



(10) **DE 10 2013 110 613 B4** 2017.05.24

(12) **Patentschrift**

(21) Aktenzeichen: **10 2013 110 613.7**  
 (22) Anmeldetag: **26.09.2013**  
 (43) Offenlegungstag: **03.04.2014**  
 (45) Veröffentlichungstag  
 der Patenterteilung: **24.05.2017**

(51) Int Cl.: **H04N 21/63 (2011.01)**  
**H04N 21/435 (2011.01)**  
**H04N 21/462 (2011.01)**

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:  
**61/706,951**                      **28.09.2012**    **US**  
**61/781,122**                      **14.03.2013**    **US**  
**13/863,662**                      **16.04.2013**    **US**

(72) Erfinder:  
**Yoakum, John H., Cary, N.C., US; Johnston, Alan B., St. Louis, Mo., US**

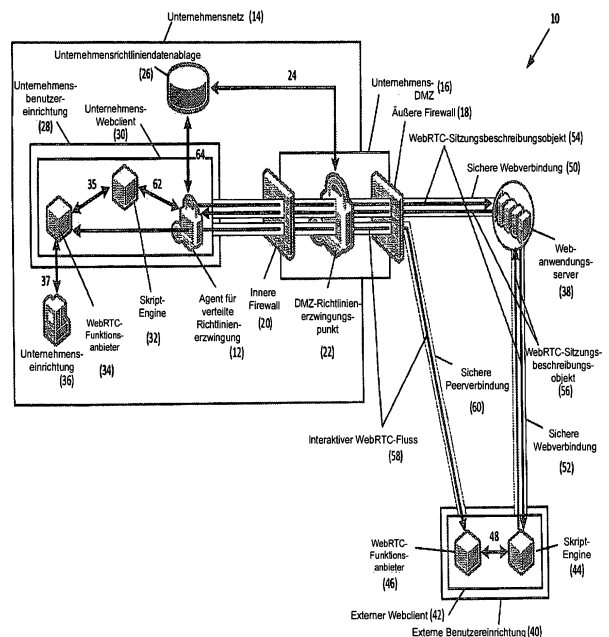
(73) Patentinhaber:  
**Avaya Inc., Basking Ridge, N.J., US**

(56) Ermittelter Stand der Technik:  
**US 2003 / 0 021 283 A1**  
**US 2004 / 0 039 803 A1**  
**US 2009 / 0 254 970 A1**  
**US 2011 / 0 209 196 A1**

(74) Vertreter:  
**Tergau & Walkenhorst Patentanwälte PartGmbH,**  
**60322 Frankfurt, DE**

(54) Bezeichnung: **Verteilte Anwendung von Unternehmensrichtlinien auf interaktive Web-Real-Time-Communications(WebRTC)-Sitzungen und verwandte Verfahren, Systeme und computerlesbare Medien**

(57) Hauptanspruch: Verfahren zum Anwenden einer Unternehmensrichtlinie auf eine interaktive Web-Real-Time-Communications(WebRTC)-Sitzung, das Folgendes umfasst: Empfangen eines von einer Sendereinrichtung ausgehenden und an eine Empfängereinrichtung gerichteten WebRTC-Sitzungsbeschreibungsobjekts durch einen Agenten für verteilte Richtlinienenerzwingung der Empfängereinrichtung;  
 Bestimmen einer oder mehrerer Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt durch den Agenten für verteilte Richtlinienenerzwingung;  
 Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt;  
 Feststellen, ob das WebRTC-Sitzungsbeschreibungsobjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat übereinstimmt; und  
 reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat nicht übereinstimmt, Verwerfen des WebRTC-Sitzungsbeschreibungsobjekts.



**Beschreibung**

## PRIORITÄTSANMELDUNGEN

**[0001]** Die vorliegende Anmeldung beansprucht die Priorität der vorläufigen US-Patentanmeldung mit dem Aktenzeichen 61/706,951, eingereicht am 28. September 2012, mit dem Titel „ENTERPRISE COMMUNICATIONS AND COLLABORATION SYSTEMS BASED ON REAL-TIME COMMUNICATIONS AND/OR MARKUP PROTOCOLS, AND RELATED METHODS, APPARATUSES, AND COMPUTER-READABLE MEDIA“, und der vorläufigen US-Patentanmeldung mit dem Aktenzeichen 61/781,122, eingereicht am 14. März 2013, mit dem Titel „DISTRIBUTED APPLICATION OF ENTERPRISE POLICIES TO WEB REAL-TIME COMMUNICATIONS (WEBRTC) INTERACTIVE SESSIONS, AND RELATED METHODS, SYSTEMS, AND COMPUTER-READABLE MEDIA“, die hiermit durch Bezugnahme in ihrem vollen Umfang hierin aufgenommen werden.

## ALLGEMEINER STAND DER TECHNIK

## Gebiet der Offenbarung

**[0002]** Die Technologie der Offenbarung betrifft allgemein interaktive Web-Real-Time-Communications(WebRTC)-Sitzungen. Derartige WebRTC-Sitzungen sowie entsprechende hierfür geeignete Verfahren und Systeme sind dem Fachmann aus der US 2004/0039803 A1, der US 2011/0209196 A1, der US 2009/0254970 A1 und der US 2003/0021283 A1 bekannt.

## Technischer Hintergrund

**[0003]** Web Real-Time Communications (WebRTC) ist eine laufende Bemühung um die Entwicklung von Industriestandards zum Integrieren von Echtzeitkommunikationsfunktionen in Webclients, etwa Webbrowsern, um direkte Interaktion mit anderen Webclients zu ermöglichen. Diese Echtzeitkommunikationsfunktionen sind für Webentwickler über Standardauszeichnungstags zugänglich, etwa diejenigen, die durch Version 5 der Hypertext Markup Language (HTML5) bereitgestellt werden, und clientseitige Skript-Anwendungsprogrammierschnittstellen (APIs) wie JavaScript-APIs. Weitere Informationen zu WebRTC finden sich in „WebRTC: APIs and RT-CWEB Protocols of the HTML5 Real-Time Web“ von Alan B. Johnston und Daniel C. Burnett (2012 Digital Codex LLC).

