(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
21. Januar 2016 (21.01.2016)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2016/008889 A1

(51) Internationale Patentklassifikation:
H04L 29/06 (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2015/066072

(22) Internationales Anmeldedatum:
14. Juli 2015 (14.07.2015)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2014 109 906.0 15. Juli 2014 (15.07.2014) DE

(71) Anmelder: **FUJITSU TECHNOLOGY SOLUTIONS INTELLECTUAL PROPERTY GMBH** [DE/DE]; Mies-van-der-Rohe-Str. 8, 80807 München (DE).

(72) Erfinder: **CLAES, Heinz-Josef**; Ostheimerstr. 27b, 61130 Nidderau (DE).

(74) Anwalt: **EPPING HERMANN FISCHER PATENTANWALTSGESELLSCHAFT MBH**; Schloßschmidstr. 5, 80639 München (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

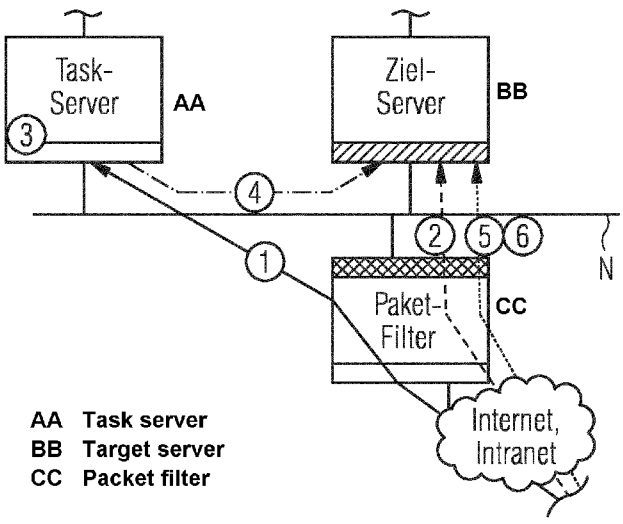
Veröffentlicht:

— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

(54) Title: METHOD FOR UNBLOCKING EXTERNAL COMPUTER SYSTEMS IN A COMPUTER NETWORK INFRASTRUCTURE, DISTRIBUTED COMPUTING NETWORK WITH A COMPUTER NETWORK INFRASTRUCTURE OF THIS TYPE, AND COMPUTER PROGRAM PRODUCT

(54) Bezeichnung : VERFAHREN ZUM FREISCHALTEN EXTERNER COMPUTERSYSTEME IN EINER COMPUTERNETZ-INFRASTRUKTUR, VERTEILTES RECHNERNETZ MIT EINER SOLCHEN COMPUTERNETZ-INFRASTRUKTUR SOWIE COMPUTERPROGRAMM-PRODUKT

FIG 1



(57) Abstract: The invention relates to a method for unblocking external computer systems for communication with secured processing computer systems in a computer network infrastructure. An authentication packet is transmitted from an external computer system to a switching computer system within the computer network infrastructure. The authentication packet contains signed information for authenticating the external computer system and/or the user thereof. In addition, the authentication packet is transmitted by the switching computer system to at least one processing computer system within the computer network infrastructure. The processing computer system keeps specific network ports closed, at least temporarily, so that an access to the network via this network port is prevented, wherein the processing computer system can, however, access the switching computer system in order to pick up the authentication packet from the switching computer system. An unblocking of a selective network port is subsequently carried out by the processing computer system and an establishment of a link to the processing computer system by the external computer system.

(57) Zusammenfassung:

[Fortsetzung auf der nächsten Seite]

WO 2016/008889 A1

Die Erfindung betrifft ein Verfahren zum Freischalten externer Computersysteme für eine Kommunikation mit abgesicherten Bearbeitungs-Computersystemen in einer Computernetz-Infrastruktur. Es wird ein Authentifizierungs-Paket von einem externen Computersystem an ein Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur übertragen. Das Authentifizierungs-Paket enthält signierte Informationen zur Authentifizierung des externen Computersystems und/oder seines Benutzers. Ferner wird das Authentifizierungs-Paket vom Vermittlungs-Computersystem an zumindest ein Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur übertragen. Das Bearbeitungs-Computersystem hält zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen, so dass ein Zugriff über Netzwerk vermittels dieser Netzwerk-Ports verhindert wird, wobei jedoch das Bearbeitungs-Computersystem auf das Vermittlungs-Computersystem zugreifen kann, um das Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen. Anschließend erfolgt ein Freischalten eines selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem und ein Aufbauen einer Verbindung zum Bearbeitungs-Computersystem durch das externe Computersystem.

Beschreibung

Verfahren zum Freischalten externer Computersysteme in einer Computernetz-Infrastruktur, verteiltes Rechnernetz mit einer solchen Computernetz-Infrastruktur sowie Computerprogramm-Produkt

Die Erfindung betrifft ein Verfahren zum Freischalten externer Computersysteme für eine Kommunikation mit abgesicherten Bearbeitungs-Computersystemen in einer Computernetz-Infrastruktur, ein verteiltes Rechnernetz mit einer Computernetz-Infrastruktur und zumindest einem externen Computersystem, sowie ein Computerprogramm-Produkt zur Durchführung eines entsprechenden Verfahrens.

Verteilte Rechnernetze beschreiben eine Mehrzahl von Computersystemen, die über Datenverbindungen in Computernetz-Infrastrukturen organisiert miteinander kommunizieren können. Anwendung finden verteilte Rechnernetze beispielsweise in Computernetz-Infrastrukturen, welche Server-Client-Topologien umfassen, wobei zum Teil vertrauliche Daten, z. B. Kundendaten oder Benutzerdaten, zwischen einem Client und einem Server ausgetauscht werden und wobei ein Zugriff Dritter auf diese Daten unterbunden werden muss.

In abgesicherten Computernetz-Infrastrukturen sind Bearbeitungs-Computersysteme, auf denen (vertrauliche) Daten verarbeitet werden, speziell abgesichert. Beispielsweise können vorbestimmte Netzwerk-Ports der Bearbeitungs-Computersysteme zunächst geschlossen sein, so dass über Netzwerk ein Zugriff beziehungsweise Verbindungsaufbau zu einem jeweiligen Bearbeitungs-Computersystem nicht möglich ist.

Herkömmliche Lösungen sehen hier vor, vorbestimmte Anklopf-Signale über Netzwerk an ein Bearbeitungs-Computersystem mit derart geschlossenen Netzwerk-Ports zu senden (so genanntes Port-Knocking), wobei eine vorbestimmte Daten-Sequenz vorbestimmte Netzwerk-Ports des Bearbeitungs-Computersystems anspricht. Diese Daten-Sequenz wird mit einer vorbestimmten Sequenz im Bearbeitungs-Computersystem verglichen, wobei das Bearbeitungs-Computersystem im Erfolgsfall einen oder mehrere Netzwerk-Ports öffnet, um einen Verbindungsaufbau von außen über Netzwerk zu erlauben.

Eine Gefahr dieser Maßnahmen besteht darin, dass ein Bearbeitungs-Computersystem somit für Angreifer (Cracker) beziehungsweise nicht-autorisierte Computersysteme, welche einen entsprechenden Port-Knocking-Prozess manipulieren, geöffnet wird. Auf diese Weise ist ein (manipulativer) Zugriff Dritter auf unter Umständen vertrauliche Daten im Bearbeitungs-Computersystem mittels der geöffneten Netzwerk-Ports möglich. Ferner ist für eine Ansprechbarkeit von Diensten im geöffneten Bearbeitungs-Computersystem ein laufendes Programm an einem oder mehreren Netzwerk-Ports des Bearbeitungs-Computersystems erforderlich. Dieses laufende Programm stellt eine potentielle Sicherheitslücke für Angriffe von außen (z. B. über Buffer-Overflow oder so genannte Denial-of-Service-Attacken, DOS) über Netzwerk dar.

Eine explizite Authentifizierung eines externen Computersystems direkt an einem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur für einen Zugriff scheidet bei herkömmlichen Lösungen aus, weil ein Bearbeitungs-Computersystem - wie oben erläutert - zunächst

vermittels geschlossener Netzwerk-Ports keinen Verbindungsaufbau von außen zulässt.

Umgekehrt gestaltet sich ein Ansprechen eines externen Computersystems, welches einen Zugriff auf ein Bearbeitungs-Computersystem verlangt, vom Bearbeitungs-Computersystem aus oftmals als schwierig oder gar unmöglich, weil das externe Computersystem unter Umständen selbst abgesichert ist und womöglich für einen Verbindungsaufbau nicht ansprechbar ist.

Zudem erfolgt ein Zugriff auf Bearbeitungs-Computersysteme innerhalb einer Computernetz-Infrastruktur meist über das Internet oder ein separates Intranet (z. B. für eine Freischaltung von Applikationen), wobei sich derartige Zugriffe dadurch auszeichnen, dass die auf die Computernetz-Infrastruktur (z. B. Rechenzentrum) zugreifenden externen Computersysteme über einen privaten Zugang kommen, der keine (eindeutige) öffentliche IP-Adresse verwendet. Beispiele hierfür sind kaskadierte Anbindungen über einen Proxy oder mittels so genannter NAT/PAT-Maskierungs-Verfahren (NAT = Network Adress Translation, PAT = Port Adress Translation).

Dies führt dazu, dass grundsätzlich keine Verbindung von einem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur auf das entsprechende externe Computersystem initiiert werden kann, weil das Bearbeitungs-Computersystem schlichtweg die exakte IP-Adresse des externen Computersystems aufgrund der Maskierung der IP-Adresse nicht kennt. Ferner ist die IP-Adresse gewöhnlich privat und nicht direkt in einem Routing verwendbar. Zudem ist sie gewöhnlich in der Kommunikation hinter einer Firewall abgesichert.

Die Aufgabe der vorliegenden Erfindung besteht darin, durch technische Maßnahmen eine gesicherte Freischaltung externer Computersysteme für eine Kommunikation mit abgesicherten Bearbeitungs-Computersystemen innerhalb einer Computernetz-Infrastruktur zu ermöglichen und dennoch den Schutz vor Angriffen auf entsprechende Computersysteme in der Computernetz-Infrastruktur zu verbessern.

In einem ersten Aspekt wird diese Aufgabe durch ein Verfahren nach Anspruch 1 gelöst.

Bei dem Verfahren werden zum Freischalten externer Computersysteme für eine Kommunikation mit abgesicherten Bearbeitungs-Computersystemen in einer Computernetz-Infrastruktur die folgenden Schritte vorgeschlagen.

Zunächst wird ein Authentifizierungs-Paket von einem externen Computersystem, welches außerhalb der Computernetz-Infrastruktur eingerichtet ist, an ein Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur übertragen. Das Authentifizierungs-Paket enthält signierte Informationen zur Authentifizierung des externen Computersystems.

Das Authentifizierungs-Paket wird automatisiert vom Vermittlungs-Computersystem an zumindest ein Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur übertragen. Das Bearbeitungs-Computersystem hält zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen, so dass ein Zugriff auf das Bearbeitungs-Computersystem über Netzwerk vermittels dieser Netzwerk-Ports verhindert wird. Jedoch kann das Bearbeitungs-Computersystem auf das Vermittlungs-Computersystem zugreifen, um das

Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen. Dieser Vorgang kann über ein gemeinsames Zugangsnetz zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem oder über ein hierzu vorgesehenes spezielles Verbindungsnetz zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem erfolgen.

Ferner erfolgt ein Freischalten zumindest eines selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem für eine Kommunikation mit dem externen Computersystem und ein nachfolgendes Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems durch das externe Computersystem.

Bei dem erläuterten Verfahren sind initial alle vorbestimmten Netzwerk-Ports des Bearbeitungs-Computersystems geschlossen. Das Bearbeitungs-Computersystem verhält sich somit als eingekapseltes (speziell abgesichertes) System. Ein Zugriff über ein Netzwerk auf das Bearbeitungs-Computersystem ist zumindest unter bestimmten Betriebsbedingungen (vorteilhaft dauerhaft während der Durchführung des hier erläuterten Verfahrens ohne gezielte Freischaltung) nicht oder nur deutlich erschwert möglich.

Der Begriff „vorbestimmte Netzwerk-Ports“ bedeutet, dass im Bearbeitungs-Computersystem sämtliche oder nur ausgewählte sicherheitskritische Netzwerk-Ports, z. B. die für dieses Verfahren verwendeten Netzwerk-Ports, dauerhaft (diese werden gemäß dem erläuterten Verfahren nie freigeschaltet) oder vorübergehend (diese können selektiv gemäß dem erläuterten Verfahren freigeschaltet werden) geschlossen sind.

Dies hat den Vorteil, dass auf dem Bearbeitungs-Computersystem für ein Freischalten einer Kommunikation mit einem externen Computersystem initial keine Programme oder Dienste eingerichtet beziehungsweise verfügbar sind, die zum Zwecke der Ansprechbarkeit beziehungsweise des Verbindungsaufbaus von außen die entsprechenden Netzwerk-Ports abhören (so genanntes „Listening") und somit eine potentielle Sicherheitslücke (z. B. für Buffer-Overflow oder DoS-Attacken bzw. sog. distributed DoS-Attacken) bilden. Somit bedeutet der Begriff „geschlossene Netzwerk-Ports" in diesem Kontext, dass diese keine „Listening Ports" sind, das heißt, (ohne verfahrensgemäße autorisierte Freischaltung) kein Verbindungsaufbau von außen zugelassen wird. Ein Dritter (Cracker) ist in diesem Fall nicht in der Lage, sich von außen über Netzwerk am Bearbeitungs-Computersystem zu authentifizieren oder einzuloggen, z. B. bei Unix-basierten Systemen über einen Secure-Shell-(SSH-)-Daemon, einen http-Daemon oder sonstige Dienste/Applikation usw., oder spezielle Aktionen auf dem Bearbeitungs-Computersystem durchzuführen.

Allerdings kann für eine vorbestimmte Benutzergruppe ein lokaler Zugriff auf das Bearbeitungs-Computersystem eingerichtet sein (z. B. für ein Sicherheitspersonal). Für andere Dritte wird jedoch ein lokaler Zugriff auf das Bearbeitungs-Computersystem verhindert.

Durch die generelle Abschottung des Bearbeitungs-Computersystems gemäß der erläuterten Art und Weise ist somit ein Angriff über Netzwerk erschwert, weil eine entscheidende Angriffsmöglichkeit, nämlich laufende Dienste oder Programme an geöffneten („Listening") Netzwerk-Ports der jeweiligen Systeme unterbunden sind. Somit sind bei dem erläuterten Verfahren insbesondere sicherheitskritische Daten, welche

lokal auf dem Bearbeitungs-Computersystem verarbeitet werden, gegen Angriffe geschützt.

Zum Freischalten einer Kommunikation zwischen dem externen Computersystem außerhalb der Computernetz-Infrastruktur und dem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur erlaubt das Verfahren im Unterschied zum Bearbeitungs-Computersystem einen Zugriff von außerhalb der Computernetz-Infrastruktur auf das zumindest eine Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur. Das Vermittlungs-Computersystem ist als „offenes" System mit wenigstens einem ansprechenbaren offenen („Listening") Netzwerk-Port über Netzwerk zugänglich. Das bedeutet, dass auf dem Vermittlungs-Computersystem beispielsweise Programme laufen und/oder Applikationen (Dienste) vorbereitet sind, so dass das Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur oder das externe Computersystem außerhalb der Computernetz-Infrastruktur jeweils auf das Vermittlungs-Computersystem zugreifen können und eine Verbindung zum Vermittlungs-Computersystem aufbauen können, um Datenpakete (über eine dann aufgebaute Verbindung, „Established") im Vermittlungs-Computersystem abzulegen oder von dort abzuholen. Unter Sicherheitsaspekten ist ein solches „offenes" Vermittlungs-Computersystem ähnlich zu bewerten wie ein traditionelles, speziell abgesichertes Computersystem.

