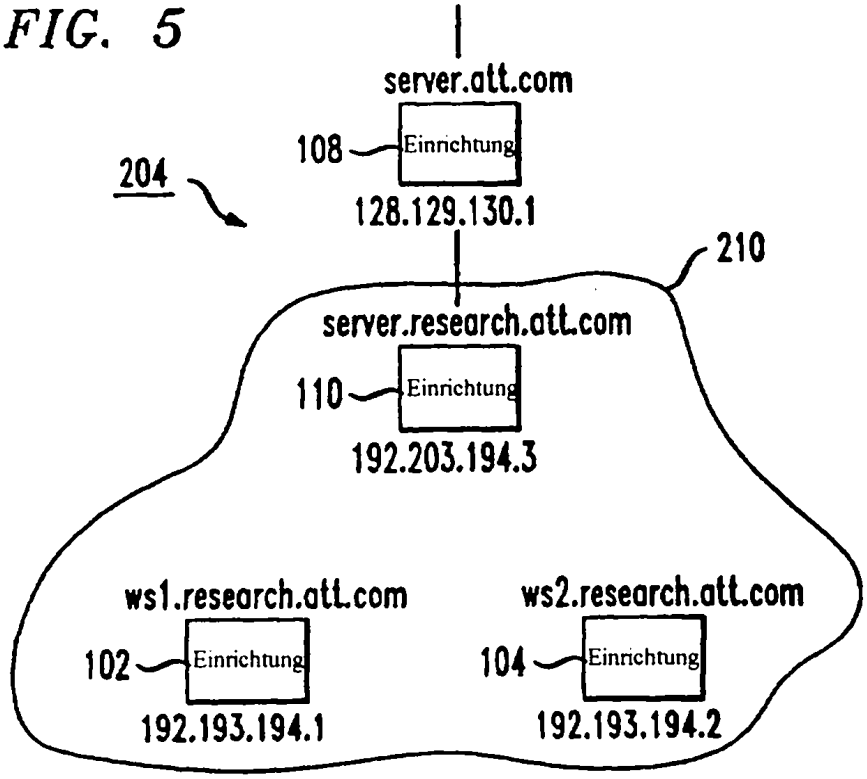

server.att.com
108
Einrichtung
204
128.129.130.1
210
server.research.att.com
110
Einrichtung
192.203.194.3
ws1.research.att.com
102
Einrichtung
192.193.194.1
ws2.research.att.com
104
Einrichtung
192.193.194.2