**[0004]** WebRTC stellt integrierte Fähigkeiten zum Herstellen von Echtzeit-Video-, -Audio- und/oder -Datenströmen sowohl bei interaktiven Punkt-zu-Punkt-Sitzungen als auch bei interaktiven Mehr-Teilnehmer-Sitzungen bereit. Die WebRTC-Standards werden derzeit vom World Wide Web Consorti-

um (W3C) und von der Internet Engineering Task Force (IETF) gemeinsam entwickelt. Informationen zum derzeitigen Stand der WebRTC-Standards finden sich z. B. unter <http://www.w3c.org> und <http://www.ietf.org>.

**[0005]** Um eine interaktive WebRTC-Sitzung (z. B. einen Echtzeit-Video-, -Audio- und/oder -Datenaustausch) herzustellen, können zwei Webclients von einem Webanwendungsserver WebRTC-fähige Webanwendungen, etwa HTML5/JavaScript-Webanwendungen, abrufen. Durch die Webanwendungen nehmen die zwei Webclients dann eine Medienaushandlung in Angriff, um zu kommunizieren und eine Vereinbarung über Parameter, die Eigenschaften der interaktiven Sitzung definieren, zu erzielen. Diese Medienaushandlung ist bekannt als WebRTC-„Angebot-Antwort“-Austausch. Ein WebRTC-„Angebot-Antwort“-Austausch erfolgt in der Regel über eine sichere Netzverbindung wie eine Hypertext-Transfer-Protocol-Secure(HTTPS)-Verbindung oder eine Secure-WebSockets-Verbindung. Bei einem Angebot-Antwort-Austausch sendet ein erster Webclient auf einer Sendereinrichtung ein „Angebot“ an einen zweiten Webclient auf einer Empfängereinrichtung. Das Angebot beinhaltet ein WebRTC-Sitzungsbeschreibungsjekt, das Medientypen und -fähigkeiten spezifiziert, welche der erste Webclient unterstützt und zur Nutzung bei der interaktiven WebRTC-Sitzung vorzieht. Der zweite Webclient reagiert dann mit einer WebRTC-Sitzungsbeschreibungsjekt-„Antwort“, die angibt, welche der angebotenen Medientypen und -fähigkeiten unterstützt werden und für die interaktive WebRTC-Sitzung akzeptabel sind. Sobald der WebRTC-Angebot-Antwort-Austausch abgeschlossen ist, können die Webclients dann eine direkte „Peerverbindung“ zueinander herstellen und können mit einem Austausch von Medien- oder Datenpaketen, welche die Echtzeitkommunikationen transportieren, anfangen. Die Peerverbindung zwischen den Webclients verwendet in der Regel das Secure Real-time Transport Protocol (SRTP), um Echtzeitmedienflüsse zu transportieren, und macht eventuell von verschiedenen anderen Protokollen für Echtzeitdatenaustausch Gebrauch.

**[0006]** Die sichere Art eines WebRTC-Angebot-Antwort-Austausches und einer Peerverbindung führt zu Schwierigkeiten bei Echtzeitkommunikationen über Unternehmensnetzgrenzen hinweg. Um zu bestimmen, ob zugelassen werden soll, dass Verkehr Netzränder überquert, verlassen sich Unternehmen oft auf Netzsicherheitselemente (z. B. Firewalls und Session Border Controller (SBCs)). Diese Netzsicherheitselemente können Protokolle auf verschiedenen Ebenen in einem Netzstapel untersuchen, einschließlich des tatsächlichen Inhalts des Netzverkehrs. Eine solche eingehende Analyse von Netzverkehr kann ermöglichen, dass ein Unternehmen Unternehmensrichtlinien anwendet, um eine differenzierte Steue-

nung des Netzverkehrs zu bewerkstelligen. Weil jedoch der WebRTC-Angebot-Antwort-Austausch und die Peerverbindung über sichere Netzverbindungen erfolgen oder anders verschlüsselt sein können, sind die zwischen den Webclients ausgetauschten WebRTC-Sitzungsbeschreibungsobjekte und interaktiven WebRTC-Flüsse für das Unternehmen eventuell undurchsichtig. Daher kann das Unternehmen gegebenenfalls keine Unternehmensrichtlinien unter Nutzung herkömmlicher Netzsicherheitselemente auf eine interaktive WebRTC-Sitzung anwenden. Die sichere Art von WebRTC birgt eventuell auch Risiken für das Unternehmen in Form eines neuen Angriffswegs für Virenträger und/oder Malware. Es ist Aufgabe der Erfindung, ein Verfahren und ein System zum Anwenden einer Unternehmensrichtlinie auf eine interaktive Web-Real-Time-Communications (WebRTC)-Sitzung anzugeben, die diese genannten Nachteile vermeiden.