Somit dient das Vermittlungs-Computersystem als (abgesicherter, aber ansprechbarer) Vermittler für eine Kommunikation zwischen dem Bearbeitungs-Computersystem und dem externen Computersystem.

Vorteilhaft erfolgt ein Verbindungsaufbau vom Bearbeitungs-Computersystem auf das Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur über ein internes Netzwerk, welches beispielsweise als „Virtual Private Network" (VPN) oder Secure-Shell-Netzwerk (SSH) oder als eine Kombination davon abgesichert ist. Alternativ oder ergänzend können auch speziell zu diesem Zweck entwickelte Protokolle eingesetzt werden.

Ein Verbindungsaufbau vom externen Computersystem außerhalb der Computernetz-Infrastruktur auf das Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur erfolgt beispielsweise über Internet oder über ein Routing von einem separaten Intranet aus (z. B. ein Client-Intranet). Beispielsweise kann das externe Computersystem ein Client sein, der hinter einem NAT- und/oder PAT-Router sitzt. Dabei erfolgt ein Verbindungsaufbau zum Vermittlungs-Computersystem von einem lokalen Client-Intranet über eine private Quell-IP-Adresse des Clients aus, welche im Router mit einer öffentlichen IP-Adresse des Routers maskiert wird.

Gemäß dem erläuterten Verfahren muss für eine Freischaltung des externen Computersystems für eine Kommunikation mit dem zunächst abgesicherten Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur eine Authentifizierung des externen Computersystems am Vermittlungs-Computersystem erfolgen. Das Authentifizierungs-Paket enthält vorteilhaft signierte Informationen über das externe Computersystem. Diese können gegebenenfalls Informationen über einen anzusprechenden Dienst oder allgemein Prozess auf dem Bearbeitungs-Computersystem umfassen, welcher vom externen Computersystem angesprochen werden soll.

Eine Signierung der Informationen im Authentifizierungs-Paket hat den Vorteil, dass eine Manipulation des Authentifizierungs-Paketes erschwert wird. Auf diese Weise kann eine im Vergleich zu herkömmlichen Port-Knocking-Prozessen (siehe oben) deutlich sicherere Authentifizierung externer Computersysteme zum Freischalten einer Kommunikation mit Bearbeitungs-Computersystemen innerhalb einer abgesicherten Computernetz-Infrastruktur durchgeführt werden.

Das Authentifizierungs-Paket, welches vom externen Computersystem an das von außen ansprechbare Vermittlungs-Computersystem übertragen worden ist, wird im weiteren Verfahren um die für das Vermittlungs-Computersystem (und damit auch für das Bearbeitungs-Computersystem) sichtbare IP-Adresse, die dem externen Computersystem zuordenbar ist, ergänzt. Diese IP-Adresse kann z.B. diejenige eines NAT-Routers sein, von dem das Vermittlungs-Computersystem das Authentifizierungs-Paket unmittelbar erhalten hat. Anschließend wird das so ergänzte Authentifizierungs-Paket vom Vermittlungs-Computersystem an das Bearbeitungs-Computersystem übermittelt.

Da das Bearbeitungs-Computersystem zunächst – wie oben erläutert – seine Netzwerk-Ports geschlossen hält und keinen Verbindungsaufbau von außen zulässt, wird zum Übertragen des Authentifizierungs-Paketes auf das Bearbeitungs-Computersystem ein Prozess angestoßen, wobei das Bearbeitungs-Computersystem selbst das Vermittlungs-Computersystem über Netzwerk anspricht und eine Verbindung zum Vermittlungs-Computersystem aufbaut. Das Authentifizierungs-Paket kann im Weiteren im Vermittlungs-Computersystem aufgerufen und automatisiert über eine hergestellte Verbindung („Established“) vom Vermittlungs-

Computersystem auf das Bearbeitungs-Computersystem übertragen werden. Vorteilhaft ist das automatisierte Übertragen so ausgestaltet, dass ein Dritter von außen darauf keine Einflussmöglichkeiten hat und somit eine Gefahr von Manipulationen der ausgetauschten Daten oder eines der beteiligten Computersysteme deutlich erschwert bzw. ausgeschlossen ist.

Nach erfolgreicher Authentifizierung vermittels des Authentifizierungs-Paketes erfolgt eine Freischaltung zumindest eines Netzwerk-Ports im Bearbeitungs-Computersystem. Der Begriff „Freischaltung" bedeutet in diesem Kontext eine Freigabe der (Quell-)IP-Adresse, welche in dem Authentifizierungs-Paket hinterlegt ist, selektiv an einem vorbestimmten Ziel-Netzwerk-Port des Bearbeitungs-Computersystems für einen Verbindungsaufbau und eine anschließende Kommunikation zu und mit dem Bearbeitungs-Computersystem (über einen aus einer Vielzahl von Quell-Netzwerk-Ports in Kombination mit der Quell-IP-Adresse). Nach dem Freischalten zumindest eines selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem erfolgt schließlich ein Aufbauen einer Verbindung (neue Session) zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems durch das externe Computersystem via der freigeschalteten IP-Adresse und einem bestimmten Quell-Netzwerk-Port.

Es ist vorteilhaft, einen entsprechenden Verbindungsaufbau nur in einem vorbestimmten Zeitrahmen, der unter Umständen applikationsabhängig entsprechend kurz sein kann (z. B. je nach Netzwerkgeschwindigkeit einige Millisekunden oder einige Sekunden, z.B. bis zu 10 Sekunden), zuzulassen. Erfolgt in dem vorgegebenen Zeitrahmen kein entsprechender

Verbindungsaufbau durch das externe Computersystem, so wird der selektiv freigeschaltete Netzwerk-Port des Bearbeitungs-Computersystems aus Sicherheitsgründen wieder geschlossen, um die Gefahr eines missbräuchlichen Verbindungsaufbaus oder die manipulative Ausnutzung des geöffneten Netzwerk-Ports (z.B. vermittels eines Port-Scannings) durch Computersysteme mit der (zufällig) selben IP-Adresse, die z.B. hinter demselben NAT-Router sitzen, zu reduzieren.

Eine Anwendung des vorliegenden Verfahrens ist beispielsweise ein Freischalten einer Applikation auf dem Bearbeitungs-Computersystem für einen externen Client, welcher über Internet eine gezielte (und in gewissem Rahmen dennoch beschränkte und abgesicherte) Freischaltung des Bearbeitungs-Computersystems innerhalb der Computernetz-Infrastruktur anfragt.

Der generelle Vorteil des hier erläuterten Verfahrens besteht darin, dass ein unsicheres und angreifbares Öffnen von Netzwerk-Ports am Bearbeitungs-Computersystem auf eine manipulierbare Anfrage eines externen Computersystems hin (z.B. via Port-Knocking) vermieden wird. Darüber hinaus muss/kann das Bearbeitungs-Computersystem keine Verbindung nach außerhalb der Computernetz-Infrastruktur aufbauen, um eine Authentifizierung einer (zunächst) unbekannten Quelle durchzuführen. Ferner wird verhindert, dass das Bearbeitungs-Computersystem eine Verbindung nach außen zulässt, ohne zu wissen, ob das Gegenüber überhaupt vertrauenswürdig ist. Vor einer Authentifizierung eines externen Computersystems erfolgt lediglich eine abgesicherte Kommunikation mit dem internen Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur seitens des Bearbeitungs-Computersystems zum Abholen einer Authentifizierungs-Datei,

die vom externen Computersystem auf das Vermittlungs-Computersystem übertragen worden ist. Erst nach erfolgreicher Authentifizierung erfolgt ein gezieltes Freischalten einer (Quell-)IP-Adresse für eine Kommunikation mit dem externen Computersystem.

Vorteilhaft wird nach dem Aufbauen einer Verbindung zum selektiv freigeschalteten Ziel-Netzwerk-Port des Bearbeitungs-Computersystems, über die die nachfolgende Kommunikation mit dem externen Computersystem läuft, folgender zusätzlicher Schritt durchgeführt:
- Begrenzen der Kommunikation zwischen dem Bearbeitungs-Computersystem und dem externen Computersystem auf den freigeschalteten Ziel-Netzwerk-Port des Bearbeitungs-Computersystems und einen Netzwerk-Port des externen Computersystems, der dem Bearbeitungs-Computersystem als Quell-Netzwerk-Port durch die aufgebaute Verbindung bekannt ist. Bei diesen Maßnahmen ist zu berücksichtigen, dass ggf. parallel stattfindende Verbindungsaufbauten mehrerer Computersysteme sich nicht gegenseitig beeinträchtigen.

Eine Begrenzung auf den selektiven Quell-Netzwerk-Port des externen Computersystems hat den Vorteil, dass anderweitige Kommunikationen unterbunden werden. So kann das externe Computersystem nur eingeschränkt auf einzelne Netzwerk-Ports (auf beiden Seiten), also Quell-Netzwerk-Port des externen Computersystems und Ziel-Netzwerk-Port des Bearbeitungs-Computersystems, mit dem Bearbeitungs-Computersystem kommunizieren. Der selektive Netzwerk-Port des externen Computersystems kann beispielsweise der Quell-Netzwerk-Port der letzten Übertragung vermittels der aufgebauten („Established") Verbindung sein. Falls beispielsweise das externe Computersystem hinter einem NAT-Router sitzt, wird

verhindert, dass nicht-autorisierte Systeme oder Angreifer, welche ebenfalls hinter dem NAT-Router sitzen, neben der bereits hergestellten Verbindung zwischen dem externen Computersystem und dem Bearbeitungs-Computersystem eine weitere Verbindung zum Bearbeitungs-Computersystem (via derselben Quell-IP-Adresse und einem anderen Quell-Netzwerk-Port des NAT-Routers) aufbauen können und somit nicht-autorisierten Zugriff auf das Bearbeitungs-Computersystem erhalten. Die vorgenannten Maßnahmen erlauben somit eine gezielte Beschränkung eines Zugriffs auf das Bearbeitungs-Computersystem über eine autorisierte (einzelne) Netzwerk-Verbindung. Andere nicht-autorisierte Verbindungen beziehungsweise deren Aufbauversuche werden im Bearbeitungs-Computersystem verworfen beziehungsweise nicht berücksichtigt.

Vorteilhaft werden nach dem Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems durch das externe Computersystem folgende Schritte durchgeführt:
- Übertragen eines Verifikations-Paketes durch das externe Computersystem unmittelbar auf das Bearbeitungs-Computersystem vermittels der aufgebauten Verbindung und
- Bestätigen der Informationen des durch das Vermittlungs-Computersystem zuvor übertragenen Authentifizierungs-Paketes durch Verifikations-Informationen im Verifikations-Paket.

Durch Senden eines Verifikations-Paketes kann sichergestellt werden, dass die Verbindung von der richtigen autorisierten Instanz (und nicht durch einen unbefugten Dritten, z. B. mit gleicher IP-Adresse hinter einem NAT-Router oder mit manipulierter IP-Adresse oder mit gestohlenem Authentifizierungs-Paket) aufgebaut worden ist. Durch die

vorgenannten Maßnahmen kann somit sichergestellt werden, dass nach einem Freischalten einer im Authentifizierungs-Paket hinterlegten IP-Adresse an einem selektiven Ziel-Netzwerk-Port des Bearbeitungs-Computersystems diejenige externe Instanz auch die Verbindung zum Bearbeitungs-Computersystem aufbaut, die eine entsprechende Verbindung über das Authentifizierungs-Paket zuvor angezeigt hat.

Der obige Schritt des Bestätigens der Informationen des Authentifizierungs-Paketes durch Verifikations-Informationen im Verifikations-Paket kann ein Überprüfen auf Identität mit dem Authentifizierungs-Paket umfassen. Dabei wird sichergestellt, dass keine Manipulationen am ursprünglich übertragenen Authentifizierungs-Paket vorgenommen werden.

Alternativ oder ergänzend kann das Bestätigen der Informationen ein notwendiges Hinterlegen von bestimmten Autorisierungs- oder Identitätsmerkmalen im Verifikations-Paket umfassen, die im Bearbeitungs-Computersystem anhand von hinterlegten Vergleichs-Informationen überprüft und bestätigt werden. Derartige Autorisierungs- oder Identitätsmerkmale können z.B. Merkmale der Hardware des externen Computersystems, biometrische Merkmale bestimmter Benutzer des externen Computersystems sowie Passwörter (Passphrasen oder Credentials, Schlüssel, usw.) umfassen.

Vorteilhaft umfasst das Verfahren der erläuterten Art den zusätzlichen Schritt:
- Überprüfen des Authentifizierungs-Paketes im Bearbeitungs-Computersystem, wobei das Freischalten des zumindest einen selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem für die Kommunikation mit dem externen

Computersystem nur erfolgt, falls das Überprüfen des Authentifizierungs-Paketes erfolgreich war.

Vorteilhaft umfasst das Verfahren alternativ und/oder ergänzend zum Überprüfen des Authentifizierungs-Paketes im Bearbeitungs-Computersystem die zusätzlichen Schritte:
- Überprüfen des Authentifizierungs-Paketes im Vermittlungs-Computersystem und
- Verwerfen des Authentifizierungs-Paketes durch das Vermittlungs-Computersystem, falls das Überprüfen nicht erfolgreich war.

Ein Überprüfen des Authentifizierungs-Paketes im Bearbeitungs-Computersystem und/oder im Vermittlungs-Computersystem auf Gültigkeit stellt eine Sicherheitsmaßnahme dar, wobei vordefinierte Informationen im Authentifizierungs-Paket erfüllt sein müssen, so dass das Authentifizierungs-Paket als gültig verifiziert werden kann und ein Freischalten des Bearbeitungs-Computersystems auslöst.

Ein Überprüfen des Authentifizierungs-Paketes bereits im Vermittlungs-Computersystem stellt eine vorgreifliche Sicherheits-Maßnahme vor dem Übertragen auf das Bearbeitungs-Computersystem dar. Ein Verwerfen eines ungültigen Authentifizierungs-Paketes kann gegebenenfalls durch ein Monitoring protokolliert werden. Nach Verwerfen erfolgt vorteilhaft der Abbruch des Verfahrens. Anderenfalls erfolgt die Übertragung des Authentifizierungs-Paketes an das Bearbeitungs-Computersystem wie oben erläutert.

Vorteilhaft enthält das Authentifizierungs-Paket eine Signatur eines (separaten) Key-Computersystems und/oder eine Signatur des externen Computersystems. Ein separates Key-

Computersystem ist dabei eine zusätzliche Sicherheits-Instanz. Eine Signatur des Key-Computersystems verhindert eine Manipulation des Authentifizierungs-Paketes im externen Computersystem. Private Schlüssel (Passphrasen, Credentials, etc.) zum Erstellen der jeweiligen Signatur sind lediglich lokal auf dem Key-Computersystem bzw. dem externen Computersystem hinterlegt, jedoch vorteilhaft nicht auf den sonstigen Computersystemen, die am Verfahren beteiligt sind, bekannt. Als zusätzliche Sicherheitsmaßnahme kann das Authentifizierungs-Paket mit einem öffentlichen Schlüssel des externen Computersystems (bzw. dessen Nutzer) und/oder des Key-Computersystems verschlüsselt sein.

