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

(10) **DE 603 14 367 T2** 2008.02.14

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 458 132 B1**
(21) Deutsches Aktenzeichen: **603 14 367.9**
(96) Europäisches Aktenzeichen: **03 025 046.8**
(96) Europäischer Anmeldetag: **30.10.2003**
(97) Erstveröffentlichung durch das EPA: **15.09.2004**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **13.06.2007**
(47) Veröffentlichungstag im Patentblatt: **14.02.2008**

(51) Int Cl.[8]: ***H04L 12/22*** (2006.01)
H04L 29/06 (2006.01)

(30) Unionspriorität:
2003064328 11.03.2003 JP

(84) Benannte Vertragsstaaten:
DE, FR, GB

(73) Patentinhaber:
Hitachi, Ltd., Tokyo, JP

(74) Vertreter:
Strehl, Schübel-Hopf & Partner, 80538 München

(72) Erfinder:
Kiyoto, Satoshi, Chiyoda-ku Tokyo 100-8220, JP; Hoshino, Kazuyoshi, Chiyoda-ku Tokyo 100-8220, JP; Yumoto, Kazuma, Chiyoda-ku Tokyo 100-8220, JP; Hidaka, Minoru, Chiyoda-ku Tokyo 100-8220, JP

(54) Bezeichnung: **Verfahren und Vorrichtung zur gleichrangigen Kommunikation**

Beschreibung

HINTERGRUND DER ERFINDUNG

(1) Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf ein Peer-to-Peer-Kommunikationsgerät für die Eins-zu-Eins-Kommunikation und insbesondere auf ein Peer-to-Peer-Kommunikationsgerät und -Verfahren, für die optimale Kommunikationssicherheitsregeln entsprechend einem Kommunikations-Peer und einer Sicherheitsumgebung in dem Netz eines von dem Kommunikations-Peer verwendeten Geräts gelten.

(2) Beschreibung des Stands der Technik

[0002] In einem durch die Internet-Telephonie wie etwa VOIP (Voice over IP) repräsentierten Peer-to-Peer-Kommunikationssystem wird ein Verschlüsseln und Authentisieren von Paketen durchgeführt, um das Mithören oder Verfälschen von Inhalten der Kommunikation durch Außenstehende zu verhindern. Das Verschlüsseln und Authentisieren der Pakete wird gemäß einer „Sicherheitsrichtlinie" durchgeführt, bei der es sich um eine Reihe von Regeln handelt, die zeigen, wie jedes der Pakete zu verschlüsseln und zu authentisieren ist. Eine Datenbank zum Speichern einer solchen Sicherheitsrichtlinie wird als Sicherheitsrichtliniendatenbank bezeichnet, die normalerweise in einem als Richtlinienserver bezeichneten Gerät gespeichert ist.

[0003] Die IETF (Internet Engineering Task Force) als eine Organisation zur Standardisierung von Internet-Technologien hat IPsec (IP-Sicherheit) als Protokolle zur Gewährleistung der Sicherheit (Verhinderung des Mithörens oder Verfälschens von Inhalten der Kommunikation durch Außenstehende) auf der IP-Paketschicht (Internet-Protokoll) im Internet definiert (Nichtpatentdokument 1: IETF RFC 2401, 25. November 1998, S. 14-17).

[0004] Gemäß den vorstehend genannten Protokollen wird eine auf die betreffende Peer-to-Peer-Kommunikation anzuwendende Sicherheitsrichtlinie unter Verwendung von Informationen über die jeweiligen IP-Adressen und Portnummern einer Quelle und eines Ziels, die Art der Protokolle auf höheren Schichten wie etwa TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) und die Richtung der Kommunikation ausgewählt, die angibt, ob ein Zielpaket, auf das die Sicherheitsrichtlinie angewendet werden soll, ein empfangenes Paket oder ein zu übermittelndes Paket ist. Durch Verwendung von in der ausgewählten Sicherheitsrichtlinie beschriebenen Sicherheitsanforderungen wird beurteilt, ob zum Beispiel ein empfangenes Paket verworfen werden soll oder nicht, ob das Verschlüsseln (Entschlüsseln) oder Authentisieren von zu übermittelnden (empfangenen) Paketen durchgeführt werden soll oder nicht, ob das Verschlüsseln oder Authentisieren obligatorisch ist oder nur durchgeführt werden soll, wenn es möglich ist, oder dergleichen. Im Einzelnen ruft ein Übermittlungsgerät mit einer IPsec-Funktion in der Sicherheitsrichtliniendatenbank die der Quelladresse und der Zieladresse entsprechende Sicherheitsrichtlinie ab, die an ein zu übermittelndes Paket angehängt werden soll, führt die Verschlüsselungs- und Authentisierungsvorgänge durch, die die in der Sicherheitsrichtlinie bezüglich des zu übermittelnden Pakets beschriebenen Sicherheitsanforderungen erfüllen, und übermittelt dann das Paket an einen Kommunikations-Peer.

[0005] In gleicher Weise ruft ein Empfangsgerät mit der IPsec-Funktion in der Sicherheitsrichtliniendatenbank die der Quelladresse und der Zieladresse entsprechende Sicherheitsrichtlinie ab, die an das empfangene Paket angehängt ist, und prüft, ob die Verschlüsselungs- und Authentisierungsvorgänge, die die in der Sicherheitsrichtlinie beschriebenen Sicherheitsanforderungen erfüllen, bezüglich des empfangenen Pakets durchgeführt worden sind oder nicht. Ein empfangenes Paket, das die Sicherheitsanforderungen nicht erfüllt, wird verworfen, ohne an eine höhere Schicht weitergegeben zu werden.

[0006] Eine Technik zur Sicherstellung der Kommunikationssicherheit unter Verwendung von IPsec in einem VPN (virtuelles privates Netz), das eine virtuelle Standleitung zwischen zwei Kommunikationsknoten im Internet herstellt, ist zum Beispiel in Takayuki Ishii et al., „Implementation of Transparent and Dynamic VPN Mechanism" (Nichtpatentdokument 2: Quarterly IPv6 Magazine, Impress Corporation, 18. August 2002, Sommer 2002, Nr. 2, S. 74-75) beschrieben. Die in Nichtpatentdokument 2 beschriebene herkömmliche Technik erfasst die bei der Peer-to-Peer-Kommunikation zu verwendende Sicherheitsrichtlinieninformation von einem IPsec-Kommunikationsmanagement-Server, der in einem Netz vorgesehen ist, mit jedem der Kommunikationsgeräte und löst ein Problem in Zusammenhang mit Detailinformationen wie etwa einem für die Verschlüsselung verwendeten Schlüssel durch Verhandlung zwischen den einzelnen Kommunikationsgeräten.

[0007] Bei der in Nichtpatentdokument 1 beschriebenen Peer-to-Peer-Kommunikation mit IPsec besteht jedoch das Problem, dass, wenn die in der auf das zu übermittelnde Paket im Übermittlungsgerät angewendeten Sicherheitsrichtlinie beschriebenen Sicherheitsanforderungen die im Empfangsgerät registrierten Sicherheitsanforderungen nicht erfüllen, das von dem Übermittlungsgerät übermittelte Paket verworfen wird, nachdem es vom Empfangsgerät empfangen worden ist.

[0008] Andererseits ist der in Nichtpatentdokument 2 beschriebene IPsec-Kommunikationsmanagement-Server ein Server, der einer externen Organisation gehört, die die Kommunikationssicherheitsrichtlinien im Netz aus der Sicht des Benutzers jedes der Kommunikationsgeräte zentral verwaltet. Daher kann der IPsec-Kommunikationsmanagement-Server die Sicherheitsrichtlinie nicht in Reaktion auf die Notwendigkeit für jedes der Kommunikationsgeräte ändern und kann keine flexible Sicherheitsfunktion bereitstellen, die es dem Benutzer ermöglicht, eine Sicherheitsrichtlinie je nach Kommunikationssituation frei zu wählen.

[0009] Ein Kommunikationssystem entsprechend dem Oberbegriff des vorliegenden Anspruchs 1 ist in US-A-5.872.847 beschrieben. EP-A-1244322 beschreibt ein mobiles Kommunikationsterminal und einen Server. Das mobile Kommunikationsgerät kann die Sicherheitsstufe des Ziels einer Kommunikation erfassen und den Benutzer über die erfasste Stufe informieren. Der Benutzer kann bestätigen, ob die Sicherheit am Ziel gewährleistet ist.

ZUSAMMENFASSUNG DER ERFINDUNG

[0010] Um die Kommunikation ohne Verwerfen von Paketen zwischen zwei Kommunikationsgeräten zu implementieren, die jeweils über die IPsec-Funktion verfügen, ist es erforderlich, dass die beiden Kommunikationsgeräte ihre jeweilige Sicherheitsrichtlinieninformation vor der Übermittlung von Datenpaketen austauschen, damit die Pakete auf der Grundlage der Sicherheitsrichtlinie übermittelt werden, die die von dem Peer-Kommunikationsgerät festgelegten Sicherheitsanforderungen erfüllt. Ändert sich die Sicherheitsumgebung aufgrund der Bewegung des Peer-Kommunikationsgeräts wie im Falle der Peer-to-Peer-Kommunikation zwischen mobilen Terminals, ist es wünschenswert, die anzuwendende Sicherheitsrichtlinie je nach der Situation eines Kommunikations-Peers zu ändern. Wenn es möglich ist, die Sicherheitsstufe abhängig von Faktoren wie zum Beispiel der Frage zu ändern, ob der Kommunikations-Peer ein Familienmitglied, Freund oder Bekannter ist und ob die Kommunikation einen geschäftlichen oder privaten Anlass hat oder lediglich der Werbung dient, kann eine weitere Optimierung der Kommunikation erwartet werden.

[0011] Zwischen zwei Kommunikationsgeräten, die an ein privates Netz angeschlossen sind, wird zum Beispiel die Peer-to-Peer-Kommunikation in einer Umgebung durchgeführt, für die ein korrektes Maß an Sicherheit garantiert ist, so dass es jedem der Geräte gestattet ist, eine leichte Kommunikation durchzuführen, die eine Sicherheitsrichtlinie auf einer niedrigen Sicherheitsstufe verwendet und keine Verschlüsselung eines Pakets oder dergleichen erfordert. Ist das Peer-Kommunikationsterminal hingegen in Bewegung und mit einem öffentlichen Netz verbunden, ist es andererseits wünschenswert, eine Sicherheitsrichtlinie auf einer höheren Sicherheitsstufe anzuwenden und die Sicherheit durch Verschlüsselung der Pakete sicherzustellen.

[0012] Es ist jedoch nicht notwendigerweise der Fall, wenn jedes der Kommunikationsgeräte eine korrekte Sicherheitsrichtlinie entsprechend einer Kommunikationsumgebung gewählt hat, wie vorstehend beschrieben. Wenn zum Beispiel ein mit einem privaten Netz verbundenes mobiles Terminal bewegt worden ist und das Netz, mit dem das Terminal verbunden ist, sich von dem privaten Netz in ein öffentliches Netz geändert hat, und wenn das mobile Terminal mit einem mit dem privaten Netz verbundenen Terminal unter weniger strengen Sicherheitsanforderungen kommuniziert, die für das private Netz unter Verwendung der vorherigen Sicherheitsrichtlinie gelten, ist das Risiko des Mithörens oder Verfälschens von Paketen durch einen Außenstehenden unvorteilhafterweise erhöht.

[0013] Daher ist ein Ziel der vorliegenden Erfindung die Bereitstellung eines Peer-to-Peer-Kommunikationsgeräts, das die Sicherheit der Kommunikation durch Anwendung einer geeigneten Sicherheitsrichtlinie entsprechend einer Kommunikationsumgebung sicherstellen kann.

[0014] Ein weiteres Ziel der vorliegenden Erfindung ist die Bereitstellung eines Peer-to-Peer-Kommunikationsgeräts, das relativ frei die Sicherheitsrichtlinie entsprechend dem gegenwärtigen Ort eines Kommunikations-Peers wählen kann.

[0015] Zur Erreichung des Ziels ist ein Peer-to-Peer-Kommunikationsgerät nach der vorliegenden Erfindung dadurch gekennzeichnet, dass es vor der Paketkommunikation eine von einem Peer-Kommunikationsgerät verwendete Sicherheitsrichtlinie und die Präsenzinformation einschließlich der Information zum Beurteilen einer Kommunikationssicherheitsumgebung des Peer-Kommunikationsgeräts daraus erfasst und es einem Benutzer ermöglicht, die Korrektheit einer Sicherheitsrichtlinie zu beurteilen und eine auf die Paketkommunikation mit dem Peer-Kommunikationsgerät anzuwendende Sicherheitsrichtlinie zu bestimmen, indem die Präsenzinformation und die Sicherheitsrichtlinie angezeigt werden.

[0016] Im Einzelnen wird das Ziel durch das Peer-to-Peer-Kommunikationsgerät nach Anspruch 1 und das in Anspruch 6 definierte Verfahren erfüllt. Die Unteransprüche beziehen sich auf bevorzugte Ausführungsformen.

[0017] Insbesondere wenn der Benutzer aus der Information über das in der Präsenzinformation enthal-

tene Ergebnis der Beurteilung der Kommunikationssicherheitsumgebung zu dem Urteil kommt, dass die Sicherheitsrichtlinie ungeeignet ist, korrigiert der Benutzer teilweise die auf dem Anzeigeschirm ausgegebene Sicherheitsrichtlinieninformation, und das erste Kommunikationsgerät führt die Datenpaketkommunikation mit dem zweiten Kommunikationsgerät gemäß der korrigierten Sicherheitsrichtlinie durch.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0018] Fig. 1 zeigt ein Blockdiagramm mit dem Aufbau eines Kommunikationsgeräts nach der vorliegenden Erfindung.