#### KURZE DARSTELLUNG DER DETAILLIERTEN BESCHREIBUNG

**[0007]** Diese Aufgabe wird erfindungsgemäß durch ein Verfahren gemäß Anspruch 1 und ein System gemäß Anspruch 9 gelöst. In der detaillierten Beschreibung offenbarte Ausführungsformen sehen eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive Web-Real-Time-Communications(WebRTC)-Sitzungen vor. Verwandte Verfahren, Systeme und computerlesbare Medien werden ebenfalls offenbart. In diesem Zusammenhang wird in einer Ausführungsform ein Verfahren zum Anwenden einer Unternehmensrichtlinie auf eine interaktive WebRTC-Sitzung bereitgestellt. Das Verfahren umfasst Empfangen eines WebRTC-Sitzungsbeschreibungsobjekts, das von einer Sendereinrichtung an die Empfängereinrichtung gerichtet ist, durch einen Agenten für verteilte Richtlinienenerzwingung der Empfängereinrichtung. Das Verfahren umfasst ferner Bestimmen einer oder mehrerer Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt durch den Agenten für verteilte Richtlinienenerzwingung. Das Verfahren umfasst auch Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt, das Feststellen, ob das WebRTC-Sitzungsbeschreibungsobjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat übereinstimmt, und reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat nicht übereinstimmt, Verwerfen des WebRTC-Sitzungsbeschreibungsobjekts. Die Nutzung des Agenten für verteilte Richtlinienenerzwingung der Empfängereinrichtung lässt eine eingehende Analyse der Inhalte des WebRTC-Sitzungsbeschreibungsobjekts zu, einschließlich der Pakete, die das WebRTC-Sitzungsbeschreibungsobjekt transportieren, nachdem es an der Empfängereinrichtung empfangen worden

ist und bevor eine interaktive WebRTC-Sitzung hergestellt wird. Auf diese Weise kann ein Unternehmen die Herstellung einer interaktiven WebRTC-Sitzung gestatten, die über eine Unternehmensnetzgrenze hinausgeht, während es gleichzeitig sicherstellt, dass die interaktive WebRTC-Sitzung mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt.

**[0008]** In einer anderen Ausführungsform wird ein System zum Anwenden einer Unternehmensrichtlinie auf eine interaktive WebRTC-Sitzung bereitgestellt. Das System umfasst mindestens eine Kommunikationsschnittstelle und eine Empfängereinrichtung, die mit der mindestens einen Kommunikationsschnittstelle assoziiert ist und einen Agenten für verteilte Richtlinienenerzwingung umfasst. Der Agent für verteilte Richtlinienenerzwingung ist konfiguriert, um ein WebRTC-Sitzungsbeschreibungsobjekt, das von einer Sendereinrichtung an die Empfängereinrichtung gerichtet ist, über eine sichere Netzverbindung zu empfangen. Der Agent für verteilte Richtlinienenerzwingung ist ferner konfiguriert, um eine oder mehrere Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt zu bestimmen. Der Agent für verteilte Richtlinienenerzwingung ist auch konfiguriert, um die eine oder die mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt anzuwenden, festzustellen, ob das WebRTC-Sitzungsbeschreibungsobjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat übereinstimmt, und reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat nicht übereinstimmt, das WebRTC-Sitzungsbeschreibungsobjekt zu verwerfen.

**[0009]** In einer anderen Ausführungsform ist ein nicht transientes computerlesbares Medium bereitgestellt. Auf dem nicht transienten computerlesbaren Medium sind computerausführbare Befehle abgelegt, die einen Prozessor zwingen, ein Verfahren zu implementieren, das Empfangen eines WebRTC-Sitzungsbeschreibungsobjekts, das von einer Sendereinrichtung an die Empfängereinrichtung gerichtet ist, durch einen Agenten für verteilte Richtlinienenerzwingung einer Empfängereinrichtung umfasst. Das durch die computerausführbaren Befehle implementierte Verfahren umfasst ferner Bestimmen einer oder mehrerer Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt durch den Agenten für verteilte Richtlinienenerzwingung. Das durch die computerausführbaren Befehle implementierte Verfahren umfasst auch Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt, das Feststellen, ob das WebRTC-Sitzungsbeschreibungsobjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat übereinstimmt, und reagierend auf das Feststellen, dass das

WebRTC-Sitzungsbeschreibungsobjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat nicht übereinstimmt, Verwerfen des WebRTC-Sitzungsbeschreibungsobjekts.

#### KURZE BESCHREIBUNG DER FIGUR

**[0010]** Die beiliegenden Zeichnungsfiguren, die in diese Patentschrift aufgenommen sind und einen Bestandteil von ihr bilden, veranschaulichen diverse Ausgestaltungen der Offenbarung und dienen zusammen mit der Beschreibung dazu, die Prinzipien der Offenbarung zu erläutern.

**[0011]** Fig. 1 ist ein Begriffsschema, das eine beispielhafte „Dreieck“-Topologie einer interaktiven Web-Real-Time-Communications(WebRTC)-Sitzung zwischen einem Unternehmens-Webclient auf einer Empfängereinrichtung, die einen Agenten für verteilte Richtlinienerzwingung beinhaltet, und einem externen Webclient auf einer Sendereinrichtung zeigt;

**[0012]** Fig. 2 ist ein Schema, das beispielhafte Kommunikationsflüsse innerhalb eines beispielhaften Systems zeigt, das einen Agenten für verteilte Richtlinienerzwingung einer Empfängereinrichtung beinhaltet;

**[0013]** Fig. 3 ist ein Ablaufschema, das beispielhafte Betriebsvorgänge für eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive WebRTC-Sitzungen veranschaulicht;

**[0014]** die Fig. 4A und Fig. 4B sind Ablaufschemata, die detailliertere beispielhafte Betriebsvorgänge für eine verteilte Anwendung von Unternehmensrichtlinien auf WebRTC-Sitzungsbeschreibungsobjekte und interaktive Flüsse veranschaulichen;

**[0015]** Fig. 5 ist ein Ablaufschema, das beispielhafte Betriebsvorgänge für eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive WebRTC-Flüsse veranschaulicht; und

**[0016]** Fig. 6 ist ein Blockschema eines beispielhaften prozessorbasierten Systems, das den Agenten für verteilte Richtlinienerzwingung von Fig. 2 beinhalten kann.