Durch signierte Informationen im Authentifizierungs-Paket, die über eine Signatur eines separaten Key-Computersystems signiert worden sind, wird die Sicherheit des Authentifizierungs-Prozesses innerhalb des erläuterten Verfahrens erhöht. Beispielsweise kann durch einen Sicherheitsbeauftragten, der Zugriff auf das Key-Computersystem hat, ein vorbestimmtes externes Computersystem für ein Freischalten einer Kommunikation mit dem zunächst abgesicherten Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur festgelegt werden. Diese Information wird durch einen privaten Schlüssel des Sicherheitsbeauftragten lokal im Key-Computersystem signiert und anschließend daraus das Authentifizierungs-Paket erstellt.

Vorteilhaft können weitere vorbestimmte Durchführungsparameter in diesem (oben erläuterten) Key-Computersystem oder in einem weiteren Key-Computersystem für einen Zugriff des externen Computersystems auf das Bearbeitungs-Computersystem festgelegt werden. Derartige

Durchführungsparameter können vom entsprechenden Key-Computersystem an das externe Computersystem übertragen werden, wobei das Authentifizierungs-Paket im externen Computersystem auf Grundlage der festgelegten Durchführungsparameter erstellt wird. Beispielsweise kann das Authentifizierungs-Paket die durch das Key-Computersystem festgelegten Durchführungsparameter unmittelbar enthalten. Derartige weitere Durchführungsparameter stellen eine zusätzliche Sicherheits-Maßnahme dar, die vorgibt, welche externen Computersysteme unter welchen Umständen in welchem Rahmen eine Freischaltung auf einem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur erhalten sollen oder dürfen.

Die letztgenannten Durchführungsparameter können ebenfalls mit wenigstens einem privaten Schlüssel durch das Key-Computersystem signiert sein. Vorteilhaft werden sämtliche Signaturen und/oder Durchführungsparameter, die im Authentifizierungs-Paket hinterlegt sind, im Bearbeitungs-Computersystem und/oder im Vermittlungs-Computersystem gemäß den oben erläuterten Maßnahmen überprüft. Dadurch wird sichergestellt, dass ein Freischalten des externen Computersystems auf dem Bearbeitungs-Computersystem durch das Key-Computersystem als Sicherheits-Instanz autorisiert ist.

Alle vorgenannten Maßnahmen sind selbstverständlich auch auf das Verifikations-Paket anwendbar, das zur Bestätigung des Authentifizierungs-Paketes unmittelbar vom externen Computersystem an das Bearbeitungs-Computersystem geschickt wird, wie dies oben im Zusammenhang mit weiteren Verfahrensschritten und Maßnahmen erläutert worden ist.

Vorteilhaft umfasst das Übertragen des Authentifizierungs-Paketes vom Vermittlungs-Computersystem auf das Bearbeitungs-Computersystem die folgenden Schritte:

- Senden einer vorbestimmten Daten-Sequenz vom Vermittlungs-Computersystem oder vom externen Computersystem an das Bearbeitungs-Computersystem, wobei die vorbestimmten Netzwerk-Ports des Bearbeitungs-Computersystems geschlossen sind und wobei die Sequenz in einer vorbestimmten Reihenfolge einen oder mehrere Netzwerk-Ports des Bearbeitungs-Computersystems anspricht,
- Überprüfen der gesendeten Daten-Sequenz auf Übereinstimmung mit einer vordefinierten Sequenz im Bearbeitungs-Computersystem, sowie
- Veranlassen des Übertragens des Authentifizierungs-Paketes durch das Bearbeitungs-Computersystem, falls die Überprüfung der gesendeten Sequenz positiv ist.

Die Maßnahmen haben den Vorteil, dass grundsätzlich die (für das Verfahren maßgeblichen) Netzwerk-Ports des Bearbeitungs-Computersystems – in oben erläutertem Sinne – initial geschlossen sind und einen Verbindungsaufbau zum Bearbeitungs-Computersystem von außen blockieren beziehungsweise einen manipulativen Zugriff deutlich erschweren. Für sämtliche externen Computersysteme, die sich nicht über entsprechende Authentifizierungs-Pakete, wie oben erläutert, innerhalb der Computernetz-Infrastruktur authentifiziere können, hat das Bearbeitungs-Computersystem dauerhaft (bis auf eine kurze Zeitspanne, in der eine bestimmte Quell-IP-Adresse gemäß den obigen Schritten freigeschaltet ist) geschlossene Netzwerk-Ports und blockiert jeglichen Verbindungsaufbau.

Das Veranlassen des Übertragens des Authentifizierungs-Paketes vermittels des Bearbeitungs-Computersystems zur Authentifizierung eines freizuschaltenden externen Computersystems kann ein automatisierter Prozess zum Übertragen des Authentifizierungs-Paketes auf das Bearbeitungs-Computersystem (z. B. über den Unix-basierten Befehl „Secure copy", scp) sein. Gemäß dem Prozess baut das Bearbeitungs-Computersystem seinerseits eine Verbindung zum Vermittlungs-Computersystem auf und holt das Authentifizierungs-Paket ab. Dieser Prozess kann durch das Bearbeitungs-Computersystem gestartet werden, nachdem eine vorbestimmte Daten-Sequenz an das Bearbeitungs-Computersystem gesendet wurde, falls diese Daten-Sequenz mit einer vordefinierten Sequenz übereinstimmt. Das Sequenz-sendende Computersystem kann das Vermittlungs-Computersystem oder alternativ das externe Computersystem sein. Die IP-Adresse des Sequenz-sendenden Computersystems kann dabei statisch im Bearbeitungs-Computersystem vorgegeben oder dynamisch aus den dem Kernel des Bearbeitungs-Computersystems bekannten Quell-IP-Adressen möglicher Sequenz-sendender Computersysteme entnommen werden.

Wie bereits eingangs erläutert, ist ein derartiges Verfahren unter dem Begriff „Port-Knocking" (Englisch: to knock = anklopfen) bekannt. Die vorgenannten Schritte können beispielsweise über einen so genannten Knock-Daemon, also ein Programm, welches Port-Knocking ermöglicht, durchgeführt werden. Der Knock-Daemon wird durch das Bearbeitungs-Computersystem über eintreffende Datenpakete an seiner Netzwerk-Schnittstelle informiert, überprüft die an das Bearbeitungs-Computersystem gesendete Daten-Sequenz und veranlasst gegebenenfalls (z. B. durch Starten eines Skriptes/Programmes) ein gesteuertes Übertragen des

Authentifizierungs-Paketes vom Vermittlungs-Computersystem an das Bearbeitungs-Computersystem, wenn die gesendete Daten-Sequenz mit der vordefinierten Sequenz übereinstimmt. Der oben beschriebene Ablauf ermöglicht somit - aktiviert durch das Bearbeitungs-Computersystem, welches einen entsprechenden Dienst auf dem Vermittlungs-Computersystem über Netzwerk anspricht - das Übertragen/Kopieren des Authentifizierungs-Paketes vom Vermittlungs-Computersystem auf das Bearbeitungs-Computersystem, ohne dass das Bearbeitungs-Computersystem hierfür einen offenen Netzwerk-Port mit einem ansprechbaren Programm vorhalten muss.

Alternativ oder ergänzend zum oben erläuterten Port-Knocking ist auch denkbar, dass das Bearbeitungs-Computersystem von sich aus in regelmäßigen Abständen beim Vermittlungs-Computersystem anfragt (so genanntes Polling), ob ein oder mehrere auszutauschende Authentifizierungs-Pakete vorliegen. Ist dies der Fall, kann eine entsprechende Übertragung der Authentifizierungs-Pakete vom Vermittlungs-Computersystem an das Bearbeitungs-Computersystem initiiert werden, wie oben erläutert. Es ist auch denkbar, dass das Bearbeitungs-Computersystem ein Polling durchführt, wenn z. B. eine bestimmte Zeitspanne überschritten wird, in der kein Port-Knocking seitens des Vermittlungs-Computersystems oder des externen Computersystems durchgeführt worden ist. Probleme beim Port-Knocking können so erkannt werden und die Funktionalität der Computernetz-Infrastruktur bleibt erhalten.

Alternativ zu den genannten Lösungen (Port-Knocking, Polling) wäre auch denkbar, ein spezielles Verbindungsnetz zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem vorzusehen, wobei das Bearbeitungs-

Computersystem zumindest einen Netzwerk-Port zur Ansprechbarkeit über dieses spezielle Verbindungsnetz geöffnet hat. Über das Verbindungsnetz könnte dann das Authentifizierungs-Paket vom Vermittlungs-Computersystem an das Bearbeitungs-Computersystem übertragen werden. Dabei kann vorteilhaft ein anderes Protokoll verwendet werden als für eine Verbindung zwischen dem externen Computersystem und dem Vermittlungs-Computersystem vorgesehen ist. Ein solcher Protokollwechsel erhöht ebenfalls die Sicherheit gegen Manipulationen von außerhalb des Netzwerks.

Vorteilhaft werden Daten-Pakete zwischen dem externen Computersystem und der Computernetz-Infrastruktur über einen Paket-Filter geleitet, wobei der Paket-Filter zum externen Computersystem hin zumindest einen Netzwerk-Port für einen Zugriff durch das externe Computersystem offen hält und wobei der Paket-Filter zur Computernetz-Infrastruktur hin vorbestimmte Netzwerk-Ports geschlossen hält, so dass zumindest ein Zugriff von einem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur auf das externe Computersystem verhindert wird.

Der Paket-Filter hat den Vorteil, dass die Computernetz-Infrastruktur nach außen hin abgesichert bleibt, so dass keine initialen Anfragen für einen Verbindungsaufbau, Informationen, und so weiter von einem internen Computersystem (zum Beispiel nach einem internen Angriff) nach außen geschickt werden können, weil der Packet-Filter die Daten nicht weiterleiten würde. Entsprechende Pakete werden somit aus Richtung der Computernetz-Infrastruktur im Paket-Filter verworfen. Andererseits ist es möglich, Authentifizierungs-Pakete externer Computersysteme über den Paket-Filter in die Computernetz-Infrastruktur hinein zu

transportieren und auf dem Vermittlungs-Computersystem abzulegen. Ein derartiger Paket-Filter ist also ein Schutz/eine Blockade nach außen.

Vorteilhaft werden Daten-Pakete zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur über einen (weiteren) Paket-Filter geleitet, wobei dieser Paket-Filter in der Kommunikationsrichtung vom Vermittlungs-Computersystem hin zum Bearbeitungs-Computersystem nur Daten-Pakete weiterleitet, welche die IP-Adresse des Vermittlungs-Computersystems enthalten und einer bereits hergestellten Verbindung zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem zugeordnet werden können.

Diese Filterung lässt vorteilhaft nur Daten-Pakete einer Verbindung mit Status „Established" oder „Related" von der exakten IP-Adresse des Vermittlungs-Computersystems zu. Ein Versuch eines Verbindungsaufbaus (z. B. via Senden von so genannten SYN-Paketen) oder auch ein Senden von Port-Knocking-Paketen initial vom Vermittlungs-Computersystem aus wird durch diesen Paket-Filter geblockt.

Die Filterung verhindert eine Fälschung einer IP-Adresse (so genanntes IP-Spoofing) eines vermeintlich vertraulichen (externen oder internen) Computersystems von dem (nach Angriff manipulierten) Vermittlungs-Computersystem aus. Damit wird der Aufbau einer manipulierten Verbindung unterbunden, die einen Port-Filter oder eine Port-Sperre am Bearbeitungs-Computersystem umgehen könnte und so manipulierten Zugriff an selektiv geöffneten Netzwerk-Ports des Bearbeitungs-Computersystems erhalten würde. Ein derartiger Paket-Filter ist hier also ein Schutz beziehungsweise eine Blockade gegen

interne Manipulationen. Wenn das Vermittlungs-Computersystem von einem Angreifer manipuliert wird, verhindern diese Maßnahmen ein Ausweiten des Angriffs auf das interne Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur über eine manipulierte „vertrauliche" IP-Adresse, die nicht der exakten IP-Adresse des Vermittlungs-Computersystems entspricht.

Selbst wenn ein Angreifer im Vermittlungs-Computersystem dessen exakte IP-Adresse für einen weitergehenden Angriff verwenden möchte, so bleiben initiale Verbindungsversuche zum Bearbeitungs-Computersystem erfolglos, weil der Paket-Filter lediglich Rückantworten innerhalb von Verbindungen zulässt, die vom Bearbeitungs-Computersystem aus aufgebaut worden sind. Auf diese Weise erschweren die Maßnahmen einen Zugriff auf unter Umständen vertrauliche Daten innerhalb des Bearbeitungs-Computersystems aufgrund eines Angriffs vom Vermittlungs-Computersystem aus.

In der Kommunikationsrichtung vom Bearbeitungs-Computersystem hin zum Vermittlungs-Computersystem kann durch den erläuterten Paket-Filter ein erlaubter Datenaustausch auf vorbestimmte Netzwerk-Ports des Vermittlungs-Computersystems für ausgewählte Dienste (z. B. scp oder alternativ andere gewählte Protokolle) freigeschaltet sein.

In einer vorteilhaften Ausgestaltung des vorliegenden Verfahrens umfasst das Übertragen des Authentifizierungs-Paketes vom externen Computersystem an das Vermittlungs-Computersystem folgende Teilschritte:

- Aufbauen einer Verbindung vom externen Computersystem zu einem Vermittlungs-Load Balancer, der einer Mehrzahl von Vermittlungs-Computersystemen vorgeschaltet ist,

- Auswahl des Vermittlungs-Computersystems aus der Mehrzahl von Vermittlungs-Computersystemen durch den Vermittlungs-Load Balancer, und
- Weiterleiten des Authentifizierungs-Paketes vom externen Computersystem über den Vermittlungs-Load Balancer an das ausgewählte Vermittlungs-Computersystem.

Ein derartiger Vermittlungs-Load Balancer findet vorteilhaft in einer Konstellation Anwendung, bei der innerhalb der Computernetz-Infrastruktur eine Mehrzahl von Vermittlungs-Computersystemen eingerichtet ist zur Vermittlung einer Vielzahl von Anfragen durch eine Vielzahl von externen Computersystemen zum Freischalten gemäß der erläuterten Art und Weise. Insbesondere im Falle eines großen Lastvolumens kann somit die Netzwerklast durch den Vermittlungs-Load Balancer auf unterschiedliche Vermittlungs-Computersysteme aufgeteilt werden, so dass eine gute Performance der Computernetz-Infrastruktur erhalten bleibt. Die einzelnen Vermittlungs-Computersysteme arbeiten jeweils nach dem oben erläuterten Verfahren.

Insbesondere leitet der Vermittlungs-Load Balancer Daten-Pakete (z.B. generell jegliche IP-Pakete), die von externen Computersystemen geschickt werden, auf ein zuvor vom Vermittlungs-Load Balancer ausgewähltes, spezifisches Vermittlungs-Computersystem weiter. Das jeweils ausgewählte Vermittlungs-Computersystem nimmt insbesondere ein über den Vermittlungs-Load Balancer weitergeleitetes Authentifizierungs-Paket eines externen Computersystems entgegen.