[0019] Fig. 2 zeigt eine Ansicht zur Illustration einer Netzarchitektur unter Verwendung des Kommunikationsgeräts nach der vorliegenden Erfindung.

[0020] Fig. 3 zeigt ein Ablaufdiagramm für eine erste Ausführungsform eines Kommunikationsverfahrens nach der vorliegenden Erfindung, das vor der Peer-to-Peer-Kommunikation zwischen den Kommunikationsgeräten **10** und **11-1** in Fig. 2 durchgeführt wird.

[0021] Fig. 4 zeigt ein Beispiel für einen Anzeigeschirm der grafischen Benutzeroberfläche auf dem Kommunikationsgerät nach der ersten Ausführungsform der vorliegenden Erfindung.

[0022] Fig. 5 zeigt ein Beispiel für die in einer Antwortmitteilung von einem Peer-Kommunikationsgerät nach der ersten Ausführungsform angegebene Präsenzinformation und Sicherheitsrichtlinie.

[0023] Fig. 6 zeigt ein Beispiel für eine Präsenzinformationsdatenbank.

[0024] Fig. 7 zeigt ein Beispiel für eine Sicherheitsrichtliniendatenbank.

[0025] Fig. 8 zeigt ein Beispiel für einen Sicherheitsrichtlinien-Anzeigeschirm nach der ersten Ausführungsform.

[0026] Fig. 9 zeigt ein Beispiel für einen Präsenzinformations-Anzeigeschirm nach der ersten Ausführungsform.

[0027] Fig. 10 zeigt ein Ablaufdiagramm für eine zweite Ausführungsform des Kommunikationsverfahrens nach der vorliegenden Erfindung, das vor der Peer-to-Peer-Kommunikation zwischen den Kommunikationsgeräten **10** und **11-2** in Fig. 2 durchgeführt wird.

[0028] Fig. 11 zeigt ein Beispiel für den Präsenzinformations-Anzeigeschirm nach der zweiten Ausführungsform der vorliegenden Erfindung.

[0029] Fig. 12 zeigt ein Beispiel für den Sicherheitsrichtlinien-Anzeigeschirm nach der zweiten Ausführungsform.

[0030] Fig. 13 zeigt ein Beispiel für einen Anzeigeschirm nach Änderung der Sicherheitsrichtlinie.

BESCHREIBUNG DER BEVORZUGTEN AUSFÜHRUNGSFORMEN

[0031] Unter Bezugnahme auf die Zeichnungen werden nachstehend die einzelnen Ausführungsformen der vorliegenden Erfindung beschrieben. Als Beispiel wird der Fall beschrieben, bei dem ein IP-Netz als Kommunikationsnetz und IPsec als Protokolle für die Sicherstellung der Kommunikationssicherheit verwendet werden.

[0032] Fig. 1 zeigt den Aufbau eines Kommunikationsgeräts **10** nach der vorliegenden Erfindung. Das Kommunikationsgerät **10** führt die Kommunikation mit einem Peer-Kommunikationsgerät **11** über ein IP-Netz **1** durch. Der Aufbau des Kommunikationsgeräts **10** ist unter Konzentration auf die Funktionsblöcke bezüglich der Bestimmung einer Sicherheitsrichtlinie gezeigt, was nachstehend ausführlich beschrieben wird. In einer realen Situation weist das Kommunikationsgerät **10** auch noch weitere Funktionsblöcke wie zum Beispiel einen mobilen PC oder ein IP-Telefon (nicht gezeigt) auf, die je nach Art des Kommunikationsgeräts unterschiedlich sind. Außerdem wird angenommen, dass das Peer-Kommunikationsgerät **11** denselben funktionalen Aufbau wie das Kommunikationsgerät **10** aufweist.

[0033] Das Kommunikationsgerät **10** nach der vorliegenden Erfindung umfasst einen IP-Funktionsblock **100**, einen IPsec-Funktionsblock **110**, einen Peer-to-Peer-Kommunikations-Funktionsblock **200**, eine Peer-to-Peer-Kommunikations-Datenschnittstelle **201**, eine Sicherheitsrichtliniendatenbank **300**, eine Sicherheitsrichtlinien-Verarbeitungseinheit **301**, eine Sicherheitsrichtlinien-E/A-Schnittstelle **302**, eine Präsenzinformationsdatenbank **400**, eine Präsenzinformations-Verarbeitungseinheit **401**, eine Präsenzinformations-E/A-Schnittstelle **402** sowie eine Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403**.

[0034] Der IP-Funktionsblock **100** ist eine Schnittstelle zum Übermitteln und Empfangen von Datenpaketen an das und von dem IP-Netz **1** und führt die Terminierung der empfangenen IP-Pakete und die Erzeugung eines zu übermittelnden IP-Pakets durch. Der IPsec-Funktionsblock **110** dient zur Sicherstellung der Sicherheit in einer IP-Schicht und führt die Authentisierung und Verschlüsselung der IP-Pakete durch. Der Peer-to-Peer-Kommunikations-Funktionsblock **200** dient zur Implementierung der Peer-to-Peer-Kommunikation und führt die Einrich-

tung einer Peer-to-Peer-Kommunikationssession zwischen den einzelnen Kommunikationsgeräten, die Peer-to-Peer-Kommunikation in der eingerichteten Session und die Trennung der Session durch. Die Peer-to-Peer-Kommunikations-Datenschnittstelle **201** führt das Empfangen und Übermitteln der Peer-to-Peer-Kommunikationsdaten zwischen einem Peripheriegerät **20** und dem Peer-to-Peer-Kommunikations-Funktionsblock **200** durch.

[0035] Die Sicherheitsrichtliniendatenbank **300** ist eine Datenbank zur Speicherung der Sicherheitsrichtlinieninformation und zur Verwaltung einer in dem IPsec-Funktionsblock **110** zu verwendenden Sicherheitsrichtlinie. In der Sicherheitsrichtliniendatenbank **300** sind mehrere Einträge zur Angabe von Sicherheitsrichtlinien für jeden Kommunikations-Peer und ein Eintrag zur Angabe einer Vorgabesicherheitsrichtlinie, die von dem Kommunikationsgerät **10** auf nicht spezifizierte Kommunikations-Peers anzuwenden ist, enthalten.

[0036] Die Sicherheitsrichtlinien-Verarbeitungseinheit **301** ist ein Funktionsblock zum Zugriff auf die Sicherheitsrichtliniendatenbank, um das Registrieren, Löschen und Abrufen einer Sicherheitsrichtlinie durchzuführen. Die Sicherheitsrichtlinien-E/A-Schnittstelle **302** ist eine Benutzerschnittstelle zum Zugriff auf die Sicherheitsrichtliniendatenbank, die einem Benutzer den Zugriff auf die Sicherheitsrichtliniendatenbank über das Peripheriegerät **20** ermöglicht.

[0037] Die Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403** ist eine Benutzerschnittstelle zum Empfang einer Anforderung zur Erfassung einer Sicherheitsrichtlinie und Präsenzinformation, die eine Anforderung zur Erfassung der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts von dem Benutzer über das Peripheriegerät **20** ermöglicht. Die Präsenzinformationsdatenbank **400** dient zur Speicherung der Präsenzinformation einschließlich der Information zur Beurteilung einer Kommunikationssicherheitsumgebung, die die jeweilige Präsenzinformation des Kommunikationsgeräts **10** und des Peer-Kommunikationsgeräts verwaltet.

[0038] Die Präsenzinformations-Verarbeitungseinheit **401** ist ein Funktionsblock zum Zugriff auf die Präsenzinformationsdatenbank **400**, um das Registrieren, Löschen, Ändern und Abrufen der Präsenzinformation durchzuführen. Wenn das Kommunikationsgerät **10** eine Mobilterminalfunktion aufweist und unterwegs bei Verbindung mit dem IP-Netz zum Beispiel eine Care-of-Adresse erhält, prüft die Präsenzinformations-Verarbeitungseinheit **401** auf der Grundlage des Adresssystems der Care-of-Adresse, ob das Kommunikationsgerät mit einem privaten Netz verbunden ist (ob der Standort des Kommunikationsgeräts in einem Büro ist) oder nicht, und aktualisiert den Ort des Kommunikationsgeräts, der als Information zur Beurteilung der Kommunikationssicherheitsumgebung des Kommunikationsgeräts **10**, die in der Datenbank **400** gespeichert ist, zu verwenden ist. Die Präsenzinformations-E/A-Schnittstelle **402** ist eine Benutzerschnittstelle zum Zugriff auf die Präsenzinformationsdatenbank **400**, die dem Benutzer den Zugriff auf die Präsenzinformationsdatenbank **400** über das Peripheriegerät **20** ermöglicht.

[0039] Die Sicherheitsrichtlinien-E/A-Schnittstelle **302**, die Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403** und die Präsenzinformations-E/A-Schnittstelle **402** sind zusammen mit einer Anzeigeeinheit, einer Tastatur und einer Maus, die außerhalb des Kommunikationsgeräts **10** vorgesehen sind, an das Peripheriegerät **20** angeschlossen und ermöglichen zum Beispiel die Anzeige von Ausgabeinformationen auf der Anzeigeeinheit und die Eingabe verschiedener Informationen durch den Benutzer über die Tastatur bzw. mit der Maus.

[0040] Fig. 2 zeigt ein Beispiel für eine Netzarchitektur unter Verwendung des Kommunikationsgeräts **10** nach der vorliegenden Erfindung. Nachstehend werden der Fall beschrieben, bei dem der Benutzer **9** des Kommunikationsgeräts **10** die Peer-to-Peer-Kommunikation mit einem Peer-Kommunikationsgerät **11-1** über ein privates Netz **2** durchführt (erste Ausführungsform), sowie der Fall, bei dem der Benutzer **9** des Kommunikationsgeräts **10** die Peer-to-Peer-Kommunikation mit einem Peer-Kommunikationsgerät **11-2** über das private Netz **2** und ein öffentliches Netz **3** durchführt (zweite Ausführungsform).

[0041] Hier wird angenommen, dass das Kommunikationsgerät **10** und das Peer-Kommunikationsgerät **11-1** als ihre jeweilige IP-Adressen die privaten Adressen „192.168.1.1" und „192.168.1.2" nach der durch RFC 1597 von der IETF, einer Organisation für die Internet-Standardisierung, definierten Klasse C aufweisen, während das Peer-Kommunikationsgerät **11-2** eine IP-Adresse „133.134.10.10" hat. Diese IP-Adresswerte sind Beispiele zum leichteren Verständnis der Ausführungsformen, so dass keine Probleme auftreten, wenn andere Adressen verwendet werden.

[0042] Als erste Ausführungsform wird zunächst anhand von Fig. 3 bis Fig. 9 ein Verfahren zur Kommunikation zwischen dem Kommunikationsgerät **10** und dem Peer-Kommunikationsgerät **11-1** beschrieben, die jeweils an das private Netz **2** angeschlossen sind. Danach wird als zweite Ausführungsform anhand von Fig. 10 bis Fig. 13 ein Verfahren zur Kommunikation zwischen dem an das private Netz **2** angeschlossenen Kommunikationsgerät **10** und dem an das öffentliche Netz **3** angeschlossenen Peer-Kommunikati-

onsgerät **11-2** beschrieben.

[0043] Fig. 3 zeigt einen von dem Benutzer **9** durchgeführten Betriebsablauf zur Bestimmung einer Sicherheitsrichtlinie vor dem Start der Peer-to-Peer-Kommunikation und eine Abfolge von zwischen dem Kommunikationsgerät **10** und dem Peer-Kommunikationsgerät **11-1** ausgetauschten Kommunikationsnachrichten nach der ersten Ausführungsform der vorliegenden Erfindung.

[0044] Der Benutzer **9** gibt von dem in Fig. 1 gezeigten Peripheriegerät **20** über die Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403** eine Anforderung zum Erhalten der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts **11-1** an das Kommunikationsgerät **10** ein (Schritt **501**). Bei Empfang der Anforderung erzeugt das Kommunikationsgerät **10** eine Nachricht, mit der das Peer-Kommunikationsgerät **11-1** aufgefordert wird, die Präsenzinformation und die Sicherheitsrichtlinie mit dem Peer-to-Peer-Kommunikations-Funktionsblock **200** zu übermitteln, wandelt die Anforderungsnachricht mit dem IP-Funktionsblock **100** in ein IP-Paket um und übermittelt das IP-Paket an das private Netz **2** (Schritt **502**).

[0045] Das IP-Paket ist ein spezielles Paket zum Austausch von Sicherheitsrichtlinieninformationen zwischen einzelnen Kommunikationsgeräten. Im Gegensatz zu einem normalen Datenpaket wird das IP-Paket entsprechend einem Format erzeugt, das zum Beispiel durch Internet-Draft (draft-IETF-impp-cpim-pidf-7.txt) definiert ist. Dementsprechend wird das IP-Paket von dem Kommunikationsgerät **11-1** empfangen, ohne verworfen zu werden, unabhängig davon, ob es die Sicherheitsrichtlinie des Kommunikationsgeräts **11-1** als Empfänger zu diesem Zeitpunkt erfüllt oder nicht.