#### DETAILLIERTE BESCHREIBUNG

**[0017]** Nunmehr werden mit Bezug auf die Zeichnungsfiguren diverse beispielhafte Ausführungsformen der vorliegenden Offenbarung beschrieben. Das Wort „beispielhaft“ wird hierin in der Bedeutung „als ein Beispiel, ein Beispielfall oder zur Veranschaulichung dienend“ genutzt. Jede hierin als „beispielhaft“ beschriebene Ausführungsform ist nicht zwangsläufig als gegenüber anderen Ausführungsformen be-

vorzugte oder vorteilhafte Ausführungsform auszulegen.

**[0018]** In der detaillierten Beschreibung offenbarte Ausführungsformen stellen eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive Web-Real-Time-Communications(WebRTC)-Sitzungen bereit. Verwandte Verfahren, Systeme und computerlesbare Medien werden ebenfalls offenbart. In diesem Zusammenhang wird in einer Ausführungsform ein Verfahren zum Anwenden einer Unternehmensrichtlinie auf eine interaktive WebRTC-Sitzung bereitgestellt. Das Verfahren umfasst Empfangen eines WebRTC-Sitzungsbeschreibungsobjekts, das von einer Sendereinrichtung an eine Empfängereinrichtung gerichtet ist, durch einen Agenten für verteilte Richtlinienerzwingung der Empfängereinrichtung. Das Verfahren umfasst ferner Bestimmen einer oder mehrerer Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt durch den Agenten für verteilte Richtlinienerzwingung. Das Verfahren umfasst auch Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt. Die Nutzung des Agenten für verteilte Richtlinienerzwingung der Empfängereinrichtung lässt eine eingehende Analyse der Inhalte des WebRTC-Sitzungsbeschreibungsobjekts zu, einschließlich der Pakete, die das WebRTC-Sitzungsbeschreibungsobjekt transportieren, nachdem es an der Empfängereinrichtung empfangen worden ist und bevor eine interaktive WebRTC-Sitzung hergestellt wird. Auf diese Weise kann ein Unternehmen die Herstellung einer interaktiven WebRTC-Sitzung gestatten, die über eine Unternehmensnetzgrenze hinausgeht, während es gleichzeitig sicherstellt, dass die interaktive WebRTC-Sitzung mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt.

**[0019]** In diesem Zusammenhang zeigt Fig. 1 ein beispielhaftes interaktives Kommunikationssystem 10, das eine verteilte Anwendung von Unternehmensrichtlinien bereitstellt, wie hierin offenbart. Vor allem beinhaltet das beispielhafte System 10 einen Agenten für verteilte Richtlinienerzwingung 12, der einen Punkt bereitstellt, an dem Unternehmensrichtlinien auf interaktive WebRTC-Sitzungen angewendet werden können, die ansonsten für Unternehmensnetzwerkselemente eventuell unzugänglich sind. Wie hierin benutzt, bezieht sich der Begriff „verteilt“ hinsichtlich des Agenten für verteilte Richtlinienerzwingung 12 darauf, dass die Anwendung von Unternehmensrichtlinien statt an einem zentralen Netzwerkelement an einem oder mehreren Endpunkten von interaktiven WebRTC-Sitzungen erfolgt.

**[0020]** Wie in Fig. 1 ersichtlich, beinhaltet das beispielhafte System 10 ein Unternehmensnetz 14, das für Benutzer innerhalb eines Unternehmens vernetzt-

te Computer- und Kommunikationsressourcen bereitstellt. Wie hierin benutzt, bezieht sich „Unternehmen“ auf einen beliebigen organisierten Zusammenschluss zum Zweck eines geschäftlichen Unterfangens oder einer anderen organisierten privaten oder öffentlichen Aktivität. Das Unternehmensnetz **14** beinhaltet eine „entmilitarisierte Zone“ (DMZ) **16** eines Unternehmens, um das Unternehmensnetz **14** zu schützen, während der Zugriff sowohl durch Unternehmensbenutzer als auch durch externe Benutzer auf Unternehmensressourcen (nicht gezeigt) innerhalb der Unternehmens-DMZ **16** gestattet wird. Die Unternehmens-DMZ **16** kann eine äußere Firewall **18** bereitstellen, die unberechtigten Zugriff auf das Unternehmensnetz **14** durch Benutzer außerhalb des Unternehmensnetzes **14** verhindert. Die Unternehmens-DMZ **16** kann auch eine innere Firewall **20** bereitstellen, die gestattet, dass nur externer Verkehr, der die Unternehmens-DMZ **16** durchquert, Benutzer innerhalb des Unternehmensnetzes **14** erreicht.

**[0021]** Die Unternehmens-DMZ **16** von **Fig. 1** kann ferner einen DMZ-Richtlinienerzwungungspunkt **22** beinhalten. Der DMZ-Richtlinienerzwungungspunkt **22** filtert oder verändert Netzwerkverkehr, der die Unternehmens-DMZ **16** durchquert, gemäß Unternehmensrichtlinien. Wie durch den in zwei Richtungen weisenden Pfeil **24** gekennzeichnet, kann der DMZ-Richtlinienerzwungungspunkt **22** kommunikativ an eine Unternehmensrichtliniendatenablage **26** gekoppelt sein, die einen zentralen Punkt zur Ablage, Wartung und Verbreitung von Unternehmensrichtlinien bereitstellt. Wie gemeinhin verständlich, ist eine Unternehmensrichtlinie eine Formulierung von Regeln, die Berechtigungsebenen und Zugriffsrechte definiert, um Daten zu schützen, Benutzerzugriffe zu steuern und den Verkehr innerhalb des Unternehmensnetzes **14** zu regeln. Praktisch alle Aspekte von Aktivität innerhalb des Unternehmensnetzes **14** können Unternehmensrichtlinien unterliegen. Unternehmensrichtlinien können spezifizieren, wobei es sich um nicht einschränkende Beispiele handelt, Benutzer, denen der Zugriff auf das Unternehmensnetz **14** gewährt wurde, externe Websites, auf die Unternehmensbenutzer zugreifen können oder Typen von zugelassenem oder nicht zugelassenem Netzwerkverkehr. Es sollte sich verstehen, dass die Unternehmens-DMZ **16** zusätzliche Elemente beinhalten kann, die in **Fig. 1** nicht veranschaulicht werden, oder mehrere in **Fig. 1** veranschaulichte Elemente in einem einzigen Element integrieren kann.