Zur Auswahl eines aus der Mehrzahl der Vermittlungs-Computersysteme kann sich der Vermittlungs-Load Balancer

eines beliebigen Algorithmus bedienen. Ein derartiger Algorithmus kann in einem einfachen Fall eine Unterscheidung nach der sichtbaren IP-Adresse, die dem externen Computersystem zuordenbar ist, vornehmen. Wie oben bereits erläutert, kann diese IP-Adresse z.B. diejenige eines NAT-Routers sein, von dem der Vermittlungs-Load Balancer das Authentifizierungs-Paket unmittelbar erhalten hat. Beispielsweise kann der Algorithmus ein so genanntes „Source Hashing Scheduling" umfassen. Dabei werden Netzwerkverbindungen zu den nachgelagerten Vermittlungs-Computersystemen aus einer Look-up Tabelle in Abhängigkeit von (öffentlichen) Quell-IP-Adressen zugeteilt, welche anfragenden externen Computersystemen zuordenbar sind.

Nach Auswahl eines spezifischen Vermittlungs-Computersystems und Weiterleiten des Authentifizierung-Paketes an dieses Vermittlungs-Computersystem durch den Vermittlungs-Load Balancer führt das Vermittlungs-Computersystem anschließend eine verfahrensgemäß erläuterte Verarbeitung bzw. Weiterleitung des Authentifizierungs-Paketes an ein entsprechendes Bearbeitungs-Computersystem durch. Unter Umständen erfolgt im Vermittlungs-Computersystem wiederum eine Auswahl eines aus einer Mehrzahl von Bearbeitungs-Computersystemen.

Nach einer erfolgreichen Authentifizierung eines externen Computersystems vermittels des Authentifizierungs-Paketes erfolgt ein Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des (ausgewählten) Bearbeitungs-Computersystems durch das externe Computersystem (wie oben erläutert). Dies kann in einer denkbaren Konstellation über den Vermittlungs-Load Balancer geschehen, welcher dann die Verbindung vom externen Computersystem an

das Bearbeitungs-Computersystem weiterleitet. In diesem Fall erfolgt vorteilhaft sowohl eine Auswahl eines spezifischen Vermittlungs-Computersystems durch den Vermittlungs-Load Balancer als auch gegebenenfalls eine Auswahl eines spezifischen Bearbeitungs-Computersystems durch das entsprechende Vermittlungs-Computersystem anhand desselben Algorithmus. Somit wird sichergestellt, dass eine Verbindunganfrage eines freigeschalteten externen Computersystems vom Vermittlungs-Load Balancer an das richtige Bearbeitungs-Computersystem weitergeleitet wird, welches seinerseits vom entsprechenden Vermittlungs-Computersystem bestimmungsgemäß das Authentifizierungs-Paket erhalten hat.

Der Vermittlungs-Load Balancer kann in einer denkbaren Konstellation gemeinsam mit einem oder mehreren der oben erläuterten Paket-Filter in einem logisch ansprechbaren System zusammengefasst sein. Zum Beispiel kann ein Server eingerichtet sein, der sowohl die Funktion des Vermittlungs-Load Balancers als auch die Funktion eines entsprechenden Paket-Filters bereitstellt.

In einer alternativen oder ergänzenden Ausgestaltung des vorliegenden Verfahrens arbeitet das Bearbeitungs-Computersystem als Bearbeitungs-Load Balancer, der einer Mehrzahl von Backend-Bearbeitungs-Computersystemen vorgeschaltet ist und folgende Maßnahmen durchführt:
- Auswahl eines Backend-Bearbeitungs-Computersystems aus der Mehrzahl der Backend-Bearbeitungs-Computersysteme, und
- Weiterleiten einer durch das externe Computersystem zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Load Balancers aufgebauten Verbindung an das ausgewählte Backend-Bearbeitungs-Computersystem.

In dieser Konstellation erfolgt ein Load Balancing auf der Ebene der Bearbeitungs-Computersysteme, wobei das verfahrensgemäße Bearbeitungs-Computersystem als Bearbeitungs-Load Balancer arbeitet und mehrere weitere Bearbeitungs-Computersysteme als Backend-Bearbeitungs-Computersysteme dem Bearbeitungs-Load Balancer nachgeschaltet sind zur weiteren Verarbeitung einer Anfrage und gegebenenfalls Freischaltung eines externen Computersystems. Eine Auswahl eines spezifischen Backend-Bearbeitungs-Computersystems erfolgt durch den Bearbeitungs-Load Balancer vorteilhaft anhand eines vorbestimmten Algorithmus. Hier ist, ähnlich zu einem oben erläuterten Vermittlungs-Load Balancer, ein „Source Hashing Scheduling" denkbar. Alternativ können auch andere Load Balancing Algorithmen Anwendung finden.

Gemäß dieser Ausgestaltung des Verfahrens wird ein automatisiertes Übertragen eines Authentifizierungs-Paketes von einem Vermittlungs-Computersystem an den Bearbeitungs-Load Balancer durchgeführt. Wie weiter oben allgemein für ein Bearbeitungs-Computersystem erläutert, hält hier der Bearbeitungs-Load Balancer zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen, so dass ein Zugriff auf den Bearbeitungs-Load Balancer über Netzwerk vermittels dieser Netzwerk-Ports verhindert wird. Allerdings kann der Bearbeitungs-Load Balancer auf das Vermittlungs-Computersystem zugreifen, um das Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen. Nach einer erfolgreichen Authentifizierung des externen Computersystems vermittels des Authentifizierungs-Paketes erfolgt ein Freischalten zumindest eines selektiven Netzwerk-Ports im Bearbeitungs-Load Balancer für eine Kommunikation mit dem externen Computersystem. Anschließend kann das externe

Computersystem eine Verbindung zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Load Balancers aufbauen, sodass eine weitere verfahrensgemäße Kommunikation durchführbar ist.

Der Bearbeitungs-Load Balancer leitet die durch das externe Computersystem aufgebaute Verbindung an ein Backend-Bearbeitungs-Computersystem weiter, welches zuvor vom Bearbeitungs-Load Balancer ausgewählt wurde. Anschließend kann dann beispielsweise durch das externe Computersystem auf eine Anwendung zugegriffen werden, die durch das Backend-Bearbeitungs-Computersystem bereitgestellt wird.

In einem weiteren Aspekt wird die obige Aufgabe durch ein verteiltes Rechnernetz nach Anspruch 11 gelöst. Das verteilte Rechnernetz weist eine Computernetz-Infrastruktur auf, welche zumindest ein Vermittlungs-Computersystem und ein Bearbeitungs-Computersystem umfasst. Ferner ist zumindest ein externes Computersystem im verteilten Rechnernetz eingerichtet, welches sich außerhalb der Computernetz-Infrastruktur befindet.

Das externe Computersystem ist eingerichtet, ein Authentifizierungs-Paket an das Vermittlungs-Computersystem zu übertragen zur Authentifizierung für eine Kommunikation mit dem Bearbeitungs-Computersystem. Das Vermittlungs-Computersystem ist eingerichtet, das Authentifizierungs-Paket automatisiert an das Bearbeitungs-Computersystem zu übertragen.

Das Bearbeitungs-Computersystem weist eine Zugriffssteuereinheit auf, die eingerichtet ist, zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen zu

halten, so dass ein Zugriff auf das Bearbeitungs-Computersystem über ein Netzwerk vermittels dieser Netzwerk-Ports verhindert ist, jedoch ein Zugriff des Bearbeitungs-Computersystems auf das Vermittlungs-Computersystem erlaubt ist, um das Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen.

Ferner ist die Zugriffssteuereinheit des Bearbeitungs-Computersystems eingerichtet, nach einer erfolgreichen Authentifizierung des externen Computersystems am Bearbeitungs-Computersystem oder an einem dem Bearbeitungs-Computersystem nachgeschalteten Backend-Bearbeitungs-Computersystem zumindest einen selektiven Netzwerk-Port für eine Kommunikation mit dem externen Computersystem freizuschalten.

Vorteilhaft ist ein derartiges verteiltes Rechnernetz eingerichtet, ein Verfahren der hier erläuterten Art durchzuführen.

Auch durch ein verteiltes Rechnernetz dieser Art ergeben sich die im Zusammenhang mit dem oben erläuterten Verfahren genannten Vorteile analog. Sämtliche vorteilhaften Maßnahmen, die im Zusammenhang mit dem obigen Verfahren erläutert wurden, finden in entsprechenden strukturellen Merkmalen des verteilten Rechnernetzes Anwendung und umgekehrt.

In einem weiteren Aspekt wird die obige Aufgabe durch ein Computerprogramm-Produkt nach Anspruch 15 gelöst, welches eingerichtet ist, auf einem oder mehreren Computersystemen ausgeführt zu werden und welches bei Ausführung ein Verfahren der oben erläuterten Art durchführt.

Weitere vorteilhafte Ausführungen sind in den Unteransprüchen sowie in der nachfolgenden Figurenbeschreibung offenbart.

Die Erfindung wird anhand zweier Zeichnungen im Folgenden näher erläutert.

Es zeigen:

Figur 1 eine schematisierte Darstellung zumindest eines Teils einer Computernetz-Infrastruktur gemäß einer ersten Konfiguration zum Freischalten eines externen Computersystems,

Figur 2 eine schematisierte Darstellung zumindest eines Teils einer Computernetz-Infrastruktur gemäß einer zweiten Konfiguration zum Freischalten eines externen Computersystems,

Figur 3 eine schematisierte Darstellung zumindest eines Teils einer Computernetz-Infrastruktur gemäß einer dritten Konfiguration mit Load Balancing zum Freischalten eines externen Computersystems,

Figur 4 eine schematisierte Darstellung zumindest eines Teils einer Computernetz-Infrastruktur gemäß einer vierten Konfiguration mit Load Balancing zum Freischalten eines externen Computersystems und

Figur 5 eine schematisierte Darstellung zumindest eines Teils einer Computernetz-Infrastruktur gemäß einer weiteren Konfiguration mit Load Balancing zur generellen Kommunikation mit einem externen Computersystem.

Figur 1 zeigt eine schematisierte Darstellung eines Teils einer Computernetz-Infrastruktur, umfassend ein Vermittlungs-Computersystem, das in Figur 1 als Task-Server deklariert ist, sowie ein Bearbeitungs-Computersystem, das in Figur 1 als Ziel-Server deklariert ist. Der Task-Server und der Ziel-Server können über ein Netzwerk N miteinander kommunizieren sowie Daten austauschen.

Ferner umfasst die Computernetz-Infrastruktur nach Figur 1 einen Paket-Filter, der nach innen zum Task-Server sowie zum Ziel-Server hin über das Netzwerk N angebunden ist und nach außen hin über Internet beziehungsweise über ein weiteres Intranet an die Außenwelt angebunden ist. Letztere Anbindung ist schematisiert in Figur 1 symbolisch als Wolke angedeutet.

Der Task-Server ist in der dargestellten Topologie als so genanntes „offenes" System eingerichtet. Das bedeutet, dass der Task-Server zumindest einen Netzwerk-Port für die in diesem Kontext erläuterten Zwecke geöffnet hat, wobei ein Dienst beziehungsweise eine Applikation auf dem Task-Server läuft, um eine Ansprechbarkeit beziehungsweise einen Verbindungsaufbau über das Netzwerk N zu ermöglichen. Beispielsweise kann eine Netzwerk-Verbindung bei diesem Computersystem über VPN („Virtual Private Network") oder SSH („Secure Shell") oder eine Kombination derartiger Sicherheitsmaßnahmen eingeschränkt sein, so dass nur vorbestimmte, verschlüsselte Netzwerk-Verbindungen über das Netzwerk N mit dedizierten Computersystemen erlaubt sind. Der Task-Server dient als Vermittler zur Kommunikation und Weiterleitung von Daten-Paketen an den Ziel-Server innerhalb der Computernetz-Infrastruktur.

Im Unterschied zum Task-Server verhält sich der Ziel-Server generell als speziell abgesichertes System mit geschlossenen Netzwerk-Ports. Dies ist durch eine schraffierte Ein-/Ausgangsebene am Ziel-Server in der Zeichnung schematisiert dargestellt. Das bedeutet, dass an den Netzwerk-Ports des Ziel-Servers initial keine laufenden Programme oder Dienste für eine Ansprechbarkeit beziehungsweise einen Verbindungsaufbau über das Netzwerk N von außen sichtbar bzw. verfügbar sind. Vielmehr ist ein nicht autorisierter Zugriff auf den Ziel-Server über das Netzwerk N aufgrund der jeweils geschlossenen Netzwerk-Ports des Ziel-Servers nicht möglich, weil nicht authentifizierte Verbindungen, z.B. durch geeignete Firewall-Regeln (z.B. iptables) - entweder auf dem Ziel-Server selbst oder auf einem vorgeschalteten System (z.B. einem Router) - unterbunden werden. Es ist jedoch denkbar, dass eine Benutzergruppe lokal auf den Ziel-Server zugreifen kann, um dort lokal vorbestimmte Aktionen durchzuführen.

Der Paket-Filter weist zum Task-Server und zum Ziel-Server hin (d. h. in Richtung des Netzwerkes N hin) Netzwerk-Ports auf, die zu den in diesem Kontext genannten Zwecken geschlossen sind. Dies ist in Figur 1 durch eine kreuz-schraffierte Ein-/Ausgangsebene am Paket-Filter in Richtung des Netzwerks N dargestellt. Das bedeutet, dass der Paket-Filter, wie im Zusammenhang mit dem Ziel-Server oben erläutert, keinerlei Daten nach außen weiterleitet und daher keinerlei Verbindungsaufbau vom Task-Server oder vom Ziel-Server über das Netzwerk N aus nach außen zulässt.

Umgekehrt umfasst der Paket-Filter in der Kommunikationsrichtung von außerhalb der Computernetz-Infrastruktur, das heißt, über das symbolisch dargestellte

Internet oder ein weiteres Intranet zumindest einen geöffneten Netzwerk-Port (so genannter „Listening" Port) auf, so dass ein Verbindungsaufbau von außerhalb (Internet, Intranet) vermittels des Paket-Filters über das Netzwerk N auf den Task-Server der Computernetz-Infrastruktur möglich ist. Der Paket-Filter gemäß Figur 1 stellt somit einen Schutz der Computernetz-Infrastruktur nach außen dar. Weiterhin verhindert er nicht-gewollten Traffic von innen nach außen.

Zur Kommunikation innerhalb der Computernetz-Infrastruktur zwischen dem Task-Server und dem Ziel-Server ist ein vorbestimmter Prozess eingerichtet. Anweisungen können vom Ziel-Server unmittelbar über eine aufgebaute Verbindung („Established") an den Task-Server übertragen werden, weil der Task-Server, wie oben erläutert, über das Netzwerk N direkt vom Ziel-Server ansprechbar ist.

In Richtung zum Ziel-Server hin muss, ausgehend vom Task-Server oder von einem externen Computersystem (nicht dargestellt) außerhalb der Computernetz-Infrastruktur, zunächst ein Port-Knocking-Prozess durchgeführt werden. Hierzu wird eine vorbestimmte Sequenz an Paket-Daten entweder vom Task-Server oder vom externen Computersystem an den Ziel-Server gesendet, wobei die Netzwerk-Ports des Ziel-Servers geschlossen sind und wobei die Sequenz in einer vorbestimmten Reihenfolge einen oder mehrere Netzwerk-Ports des entsprechenden Bearbeitungs-Computersystems anspricht. Anschließend erfolgt eine Überprüfung der gesendeten Sequenz im Ziel-Server auf Übereinstimmung mit einer vordefinierten Sequenz. Im Erfolgsfall erfolgt für eine Kommunikation zwischen dem Ziel-Server und dem Task-Server ein Verbindungsaufbau ausgehend vom Ziel-Server hin zum Task-Server sowie ein Veranlassen eines Übertragens eines

entsprechenden Daten-Paketes und/oder einer Anweisung über die aufgebaute Verbindung („Established").