[0046] Bei Empfang des IP-Pakets mit der Anforderungsnachricht liefert das Peer-Kommunikationsgerät **11-1** als Antwort eine Antwortmitteilung, die die Präsenzinformation und Sicherheitsrichtlinie des Kommunikationsgeräts **11-1** angibt, in Form eines IP-Pakets an den Kommunikations-Peer **10** (Schritt **503**). Bei Empfang des Antwortpakets mit der Antwortmitteilung von dem Peer-Kommunikationsgerät **11-1** gibt das Kommunikationsgerät **10** das Antwortpaket über den Peer-to-Peer-Kommunikations-Funktionsblock **200** an die Präsenzinformations-Verarbeitungseinheit **401** und die Sicherheitsrichtlinien-Verarbeitungseinheit **301** weiter.

[0047] Die Präsenzinformations-Verarbeitungseinheit **401** analysiert den Inhalt des Antwortpakets, registriert die aus der Antwortmitteilung extrahierte Präsenzinformation des Peer-Kommunikationsgeräts **11-1** in der Präsenzinformationsdatenbank **400** (Schritt **504**) und zeigt die Präsenzinformation des Peer-Kommunikationsgeräts **11-1** über die Präsenzinformations-E/A-Schnittstelle **402** auf dem Peripheriegerät **200** an (Schritt **505**). In gleicher Weise analysiert die Sicherheitsrichtlinien-Verarbeitungseinheit **301** das Antwortpaket von dem Peer-Kommunikationsgerät **11-1**, extrahiert die Sicherheitsrichtliniendaten des Peer-Kommunikationsgeräts **11-1** aus der Antwortmitteilung, zeigt die Sicherheitsrichtlinie auf dem Peripheriegerät **20** über die Sicherheitsrichtlinien-E/A-Schnittstelle **302** an (Schritt **506**) und wartet auf eine Reaktion des Benutzers.

[0048] Der Benutzer **9** prüft den Inhalt der Sicherheitsrichtlinie des Peer-Kommunikationsgeräts **11-1** an das Kommunikationsgerät **10**, die auf dem Peripheriegerät **20** angezeigt wird, ändert teilweise die Sicherheitsrichtlinie, indem zum Beispiel die Sicherheitsstufe bei Bedarf erhöht oder verringert wird, und weist dann die Registrierung der Sicherheitsrichtlinie an (Schritt **507**). Die Registrierungsanweisung wird über die E/A-Schnittstelle **302** in die Sicherheitsrichtlinien-Verarbeitungseinheit **301** eingegeben. Nach Empfang der Registrierungsanweisung speichert die Sicherheitsrichtlinien-Verarbeitungseinheit **301** die aus der Antwortmitteilung extrahierte Sicherheitsrichtlinie des Peer-Kommunikationsgeräts oder die vom Benutzer korrigierte Sicherheitsrichtlinie in der Sicherheitsrichtliniendatenbank **300** (Schritt **508**).

[0049] Nach der Anweisung zur Registrierung der Sicherheitsrichtlinie (Schritt **507**) weist der Benutzer **9** den Start der Peer-to-Peer-Kommunikation mit dem Peer-Kommunikationsgerät **11-1** von dem Peripheriegerät **20** an (Schritt **509**). Bei Empfang der Anweisung zum Starten der Peer-to-Peer-Kommunikation aktiviert das Kommunikationsgerät **10** den Peer-to-Peer-Kommunikations-Funktionsblock **200** und startet die Peer-to-Peer-Kommunikation mit dem Peer-Kommunikationsgerät **11-1** (Schritt **510**).

[0050] Bei der Peer-to-Peer-Kommunikation werden die von dem Peripheriegerät **20** oder von einem nicht gezeigten externen Gerät, Terminal oder dergleichen gelieferten Sendedaten über die Peer-to-Peer-Kommunikations-Datenschnittstelle **201** in den Peer-to-Peer-Kommunikations-Funktionsblock **200** eingegeben. Bei Empfang der an das Peer-Kommunikationsgerät zu übermittelnden normalen Sendedaten von der Schnittstelle **201** gibt der Peer-to-Peer-Kommunikations-Funktionsblock **200** die Sendedaten und die Attributinformation in Verbindung mit den Sendedaten an den IPsec-Funktionsblock **110**. Die Attributinformation enthält eine IP-Adresse, eine Portnummer und den Typ des Protokolls einer höheren Schicht. Der IPsec-Funktionsblock **110** ruft basierend auf der Attributinformation die in der Sicherheitsrichtliniendatenbank **300** gespeicherte Sicherheitsrichtlinie des Peer-Kommunikationsgeräts auf, führt einen Verschlüsselungsvor-

gang, einen Authentisierungsvorgang und dergleichen an den Sendedaten gemäß der Sicherheitsrichtlinie durch und übermittelt die als Ergebnis erhaltenen Daten an den IP-Funktionsblock **100**.

[0051] Fig. 4 zeigt ein Beispiel für einen Anzeigeschirm **410** einer grafischen Benutzeroberfläche (GUI), der in Schritt **501** zur Anforderung der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts in Fig. 3 von der Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403** an die Anzeigeeinheit als Teil des Peripheriegeräts **20** gegeben wird. Der Benutzer des Kommunikationsgeräts **10** gibt die IP-Adresse des Peer-Kommunikationsgeräts, zum Beispiel „192.168.1.2", in ein Textfeld **411** ein, wählt oder markiert mindestens eines der Kontrollfelder **412** und **413**, die die Informationsarten angeben, die den vom Benutzer benötigten Informationen entsprechen, und drückt dann eine OK-Taste **414**, um dadurch die Anforderung für die Sicherheitsrichtlinie und die Präsenzinformation an das Kommunikationsgerät **10** einzugeben. Obwohl bei der vorliegenden Ausführungsform der Kommunikations-Peer durch Eingeben der IP-Adresse in das Textfeld **411** spezifiziert wird, ist es auch möglich, eine andere dem Kommunikations-Peer zugewiesene Kennungsinformation wie zum Beispiel eine E-Mail-Adresse oder eine Mobiltelefonnummer anstelle der IP-Adresse einzugeben.

[0052] Fig. 5 zeigt ein Beispiel für einen Teil zur Beschreibung der in der Antwortmitteilung von dem Peer-Kommunikationsgerät **11-1** in dem Antwortschritt **503** in Fig. 3 übermittelten Präsenzinformation und Sicherheitsrichtlinie. In diesem Beispiel sind die Präsenzinformation und die Sicherheitsrichtlinie jeweils gemäß einem Format beschrieben, das auf PIDF (Presence Information Data Format) basiert, das in einer WG (Working Group) für das IMPP (Instant Messaging and Presence Protocol) der IETF (Internet Engineering Task Force) erarbeitet wird.

[0053] In Fig. 5 enthalten die Zeilen **520** bis **526** Informationen über die Sicherheitsrichtlinie, und die Zeilen **527** und **528** enthalten die Präsenzinformation. In diesem Beispiel spezifiziert die Sicherheitsrichtlinieninformation die IP-Adresse **520** und die Portnummer **521** des Kommunikationsgeräts **10** als Anforderungsquelle, die IP-Adresse **522** und die Portnummer **523** des Peer-Kommunikationsgeräts **11-1**, den Protokolltyp **524** einer Transportschicht, eine Richtung **525**, die angibt, ob ein Zielpaket, auf das die Sicherheitsrichtlinie angewendet werden soll, ein zu übermittelndes Paket („out") oder ein zu empfangendes Paket ist („in"), und eine Aktion **526** für das Paket. Andererseits gibt die Präsenzinformation den Benutzernamen **528** des Peer-Kommunikationsgeräts und dessen Standort **528** an. Die Zeile **529** enthält einen Uhrzeitstempel, und die Zeile **530** gibt die Identifizierungsinformation (Entität) des Peer-Kommunikationsgeräts **11-1** an. Die betreffende Nachricht wird gemäß Protokollen für die Peer-to-Peer-Kommunikation übermittelt, die zum Beispiel durch SIP repräsentiert sind, das im RFC (Request for Comments) der IETF definiert ist.

[0054] Fig. 6 zeigt ein Beispiel für einen in Schritt **504** in Fig. 3 in der Präsenzinformationsdatenbank **400** registrierten Präsenzinformationseintrag. Jeder entsprechend einem Peer-Kommunikationsgerät gespeicherte Präsenzinformationseintrag **600** besteht aus der Identifizierungsinformation (Entität) **620** des Kommunikationsgeräts, der IP-Adresse **621** des Kommunikationsgeräts, dem gegenwärtigen Benutzernamen **622** des Kommunikationsgeräts, dem Standort **623** des Kommunikationsgeräts und der Erzeugungszeit **624** der Präsenzinformation. In einem Eintrag **600-1**, der dem Kommunikationsgerät **11-1** entspricht, entsprechen die jeweiligen Inhalte der Positionen **620** und **622** bis **624** den jeweiligen Inhalten der aus der Antwortmitteilung in Fig. 5 extrahierten Zeilen **530** und **527** bis **529**. Die IP-Adresse **621** entspricht der IP-Quelladresse, die im IP-Header der Antwortmitteilung enthalten ist.

[0055] Fig. 7 zeigt ein Beispiel für einen in Schritt **508** in Fig. 3 in der Sicherheitsrichtliniendatenbank **300** registrierten Sicherheitsrichtlinieneintrag. Jeder entsprechend einem Peer-Kommunikationsgerät gespeicherte Sicherheitsrichtlinieneintrag enthält die IP-Adresse **710** und die Portnummer **711** eines Quellgeräts, die IP-Adresse **712** und die Portnummer **713** eines Zielgeräts, ein Transportschichtprotokoll **714**, eine Richtung **715**, die Übermittlung oder Empfang angibt, und eine Aktion **716**, die einen Vorgang angibt, der bezüglich eines Pakets durchgeführt werden soll.

[0056] Wenn in der Aktion **716** „ipsec" spezifiziert ist, werden außerdem ein Protokoll **717**, ein Modus **718**, ein Endpunkt **719** und eine Stufe **720** zu dem Sicherheitsrichtlinieneintrag hinzugefügt. In einem Sicherheitsrichtlinieneintrag **300-1** für das Kommunikationsgerät **11-1** entsprechen die Positionen **710** bis **716** den jeweiligen Inhalten der Zeilen **520** bis **526** in der in Fig. 5 gezeigten Antwortmitteilung.

[0057] Fig. 8 zeigt ein Beispiel für einen Anzeigeschirm **800** für die Sicherheitsrichtlinie, die in Schritt **506** von der Sicherheitsrichtlinien-E/A-Schnittstelle **302** an eine Anzeigeeinheit oder dergleichen gegeben wird. Die jeweiligen IP-Adressen der Quelle (Kommunikationsgerät **10**) und des Ziels (Kommunikationsgerät **11-1**) werden in den Textfeldern **810** bzw. **814** angezeigt. Wenn ein bestimmter Port von der Sicherheitsrichtlinie spezifiziert worden ist, ist das Kontrollfeld **811** und/oder **815** markiert, und bestimmte Portnummern werden in den Textfeldern **812** und **816** angezeigt. Ist kein bestimmter Port spezifiziert

worden, ist das Kontrollfeld **813** und/oder **817** für „any" [beliebig] markiert.

[0058] Für das Transportschichtprotokoll ist ein Radioschalter **818** oder **819** entsprechend einem von der Sicherheitsrichtlinie spezifizierten Protokollnamen markiert. Ist kein Protokoll spezifiziert, ist der Radioschalter **820** für „any" markiert. Für die Richtung der Paketübertragung ist ein Radioschalter **821** für „in" [Eingang] markiert, wenn es sich um ein empfangenes Paket handelt, während im Falle eines zu übermittelnden Pakets ein Radioschalter **822** für „out" [Ausgang] markiert ist.

[0059] Wenn ein Vorgang zum Verwerfen des Pakets als „Aktion" für ein Paket durchgeführt werden soll, ist ein Radioschalter **823** für „discard" [Verwerfen] markiert. Soll kein spezieller Vorgang durchgeführt werden, ist der Radioschalter **824** für „none" [keine] markiert. Soll ein Vorgang „ipsec" durchgeführt werden, ist der Radioschalter **825** für „ipsec" markiert. Wenn der Radioschalter für „ipsec" markiert ist, ist außerdem „ah" [Authentisierung] **826**, „esp" [Verschlüsselung] **827** und/oder „ipcomp" [Komprimierung] **828** gewählt, die jeweils den Typ des anzuwendenden Sicherheitsprotokolls angeben. Die Radioschalter **829** und **830** geben an, ob als Modus der Transportmodus oder der Tunnelmodus anzuwenden ist. Wenn der Tunnelmodus spezifiziert ist, wird ein Textfeld **831** angezeigt, in dem das Kommunikationsgerät angegeben ist, das das andere Ende eines Tunnels bildet. Als Sicherheitsstufe wird die Option „default" [Vorgabe] **832**, „use" [Verwenden] **833**, die die Ausführung eines Sicherheitsvorgangs empfiehlt, wenn dies möglich ist, oder „require" [Erforderlich] **834** angezeigt, die die Ausführung des Sicherheitsvorgangs vorschreibt.

[0060] In Fig. 8 stellt der Doppelkreis den Radioschalter dar, der gemäß der Sicherheitsrichtlinieninformation gewählt ist. Aus der Abbildung ist ersichtlich, dass in dem hier gezeigten Beispiel als Sicherheitsrichtlinie für das Peer-Kommunikationsgerät **11-1** die IP-Quelladresse „192.168.1.1", der Quellport „any", die IP-Zieladresse „192.168.1.2", der Zielport „any", der Transport „udp", die Richtung „out" und die Aktion „none" auf der Grundlage der in Fig. 3 gezeigten Sicherheitsrichtlinieninformation spezifiziert worden sind.