FIG. 6

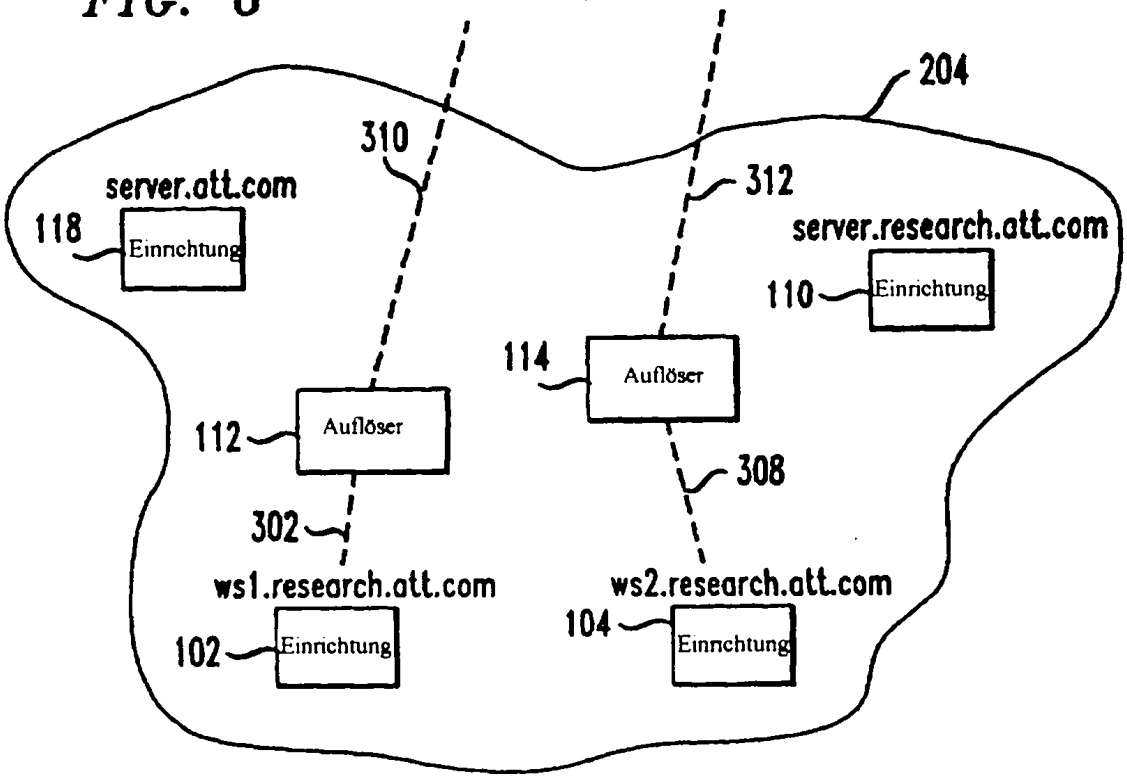

204
310
312
server.att.com
118
Einrichtung
server.research.att.com
110
Einrichtung
114
Auflöser
112
Auflöser
308
302
ws1.research.att.com
102
Einrichtung
ws2.research.att.com
104
Einrichtung