Insbesondere startet der Ziel-Server einen Prozess, der ein zu übertragendes Daten-Paket vom Task-Server abholt. Ein derartiger Prozess kann beispielsweise über den Unix-basierten Befehl „Secure Copy" (scp) erfolgen. Auf diese Weise können die beteiligten Computersysteme trotz geschlossener Netzwerk-Ports des Ziel-Servers innerhalb der Computernetz-Infrastruktur miteinander kommunizieren, Daten-Pakete weiterleiten und/oder Anweisungen erteilen.

Nachfolgend soll anhand mehrerer Verfahrensschritte, welche in der Zeichnung als Nummerierungen 1 bis 6 aufgeführt sind, ein Verfahren zum Freischalten einer Kommunikation zwischen dem abgesicherten Ziel-Server innerhalb der Computernetz-Infrastruktur und einem externen Computersystem außerhalb der Computernetz-Infrastruktur, welches in Figur 1 nicht dargestellt ist, erläutert werden.

In einem Schritt 1 verlangt ein externes Computersystem über das Internet und/oder ein von der Computernetz-Infrastruktur (Netzwerk N) getrenntes Intranet eine Freischaltung einer Kommunikation mit dem Ziel-Server. Das externe Computersystem kann beispielsweise ein Client sein, der eine Applikation auf dem Ziel-Server innerhalb der Computernetz-Infrastruktur freischalten will. Der Ziel-Server hat jedoch zu diesem Zeitpunkt für das externe Computersystem keine offenen Netzwerk-Ports und gestattet keinen Verbindungsaufbau von extern.

Das externe Computersystem kann beispielsweise hinter einem NAT-/PAT-Router sitzen, der eine lokale private IP-Adresse

des externen Computersystems mit einer (eindeutigen) öffentlichen IP-Adresse des Routers maskiert. Auf diese Weise ist jedoch das externe Computersystem durch den Ziel-Server nicht direkt ansprechbar, weil der Ziel-Server die genaue (private) IP-Adresse des externen Computersystems nicht kennt. Ferner kann gemäß der Konfiguration aus Figur 1 der Ziel-Server über den Paket-Filter gar keine Verbindung nach außerhalb der Computernetz-Infrastruktur initiieren, weil der Paket-Filter in Richtung des Netzwerks N, wie oben erläutert, keine Daten weiterleitet und keinen Verbindungsaufbau nach außen zulässt.

Für eine Authentifizierung des externen Computersystems zum Freischalten einer Kommunikation mit dem Ziel-Server, der initial ebenfalls geschlossene Netzwerk-Ports aufweist und keinen unmittelbaren Verbindungsaufbau vom externen Computersystem aus zulässt, muss somit ein spezielles Authentifizierungs-Verfahren durchgeführt werden.

Hierzu schickt das externe Computersystem im Schritt 1 über das Internet/Intranet (vgl. das Wolkensymbol in Figur 1) und via dem Paket-Filter ein Authentifizierungs-Paket über das Netzwerk N an den von außen ansprechbaren Task-Server innerhalb der Computernetz-Infrastruktur. Zur Übertragung dieses Paketes kann eine Authentifizierung des externen Computersystems am Task-Server (z. B. über ein VPN und/oder ähnliches) notwendig sein.

Das Authentifizierungs-Paket enthält signierte Informationen zur Authentifizierung des externen Computersystems am Ziel-Server. Diese signierten Informationen können beispielsweise Signaturen des externen Computersystems und/oder eines separaten Key-Computersystems (nicht dargestellt) enthalten,

wobei das Key-Computersystem eine Sicherheits-Instanz zum Festlegen und Signieren des externen Computersystems als erlaubtes Computersystem für einen Zugriff auf den Ziel-Server darstellt. Ein separates Key-Computersystem als getrennte Sicherheits-Instanz hat den Vorteil, dass eine Authentifizierung allein im externen Computersystem nicht oder nur erschwert gefälscht werden kann. Auf diese Weise wird sichergestellt, dass ein externes Computersystem, welches den Ziel-Server für eine Kommunikation zumindest partiell freischalten will, tatsächlich autorisiert ist.

Ferner können die signierten Informationen im Authentifizierungs-Paket auch Informationen über das externe Computersystem (z. B. welchen Dienst das externe Computersystem ansprechen will) und/oder gegebenenfalls Durchführungsparameter zur vorbestimmten Durchführung eines Freischaltens beziehungsweise eines nach dem Freischalten durchzuführenden Prozesses im Ziel-Server enthalten. Das Authentifizierungs-Paket kann auch aus Passwörtern (von Benutzern) generierte Daten, wie z.B. Hashes oder Signaturen, enthalten. Eine weitere oder endgültige Authentifizierung ist optional am Ziel-Server möglich.

In einem Schritt 2 schickt das externe Computersystem über das Internet/Intranet und den Paket-Filter der Computernetz-Infrastruktur vermittels des Netzwerks N unmittelbar an den Ziel-Server ein Anklopfsignal im Sinne eines Port-Knockings (wie oben mehrfach erläutert). Eine vorbestimmte Daten-Sequenz des Anklopfsignals wird an den zunächst geschlossenen Netzwerk-Ports des Ziel-Servers über einen Dienst (z. B. einen Knock-Daemon) ausgewertet und mit einer vordefinierten Daten-Sequenz verglichen. Bei Übereinstimmung wird beispielsweise ein Skript oder Programm im Ziel-Server

gestartet zur weiteren Prozessierung des im Task-Server vorliegenden Authentifizierungs-Paketes.

Die Maßnahmen des Schrittes 2 (Anklopfen am Ziel-Server) stellen gewissermaßen eine Initiierung für den Ziel-Server dar, dass im Task-Server ein Daten-Paket für weitergehende Aktionen vorliegt. Ein Port-Knocking am Ziel-Server kann alternativ zum externen Computersystem auch vom Task-Server aus in Richtung Ziel-Server erfolgen.

Das im Task-Server vorliegende Authentifizierungs-Paket wird in einem Schritt 3 zunächst lokal verarbeitet. Diese Verarbeitung kann eine Signaturprüfung und/oder eine Prüfung von weiteren Informationen im Authentifizierungs-Paket, wie z. B. von Durchführungsparametern, umfassen. Weiterhin wird in diesem Schritt das Authentifizierungs-Paket um die sichtbare Quell-IP-Adresse ergänzt, die dem externen anfragenden Computersystem zugeordnet werden kann und beispielsweise die öffentliche IP-Adresse eines NAT-Routers ist, der das Authentifizierungs-Paket an den Task-Server gesendet hat. Auf diese Weise weiß der Ziel-Server im nachfolgenden Verfahren, dass diese ergänzte Quell-IP-Adresse temporär freigeschaltet werden soll.

Ferner erfolgt im Schritt 3 das Verschieben des Authentifizierungs-Paketes in eine Ablage für die Abholung durch den Ziel-Server, falls die Überprüfung des Authentifizierungs-Paketes im Task-Server erfolgreich war. Andernfalls (falls eine Überprüfung nicht erfolgreich war) kann das Authentifizierungs-Paket im Task-Server beispielsweise verworfen werden. Dann erfolgt keine weitergehende Aktion und das Verfahren ist beendet.

Ferner kann bei erfolgreicher Überprüfung und Ablage des Authentifizierungs-Paketes im Task-Server zur Abholung durch den Ziel-Server ein Routing des Authentifizierungs-Paketes zum Ziel-Server ermittelt werden. Dies ist beispielsweise bei einer Computernetz-Infrastruktur mit mehreren Ziel-Servern sinnvoll, so dass sichergestellt werden kann, dass ein Authentifizierungs-Paket an das richtige Ziel-Computersystem innerhalb der Computernetz-Infrastruktur verteilt wird.

Im Schritt 4 veranlasst der Ziel-Server einen Verbindungsaufbau über das Netzwerk N zum Task-Server und startet einen Prozess zum Übertragen des Authentifizierungs-Paketes vom Task-Server an den Ziel-Server über die aufgebaute Verbindung („Established"). Ein derartiger Prozess kann beispielsweise über den Unix-basierten Befehl scp erfolgen.

Anschließend wird das Authentifizierungs-Paket vom Task-Server an den Ziel-Server über das Netzwerk N der Computernetz-Infrastruktur übertragen.

Vorteilhaft wird das Authentifizierungs-Paket nochmals im Ziel-Server überprüft. Hierzu können Prüfschritte durchgeführt werden, wie sie auch in Schritt 3 im Task-Server durchgeführt worden sind. Zusätzliche Prüfschritte, z. B. ein Überprüfen eines Prozesses im Ziel-Server, der durch das Authentifizierungs-Paket angewiesen werden soll, und so weiter, sind denkbar.

Falls auch hier eine Überprüfung des Authentifizierungs-Paketes erfolgreich ist, erfolgt ein Freischalten der Quell-IP-Adresse, die dem Ziel-Server vermittels des ergänzten Authentifizierungs-Paketes als die externe Quell-IP-Adresse

(die dem externen anfragenden Computersystem zugeordnet werden kann) bekannt ist (siehe oben). Das Freischalten kann selektiv an einem oder mehreren einzelnen Ziel-Netzwerk-Ports des Ziel-Servers erfolgen. Somit ist der Ziel-Server für einen Verbindungsaufbau ausgehend von der Quell-IP-Adresse (und nur von dieser) selektiv an einem oder mehreren bestimmten Ziel-Netzwerk-Ports ansprechbar.

In einem folgenden Schritt 5, welcher vorteilhaft in einem fest vorgegebenen (kurzen) Zeitraum nach Freischalten des/der selektiven Ziel-Netzwerk-Ports am Ziel-Server erfolgen soll, baut nun das externe Computersystem, welches aus dem Internet/Intranet via dem Paket-Filter über das Netzwerk N auf die Computernetz-Infrastruktur zugreifen kann, eine erneute Verbindung (neue Session mit der Kombination „externe bekannte Quell-IP-Adresse/ausgewählter Quell-Netzwerk-Port) zu dem/einem geöffneten Ziel-Netzwerk-Port des Ziel-Servers auf. Falls beispielsweise in einem vorbestimmten Zeitraum kein solcher Verbindungsaufbau seitens des externen Computersystems erfolgt, werden alle verfahrensgemäß selektiv geöffneten Ziel-Netzwerk-Ports für die betroffene IP-Adresse am Ziel-Server wieder geschlossen (sofern keine anderen externen Computersysteme im selben Zeitfenster anfragen), so dass der Ziel-Server für sämtliche externen Computersysteme mit derselben Quell-IP-Adresse nicht mehr ansprechbar ist (Initialzustand). Externe Computersysteme mit einer anderen IP-Adresse können hiervon unberührt während des gesamten Verfahrensablaufs keine Verbindung zum Ziel-Server aufbauen.

Anderenfalls - bei rechtzeitigem Verbindungsaufbau einer neuen Session - erfolgt über die somit aufgebaute und bestehenbleibende („established") Verbindung zwischen dem externen Computersystem (vermittels der bekannten Quell-IP-

Adresse) und dem Ziel-Server ein nochmaliges Übertragen eines Verifikations-Paketes unmittelbar an den nunmehr selektiv geöffneten Ziel-Server. Das Verifikations-Paket kann die identischen Informationen des Authentifizierungs-Paketes enthalten, welches zuvor vermittels des Task-Servers auf den Ziel-Server gelangt ist. Alternativ oder ergänzend kann das Verifikationspaket auch weitere Verifikationsmerkmale (z.B. Identitätsmerkmale des externen Computersystems oder dessen Benutzer, biometrische Daten, Passwörter, Passphrasen, Schlüssel, usw.) enthalten.

Im Ziel-Server erfolgt dann eine Überprüfung der Identität des Verifikations-Paketes mit dem zuvor gesendeten Authentifizierungs-Paket bzw. eine Überprüfung und Bestätigung der Informationen des Authentifizierungs-Paketes anhand der weiteren Verifikationsmerkmale, je nachdem, wie das Verifikations-Paket ausgestaltet ist. Diese Überprüfung stellt eine Sicherheitsmaßnahme dar, dass die aufgebaute Verbindung tatsächlich von demjenigen externen Computersystem (und nur von diesem) initiiert worden ist, welches zuvor eine Freischaltung des Ziel-Servers angefragt hat. Insbesondere ist diese Überprüfung eine Sicherheitsmaßnahme gegen Angreifer, die das Authentifizierungs-Paket nicht geschickt haben, jedoch hinter einem NAT-Router mit der im Ziel-Server freigeschalteten Quell-IP-Adresse sitzen und die Freischaltung für einen manipulierten Zugriff auf den Ziel-Server als Angriff ausnutzen wollen. Derartige Angreifer könnten dann entweder kein Verifikations-Paket oder ein falsches Verifikations-Paket vorweisen, so dass der Ziel-Server erkennt, dass eine nicht-autorisierte Verbindung aufgebaut worden ist. Eine derartige Sicherheitsmaßnahme erschwert somit eine Manipulation des Verfahrens durch Angreifer von außen.

Wenn die Übereinstimmung bzw. Bestätigung des Authentifizierungs-Paketes durch das Verifikations-Paket erfolgreich abgeprüft worden ist, erfolgt eine Beschränkung der aufgebauten Verbindung ausschließlich auf die Kombination der freigeschalteten Quell-IP-Adresse in Verbindung mit dem Quell-Netzwerk-Port, von dem aus das Verifikations-Paket zuletzt übertragen worden ist. Auf diese Weise beschränkt der Ziel-Server die aufgebaute Verbindung nicht nur auf die Quell-IP-Adresse, sondern auch auf die tatsächliche Quell-Verbindung via verwendetem Quell-Netzwerk-Port des autorisierten externen Computersystems. Weitere Verbindungen über die gleiche Quell-IP-Adresse, aber über andere Quell-Netzwerk-Ports auf den Ziel-Server werden dadurch unterbunden. Auch auf diese Weise werden mögliche Angriffsszenarien deutlich erschwert beziehungsweise unterbunden. Bei diesen Maßnahmen ist zu berücksichtigen, dass ggf. parallel stattfindende Verbindungsaufbauten mehrerer Computersysteme sich nicht gegenseitig beeinträchtigen.

Nach diesem Procedere steht somit lediglich eine selektiv aufgebaute Verbindung zwischen dem Quell-Netzwerk-Port des externen Computersystems (womöglich via maskiertem Quell-Netzwerk-Port eines NAT-Routers) und einem selektiv freigeschalteten Ziel-Netzwerk-Port am Ziel-Server. In einem weiterführenden Schritt 6 kann dann eine applikationsspezifische weitere Kommunikation vermittels dieser eingeschränkten Verbindung zwischen dem externen Computersystem und dem Ziel-Server innerhalb der Computernetz-Infrastruktur erfolgen.

Auf diese Weise hat das externe Computersystem über eine Authentifizierung eine Freischaltung des Ziel-Servers für eine Kommunikation erwirkt. Dennoch ist das Verfahren im Gegensatz zu herkömmlichen Maßnahmen deutlich sicherer gegen Angriffe von außen.

Figur 2 zeigt die Konfiguration der Computernetz-Infrastruktur gemäß Figur 1, jedoch zusätzlich mit einem weiteren Paket-Filter FW, welcher im Netzwerk N zwischen dem Task-Server und dem Ziel-Server als Sicherheitsmaßnahme gegen Angriffe innerhalb der Computernetz-Infrastruktur eingerichtet ist. Sämtliche weiteren Instanzen, Maßnahmen und Verfahrensschritte sind identisch mit dem Vorgehen gemäß Figur 1 und bedürfen an dieser Stelle keiner weiteren Erläuterung.