[0061] Fig. 9 zeigt ein Beispiel für den Präsenzinformations-Anzeigeschirm **900** des Peer-Kommunikationsgeräts, der in Schritt **505** in Fig. 3 von der Präsenzinformations-E/A-Schnittstelle **402** an die Anzeigeeinheit gegeben wird. Der Präsenzinformations-Anzeigeschirm **900** und der Sicherheitsrichtlinien-Anzeigeschirm **800** werden in einem Mehrfenster-Modus auf demselben Anzeigeschirm gebildet, damit der Benutzer sie gleichzeitig einsehen kann. Alternativ können die Anzeigeschirme **800** und **900** abwechselnd umschaltbar auf der Anzeige angezeigt werden.

[0062] Der Präsenzinformations-Anzeigeschirm **900** zeigt „entity" [Entität] **910** für die Identifizierungsinformation des Peer-Kommunikationsgeräts, die IP-Adresse **911** des Peer-Kommunikationsgeräts, den gegenwärtigen Benutzer **912** des Peer-Kommunikationsgeräts, den Standort **913** des Peer-Kommunikationsgeräts und die Erzeugungszeit **914** der Präsenzinformation an. In dem in Fig. 9 gezeigten Beispiel werden „peerA@example.com" (917) „192.168.1.2" (918), „John" (919), „Büro" (920) und „2002-09-28 10:49:29" (921) als die Präsenzinformation für das Peer-Kommunikationsgerät **11-1** angezeigt.

[0063] Die durch die Spezifikation des Peer-Kommunikationsgeräts durch den Benutzer erhaltene Präsenzinformation wird automatisch in der Präsenzinformationsdatenbank **400** gespeichert. Wenn der Benutzer die Angaben für den Benutzer **919** und den Standort **920** des Peer-Kommunikationspartners, die auf dem Präsenzinformations-Anzeigeschirm **900** angezeigt werden, jedoch in vertraute Werte entsprechend seinen Präferenzen ändert, ist es auch möglich, dass die Präsenzinformations-Verarbeitungseinheit **401** das Ergebnis der Korrektur in der bereits in der Datenbank gespeicherten Präsenzinformation widerspiegelt.

[0064] Daher kann der Benutzer des Kommunikationsgeräts **10** auf dem Präsenzinformations-Anzeigeschirm **900** erkennen, dass sich das Peer-Kommunikationsgerät **11-1** im Büro befindet und mit dem privaten IP-Netz verbunden ist. In diesem Fall entscheidet der Benutzer, dass die Änderung der Sicherheitsrichtlinie auf dem in Fig. 8 gezeigten Sicherheitsrichtlinien-Anzeigeschirm **800** nicht erforderlich ist, und drückt eine Speichertaste **835**. Als Ergebnis wird die Sicherheitsrichtlinieninformation mit dem auf dem Präsenzinformations-Anzeigeschirm angezeigten Inhalt in der Sicherheitsrichtliniendatenbank **300** gespeichert und im IPsec-Funktionsblock verwendet.

[0065] Als ein zweites Beispiel der vorliegenden Erfindung wird als Nächstes ein Verfahren zur Kommunikation zwischen dem Kommunikationsgerät **10** und dem Kommunikationsgerät **11-2** über das private IP-Netz **2** und das öffentliche Netz **3** beschrieben.

[0066] Fig. 10 zeigt den von dem Benutzer **9** vor dem Start der Peer-to-Peer-Kommunikation durchzuführenden Betriebsablauf und eine Abfolge von zwischen dem Kommunikationsgerät **10** und dem Peer-Kommunikationsgerät **11-2** ausgetauschten Kommunikationsnachrichten nach der zweiten Ausführungsform der vorliegenden Erfindung.

[0067] Der Benutzer **9** übermittelt über einen von

der Sicherheitsrichtlinien- und Präsenzinformations-Anforderungsschnittstelle **403** an die Anzeigeeinheit gegebenen GUI-Anzeigeschirm eine Anforderung zum Erhalten der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts **11-2** an das Kommunikationsgerät **10** (Schritt **601**), in gleicher Weise wie bei der ersten Ausführungsform, die die vorstehend beschriebene Kommunikation mit dem Kommunikationsgerät **11-1** durchführt. Bei Empfang der Anforderung übermittelt das Kommunikationsgerät **10** eine Nachricht zur Anforderung der Präsenzinformation und der Sicherheitsrichtlinie an das Peer-Kommunikationsgerät **11-2** (Schritt **602**), und das Peer-Kommunikationsgerät **11-2** liefert als Antwort eine Antwortmitteilung mit der Präsenzinformation und der Sicherheitsrichtlinie (Schritt **603**).

[0068] In dem Kommunikationsgerät **10**, das die Antwortmitteilung erhalten hat, speichert die Präsenzinformations-Verarbeitungseinheit **401** die Präsenzinformation des Peer-Kommunikationsgeräts **11-2** in der Präsenzinformationsdatenbank **400** (Schritt **604**) und zeigt die Präsenzinformation des Peer-Kommunikationsgeräts **11-2** auf der Anzeigeeinheit des Peripheriegeräts **20** über die Präsenzinformations-E/A-Schnittstelle **402** an (Schritt **605**). Dabei zeigt die Sicherheitsrichtlinien-Verarbeitungseinheit **301** die Sicherheitsrichtlinie des Peer-Kommunikationsgeräts **11-2** auf der Anzeigeeinheit über die Sicherheitsrichtlinien-E/A-Schnittstelle **302** an (Schritt **606**). Der vorstehende Ablauf ist identisch mit dem Ablauf für den Austausch von Kommunikationsnachrichten zwischen dem Kommunikationsgerät **10** und dem Peer-Kommunikationsgerät **11-1** über das private IP-Netz **2** nach der anhand von Fig. 3 beschriebenen ersten Ausführungsform.

[0069] Fig. 11 zeigt ein Beispiel für den Präsenzinformations-Anzeigeschirm **110**, der in Schritt **605** auf der Anzeigeeinheit angezeigt wird. In diesem Beispiel ist der Standort **930** „external" [extern], was angibt, dass das Peer-Kommunikationsgerät **11-2** mit einem öffentlichen Netz verbunden ist. Der Benutzer **9** analysiert dann den von der Sicherheitsrichtlinien-Verarbeitungseinheit **301** angezeigten Sicherheitsrichtlinien-Anzeigeschirm des Peer-Kommunikationsgeräts **11-2** und beurteilt, ob die Sicherheitsstufe für die vorliegende Situation korrekt ist oder nicht.

[0070] Fig. 12 zeigt ein Beispiel für einen in Schritt **605** angezeigten Sicherheitsrichtlinien-Anzeigeschirm **1200**. Die hier angezeigte Sicherheitsrichtlinie ist bis auf den Wert der IP-Adresse für das Ziel dieselbe wie in Fig. 8 und gibt an, dass die Aktion für ein Paket „none" [keine] (850) lautet, das heißt es wird kein Sicherheitsvorgang bezüglich des Pakets durchgeführt.

[0071] In diesem Fall entscheidet der Benutzer **9**, dass die Sicherheitsrichtlinie hinsichtlich der Sicherstellung der Kommunikationssicherheit unzureichend ist, ändert die Sicherheitsrichtlinie für das Peer-Kommunikationsgerät **11-2** auf eine höhere Stufe (Schritt **608**) und weist dann das Kommunikationsgerät **10** an, die geänderte Sicherheitsrichtlinie zu registrieren (Schritt **609**). Bei Empfang der Registrierungsanweisung speichert das Kommunikationsgerät **10** die geänderte Sicherheitsrichtlinie in der Sicherheitsrichtliniendatenbank **300** (Schritt **610**).

[0072] Fig. 13 zeigt ein Beispiel für einen Anzeigeschirm **1300** der in Schritt **608** geänderten Sicherheitsrichtlinie. Aus der Abbildung ist im Vergleich mit dem in Fig. 12 gezeigten Anzeigeschirm vor der Änderung ersichtlich, dass der Benutzer **9** den Sicherheitsvorgang „ipsec" (860) als Aktion, die Authentisierung „ah" (861) und die Verschlüsselung „esp" (862) als Protokolle sowie die Anweisung „require" [erforderlich] (865) als Sicherheitsstufe spezifiziert hat. Wenn der Benutzer **9** nach der Speicherung der Sicherheitsrichtlinie den Start der Peer-to-Peer-Kommunikation mit dem Peer-Kommunikationsgerät **11-2** anweist (Schritt **611**), aktiviert das Kommunikationsgerät **10** den Peer-to-Peer-Kommunikations-Funktionsblock **200**, um die Peer-to-Peer-Kommunikation mit dem Peer-Kommunikationsgerät **11-2** zu starten (Schritt **612**).

[0073] Wenn das Kommunikationsgerät **10** die von dem Peer-Kommunikationsgerät erhaltene Sicherheitsstufe der Sicherheitsrichtlinie ändert und die Kommunikation entsprechend der geänderten Sicherheitsrichtlinie wie im Falle der zweiten Ausführungsform startet, kommt es zu einer Diskrepanz zwischen der von dem Peer-Kommunikationsgerät **11-2** auf ein empfangenes Paket angewendeten Sicherheitsrichtlinie (SP1) und der von dem Kommunikationsgerät **10** auf ein an das Peer-Kommunikationsgerät **11-2** übermitteltes Paket angewendeten Sicherheitsrichtlinie (SP2), so dass die Sicherheitsrichtlinie SP2 eine höhere Sicherheitsstufe als die Sicherheitsrichtlinie SP1 aufweist.

[0074] Ein Paket, das auf einer höheren Sicherheitsstufe als der durch die Sicherheitsrichtlinie des Peer-Kommunikationsgeräts **11-2** spezifizierten Sicherheitsstufe übermittelt wird, verursacht jedoch kein Problem wie etwa die Ablehnung des Empfangsvorgangs in dem Peer-Kommunikationsgerät **11-2**. In diesem Fall ist es daher nicht nötig, dass das Kommunikationsgerät **10** das Peer-Kommunikationsgerät B **11-2** über die Änderung der Sicherheitsrichtlinie informiert und die Verhandlung für die Änderung der Sicherheitsrichtlinie durchführt.

[0075] Wenn hingegen die Sicherheitsstufe nach der Änderung der Sicherheitsrichtlinie niedriger als die Sicherheitsstufe des Peer-Kommunikationsgeräts **11-2** in Schritt **608** in Fig. 10 wird, wird ein von

dem Kommunikationsgerät **10** übermitteltes Paket einem Vorgang des Verwerfens gemäß der Sicherheitsrichtlinie des Peer-Kommunikationsgeräts **11-2** unterzogen. Daher ist es nötig, dass das Kommunikationsgerät **10** vor der Übermittlung des Datenpakets die Verhandlung bezüglich der Änderung der Sicherheitsrichtlinie mit dem Peer-Kommunikationsgerät **11-2** durchführt.

[0076] Obwohl die vorstehenden Ausführungsformen Beispiele beschreiben, bei denen das Kommunikationsgerät **10** jeweils die Sicherheitsrichtlinie und die Präsenzinformation von dem Peer-Kommunikationsgerät erhält, die Korrektheit der Sicherheitsrichtlinie auf der Grundlage der Präsenzinformation beurteilt und die Sicherheitsrichtlinie wenn nötig ändert, wenn das Kommunikationsgerät **10** eine Anforderung für die Sicherheitsrichtlinie und die Präsenzinformation dafür von einem weiteren Kommunikationsgerät empfängt, liefert das Kommunikationsgerät **10** eine Antwortmitteilung mit der Sicherheitsrichtlinie und Präsenzinformation des Kommunikationsgeräts **10** an den Anforderer, ähnlich den Peer-Kommunikationsgeräten **11-1** und **11-2** in den Ausführungsformen. Die Antwortmitteilung wird auf der Grundlage der Präsenzinformation des Kommunikationsgeräts **10**, die von dem Peer-to-Peer-Kommunikations-Funktionsblock **200** aus der Datenbank **400** über die Präsenzinformations-Verarbeitungseinheit **401** ausgelesen wird, und der Sicherheitsrichtlinie des Kommunikationsgeräts **10** erzeugt, die von dem Peer-to-Peer-Kommunikations-Funktionsblock **200** aus der Datenbank **300** über die Sicherheitsrichtlinien-Verarbeitungseinheit **301** ausgelesen wird. Wenn der der IP-Adresse des Anforderers entsprechende Eintrag in der Datenbank **300** gespeichert ist, wird die durch den Eintrag angegebene Sicherheitsrichtlinie übernommen; anderenfalls wird die Vorgabesicherheitsrichtlinie übernommen.

[0077] Obwohl bei den Ausführungsformen jeweils IPsec als das Kommunikationssicherheitsprotokoll angewendet worden ist, ist es auch möglich, ein anderes Protokoll für die Kommunikationssicherheit anzuwenden, indem der IPsec-Funktionsblock **110** ausgetauscht wird. Obwohl bei den Ausführungsformen jeweils die Sicherheitsrichtlinieninformation und die Präsenzinformation in den entsprechenden Datenbanken **300** und **400** gespeichert worden sind, müssen die Einrichtungen zur Speicherung der Informationen nicht unbedingt Datenbanken sein. So kann zum Beispiel stattdessen auch eine Tabelle in einem Speicher verwendet werden.