**[0022]** Die Fähigkeit des DMZ-Richtlinienerzwungungspunkts **22** zum Anwenden von Unternehmensrichtlinien auf Netzwerkverkehr, der die Unternehmens-DMZ **16** durchquert, ist gegebenenfalls davon abhängig, ob der Netzwerkverkehr unverschlüsselt ist oder in einem verschlüsselten Format transportiert wird. Im ersteren Szenario kann der DMZ-Richtlinienerzwungungspunkt **22** verschiedene Protokolle inner-

halb des Netzstapels und/oder den tatsächlichen Inhalt des Netzwerkverkehrs analysieren und Unternehmensrichtlinien basierend auf seiner Analyse auf den Netzwerkverkehr anwenden. Jedoch hat der DMZ-Richtlinienerzwungungspunkt **22** im letzteren Szenario möglicherweise nur Zugriff auf eingeschränkte Informationen zum Netzwerkverkehr, etwa eine Internetprotokoll(IP)-Quelladresse, eine IP-Zieladresse, eine Quellportnummer, eine Zielportnummer und/oder ein Netzwerkprotokoll, das genutzt wird. In diesem Fall kann der DMZ-Richtlinienerzwungungspunkt **22** gezwungen sein, Unternehmensrichtlinien nur basierend auf diesen eingeschränkten Informationen anzuwenden. Zudem ist der DMZ-Richtlinienerzwungungspunkt **22**, selbst wenn der Netzwerkverkehr unverschlüsselt ist, möglicherweise nicht fähig, Unternehmensrichtlinien an einem Endpunkt innerhalb des Unternehmensnetzes **14** basierend auf Daten, die am Endpunkt empfangen werden, anzuwenden. Folglich, wie unten noch detaillierter erörtert wird, wird der Agent für verteilte Richtlinienerzwungung **12** bereitgestellt, damit das Unternehmen Unternehmensrichtlinien an einem Endpunkt innerhalb des Unternehmensnetzes **14** basierend auf einer eingehenden Analyse von Paketen und ihren Inhalten, die am Endpunkt empfangen werden, erzwingen kann.

**[0023]** Bevor Details des Agenten für verteilte Richtlinienerzwungung **12** erörtert werden, wird zunächst die Herstellung einer interaktiven WebRTC-Sitzung im System **10** von **Fig. 1** beschrieben. Wie hierin benutzt, bezieht sich eine interaktive WebRTC-Sitzung auf Betriebsvorgänge zum Ausführen eines WebRTC-Angebot-Antwort-Austausches, zum Herstellen einer Peerverbindung und zum Beginnen eines interaktiven WebRTC-Flusses zwischen zwei oder mehr Endpunkten. Ein interaktiver WebRTC-Fluss kann einen interaktiven Medienfluss und/oder einen interaktiven Datenfluss zwischen den zwei oder mehr Endpunkten umfassen. Innerhalb des Unternehmensnetzes **14** von **Fig. 1** befindet sich eine Unternehmensbenutzereinrichtung **28**, die einen Unternehmens-Webclient **30** ausführt. In einigen Ausführungsformen kann die Unternehmensbenutzereinrichtung **28** eine beliebige Computer- oder Kommunikationseinrichtung mit Netzkommunikationsfähigkeiten sein, etwa ein Smartphone, ein Tabletcomputer, eine dedizierte Web-Appliance oder ein Desktopcomputer, wobei es sich um nicht einschränkende Beispiele handelt. Der Unternehmens-Webclient **30** in diesem Beispiel kann eine Webbrowseranwendung, eine dedizierte Kommunikationsanwendung oder eine schnittstellenlose Anwendung wie eine Daemon- oder Dienstanwendung sein, wobei es sich um nicht einschränkende Beispiele handelt.

**[0024]** In dieser Ausführungsform umfasst der Unternehmens-Webclient **30** eine Skript-Engine **32** und einen WebRTC-Funktionsanbieter **34**. Die Skript-Engine **32** ermöglicht, dass clientseitige Anwendungen,

die in einer Skriptsprache wie JavaScript geschrieben sind, innerhalb des Unternehmens-Webclients **30** ausgeführt werden. Die Skript-Engine **32** stellt auch eine Anwendungsprogrammierschnittstelle (API) bereit, um Kommunikationen mit anderen Funktionsanbietern innerhalb des Unternehmens-Webclients **30** und/oder der Unternehmensbenutzereinrichtung **28** und/oder mit anderen Webclients, Benutzereinrichtungen oder Webservern zu erleichtern. Der WebRTC-Funktionsanbieter **34** implementiert die Protokolle, die Codecs und die APIs, die zum Ermöglichen interaktiver Echtzeitsitzungen über WebRTC nötig sind. Die Skript-Engine **32** und der WebRTC-Funktionsanbieter **34** sind über eine Menge definierter APIs kommunikativ gekoppelt, wie durch den in zwei Richtungen weisenden Pfeil **35** gekennzeichnet.

**[0025]** Das Unternehmensnetz **14** kann auch eine Unternehmenseinrichtung **36** beinhalten, die kommunikativ an den WebRTC-Funktionsanbieter **34** gekoppelt ist, wie durch den in zwei Richtungen weisenden Pfeil **37** gekennzeichnet. Wie unten noch detaillierter erörtert wird, kann die Unternehmenseinrichtung **36** in der Lage sein, einen interaktiven WebRTC-Fluss, der vom WebRTC-Funktionsanbieter **34** empfangen wird, gemäß Unternehmensrichtlinien aufzuzeichnen, zu protokollieren oder umzuleiten.