Der Paket-Filter FW dient im Wesentlichen der Vereitelung eines Angriffs auf den Ziel-Server ausgehend vom Task-Server. Ein Eindringling, der im Task-Server entsprechende Rechte (z. B. Administrator-Rechte) erlangt hat, hätte die Möglichkeit eines Angriffs mittels IP-Spoofing, um sich beispielsweise als externer Client mit einer autorisierten externen IP-Adresse auszugeben. So könnte ein optionaler Port-Filter auf dem Ziel-Server (der keinen Verbindungsaufbau von anderen Computersystemen zulässt) umgangen werden. Auf diese Weise könnte ausgehend vom Task-Server über eine gefälschte IP-Adresse ein autorisierter Zugang zum Ziel-Server vorgetäuscht werden.

Als Gegenmaßnahme ist der Paket-Filter FW eingerichtet, der in der Kommunikationsrichtung vom Task-Server zum Ziel-Server lediglich Daten-Pakete einer bereits aufgebauten Verbindung („Established" oder „Related") zulässt, die von der exakten

IP-Adresse des Task-Servers ausgehen. Andere Daten-Pakete werden am Paket-Filter FW in dieser Kommunikationsrichtung verworfen beziehungsweise ignoriert und nicht weitergeleitet. Somit gelangen zum Ziel-Server lediglich Daten-Pakete, die verlässlich und vertrauenswürdig vom Task-Server stammen. Eine Fälschung einer IP-Adresse, ausgehend vom Task-Server (IP-Spoofing), wird dadurch extrem erschwert beziehungsweise unterbunden.

In umgekehrter Kommunikationsrichtung vom Ziel-Server hin zum Task-Server kann der Paket-Filter FW vorteilhaft lediglich Daten-Pakete zulassen, die einen speziellen Dienst am Task-Server (z. B. scp oder ssh oder eine Kombination davon, usw.) ansprechen. Auf diese Weise ist der Task-Server in Richtung Ziel-Server gänzlich abgeschnitten, so dass kein Angriff ausgehend vom Task-Server auf den Ziel-Server erfolgreich ist. In umgekehrter Richtung kann der Ziel-Server jedoch wie gemäß Figur 1 erläutert beispielsweise ein Authentifizierungs-Paket über den Dienst scp vom Task-Server abholen.

Der Paket-Filter FW gemäß Figur 2 kann beispielsweise als speziell abgesicherter 1:1 NAT-Router (IP-Adress-Umsetzer) realisiert sein. Es ist auch denkbar, in diesem Router spezielle Überprüfungsmechanismen, auch in Bezug zum Authentifizierungs-Paket, vorzusehen. Bei 1:1 NAT-Routing werden IP-Adressen eingehender Pakete statisch in andere IP-Adressen umgesetzt. Beispielsweise könnte ein eingehendes Paket mit der beispielhaften Adresse 10.10.10.10 in die IP-Adresse 11.11.11.11 umgesetzt werden.

Figur 3 zeigt eine dritte Konfiguration einer Computernetz-Infrastruktur, die grundsätzlich wie die Computernetz-

Infrastruktur gemäß Figur 2 eingerichtet ist und entsprechend arbeitet. Allerdings umfasst die Computernetz-Infrastruktur gemäß Figur 3 zwei Vermittlungs-Computersysteme, nämlich Task-Server 1 und Task-Server 2, sowie zwei Bearbeitungs-Computersysteme, nämlich Ziel-Server 1 und Ziel-Server 2. Zusätzlich ist in dem Paket-Filter, vergleiche auch Figur 1, ein Load Balancer integriert, der in der Konstellation gemäß Figur 3 als Vermittlungs-Load Balancer arbeitet. Die Funktionsweise der Computernetz-Infrastruktur gemäß Figur 3 wird nachfolgend erläutert.

In einem Schritt 1 baut ein externes Computersystem, das analog zu den Erläuterungen zu Figuren 1 und 2 als externer Client eingerichtet sein kann, über das Internet und/oder ein von der Computernetz-Infrastruktur (Netzwerk N) getrenntes Intranet eine Verbindung über den Paket-Filter zum Load Balancer auf. Die beiden Bearbeitungs-Computersysteme, Ziel-Server 1 und Ziel-Server 2, haben jedoch zu diesem Zeitpunkt für das externe Computersystem über das Netzwerk N keine offenen Netzwerk-Ports und gestatten keinen Verbindungsaufbau von extern. Gegenüber Task-Server 1 und Task-Server 2 sind Ziel-Server 1 und Ziel-Server 2 im Übrigen über den weiteren Paket-Filter FW abgesichert, wie im Zusammenhang mit Figur 2 erläutert.

Der Load Balancer leitet die Daten-Pakete (generell IP-Pakete) des externen Computersystems mittels eines beliebigen Load-Balancing-Algorithmus an eines der Vermittlungs-Computersysteme, Task-Server 1 oder Task-Server 2, weiter. Zur Auswahl von Task-Server 1 oder Task-Server 2 kann sich der Load Balancer zum Beispiel eines Algorithmus gemäß dem so genannten „Source Hashing Scheduling“ bedienen. Dabei wählt der Load Balancer in Abhängigkeit von der öffentlichen IP-

Adresse, die dem externen Computersystem zugeordnet werden kann, einen entsprechenden Task-Server aus der Gruppe der Task-Server 1 und Task-Server 2 aus, hier beispielhaft Task-Server 1.

Auf diese Weise wird verfahrensgemäß das bereits erläuterte Authentifizierungs-Paket vom externen Computersystem vermittels des Load Balancers in Schritt 1 an Task-Server 1 übertragen und dort, wie oben im Zusammenhang mit Figur 1 erläutert, in einem Schritt 2 weiterverarbeitet. Dies umfasst zum Beispiel eine Überprüfung auf Gültigkeit und ein Ergänzen um die IP-Adresse, die dem externen Computersystem zugeordnet werden kann.

Generell können in dieser Konfiguration auch Task-Server 1 und Task-Server 2 zwischen Ziel-Server 1 und Ziel-Server 2 anhand eines vorbestimmten Algorithmus auswählen. Vorteilhaft ist hierbei der Algorithmus zur Auswahl eines der Ziel-Server 1 und Ziel-Server 2 derselbe wie der Algorithmus im Load Balancer zur Auswahl eines der Task-Server 1 und Task-Server 2 in Abhängigkeit von der IP-Adresse, die dem externen Computersystem zugeordnet werden kann. Somit ist sichergestellt, dass eine Zuordnung eines externen Computersystems zur Freischaltung für einen Verbindungsaufbau auf einen entsprechenden Ziel-Server sowohl im Load Balancer als auch in Task-Server 1 und Task-Server 2 identisch erfolgt. Dies hat den Effekt, dass ein Verbindungsaufbau von einem freigeschalteten externen Computersystem vermittels des Load Balancers auch auf denjenigen Ziel-Server aus Ziel-Server 1 oder Ziel-Server 2 erfolgt, an den das entsprechende Authentifizierungs-Paket des externen Computersystems zu dessen Freischaltung übermittelt worden ist.

Beispielhaft führt Task-Server 1 in einem Schritt 3 ein Port-Knocking am zuvor von ihm ausgewählten Ziel-Server 1 durch, um dem Ziel-Server 1 zu signalisieren, dass ein Authentifizierungs-Paket in Task-Server 1 abholbereit ist. Anschließend kann Ziel-Server 1 in Schritt 4 eine Verbindung zum Task-Server 1 aufbauen und das Authentifizierung-Paket zu sich abholen, wie verfahrensgemäß im Zusammenhang mit Figur 1 und 2 erläutert.

In einem Schritt 5 überprüft Ziel-Server 1 analog zum oben erläuterten Verfahren die Berechtigung des externen Computersystems anhand des Authentifizierungs-Paketes für den weiteren Verbindungsaufbau. Im Erfolgsfall wird entsprechend ein Netzwerk-Port im Ziel-Server 1 für die IP-Adresse, die dem externen Computersystem zugeordnet werden kann, für einen Zugriff durch das externe Computersystem freigeschaltet.

In einem weiteren Schritt 6 erfolgt schließlich, gegebenenfalls nach einer gesteuerten (kurzen) Wartezeit, ein Verbindungsaufbau einer neuen Session vom externen Computersystem an den Load Balancer, der ihn (mit demselben Algorithmus wie dem von Task-Server 1 verwendeten) an Ziel-Server 1 weiterleitet. Dieser Verbindungsversuch wird eventuell mehrmals wiederholt, falls dieser nicht direkt erfolgreich ist. Diese neue Session kann zum Beispiel direkt die gewünschte Verbindung zu einer Anwendung im Ziel-Server 1 sein, beispielsweise eine VPN-Verbindung, in der die weitere Kommunikation gemäß einem Schritt 7 abgesichert erfolgt.

Im Übrigen sei für die weitere Funktionalität der Computernetz-Infrastruktur gemäß Figur 3 auf die Erläuterungen zu Figur 1 und Figur 2 verwiesen.

Figur 4 zeigt eine weitere Konfiguration einer Computernetz-Infrastruktur, die die Struktur aus Figur 3 weiterbildet. Auch in der Computernetz-Infrastruktur gemäß Figur 4 sind mehrere Vermittlungs-Computersysteme, Task-Server 1 und Task-Server 2, eingerichtet, denen ein Load Balancer 1 vorgeschaltet ist. Load Balancer 1 arbeitet analog zum Load Balancer gemäß Figur 3 als so genannter Vermittlungs-Load Balancer zur Auswahl eines aus Task-Server 1 und Task-Server 2 zur Entgegennahme von Daten-Paketen eines externen Computersystems.

Die Gruppe der Bearbeitungs-Computersysteme umfasst gemäß Figur 4 einen Load Balancer 2, der als so genannter Bearbeitungs-Load Balancer arbeitet, sowie analog zu Figur 3 einen Ziel-Server 1 sowie einen Ziel-Server 2, die beide als so genannte Backend-Bearbeitungs-Computersysteme dem Load Balancer 2 in der Kommunikation nachgeschaltet sind. Die Funktionsweise der Computernetz-Infrastruktur gemäß Figur 4 wird nachfolgend erläutert.

In einem Schritt 1 baut ein externes Computersystem über das Internet und/oder ein von der Computernetz-Infrastruktur getrenntes Intranet eine Verbindung über den optionalen Paket-Filter vermittels Netzwerk N1 zum Load Balancer 1 auf. Load Balancer 2 hat jedoch zu diesem Zeitpunkt für das externe Computersystem keine offenen Netzwerk-Ports und gestattet keinen Verbindungsaufbau von extern.

Analog zu der bereits erläuterten Vorgehensweise wählt Load Balancer 1 in diesem Beispiel Task-Server 2 aus und übergibt diesem vermittels Netzwerk N2 das Authentifizierungs-Paket des externen Computersystems. In einem Schritt 2 wird das Authentifizierung-Paket im Task-Server 2 weiterverarbeitet,

zum Beispiel auf seine Gültigkeit hin überprüft und um die IP-Adresse, die dem externen Computersystem zugeordnet werden kann, ergänzt.

Beispielhaft führt Task-Server 2 in einem Schritt 3 vermittels Netzwerk N3 ein Port-Knocking am Load Balancer 2 durch, um dem Load Balancer 2 zu signalisieren, dass ein Authentifizierungs-Paket in Task-Server 2 abholbereit ist. Anschließend kann Load Balancer 2 in Schritt 4 über das Netzwerk N3 eine Verbindung zum Task-Server 2 aufbauen und das Authentifizierung-Paket zu sich abholen, wie verfahrensgemäß im Zusammenhang mit Figur 1 und 2 erläutert.

In einem Schritt 5 überprüft Load Balancer 2 analog zum oben erläuterten Verfahren die Berechtigung des externen Computersystems anhand des Authentifizierungs-Paketes für den weiteren Verbindungsaufbau. Im Erfolgsfall wird entsprechend ein Netzwerk-Port im Load Balancer 2 für die IP-Adresse, die dem externen Computersystem zugeordnet werden kann, für einen Zugriff durch das externe Computersystem freigeschaltet.

In einem weiteren Schritt 6 erfolgt schließlich, gegebenenfalls nach einer gesteuerten (kurzen) Wartezeit, ein Verbindungsaufbau einer neuen Session vom externen Computersystem an den nun für das externe Computersystem freigeschalteten Load Balancer 2. Dieser Verbindungsversuch wird eventuell mehrmals wiederholt, falls dieser nicht direkt erfolgreich ist. Load Balancer 2 kann über einen beliebigen Algorithmus zwischen Ziel-Server 1 und Ziel-Server 2 zur Weiterleitung einer Verbindung vom externen Computersystem auswählen, wobei Ziel-Server 1 und Ziel-Server 2 über geöffnete Netzwerk-Ports am Netzwerk N4 zum Load Balancer 2 hin durch diesen ansprechbar sind. In dem Beispiel gemäß

Figur 4 leitet Load Balancer 2 in Schritt 7 die Verbindung des externen Computersystems über das Netzwerk N4 an Ziel-Server 1 weiter. Diese neue Session kann zum Beispiel direkt die gewünschte Verbindung zu einer Anwendung im Ziel-Server 1 sein, beispielsweise eine VPN-Verbindung, in der die weitere Kommunikation gemäß einem Schritt 7 abgesichert erfolgt.

Es sei angemerkt, dass Load Balancer 1 und Load Balancer 2 gegebenenfalls in einem physischen Gerät integriert sein können. Zudem können einer oder beide Load Balancer 1 und/oder 2 gegebenenfalls redundant ausgelegt sein. Dabei sollte die aktuelle Konfiguration entsprechend auf den redundanten Load Balancer gespiegelt werden, zum Beispiel über ein Storage Area Network.

Im Übrigen sei für die weitere Funktionalität der Computernetz-Infrastruktur gemäß Figur 4 auf die Erläuterungen zu Figur 1 bis 3 verwiesen.

Figur 5 zeigt eine Konfiguration einer Computernetz-Infrastruktur mit einer Funktionalität ähnlich den Erläuterungen zu den Figuren 3 und 4. Im Unterschied zur Konstellationen in Figur 4 weist die Computernetz-Infrastruktur gemäß Figur 5 lediglich einen Load Balancer 1 sowie einen optionalen Paket-Filter auf. Im Übrigen sind in der Computernetz-Infrastruktur gemäß Figur 5 wiederum zwei Task-Server 1 und 2 sowie zwei Ziel-Server 1 und 2 eingerichtet. Im Wesentlichen dient die Konstellation gemäß Figur 5 einem Zugriff auf einen der Ziel-Server 1 oder 2 vermittels eines Load Balancers durch ein externes Computersystem ohne Aufbau einer permanenten Session. Auf diese Weise können beispielsweise Daten-Pakete von einem externen Computersystem an einen der Ziel-Server 1 oder 2 zur

weiteren Verarbeitung innerhalb der abgesicherten Computernetz-Infrastruktur weitergegeben werden. Vermittels des Load Balancers 1 kann eine hohe Netzwerklast abgewickelt werden, so dass die Performance der Computernetz-Infrastruktur erhalten bleibt.
Gemäß Figur 5 baut ein externes Computersystem über das Internet und/oder ein von der Computernetz-Infrastruktur getrenntes Intranet eine Verbindung über den optionalen Paket-Filter vermittels Netzwerk N1 zum Load Balancer 1 auf.

Analog zu der bereits erläuterten Vorgehensweise wählt Load Balancer 1 in diesem Beispiel Task-Server 2 aus und übergibt diesem vermittels Netzwerk N2 ein oder mehrere Daten-Pakete des externen Computersystems. In einem Schritt 2 werden die Daten-Pakete im Task-Server 2 weiterverarbeitet, zum Beispiel auf ihre Gültigkeit hin überprüft.