FIG. 7

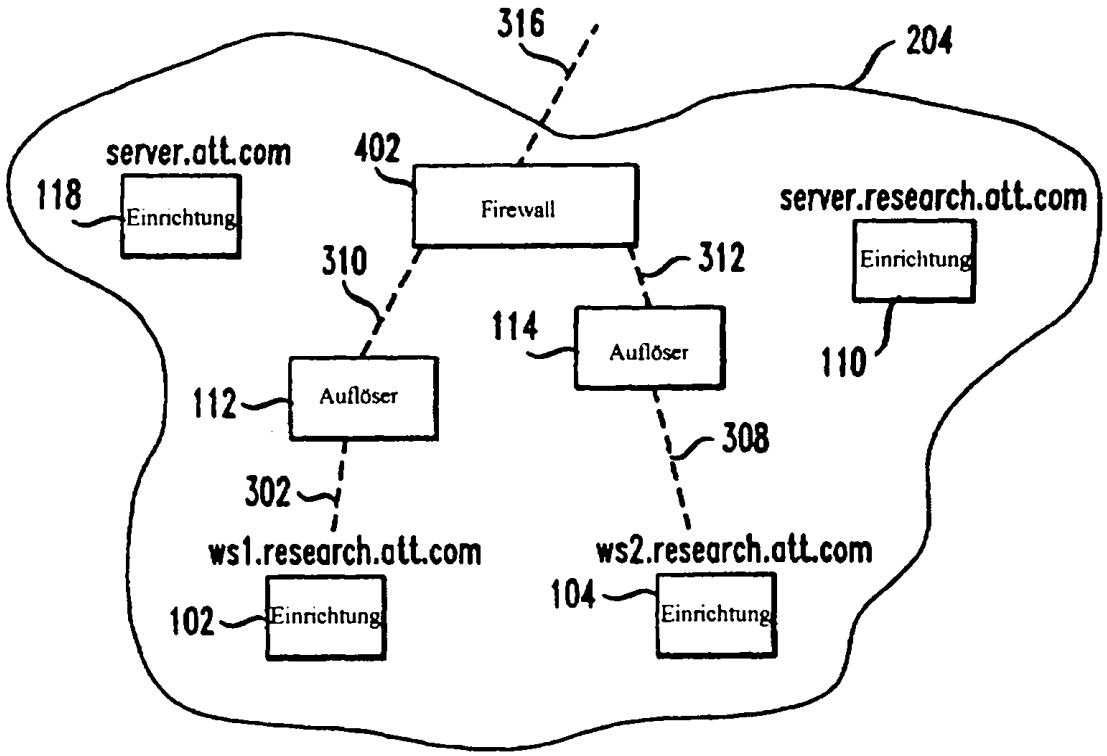


FIG. 8

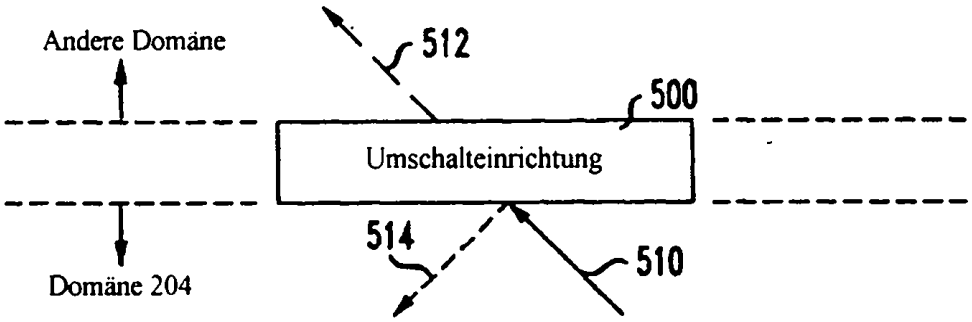


FIG. 9

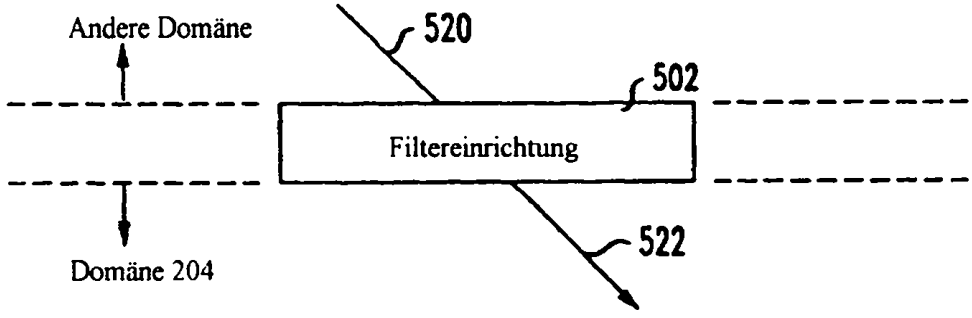


FIG. 10

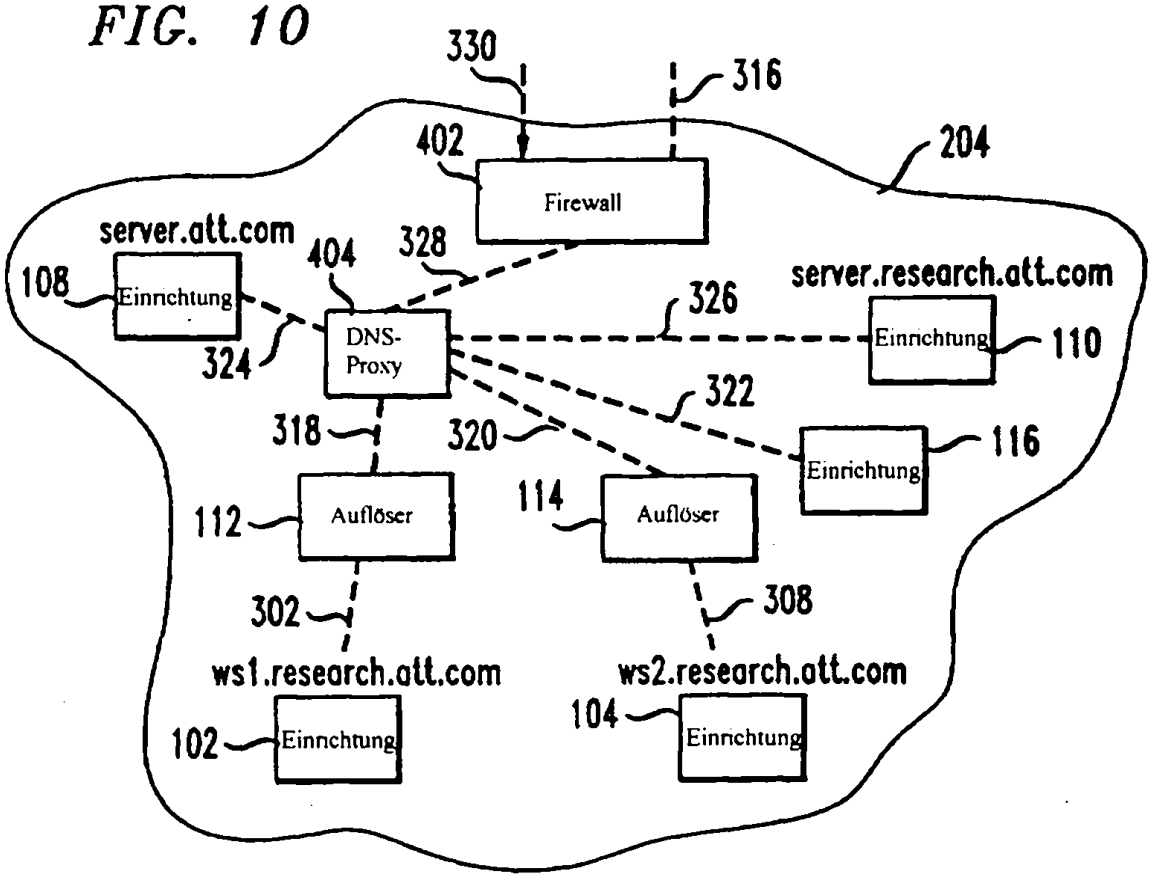

330
316
402
204
Firewall
server.att.com
404
328
108
Einrichtung
server.research.att.com
326
DNS-
Proxy
Einrichtung
110
324
322
318
320
Einrichtung
116
112
Auflöser
114
Auflöser
302