**[0026]** Außerhalb des Unternehmensnetzes **14** befindet sich ein Webanwendungsserver **38**, der anfordernde Webclients mit einer WebRTC-fähigen Webanwendung (nicht gezeigt) bedient. In einigen Ausführungsformen kann der Webanwendungsserver **38** ein einzelner Server sein, während der Webanwendungsserver **38** in einigen Ausführungsformen mehrere Server umfassen kann, die kommunikativ aneinander gekoppelt sind. Es sollte sich verstehen, dass sich der Webanwendungsserver **38** in der Unternehmens-DMZ **16** des Unternehmensnetzes **14** oder innerhalb einer Unternehmens-DMZ eines Unternehmensnetzes außerhalb des Unternehmensnetzes **14** befinden kann.

**[0027]** Ebenfalls außerhalb des Unternehmensnetzes **14** befindet sich eine externe Benutzereinrichtung **40**, die einen externen Webclient **42** ausführt. Die externe Benutzereinrichtung **40** kann eine beliebige Computer- oder Kommunikationseinrichtung mit Netzkommunikationsfähigkeiten sein, etwa ein Smartphone, ein Tabletcomputer, eine dedizierte Web-Appliance oder ein Desktopcomputer, wobei es sich um nicht einschränkende Beispiele handelt. Der externe Webclient **42** kann eine Webbrowseranwendung, eine dedizierte Kommunikationsanwendung oder eine schnittstellenlose Anwendung wie eine Daemon- oder Dienstanwendung sein, wobei es sich um nicht einschränkende Beispiele handelt. In dieser Ausführungsform umfasst der externe Webclient **42** eine Skript-Engine **44** und einen WebRTC-Funktionsanbieter **46**, dessen Funktionen der Funktionalität der Skript-Engine **32** bzw. des WebRTC-Funktionsanbieters **34** des Unternehmens-Webclients **30** entspricht. Die Skript-Engine **44** und der WebRTC-Funktionsanbieter **46** sind über eine Menge definierter APIs kommunikativ gekoppelt, wie durch den in zwei Richtungen weisenden Pfeil **48** gekennzeichnet. Es sollte sich ferner verstehen, dass sich der externe Webclient **42** innerhalb eines Unternehmensnetzes außerhalb des Unternehmensnetzes **14** befinden kann.

lität der Skript-Engine **32** bzw. des WebRTC-Funktionsanbieters **34** des Unternehmens-Webclients **30** entspricht. Die Skript-Engine **44** und der WebRTC-Funktionsanbieter **46** sind über eine Menge definierter APIs kommunikativ gekoppelt, wie durch den in zwei Richtungen weisenden Pfeil **48** gekennzeichnet. Es sollte sich ferner verstehen, dass sich der externe Webclient **42** innerhalb eines Unternehmensnetzes außerhalb des Unternehmensnetzes **14** befinden kann.

**[0028]** Fig. 1 veranschaulicht ferner die charakteristische WebRTC-„Dreieck“-Topologie, die aus dem Herstellen einer interaktiven WebRTC-Sitzung zwischen dem Unternehmens-Webclient **30** und dem externen Webclient **42** resultiert. Um eine interaktive WebRTC-Sitzung herzustellen, laden sowohl der Unternehmens-Webclient **30** als auch der externe Webclient **42** dieselbe WebRTC-Webanwendung (nicht gezeigt) vom Webanwendungsserver **38** herunter. In einigen Ausführungsformen umfasst die WebRTC-Webanwendung eine HTML5/JavaScript-Webanwendung, die unter Nutzung von HTML5 ein Rich User Interface bereitstellt, und nutzt JavaScript zum Bearbeiten von Benutzereingaben und zum Kommunizieren mit dem Webanwendungsserver **38**.

**[0029]** Der Unternehmens-Webclient **30** und der externe Webclient **42** stellen dann sichere Webverbindungen **50** bzw. **52** zum Webanwendungsserver **38** her und nehmen einen WebRTC-Angebot-Austausch in Angriff. Dies wird durch einen Austausch von WebRTC-Sitzungsbeschreibungsobjekten bewerkstelligt, die durch die Pfeile **54** und **56** gekennzeichnet sind. Die ausgetauschten WebRTC-Sitzungsbeschreibungsobjekte **54** und **56** werden genutzt, um die Medientypen und -fähigkeiten für die gewünschte interaktive WebRTC-Sitzung zu bestimmen. Sobald der WebRTC-Angebot-Austausch abgeschlossen ist, kann über eine sichere Peerverbindung **60** zwischen dem Unternehmens-Webclient **30** und dem externen Webclient **42** ein interaktiver WebRTC-Fluss **58** hergestellt werden. Folglich bilden in Fig. 1 der Webanwendungsserver **38**, die äußere Firewall **18** (die als äußerer Rand des Unternehmensnetzes **14** dient, durch welches der Unternehmens-Webclient **30** kommuniziert) und der externe Webclient **42** die Spitzen des WebRTC-„Dreiecks“. Die Ränder des „Dreiecks“ werden durch die sicheren Webverbindungen **50** und **52** und die sichere Peerverbindung **60** dargestellt.