Beispielhaft führt Task-Server 2 in einem Schritt 3 vermittels Netzwerk N3 ein Port-Knocking am zuvor ausgewählten Ziel-Server 1 durch, um dem Ziel-Server 1 zu signalisieren, dass Daten-Pakete in Task-Server 2 abholbereit sind. Ziel-Server 1 hält dabei sämtliche für das Verfahren maßgebliche Netzwerk-Ports für eine Ansprechbarkeit gegenüber Netzwerk N3 geschlossen. Allerdings kann Ziel-Server 1 in Schritt 4 über das Netzwerk N3 von sich aus eine Verbindung zum Task-Server 2 aufbauen und die Daten-Pakete zu sich abholen, wie verfahrensgemäß oben mehrfach erläutert. Eine weitere Verarbeitung der Daten-Pakete kann anschließend in einem letzten Schritt 5 im Ziel-Server 1 erfolgen. Auf diese Weise ist ein einfacher Datentransfer von einem externen Computersystem über einen Load Balancer zu einem Ziel-Server möglich. Eine VPN-Verbindung zwischen einem externen

Computersystem und einem der Ziel-Server wird in diesem Ausführungsbeispiel nicht aufgebaut.

Die hier dargestellten Verfahren haben den Vorteil, dass ein Freischalten externer Computersysteme für eine Kommunikation mit einem abgesicherten Bearbeitungs-Computersystem oder einem abgesicherten Bearbeitungs-Load Balancer zur Lastverteilung auf eine Mehrzahl von Backend-Bearbeitungs-Computersystemen innerhalb einer Computernetz-Infrastruktur auf sichere Art und Weise möglich ist, ohne das Bearbeitungs-Computersystem oder den Bearbeitungs-Load Balancer (auch) für externe oder interne Angreifer zu öffnen.

Bezugszeichenliste

Task-Server	Vermittlungs-Computersystem
Task-Server1, 2	Vermittlungs-Computersystem
Ziel-Server	Bearbeitungs-Computersystem
Ziel-Server1, 2	(Backend-) Bearbeitungs-Computersystem
Load Balancer	Vermittlungs-Load Balancer
Load Balancer1	Vermittlungs-Load Balancer
Load Balancer2	Bearbeitungs-Load Balancer
N, N1, N2, N3, N4	Netzwerk
FW	Paket-Filter
1 bis 7	Verfahrensschritte

Patentansprüche

1. Verfahren zum Freischalten externer Computersysteme für eine Kommunikation mit abgesicherten Bearbeitungs-Computersystemen in einer Computernetz-Infrastruktur, umfassend die Schritte:
- Übertragen eines Authentifizierungs-Paketes von einem externen Computersystem, welches außerhalb der Computernetz-Infrastruktur eingerichtet ist, an ein Vermittlungs-Computersystem innerhalb der Computernetz-Infrastruktur, wobei das Authentifizierungs-Paket signierte Informationen zur Authentifizierung des externen Computersystems enthält,
- automatisiertes Übertragen des Authentifizierungs-Paketes vom Vermittlungs-Computersystem an zumindest ein Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur,
wobei das Bearbeitungs-Computersystem zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen hält, so dass ein Zugriff auf das Bearbeitungs-Computersystem über Netzwerk vermittels dieser Netzwerk-Ports verhindert wird,
wobei jedoch das Bearbeitungs-Computersystem auf das Vermittlungs-Computersystem zugreifen kann, um das Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen,
- Freischalten zumindest eines selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem für eine Kommunikation mit dem externen Computersystem,
- Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems durch das externe Computersystem.

2. Verfahren nach Anspruch 1, wobei nach dem Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des

Bearbeitungs-Computersystems folgender zusätzlicher Schritt durchgeführt wird:
- Begrenzen der Kommunikation zwischen dem Bearbeitungs-Computersystem und dem externen Computersystem auf den freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems und einen Netzwerk-Port des externen Computersystems, der dem Bearbeitungs-Computersystem durch die aufgebaute Verbindung bekannt ist.

3. Verfahren nach Anspruch 1 oder 2, wobei nach dem Aufbauen einer Verbindung zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Computersystems durch das externe Computersystem folgende Schritte durchgeführt werden:
- Übertragen eines Verifikations-Paketes durch das externe Computersystem unmittelbar auf das Bearbeitungs-Computersystem vermittels der aufgebauten Verbindung und
- Bestätigen der Informationen des durch das Vermittlungs-Computersystem zuvor übertragenen Authentifizierungs-Paketes durch Verifikations-Informationen im Verifikations-Paket.

4. Verfahren nach einem der Ansprüche 1 bis 3, umfassend den zusätzlichen Schritt:
- Überprüfen des Authentifizierungs-Paketes im Bearbeitungs-Computersystem,
wobei das Freischalten des zumindest einen selektiven Netzwerk-Ports durch das Bearbeitungs-Computersystem für die Kommunikation mit dem externen Computersystem nur erfolgt, falls das Überprüfen des Authentifizierungs-Paketes erfolgreich war.

5. Verfahren nach einem der Ansprüche 1 bis 4, umfassend die zusätzlichen Schritte:

- Überprüfen des Authentifizierungs-Paketes im Vermittlungs-Computersystem und
- Verwerfen des Authentifizierungs-Paketes durch das Vermittlungs-Computersystem, falls das Überprüfen nicht erfolgreich war.

6. Verfahren nach einem der Ansprüche 1 bis 5, wobei das Übertragen des Authentifizierungs-Paketes vom Vermittlungs-Computersystem auf das Bearbeitungs-Computersystem die folgenden Schritte umfasst:
- Senden einer vorbestimmten Daten-Sequenz vom Vermittlungs-Computersystem oder vom externen Computersystem an das Bearbeitungs-Computersystem, wobei die vorbestimmten Netzwerk-Ports des Bearbeitungs-Computersystems geschlossen sind und wobei die Sequenz in einer vorbestimmten Reihenfolge einen oder mehrere Netzwerk-Ports des Bearbeitungs-Computersystems anspricht,
- Überprüfen der gesendeten Daten-Sequenz auf Übereinstimmung mit einer vordefinierten Sequenz im Bearbeitungs-Computersystem, sowie
- Veranlassen des Übertragens des Authentifizierungs-Paketes durch das Bearbeitungs-Computersystem, falls die Überprüfung der gesendeten Sequenz positiv ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, wobei Daten-Pakete zwischen dem externen Computersystem und der Computernetz-Infrastruktur über einen Paket-Filter geleitet werden,
wobei der Paket-Filter zum externen Computersystem hin zumindest einen Netzwerk-Port für einen Zugriff durch das externe Computersystem offen hält und wobei der Paket-Filter zur Computernetz-Infrastruktur hin vorbestimmte Netzwerk-Ports geschlossen hält, so dass zumindest ein Zugriff von

einem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur auf das externe Computersystem verhindert wird.

8. Verfahren nach einem der Ansprüche 1 bis 7, wobei Daten-Pakete zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem innerhalb der Computernetz-Infrastruktur über einen Paket-Filter geleitet werden, wobei der Paket-Filter in der Kommunikationsrichtung vom Vermittlungs-Computersystem hin zum Bearbeitungs-Computersystem nur Daten-Pakete weiterleitet, welche die IP-Adresse des Vermittlungs-Computersystems enthalten und einer bereits hergestellten Verbindung zwischen dem Vermittlungs-Computersystem und dem Bearbeitungs-Computersystem zugeordnet werden können.

9. Verfahren nach einem der Ansprüche 1 bis 8, wobei das Übertragen des Authentifizierungs-Paketes vom externen Computersystem an das Vermittlungs-Computersystem folgende Teilschritte umfasst:
- Aufbauen einer Verbindung vom externen Computersystem zu einem Vermittlungs-Load Balancer, der einer Mehrzahl von Vermittlungs-Computersystemen vorgeschaltet ist,
- Auswahl des Vermittlungs-Computersystems aus der Mehrzahl von Vermittlungs-Computersystemen durch den Vermittlungs-Load Balancer, und
- Weiterleiten des Authentifizierungs-Paketes vom externen Computersystem über den Vermittlungs-Load Balancer an das ausgewählte Vermittlungs-Computersystem.

10. Verfahren nach einem der Ansprüche 1 bis 9, wobei das Bearbeitungs-Computersystem als Bearbeitungs-Load Balancer arbeitet, der einer Mehrzahl von Backend-Bearbeitungs-

Computersystemen vorgeschaltet ist und folgende Maßnahmen durchführt:
- Auswahl eines Backend-Bearbeitungs-Computersystems aus der Mehrzahl der Backend-Bearbeitungs-Computersysteme, und
- Weiterleiten einer durch das externe Computersystem zum selektiv freigeschalteten Netzwerk-Port des Bearbeitungs-Load Balancers aufgebauten Verbindung an das ausgewählte Backend-Bearbeitungs-Computersystem.

11. Verteiltes Rechnernetz mit
- einer Computernetz-Infrastruktur, welche zumindest ein Vermittlungs-Computersystem und ein Bearbeitungs-Computersystem umfasst, und
- zumindest einem externen Computersystem, welches sich außerhalb der Computernetz-Infrastruktur befindet,
wobei das externe Computersystem eingerichtet ist, ein Authentifizierungs-Paket an das Vermittlungs-Computersystem zu übertragen zur Authentifizierung für eine Kommunikation mit dem Bearbeitungs-Computersystem,
wobei das Vermittlungs-Computersystem eingerichtet ist, das Authentifizierungs-Paket automatisiert an das Bearbeitungs-Computersystem zu übertragen, und
wobei das Bearbeitungs-Computersystem eine Zugriffssteuereinheit aufweist, die eingerichtet ist, zumindest vorübergehend vorbestimmte Netzwerk-Ports geschlossen zu halten, so dass ein Zugriff auf das Bearbeitungs-Computersystem über ein Netzwerk vermittels dieser Netzwerk-Ports verhindert ist, jedoch ein Zugriff des Bearbeitungs-Computersystems auf das Vermittlungs-Computersystem erlaubt ist, um das Authentifizierungs-Paket vom Vermittlungs-Computersystem abzuholen,
wobei die Zugriffssteuereinheit ferner eingerichtet ist,

nach einer erfolgreichen Authentifizierung des externen Computersystems am Bearbeitungs-Computersystem oder an einem dem Bearbeitungs-Computersystem nachgeschalteten Backend-Bearbeitungs-Computersystem zumindest einen selektiven Netzwerk-Port für eine Kommunikation mit dem externen Computersystem freizuschalten.

12. Verteiltes Rechnernetz nach Anspruch 11, wobei die Computernetz-Infrastruktur eine Mehrzahl von Vermittlungs-Computersystemen sowie einen Vermittlungs-Load Balancer umfasst, der der Mehrzahl der Vermittlungs-Computersysteme vorgeschaltet ist.

13. Verteiltes Rechnernetz nach Anspruch 11 oder 12, wobei das Bearbeitungs-Computersystem als Bearbeitungs-Load Balancer eingerichtet ist und die Computernetz-Infrastruktur weiterhin eine Mehrzahl von Backend-Bearbeitungs-Computersystemen umfasst, denen der Bearbeitungs-Load Balancer vorgeschaltet ist.

14. Verteiltes Rechnernetz nach einem der Ansprüche 11 bis 13, welches eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 bis 10 durchzuführen.

15. Computerprogramm-Produkt, welches eingerichtet ist, auf einem oder mehreren Computersystemen ausgeführt zu werden und welches bei Ausführung ein Verfahren nach einem der Ansprüche 1 bis 10 durchführt.