[0078] Obwohl der Benutzer die Korrektheit der Sicherheitsumgebung auf der Grundlage des auf dem Präsenzinformations-Anzeigeschirm angezeigten Standorts des Peer-Kommunikationsgeräts beurteilt hat und die auf die Kommunikation mit dem Peer-Kommunikationsgerät anzuwendende Sicherheitsrichtlinie bestimmt hat, ist es auch möglich, die Anzeige des Standorts des Peer-Kommunikationsgeräts auf dem Präsenzinformations-Anzeigeschirm wegzulassen und es dem Benutzer zu ermöglichen, das Netz, mit dem das Peer-Kommunikationsgerät verbunden ist, zum Beispiel aus dem Unterschied im Adressformat zwischen der Quelladresse und der Zieladresse zu bestimmen und die Kommunikationssicherheitsumgebung abzuschätzen. Alternativ ist es auch möglich, dem sich bewegenden Benutzer zu ermöglichen, den gegenwärtigen Standort mit dem Peripheriegerät **20** einzugeben, so dass ein bestimmter Standortname auf dem Präsenzinformations-Anzeigeschirm ausgegeben wird. Der Benutzer kann die Korrektheit der Sicherheitsrichtlinie auch anhand zusätzlicher Faktoren beurteilen, die nicht auf dem Präsenzinformations-Anzeigeschirm erscheinen, zum Beispiel dem Zweck der Kommunikation, der Art der zu übermittelnden Informationen und der Beziehung zwischen dem Benutzer und dem Kommunikations-Peer, zusätzlich zu den Informationen über den Standort des Peer-Kommunikationsgeräts.

[0079] Wie aus den vorstehenden Ausführungsformen ersichtlich, ermöglicht die vorliegende Erfindung die Peer-to-Peer-Kommunikation mit einer geeigneten Sicherheitsrichtlinie entsprechend der Kommunikationssicherheitsumgebung und dem Kommunikations-Peer. Durch Auswahl einer geeigneten Sicherheitsrichtlinie entsprechend der Kommunikationssicherheitsumgebung und Umgehen der Peer-to-Peer-Kommunikation auf einer zu hohen Sicherheitsstufe nach der vorliegenden Erfindung können CPU-Ressourcen eines Kommunikationsgeräts und Bandbreite eines Kommunikationsnetzes gespart werden.

Patentansprüche

1. Peer-to-Peer-Kommunikationsgerät zum Durchführen einer Eins-zu-Eins-Kommunikation mit einem anderen Kommunikationsgerät über ein IP-Netz (**1**), mit
einer ersten Einrichtung (**110**) zum Durchführen eines Verschlüsselungsvorgangs und/oder eines Prüfvorgangs bezüglich eines Pakets,
einer zweiten Einrichtung (**301**), um von einem durch einen Benutzer (**9**) des Kommunikationsgeräts (**10**) spezifizierten Peer-Kommunikationsgerät (**11**) Sicherheitsrichtlinieninformation einschließlich einer Verschlüsselungsregel und einer Authentisierungsregel zu erhalten, die jeweils durch das Peer-Kommunikationsgerät auf Pakete anzuwenden sind,
gekennzeichnet durch
eine dritte Einrichtung (**401**), um von dem durch den Benutzer (**9**) des Kommunikationsgeräts (**10**) spezifizierten Peer-Kommunikationsgerät (**11**) Präsenzinformation einschließlich Ortsinformation zum Beurteilen einer Kommunikationssicherheitsumgebung des Peer-Kommunikationsgeräts (**11**) zu erhalten,

eine vierte Einrichtung (**402**, **302**) zum Anzeigen der Präsenzinformation und der Sicherheitsrichtlinieninformation, so daß der Benutzer (**9**) auf Grundlage der Präsenzinformation die Korrektheit der Sicherheitsrichtlinieninformation beurteilt,
wobei die vierte Einrichtung (**402**, **302**) dazu ausgelegt ist, dem Benutzer (**9**) eine Genehmigung der Sicherheitsrichtlinien sowie eine teilweise Änderung der Sicherheitsrichtlinieninformation zu ermöglichen, und
wobei die erste Einrichtung (**110**) dazu ausgelegt ist, ein an das Peer-Kommunikationsgerät (**11**) zu übermittelndes Paket gemäß einer durch den Benutzer (**9**) genehmigten Sicherheitsrichtlinie zu verarbeiten.

2. Gerät nach Anspruch 1, ferner mit einem Speicher (**300**) zum Speichern der durch das Peer-Kommunikationsgerät (**11**) erhaltenen Sicherheitsrichtlinieninformation, oder der durch den Benutzer (**9**) über die vierte Einrichtung (**302**) teilweise geänderten Sicherheitsrichtlinieninformation, wobei die erste Einrichtung (**110**) das an das Peer-Kommunikationsgerät (**11**) zu übermittelnde Paket gemäß einer in dem Speicher (**300**) gespeicherten Sicherheitsrichtlinie verarbeitet.

3. Gerät nach Anspruch 1, ferner mit
einem ersten Speicher (**300**) zum Speichern von Vorgabesicherheitsrichtlinieninformation, die durch das Kommunikationsgerät (**10**) für Peer-to-Peer-Kommunikation mit dem anderen Kommunikationsgerät anzuwenden ist,
einem zweiten Speicher (**400**) zum Speichern der Präsenzinformation einschließlich der Information zum Beurteilen der Kommunikationssicherheitsumgebung des Kommunikationsgeräts (**10**), und
einer Einrichtung (**301**, **401**), um in Reaktion auf eine Anfrage nach der Präsenzinformation und der Sicherheitsrichtlinieninformation von dem anderen Kommunikationsgerät eine Antwortmitteilung zurückzugeben, die die von dem ersten Speicher (**300**) ausgelesene Vorgabesicherheitsrichtlinieninformation und die von dem zweiten Speicher (**400**) ausgelesene Präsenzinformation aufweist.

4. Gerät nach Anspruch 3, ferner mit einer Präsenzinformations-Verarbeitungseinheit (**401**) zum teilweisen Ändern der in dem zweiten Speicher (**400**) gespeicherten Präsenzinformation nach dem Auftreten einer Änderung in der Kommunikationsumgebung, die aus einer Bewegung des Kommunikationsgeräts (**10**) resultiert.

5. Gerät nach Anspruch 1, wobei die erste Einrichtung (**110**) ein zu übermittelndes Datenpaket und ein von dem IP-Netz (**1**) empfangenes Datenpaket gemäß einer Sicherheitsrichtlinie von durch den IETF definierten IP-Sicherheitsprotokollen verarbeitet.

6. Verfahren zur Peer-to-Peer-Kommunikation zwischen einem ersten Kommunikationsgerät (**10**) und einem zweiten Kommunikationsgerät, die jeweils an ein IP-Netz (**1**) angeschlossen sind, wobei in dem Verfahren
das erste Kommunikationsgerät (**10**) von dem zweiten Kommunikationsgerät Präsenzinformation, einschließlich Ortsinformation zum Beurteilen einer Kommunikationssicherheitsumgebung des zweiten Kommunikationsgeräts, und Sicherheitsrichtlinieninformation einschließlich einer Verschlüsselungsregel und einer Authentisierungsregel, die durch das zweite Kommunikationsgerät auf ein Paket anzuwenden sind, fordert,
die Präsenzinformation und die Sicherheitsrichtlinieninformation des zweiten Kommunikationsgeräts von dem zweiten Kommunikationsgerät an das erste Kommunikationsgerät (**10**) übermittelt werden,
auf einem Anzeigeschirm (**800**, **900**) durch das erste Kommunikationsgerät (**10**) die von dem zweiten Kommunikationsgerät empfangene Präsenz- und Sicherheitsrichtlinieninformation ausgegeben werden, so daß ein Benutzer (**9**) die Korrektheit der Sicherheitsrichtlinieninformation auf Grundlage der Präsenzinformation beurteilen kann, und
Paketkommunikation mit dem zweiten Kommunikationsgerät durch das erste Kommunikationsgerät (**10**) gemäß der durch den Benutzer (**9**) auf dem Anzeigeschirm (**800**, **900**) genehmigten Sicherheitsrichtlinie durchgeführt wird.

7. Verfahren nach Anspruch 6, wobei dem Benutzer (**9**) ferner ermöglicht wird, die durch das erste Kommunikationsgerät (**10**) auf dem Anzeigeschirm (**800**, **900**) ausgegebene Sicherheitsrichtlinieninformation teilweise zu korrigieren, wobei das erste Kommunikationsgerät (**10**) die Paketkommunikation mit dem zweiten Kommunikationsgerät gemäß der berichtigten Sicherheitsrichtlinie durchführt.