308
ws1.research.att.com
ws2.research.att.com
102
Einrichtung
104
Einrichtung

FIG. 11

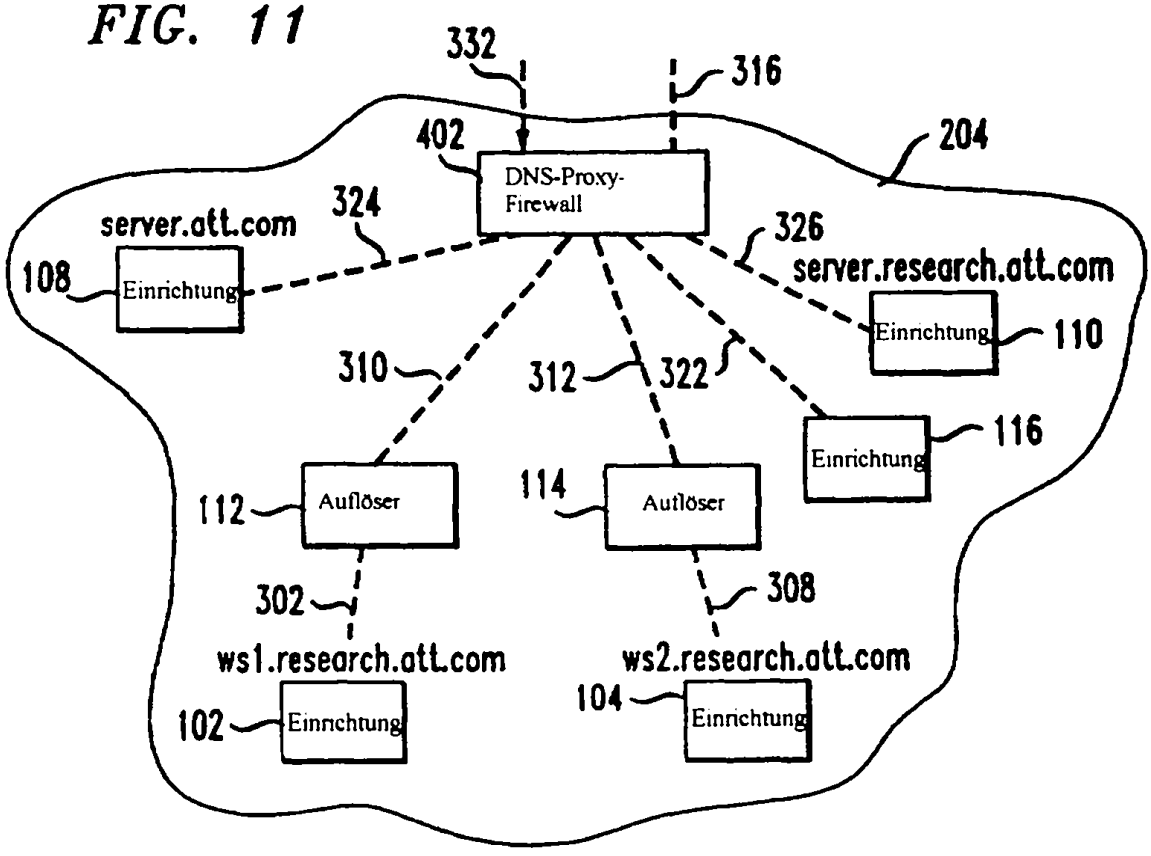

332
316
402
204
DNS-Proxy-
Firewall
server.att.com
324
326
108
Einrichtung
server.research.att.com
Einrichtung
110
310
312
322
Einrichtung
116
112
Auflöser
114
Auflöser
302
308
ws1.research.att.com
ws2.research.att.com
102
Einrichtung
104
Einrichtung