FIG 1

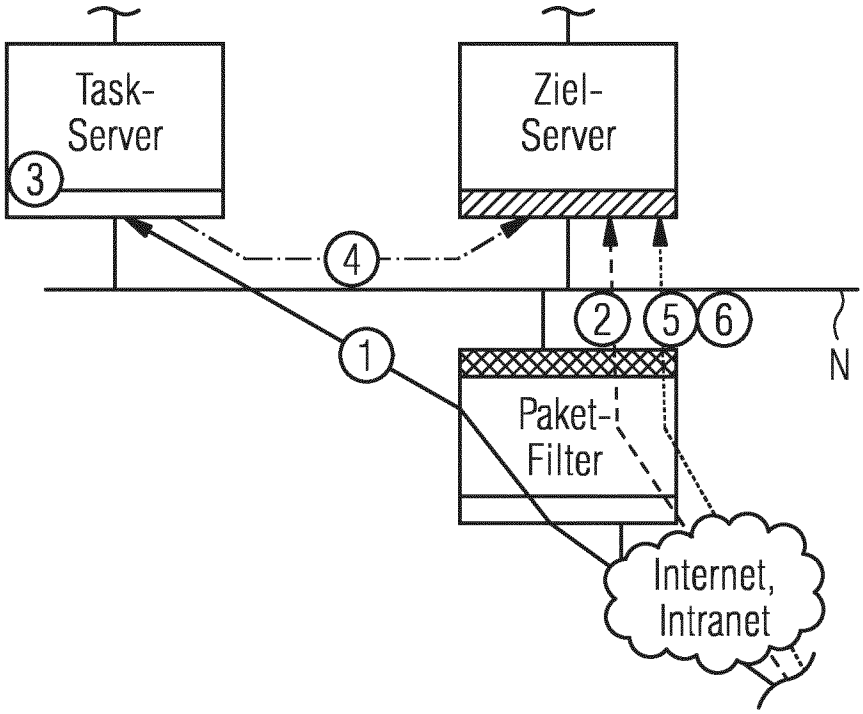

Task-
Server
3
Ziel-
Server
4
2
5
6
1
N
Paket-
Filter
Internet,
Intranet

FIG 2

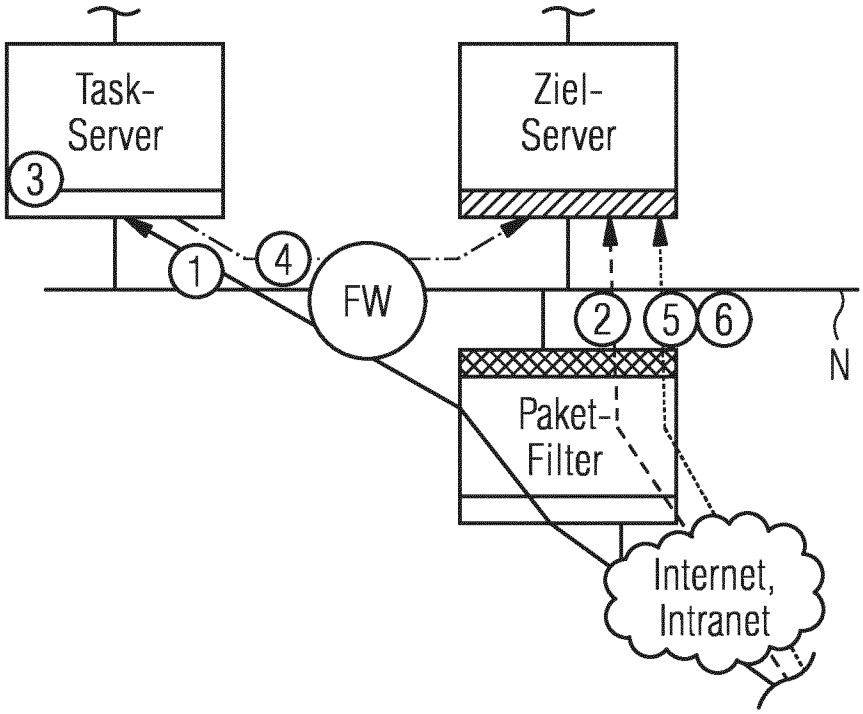

Task-
Server
3
Ziel-
Server
1
4
FW
2
5
6
N
Paket-
Filter
Internet,
Intranet

FIG 3

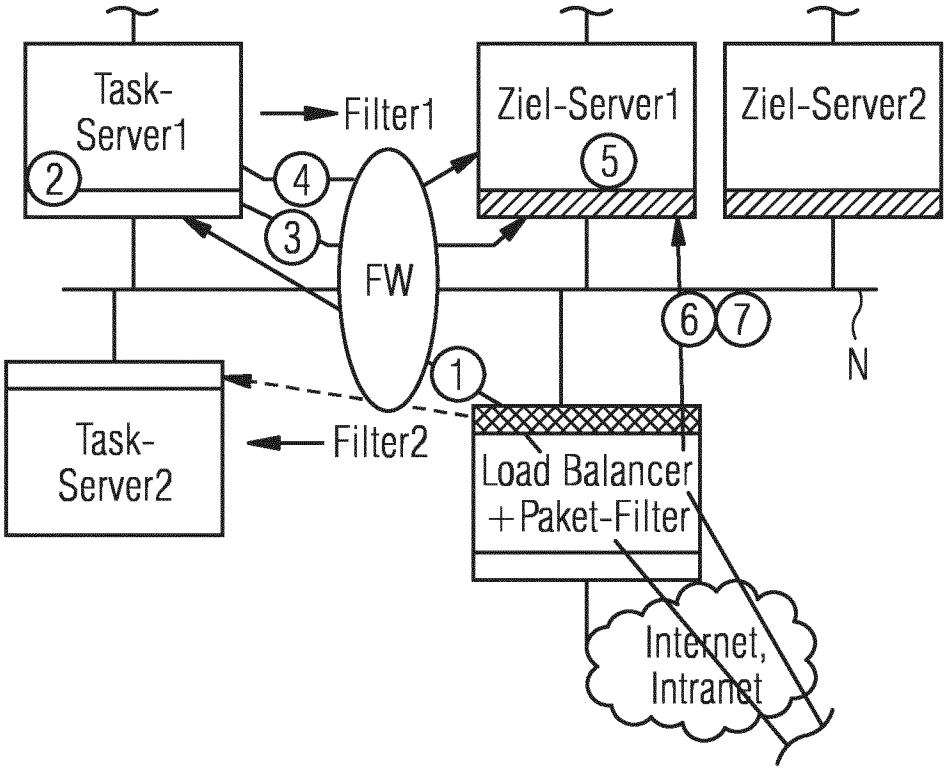

Task-
Server1
Filter1
Ziel-Server1
Ziel-Server2
2
4
3
5
FW
6
7
N
1
Task-
Server2
Filter2
Load Balancer
+Paket-Filter
Internet,
Intranet

FIG 4

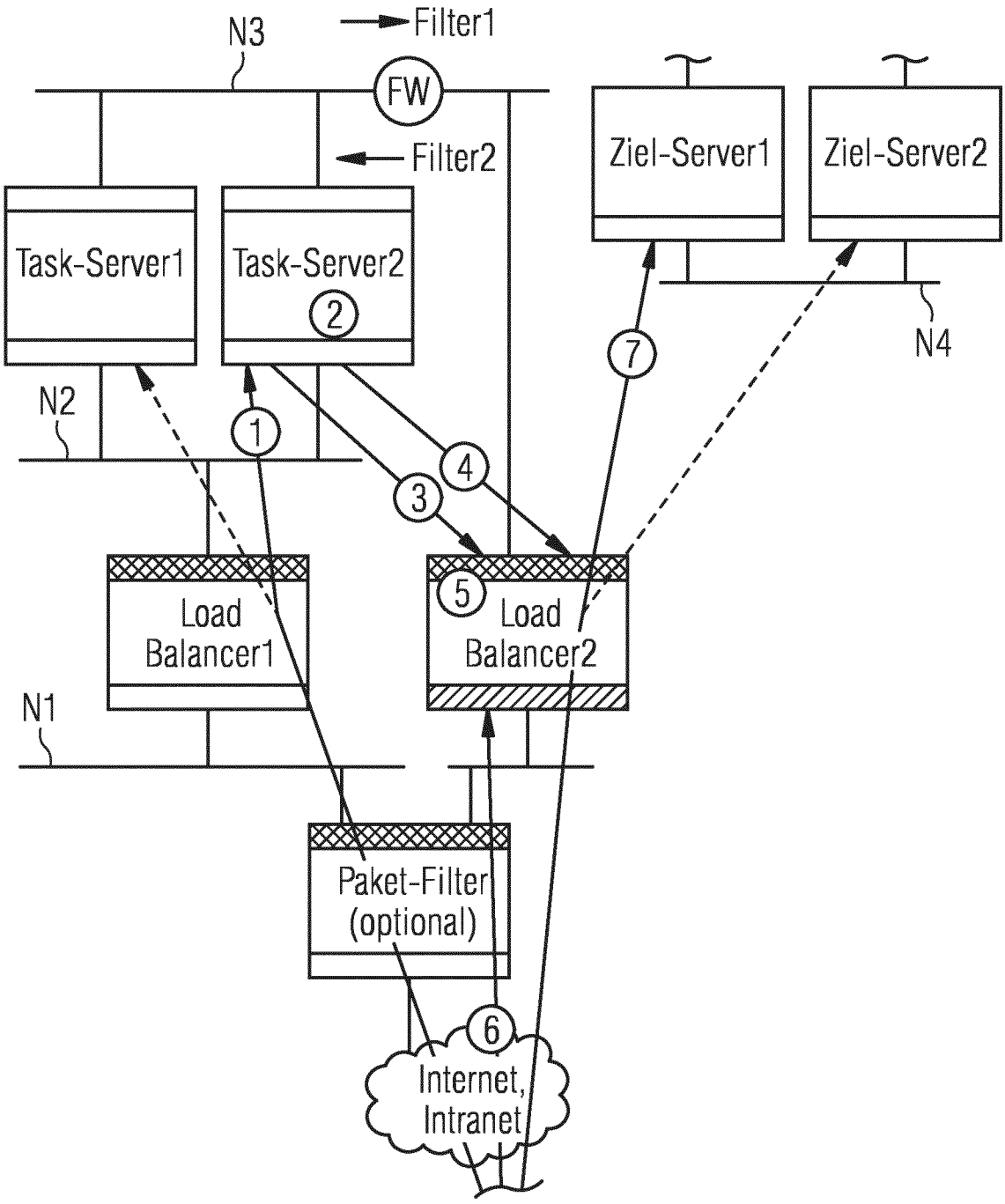
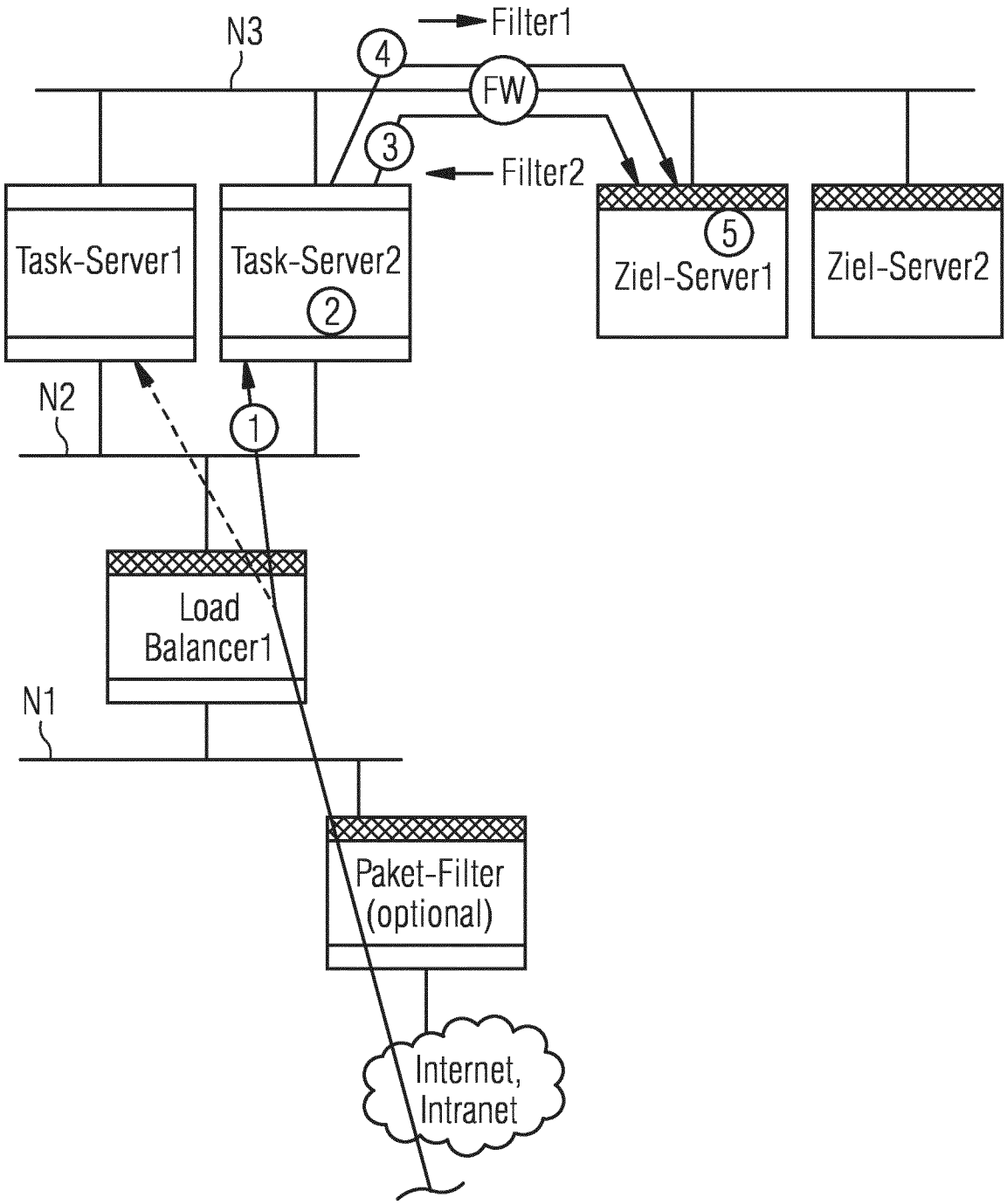

N3
Filter1
FW
Filter2
Ziel-Server1
Ziel-Server2
Task-Server1
Task-Server2
2
N4
7
N2
1
4
3
Load
Balancer1
5
Load
Balancer2
N1
Paket-Filter
(optional)
6
Internet,
Intranet

FIG 5


N3
Filter1
4
FW
3
Filter2
Task-Server1
Task-Server2
2
5
Ziel-Server1
Ziel-Server2
N2
1
Load
Balancer1
N1
Paket-Filter
(optional)
Internet,
Intranet

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/066072

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	GREEN M L ET AL: "Grid-Enabled Virtual Organization Based Dynamic Firewall", GRID COMPUTING, 2004. PROCEEDINGS. FIFTH IEEE/ACM INTERNATIONAL WORKSH OP ON PITTSBURGH, PA, USA 08-08 NOV. 2004, PISCATAWAY, NJ, USA,IEEE, 8 November 2004 (2004-11-08), pages 208-216, XP010769500, DOI: 10.1109/GRID.2004.35 ISBN: 978-0-7695-2256-2 page 208, left-hand column, line 16 - page 209, left-hand column, line 8 page 209, right-hand column, line 23 - page 213, left-hand column, line 11; figures 1,3-5	1-15

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 September 2015	07/10/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schwibinger, Hans

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2 448 171 A1 (PANASONIC ELEC WORKS CO LTD [JP]) 2 May 2012 (2012-05-02) paragraph [0006] - paragraph [0007] paragraph [0064] - paragraph [0068]; claim 1; figure 3	1-15
A	Barry Rhodes ET AL: "On Securing the Public Health Information Network Messaging System", Proceedings of the 4th Annual PKI R&D Workshop "Multiple Paths to Trust", 1 August 2005 (2005-08-01), pages 194-201, XP55191980, ISBN: 978-1-88-684338-7 Retrieved from the Internet: URL:http://csrc.nist.gov/publications/nistir/ir7224/NISTIR-7224.pdf [retrieved on 2015-05-28] page 195, right-hand column, line 17 - page 199, right-hand column, line 19	1-15
A,P	EP 2 772 856 A1 (FUJITSU TECH SOLUTIONS IP GMBH [DE]) 3 September 2014 (2014-09-03) the whole document	1-15

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/066072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2448171 A1	02-05-2012	CN 102461061 A	16-05-2012
		EP 2448171 A1	02-05-2012
		JP 5297529 B2	25-09-2013
		SG 176968 A1	28-02-2012
		US 2012096266 A1	19-04-2012
		WO 2010150817 A1	29-12-2010
EP 2772856 A1	03-09-2014	DE 102013102229 A1	28-08-2014
		EP 2772856 A1	03-09-2014
		US 2014245310 A1	28-08-2014

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2015/066072

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. H04L29/06
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, COMPENDEX

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	GREEN M L ET AL: "Grid-Enabled Virtual Organization Based Dynamic Firewall", GRID COMPUTING, 2004. PROCEEDINGS. FIFTH IEEE/ACM INTERNATIONAL WORKSH OP ON PITTSBURGH, PA, USA 08-08 NOV. 2004, PISCATAWAY, NJ, USA,IEEE, 8. November 2004 (2004-11-08), Seiten 208-216, XP010769500, DOI: 10.1109/GRID.2004.35 ISBN: 978-0-7695-2256-2 Seite 208, linke Spalte, Zeile 16 - Seite 209, linke Spalte, Zeile 8 Seite 209, rechte Spalte, Zeile 23 - Seite 213, linke Spalte, Zeile 11; Abbildungen 1,3-5 ----- -/--	1-15

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen [X] Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
30. September 2015	07/10/2015

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Schwibinger, Hans

1

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 2 448 171 A1 (PANASONIC ELEC WORKS CO LTD [JP]) 2. Mai 2012 (2012-05-02) Absatz [0006] - Absatz [0007] Absatz [0064] - Absatz [0068]; Anspruch 1; Abbildung 3	1-15
A	Barry Rhodes ET AL: "On Securing the Public Health Information Network Messaging System", Proceedings of the 4th Annual PKI R&D Workshop "Multiple Paths to Trust", 1. August 2005 (2005-08-01), Seiten 194-201, XP55191980, ISBN: 978-1-88-684338-7 Gefunden im Internet: URL:http://csrc.nist.gov/publications/nistir/ir7224/NISTIR-7224.pdf [gefunden am 2015-05-28] Seite 195, rechte Spalte, Zeile 17 - Seite 199, rechte Spalte, Zeile 19	1-15
A,P	EP 2 772 856 A1 (FUJITSU TECH SOLUTIONS IP GMBH [DE]) 3. September 2014 (2014-09-03) das ganze Dokument	1-15

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2015/066072

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 2448171 A1	02-05-2012	CN 102461061 A	16-05-2012
		EP 2448171 A1	02-05-2012
		JP 5297529 B2	25-09-2013
		SG 176968 A1	28-02-2012
		US 2012096266 A1	19-04-2012
		WO 2010150817 A1	29-12-2010
EP 2772856 A1	03-09-2014	DE 102013102229 A1	28-08-2014
		EP 2772856 A1	03-09-2014
		US 2014245310 A1	28-08-2014