Es folgen 12 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1

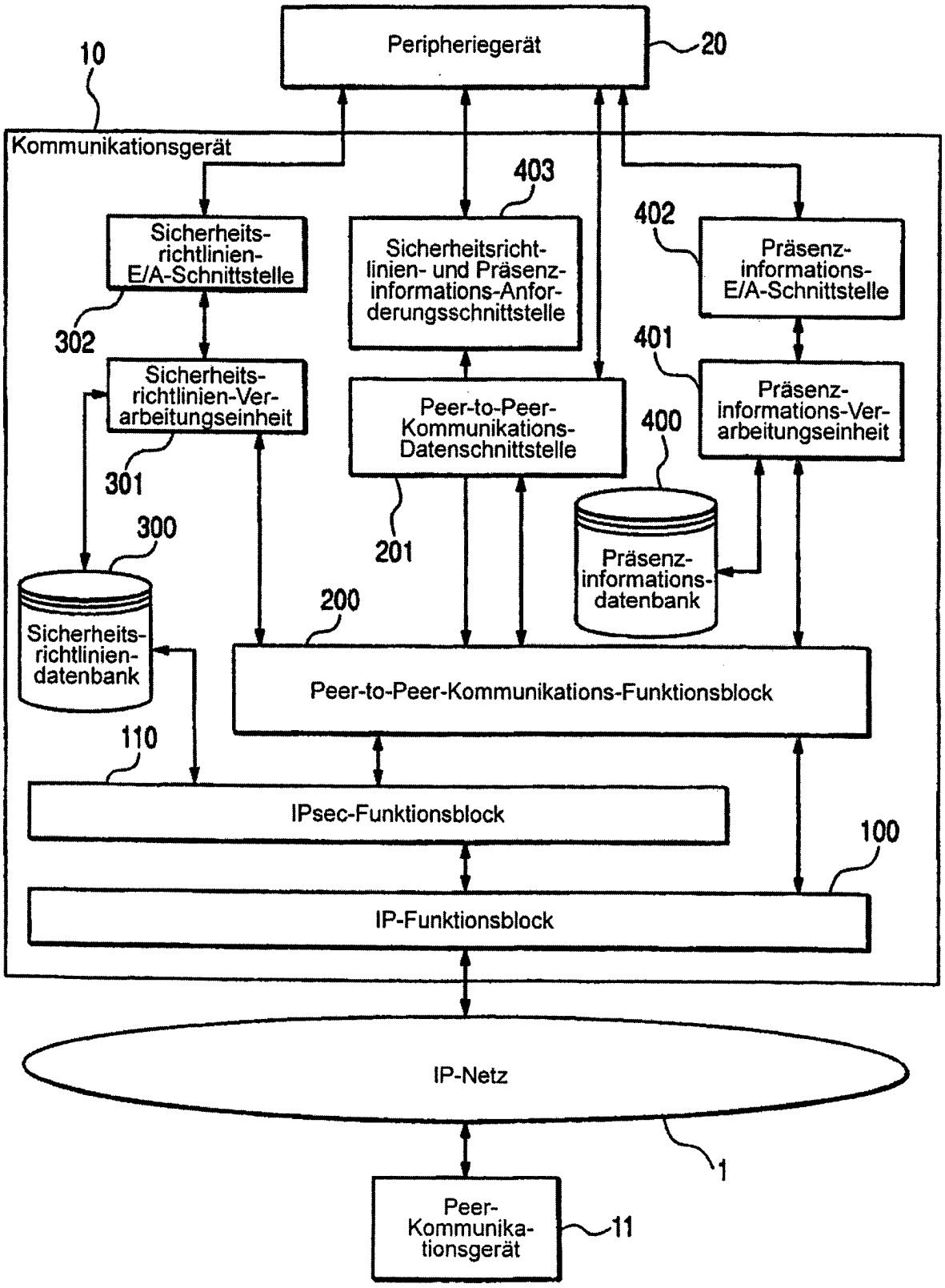


FIG. 2

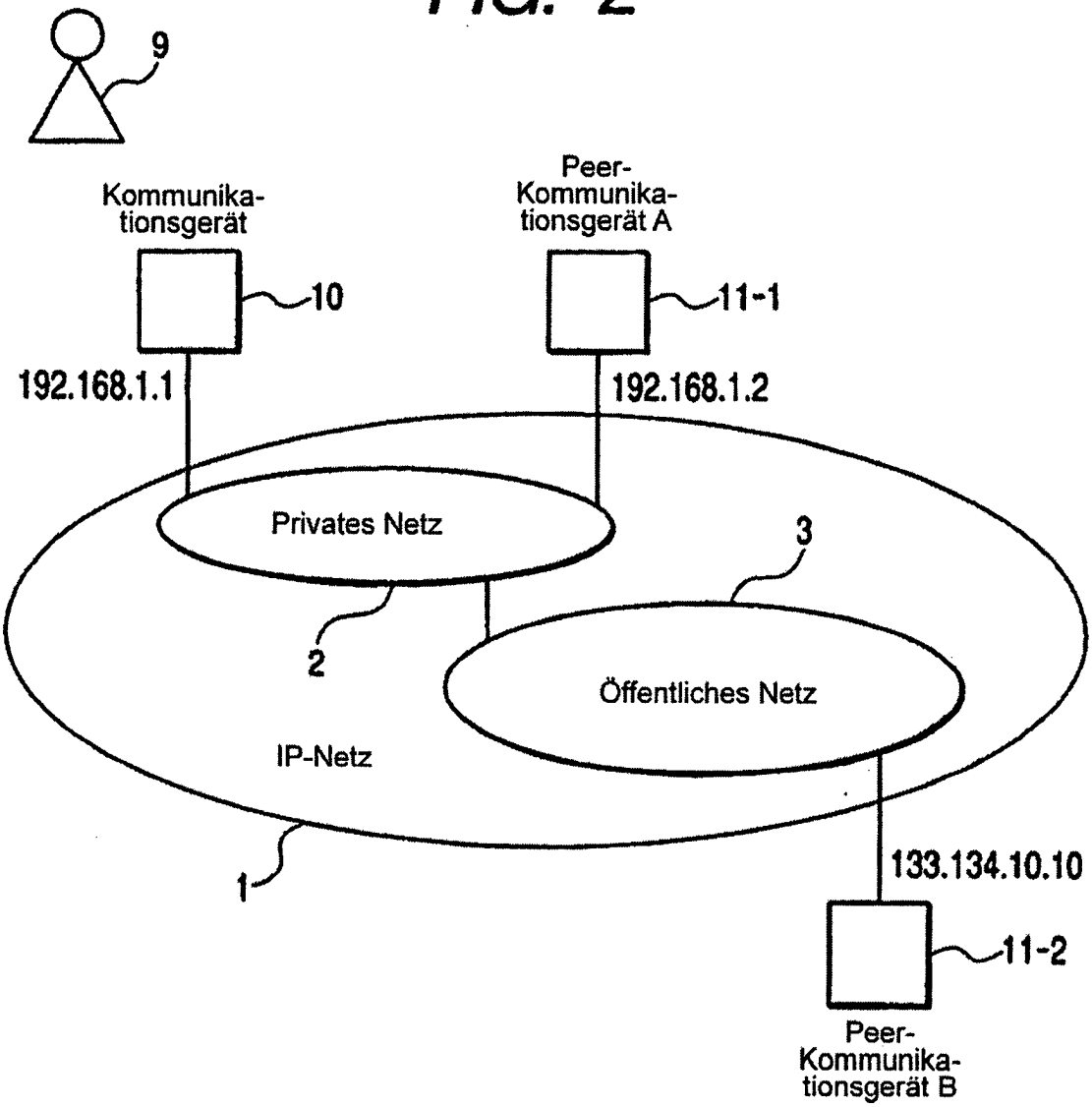

9
Kommunika-
tionsgerät
10
Peer-
Kommunika-
tionsgerät A
11-1
192.168.1.1
192.168.1.2
Privates Netz
3
2
Öffentliches Netz
IP-Netz
1
133.134.10.10
11-2
Peer-
Kommunika-
tionsgerät B

FIG. 3

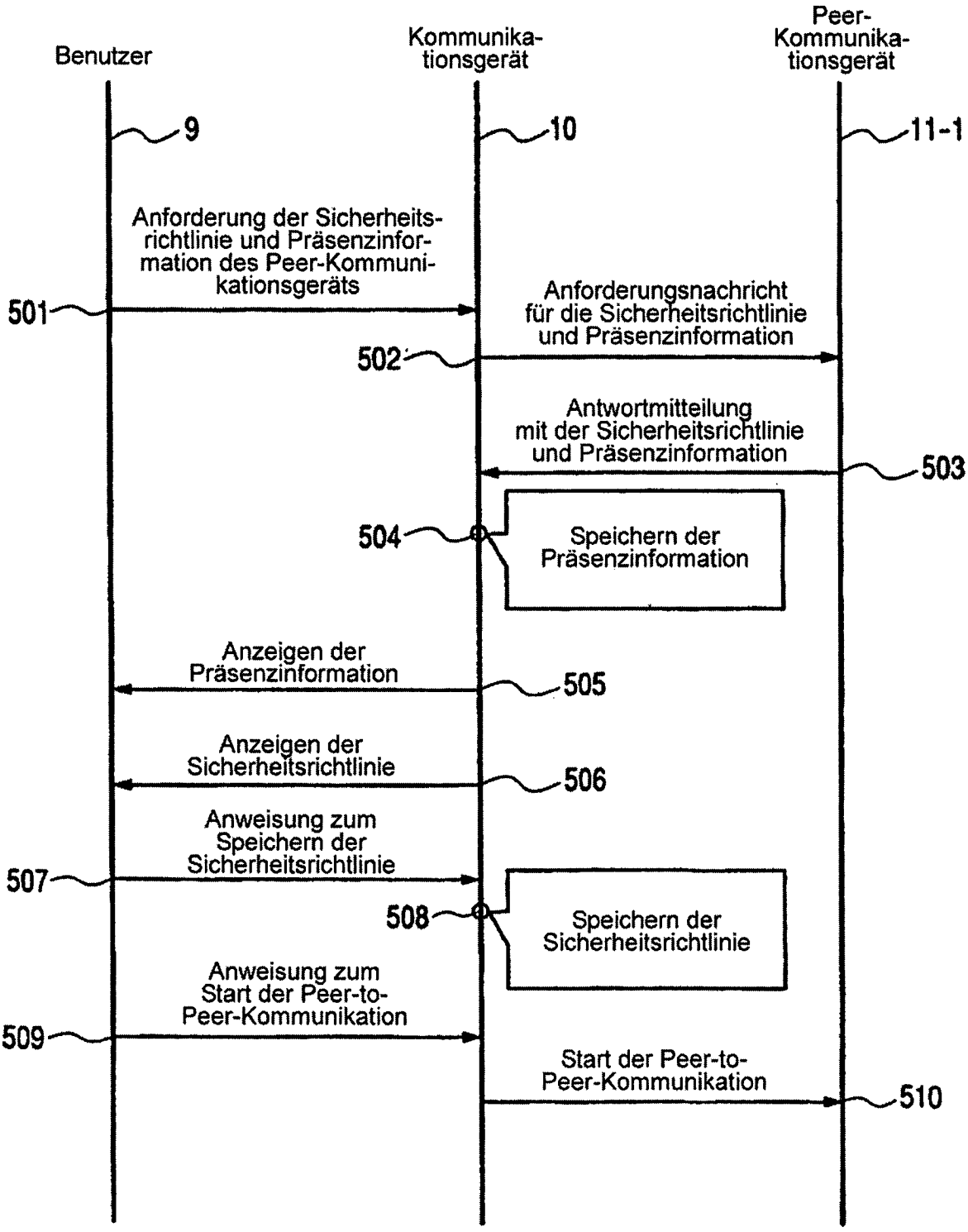

Benutzer
Kommunikationsgerät
Peer-Kommunikationsgerät
9
10
11-1
Anforderung der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts
501
Anforderungsnachricht für die Sicherheitsrichtlinie und Präsenzinformation
502
Antwortmitteilung mit der Sicherheitsrichtlinie und Präsenzinformation
503
504
Speichern der Präsenzinformation
Anzeigen der Präsenzinformation
505
Anzeigen der Sicherheitsrichtlinie
506
Anweisung zum Speichern der Sicherheitsrichtlinie
507
508
Speichern der Sicherheitsrichtlinie
Anweisung zum Start der Peer-to-Peer-Kommunikation
509
Start der Peer-to-Peer-Kommunikation
510

FIG. 4

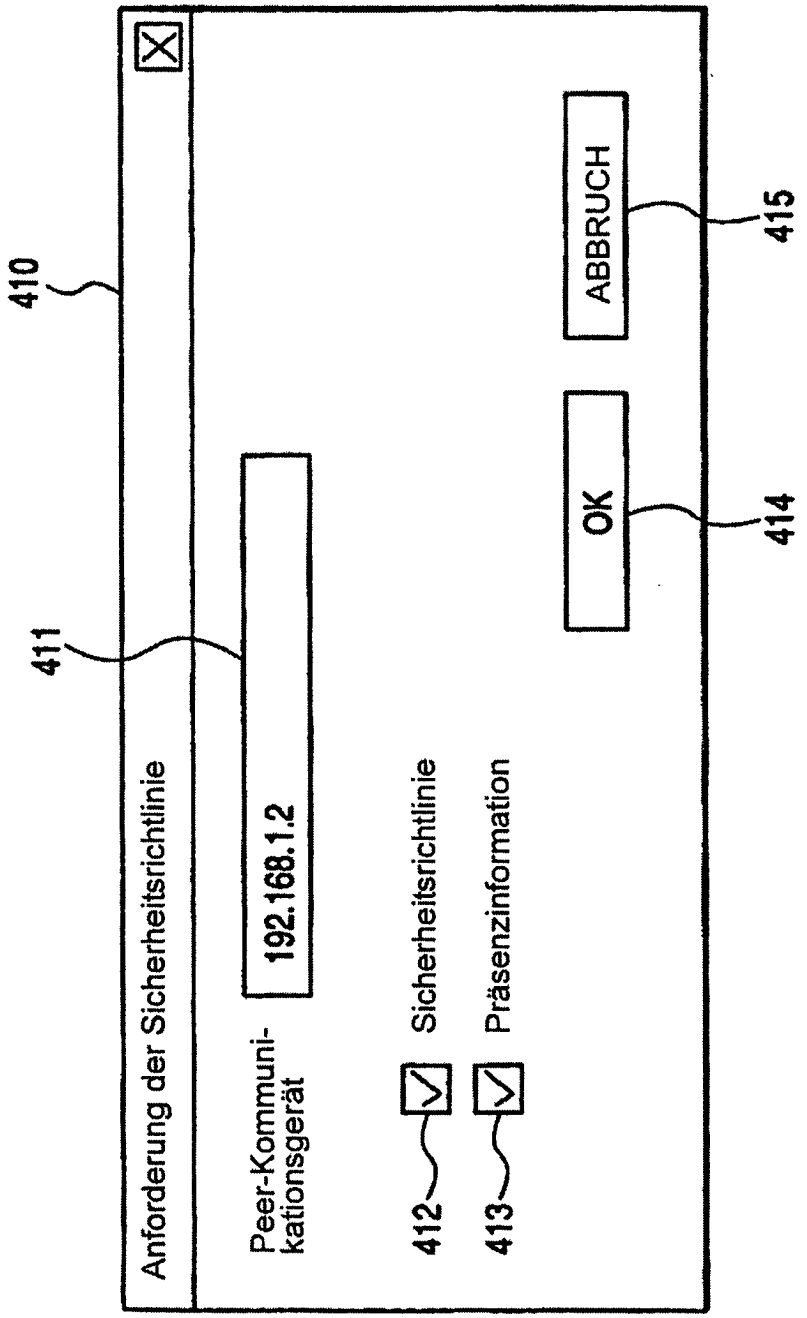

Anforderung der Sicherheitsrichtlinie
Peer-Kommunikationsgerät
192.168.1.2
Sicherheitsrichtlinie
Präsenzinformation
OK
ABBRUCH
410
411
412
413
414
415

FIG. 5

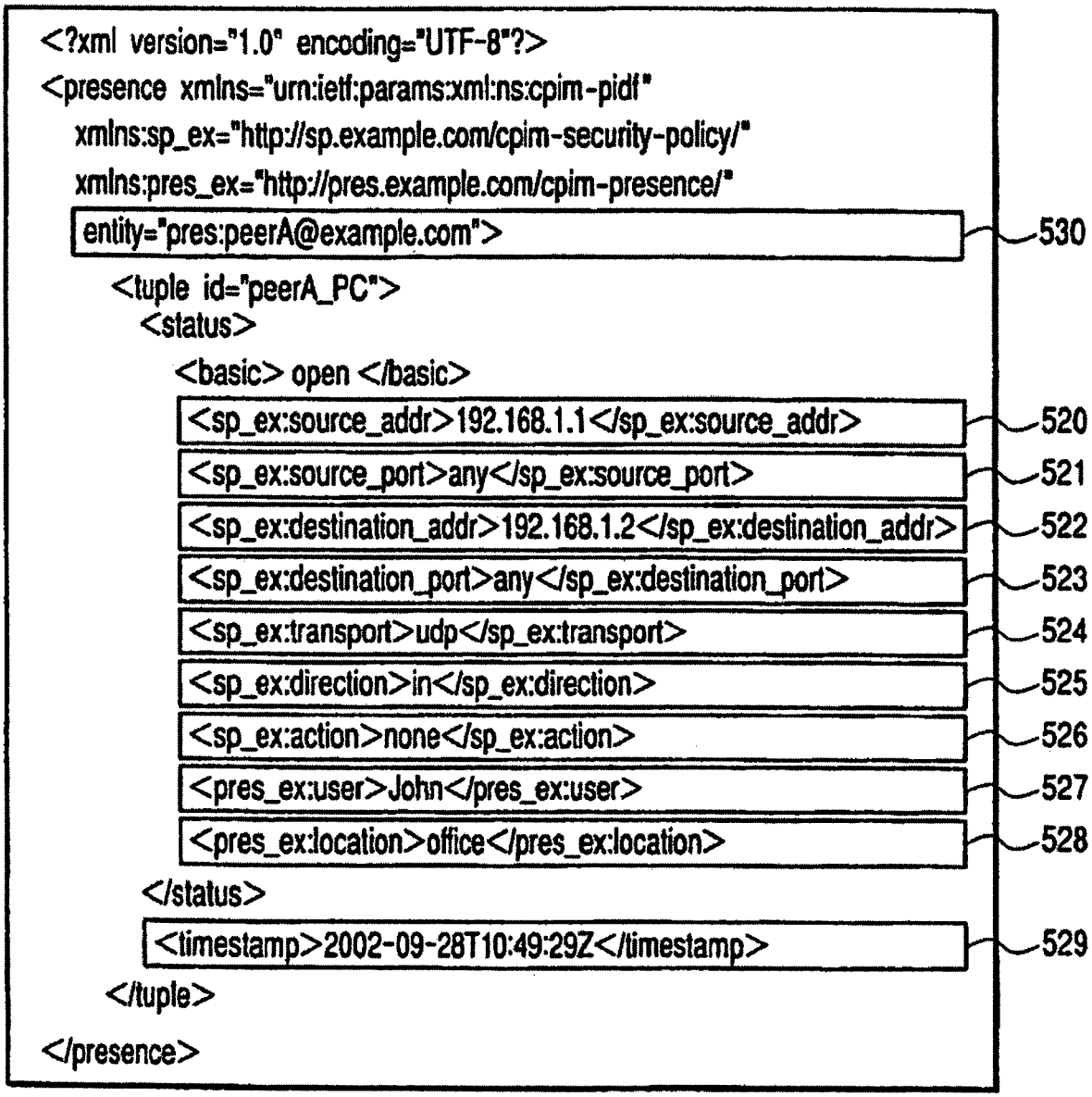

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:cpim-pidf"
xmlns:sp_ex="http://sp.example.com/cpim-security-policy/"
xmlns:pres_ex="http://pres.example.com/cpim-presence/"
entity="pres:peerA@example.com">
530
<tuple id="peerA_PC">
<status>
<basic> open </basic>
<sp_ex:source_addr>192.168.1.1</sp_ex:source_addr>
520
<sp_ex:source_port>any</sp_ex:source_port>
521
<sp_ex:destination_addr>192.168.1.2</sp_ex:destination_addr>
522
<sp_ex:destination_port>any</sp_ex:destination_port>
523
<sp_ex:transport>udp</sp_ex:transport>
524
<sp_ex:direction>in</sp_ex:direction>
525
<sp_ex:action>none</sp_ex:action>
526
<pres_ex:user>John</pres_ex:user>
527
<pres_ex:location>office</pres_ex:location>
528
</status>
<timestamp>2002-09-28T10:49:29Z</timestamp>
529
</tuple>
</presence>