FIG. 12

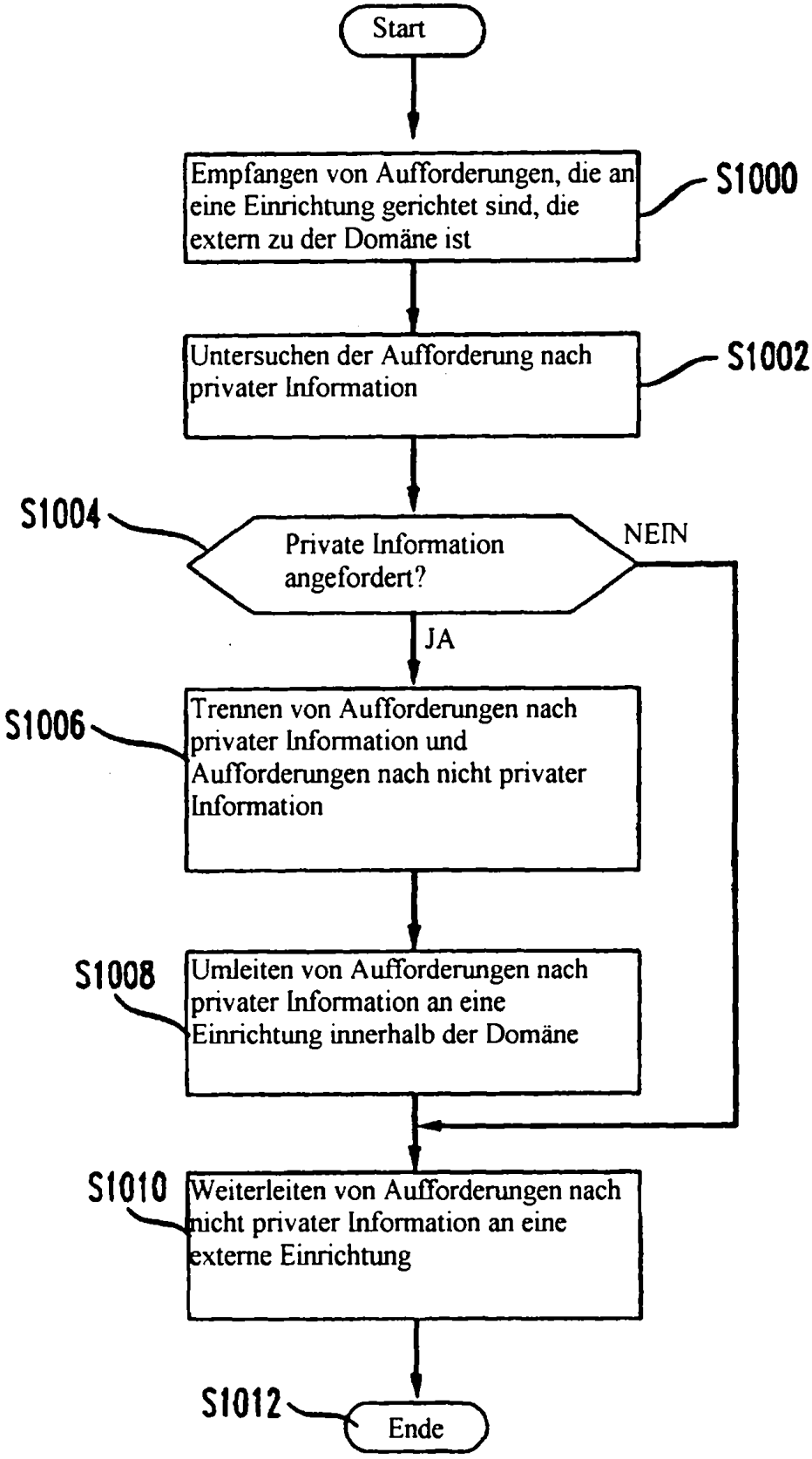
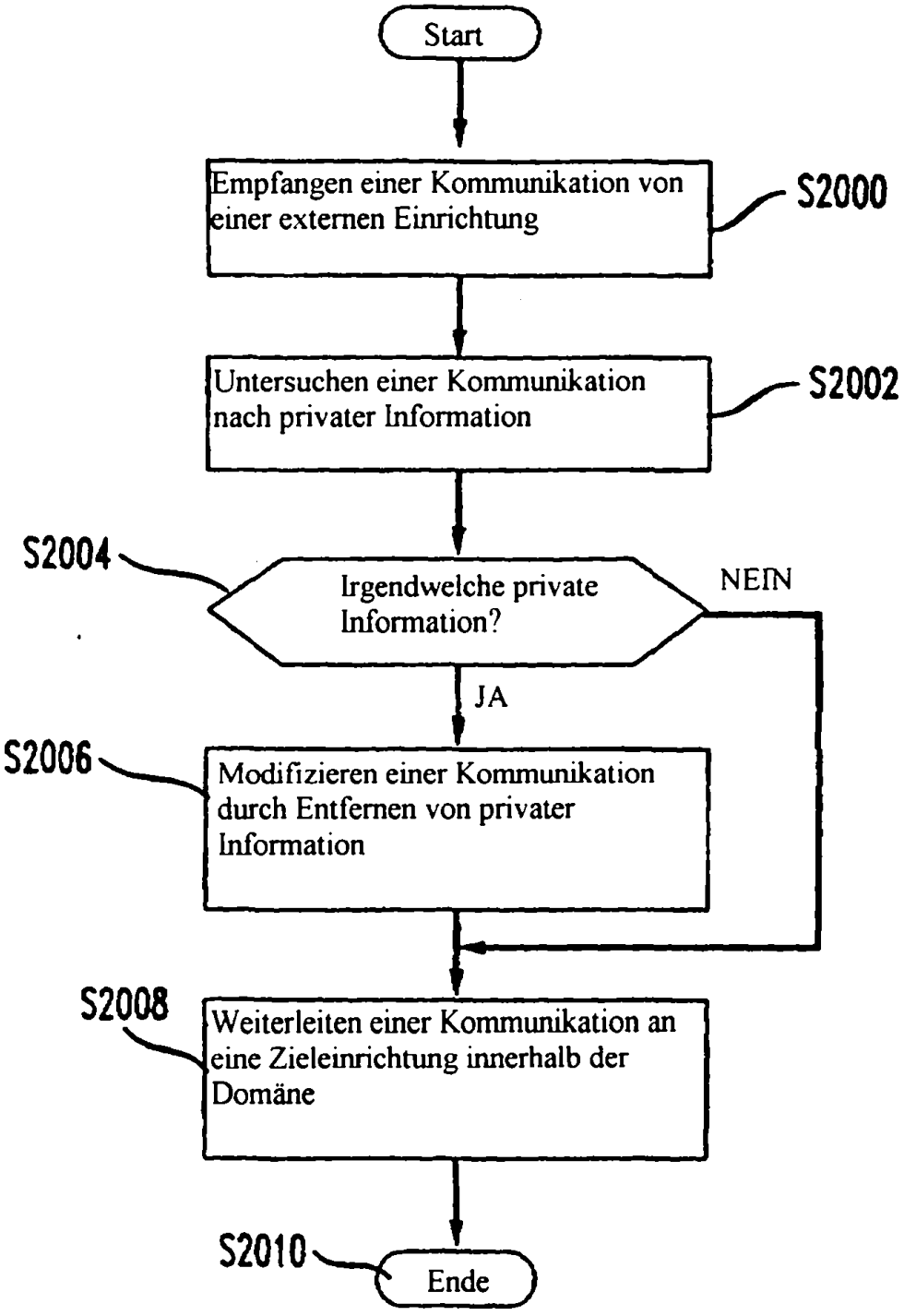

Start
Empfangen von Aufforderungen, die an eine Einrichtung gerichtet sind, die extern zu der Domäne ist
S1000
Untersuchen der Aufforderung nach privater Information
S1002
S1004
Private Information angefordert?
NEIN
JA
S1006
Trennen von Aufforderungen nach privater Information und Aufforderungen nach nicht privater Information
S1008
Umleiten von Aufforderungen nach privater Information an eine Einrichtung innerhalb der Domäne
S1010
Weiterleiten von Aufforderungen nach nicht privater Information an eine externe Einrichtung
S1012
Ende

FIG. 13


Start
Empfangen einer Kommunikation von einer externen Einrichtung
S2000
Untersuchen einer Kommunikation nach privater Information
S2002
S2004
Irgendwelche private Information?
NEIN
JA
S2006
Modifizieren einer Kommunikation durch Entfernen von privater Information
S2008
Weiterleiten einer Kommunikation an eine Zieleinrichtung innerhalb der Domäne
S2010
Ende