**[0030]** Es sollte sich verstehen, dass einige Ausführungsformen gegebenenfalls von anderen Topografien als der in Fig. 1 veranschaulichten WebRTC-„Dreieck“-Topografie Gebrauch machen. Zum Beispiel können einige Ausführungsformen eine „Trapez“-Topografie verwenden, in der zwei Webserver über Protokolle wie Session Initiation Protocol (SIP) oder Jingle, wobei es sich um nicht einschränken-

de Beispiele handelt, direkt miteinander kommunizieren. Es sollte sich ferner verstehen, dass die Unternehmensbenutzereinrichtung **28** und/oder die externe Benutzereinrichtung **40** anstelle des Unternehmens-Webclients **30** und/oder des externen Webclients **42** jeweils eine SIP-Clienteinrichtung, eine Jingle-Clienteinrichtung oder ein Gatewaygerät eines öffentlichen Fernsprechnetzes (PSTN), das kommunikativ an ein Telefon gekoppelt ist, umfassen können.

**[0031]** Wie in **Fig. 1** ersichtlich, muss das durch den Unternehmens-Webclient **30** vom externen Webclient **42** während des WebRTC-Angebot-Antwort-Austausches sowie des resultierenden interaktiven WebRTC-Flusses **58** empfangene WebRTC-Sitzungsbeschreibungsjekt **54** die Unternehmens-DMZ **16** über die sichere Webverbindung **50** bzw. die sichere Peerverbindung **60** durchqueren. Mithin kennt der DMZ-Richtlinienerzwingungspunkt **22** nicht die tatsächlichen Inhalte des WebRTC-Sitzungsbeschreibungsjekts **54** oder des interaktiven WebRTC-Flusses **58**, das oder der durch den Unternehmens-Webclient **30** empfangen wird. Daher kann der DMZ-Richtlinienerzwingungspunkt **22** auf die interaktive WebRTC-Sitzung basierend auf dem Inhalt des WebRTC-Sitzungsbeschreibungsjekts **54** oder des interaktiven WebRTC-Flusses **58** keine Unternehmensrichtlinien anwenden.

**[0032]** In diesem Zusammenhang wird der Agent für verteilte Richtlinienerzwingung **12** von **Fig. 1** bereitgestellt. In einigen Ausführungsformen ist der Agent für verteilte Richtlinienerzwingung **12** als Erweiterung oder Plug-In für den Unternehmens-Webclient **30** zum Empfangen und Verarbeiten von durch den Unternehmens-Webclient **30** empfangenen Paketen implementiert. Für den Fall, dass Netzverkehr verschlüsselt ist, kann der Agent für verteilte Richtlinienerzwingung **12** auf den Inhalt des verschlüsselten Netzverkehrs zugreifen, nachdem er innerhalb des Unternehmens-Webclients **30** entschlüsselt worden ist. Der Agent für verteilte Richtlinienerzwingung **12** kann auch auf Daten zugreifen, welche durch die Pakete, die den Netzverkehr transportieren, bereitgestellt werden, etwa eine Internetprotokoll(IP)-Quelladresse, eine IP-Zieladresse, eine Quellportnummer, eine Zielportnummer und/oder ein genutztes Netzprotokoll, wobei es sich um nicht einschränkende Beispiele handelt. Folglich empfängt der Agent für verteilte Richtlinienerzwingung **12** während der Herstellung einer interaktiven WebRTC-Sitzung ein WebRTC-Sitzungsbeschreibungsjekt **54**, das über die sichere Webverbindung **50** transportiert wird. Der Agent für verteilte Richtlinienerzwingung **12** bestimmt und wendet dann Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsjekt **54** an, einschließlich des Inhalts des WebRTC-Sitzungsbeschreibungsjekts **54** und/oder Daten, welche durch die Pakete, die das WebRTC-Sitzungsbeschreibungsjekt **54** transportieren, bereitgestellt

werden. Für den Fall, dass Netzverkehr ungeschützt ist, analysiert der Agent für verteilte Richtlinienerzwingung **12** möglicherweise ähnlich das WebRTC-Sitzungsbeschreibungsjekt **54** zum Zweck des Anwendens von Unternehmensrichtlinien am Unternehmens-Webclient **30**. Der Agent für verteilte Richtlinienerzwingung **12** kann Unternehmensrichtlinien über ein oder mehrere der folgenden Verfahren anwenden, wobei es sich um nicht einschränkende Beispiele handelt: Validieren des WebRTC-Sitzungsbeschreibungsjektformats; Herstellen oder Ablehnen einer interaktiven WebRTC-Sitzung; Bereitstellen von Optionen für eine alternative interaktive WebRTC-Sitzung für die externe Benutzereinrichtung **40**; Abwandeln der Inhalte eines WebRTC-Sitzungsbeschreibungsjekts; und/oder Verursachen, dass ein interaktiver WebRTC-Fluss umgeleitet, geklont, protokolliert oder aufgezeichnet wird.

**[0033]** In einigen Ausführungsformen ist der Agent für verteilte Richtlinienerzwingung **12** kommunikativ an die Skript-Engine **32** gekoppelt, wie durch den in zwei Richtungen weisenden Pfeil **62** in **Fig. 1** gekennzeichnet. Einige Ausführungsformen können vorsehen, dass der Agent für verteilte Richtlinienerzwingung **12** ferner über eine Kommunikationsstrecke **64** kommunikativ an die Unternehmensrichtliniendatenablage **26** gekoppelt ist. Auf diese Weise kann der Agent für verteilte Richtlinienerzwingung **12** die Unternehmensrichtliniendatenablage **26** nach Unternehmensrichtlinien abfragen, die auf die sichere Webverbindung **50** angewendet werden sollen. Einige Ausführungsformen können vorsehen, dass zwischen der externen Benutzereinrichtung **40** und der Unternehmensbenutzereinrichtung **28** ausgetauschte Daten im Rahmen der Herstellung der sicheren Peerverbindung **60** oder im Rahmen des interaktiven WebRTC-Flusses **58** durch den Agenten für verteilte Richtlinienerzwingung **12** empfangen und analysiert werden, bevor sie an den WebRTC-Funktionsanbieter **34** geleitet werden. Wie unten erörtert, kann dadurch gestattet werden, dass der Agent für verteilte Richtlinienerzwingung **12** während der Herstellung der sicheren Peerverbindung **60** und/oder während des Austausches des interaktiven WebRTC-Flusses **58** Unternehmensrichtlinien anwendet. In Ausführungsformen, in denen der interaktive WebRTC-Fluss **58** einen interaktiven Datenaustausch umfasst, kann der Agent für verteilte Richtlinienerzwingung **12** die Inhalte des interaktiven WebRTC-Flusses **58** untersuchen, um Malware, Viren oder geistiges Eigentum des Unternehmens, für das keine Berechtigung vorliegt, zu detektieren, wobei es sich um nicht einschränkende Beispiele handelt.