FIG. 6

Präsenzinformations-
datenbank 400

600-1

620 Entität	621 IP-Adresse	622 Benutzer-name	623 Standort	624 Uhrzeit
peerA@example.com	196.128.1.2	John	Büro	2002-09-28 10:49:29
●●●	●●●	●●●	●●●	●●●

FIG. 7

Sicherheitsrichtlinien-
datenbank 300

710 Quelle		712 Ziel		713 Transport-schicht-protokoll	715 Richtung	716 Aktion	717 Protokoll	718 Modus	719 End-punkt	720 Stufe
711 IP-Adresse	Port-Nr.	IP-Adresse	Port-Nr.							
192.168.1.1	bel.	192.168.1.2	bel.	udp	out	keine	—	—	—	—
...	...	...	...	...	...	...	...	...	...	...

300-1

FIG. 8

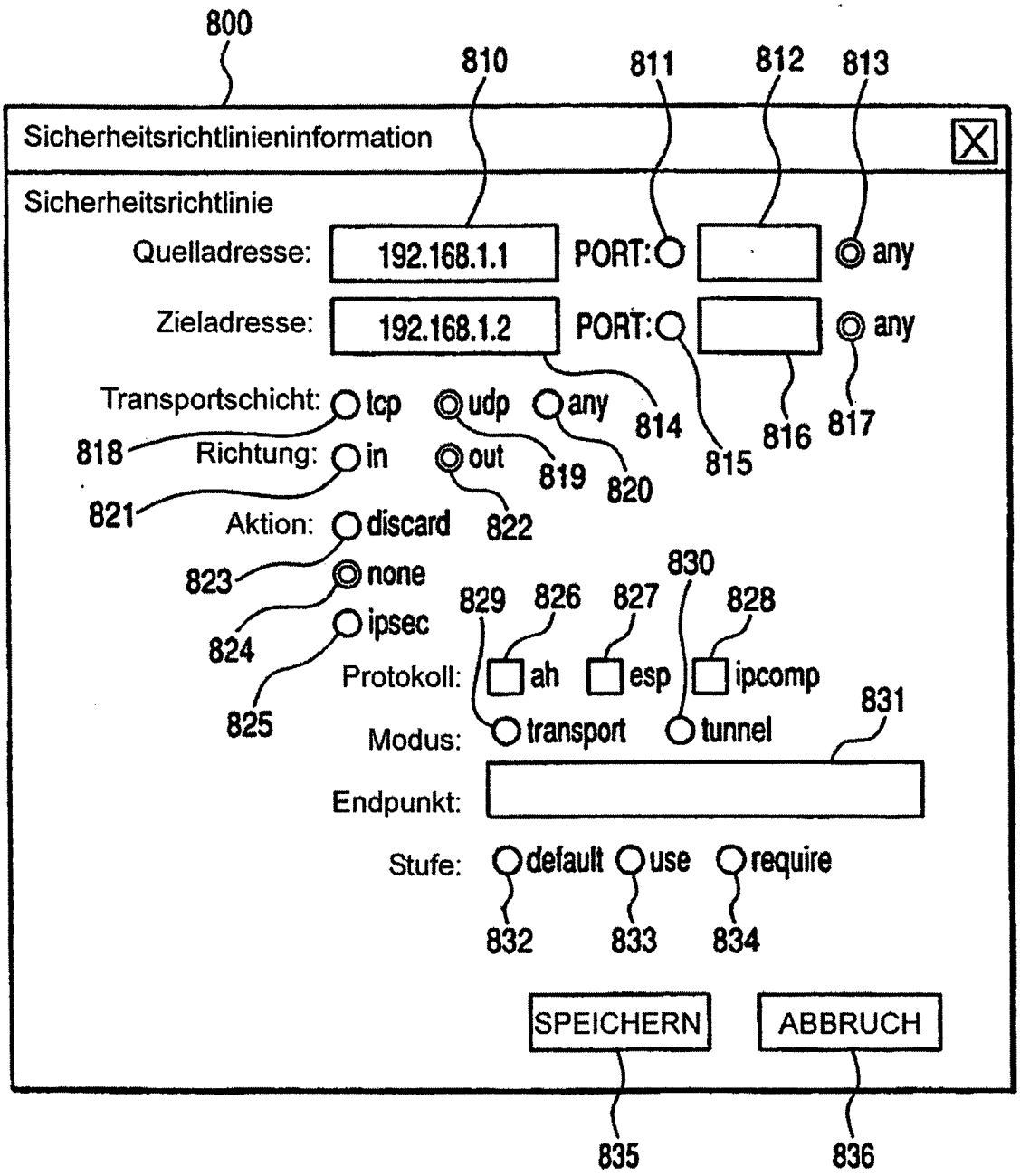

800
810
811
812
813
Sicherheitsrichtlinieninformation
Sicherheitsrichtlinie
Quelladresse:
192.168.1.1
PORT:
any
Zieladresse:
192.168.1.2
PORT:
any
Transportschicht:
tcp
udp
any
Richtung:
in
out
Aktion:
discard
none
ipsec
Protokoll:
ah
esp
ipcomp
Modus:
transport
tunnel
Endpunkt:
Stufe:
default
use
require
SPEICHERN
ABBRUCH
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836

FIG. 9

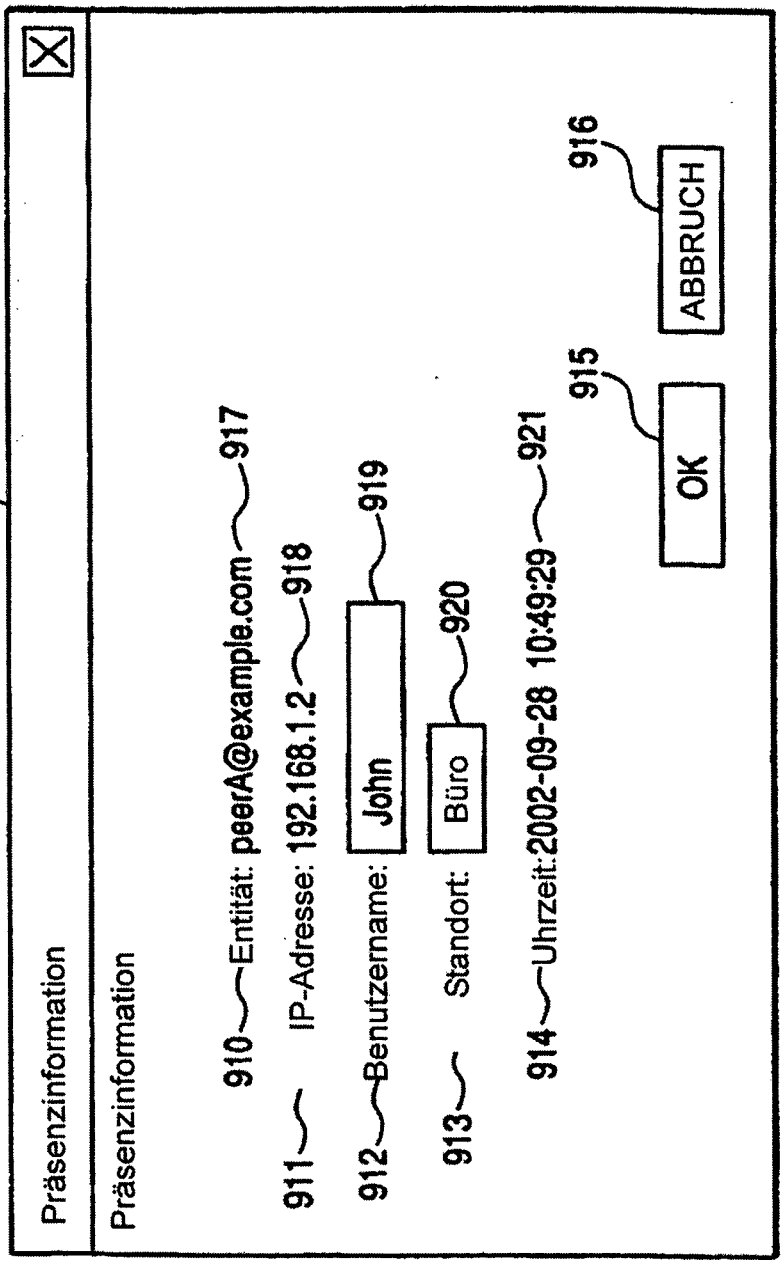

900
Präsenzinformation
Präsenzinformation
910
Entität: peerA@example.com
917
911
IP-Adresse: 192.168.1.2
918
912
Benutzername:
John
919
913
Standort:
Büro
920
914
Uhrzeit: 2002-09-28 10:49:29
921
915
OK
916
ABBRUCH

FIG. 10

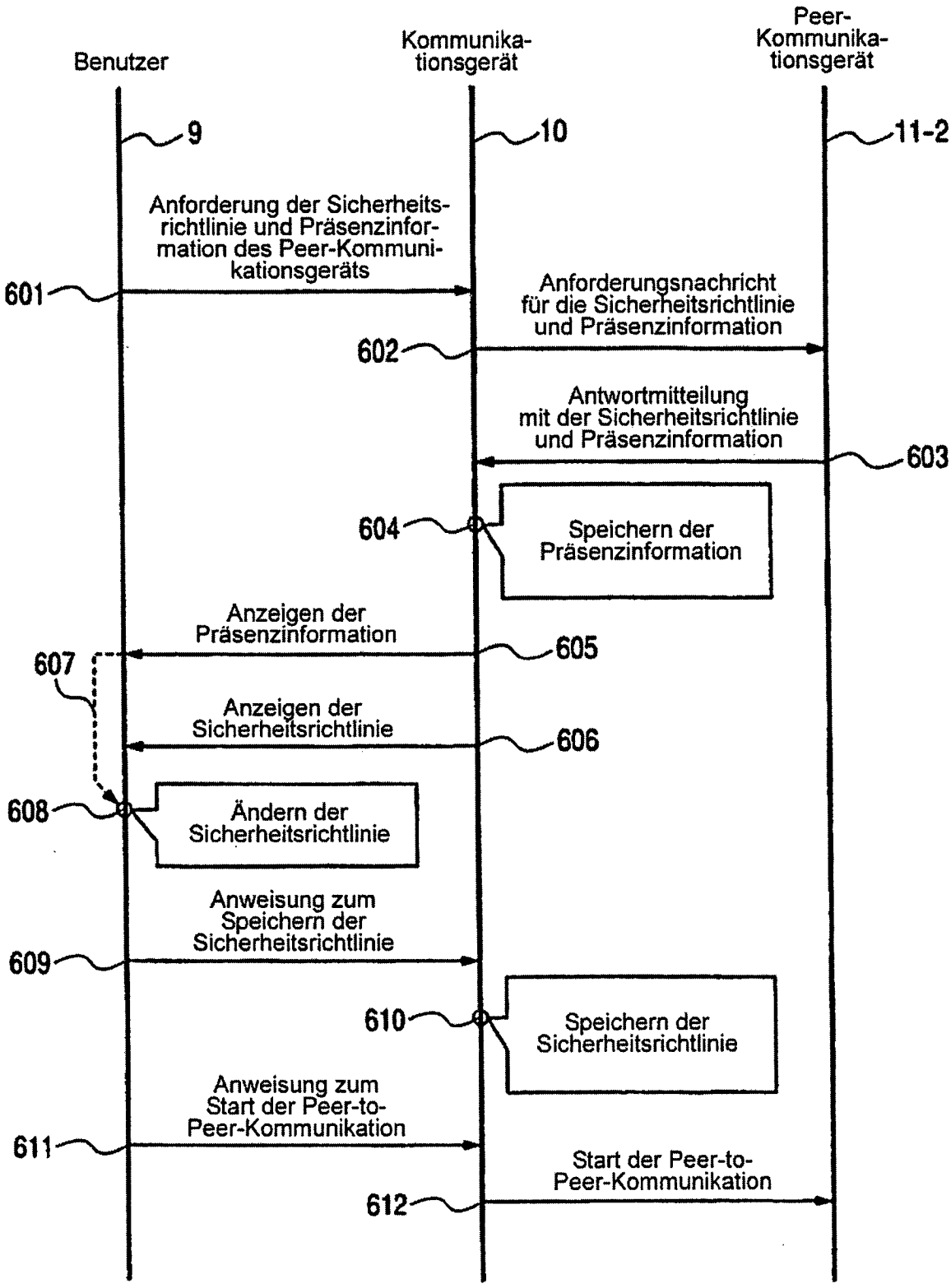

Benutzer
Kommunikationsgerät
Peer-Kommunikationsgerät
9
10
11-2
Anforderung der Sicherheitsrichtlinie und Präsenzinformation des Peer-Kommunikationsgeräts
601
Anforderungsnachricht für die Sicherheitsrichtlinie und Präsenzinformation
602
Antwortmitteilung mit der Sicherheitsrichtlinie und Präsenzinformation
603
604
Speichern der Präsenzinformation
Anzeigen der Präsenzinformation
605
607
Anzeigen der Sicherheitsrichtlinie
606
608
Ändern der Sicherheitsrichtlinie
Anweisung zum Speichern der Sicherheitsrichtlinie
609
610
Speichern der Sicherheitsrichtlinie
Anweisung zum Start der Peer-to-Peer-Kommunikation
611
Start der Peer-to-Peer-Kommunikation
612

FIG. 11

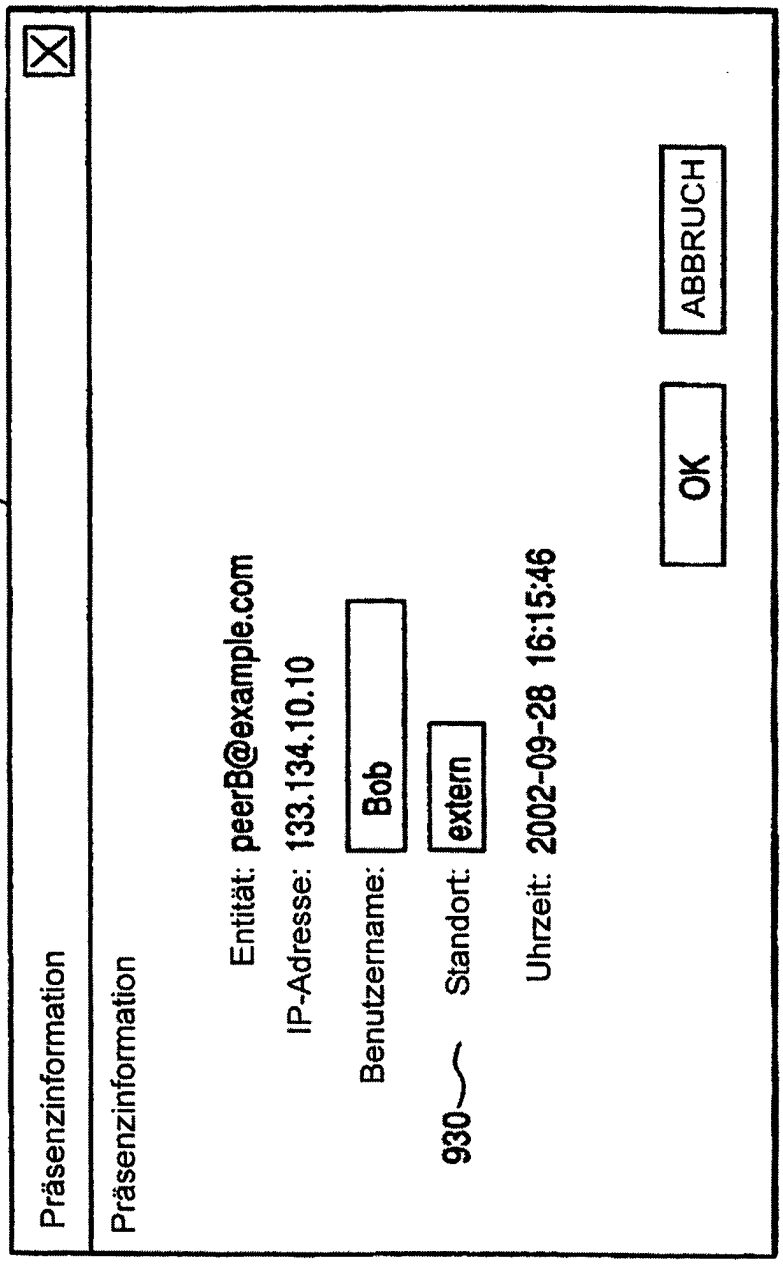

1100
Präsenzinformation
Präsenzinformation
Entität: peerB@example.com
IP-Adresse: 133.134.10.10
Benutzername: Bob
930
Standort: extern
Uhrzeit: 2002-09-28 16:15:46
OK
ABBRUCH

FIG. 12

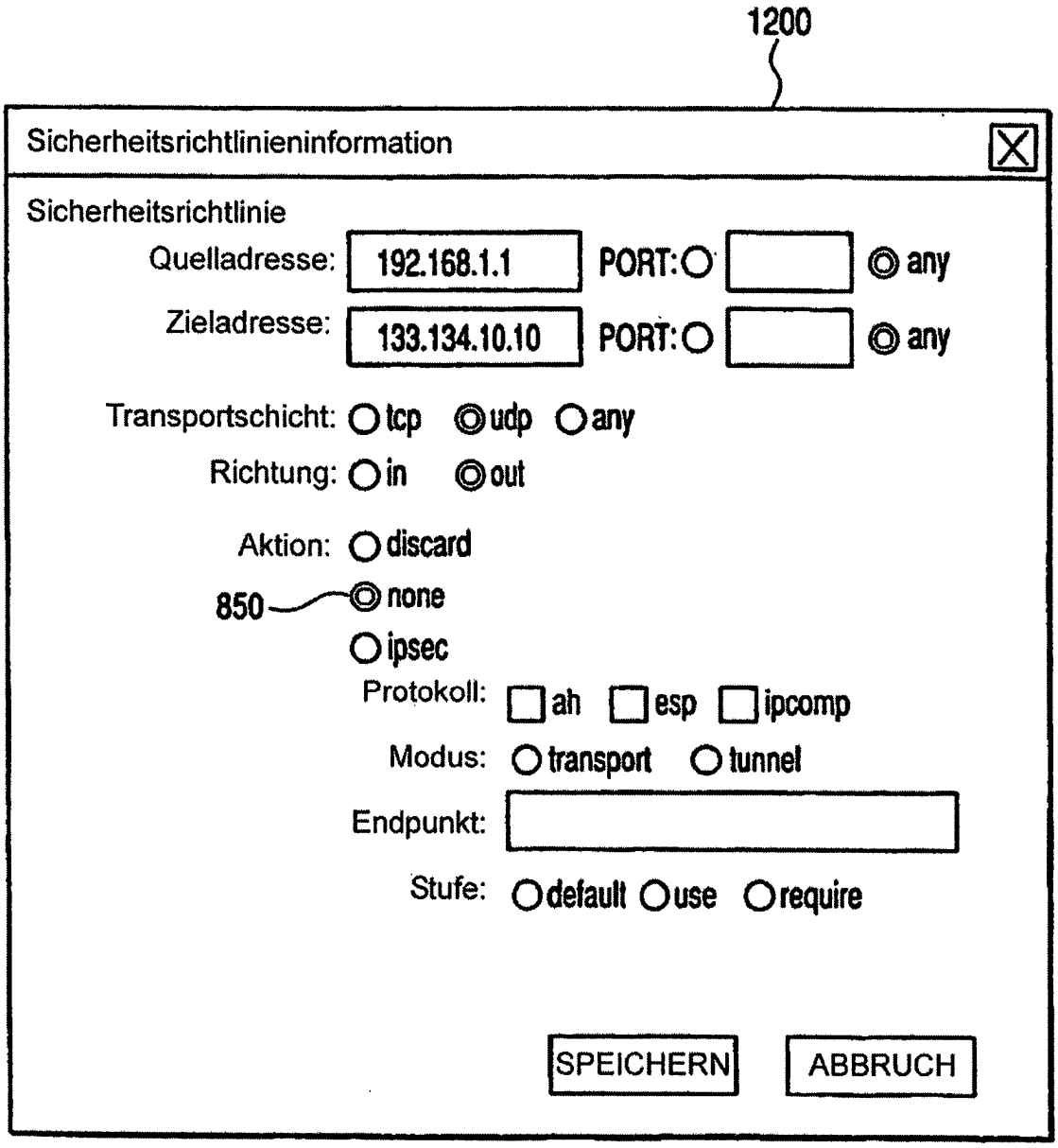
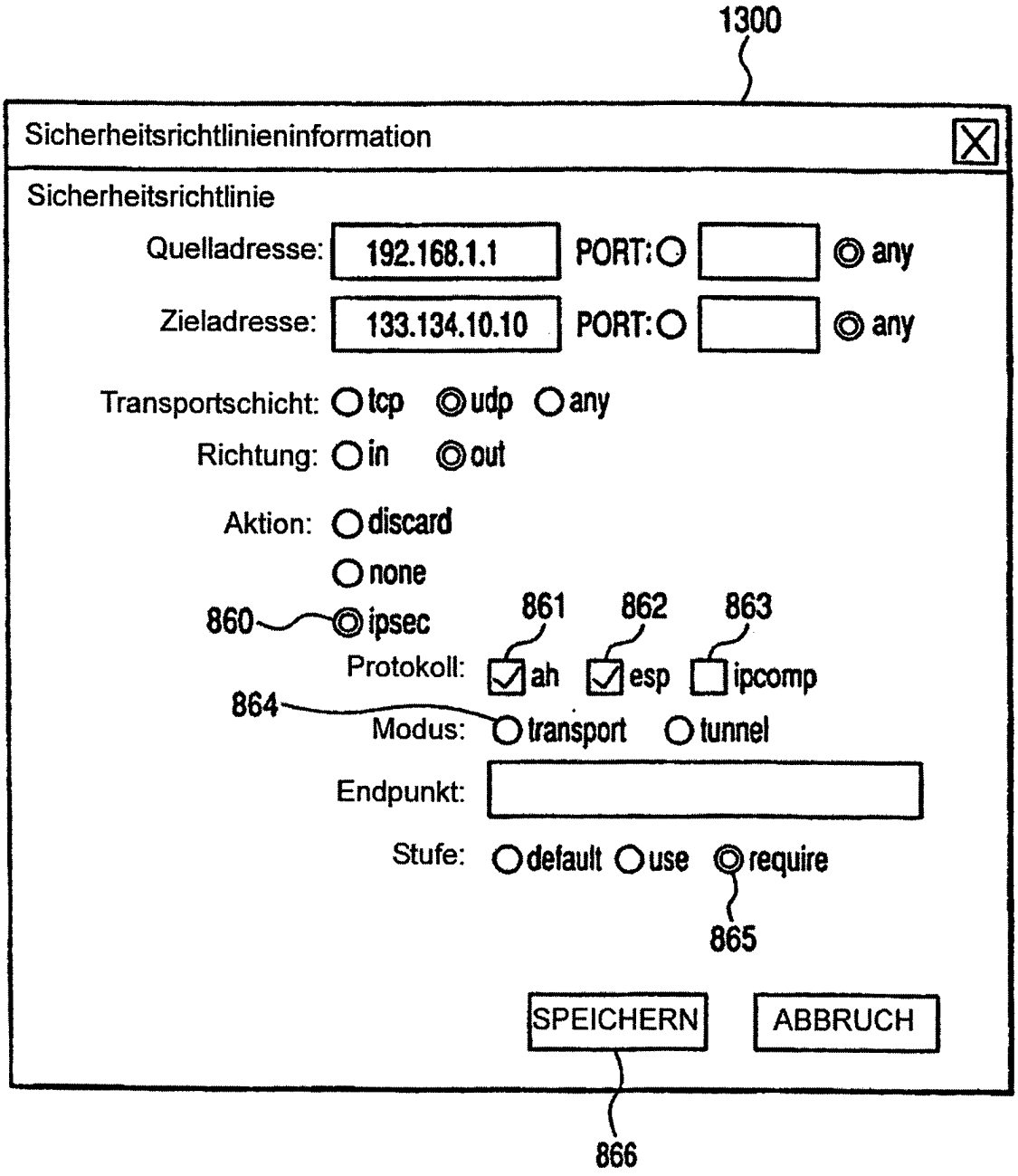

1200
Sicherheitsrichtlinieninformation
Sicherheitsrichtlinie
Quelladresse:
192.168.1.1
PORT:
any
Zieladresse:
133.134.10.10
PORT:
any
Transportschicht:
tcp
udp
any
Richtung:
in
out
Aktion:
discard
850
none
ipsec
Protokoll:
ah
esp
ipcomp
Modus:
transport
tunnel
Endpunkt:
Stufe:
default
use
require
SPEICHERN
ABBRUCH

FIG. 13


1300
Sicherheitsrichtlinieninformation
Sicherheitsrichtlinie
Quelladresse:
192.168.1.1
PORT:
any
Zieladresse:
133.134.10.10
PORT:
any
Transportschicht:
tcp
udp
any
Richtung:
in
out
Aktion:
discard
none
860
ipsec
861
862
863
Protokoll:
ah
esp
ipcomp
864
Modus:
transport
tunnel
Endpunkt:
Stufe:
default
use
require
865
SPEICHERN
ABBRUCH
866