**[0034]** Um beispielhafte Kommunikationsflüsse während der Herstellung einer interaktiven WebRTC-Sitzung, einschließlich des Agenten für verteilte Richtlinienerzwingung **12** von **Fig. 1**, zu veranschaulichen, wird **Fig. 2** bereitgestellt. In **Fig. 2** werden

die Unternehmensrichtliniendatenablage **26**, der Unternehmens-Webclient **30** auf der Unternehmensbenutzereinrichtung **28**, der Webanwendungsserver **38** und der externe Webclient **42** auf der externen Benutzereinrichtung **40** von **Fig. 1** je durch vertikale gestrichelte Linien dargestellt. Der WebRTC-Funktionsanbieter **34**, die Skript-Engine **32** und der Agent für verteilte Richtlinienerzwingung **12** des Unternehmens-Webclients **30** werden als separate Elemente gezeigt, um Kommunikationsflüsse dazwischen besser zu veranschaulichen. Es sollte sich verstehen, dass der externe Webclient **42** eine Skript-Engine **44** und einen WebRTC-Funktionsanbieter **46** umfassen kann, die zur Förderung der Übersichtlichkeit in diesem Beispiel weggelassen wurden. Es sollte sich ferner verstehen, dass der Agent für verteilte Richtlinienerzwingung **12** auf der Unternehmensbenutzereinrichtung **28** in diesem Beispiel das von der externen Benutzereinrichtung **40** empfangene WebRTC-Sitzungsbeschreibungsojekt untersucht. Folglich wird die Unternehmensbenutzereinrichtung **28** als „Empfänger“-Einrichtung angesehen, während die externe Benutzereinrichtung **40** als „Sender“-Einrichtung angesehen wird. Schließlich wird für dieses Beispiel davon ausgegangen, dass der Unternehmens-Webclient **30** und der externe Webclient **42** je eine WebRTC-fähige Webanwendung, etwa eine HTML5/JavaScript-WebRTC-Anwendung, vom Webanwendungsserver **38** heruntergeladen haben.

**[0035]** Wie in **Fig. 2** ersichtlich, fängt die Herstellung einer interaktiven WebRTC-Sitzung damit an, dass der externe Webclient **42** ein Sitzungsbeschreibungsojekt (Session Description Object, SDP) in einem verschlüsselten Format (in diesem Beispiel über eine HTTPS-Verbindung) an den Webanwendungsserver **38** sendet. In diesem Beispiel wird das WebRTC-Sitzungsbeschreibungsojekt als SDP-Objekt A bezeichnet und durch den Pfeil **66** gekennzeichnet. Das SDP-Objekt A stellt bei einem WebRTC-Angebot-Antwort-Austausch das „Angebot“ dar. Das SDP-Objekt A spezifiziert die Medientypen und -fähigkeiten, welche der externe Webclient **42** unterstützt und für die Nutzung bei der interaktiven WebRTC-Sitzung vorzieht. Der Webanwendungsserver **38** leitet das SDP-Objekt A über eine sichere Webverbindung an den Agenten für verteilte Richtlinienerzwingung **12** des Unternehmens-Webclients **30** der Unternehmensbenutzereinrichtung **28** weiter, wie durch den Pfeil **68** gekennzeichnet.

**[0036]** Wie oben angemerkt, kann der Agent für verteilte Richtlinienerzwingung **12** auf die Inhalte von über eine sichere Webverbindung empfangenem Netzverkehr zugreifen, nachdem der Netzverkehr entschlüsselt worden ist, und zusätzlich Daten untersuchen, welche durch die Pakete, die den Netzverkehr transportieren, bereitgestellt werden. Daher kann der Agent für verteilte Richtlinienerzwingung **12** die Inhalte des SDP-Objekts A sowie Daten un-

tersuchen, welche durch Pakete, die das SDP-Objekt A transportieren, bereitgestellt werden. In einigen Ausführungsformen vergleicht der Agent für verteilte Richtlinienerzwingung **12** an dieser Stelle das Format des SDP-Objekts A mit einem erwarteten WebRTC-Sitzungsbeschreibungsojektformat. Falls das SDP-Objekt A mit dem erwarteten Format nicht übereinstimmt, kann der Agent für verteilte Richtlinienerzwingung **12** das SDP-Objekt A verwerfen und es wird keine interaktive WebRTC-Sitzung hergestellt. Falls das SDP-Objekt A gültig zu sein scheint, kann die Herstellung der interaktiven WebRTC-Sitzung fortgesetzt werden.

**[0037]** Basierend auf den Inhalten des SDP-Objekts A sendet der Agent für verteilte Richtlinienerzwingung **12** eine Abfrage von Unternehmensrichtlinien an die Unternehmensrichtliniendatenablage **26**, wie durch den Pfeil **70** gekennzeichnet. Die Abfrage kann auf Daten, die aus Inhalten des SDP-Objekts A extrahiert wurden, und/oder anderen verfügbaren Daten bezüglich des SDP-Objekts A, etwa Eigenschaften von oder Daten in den Paketen, die das SDP-Objekt A umfassen, basieren oder solche Daten beinhalten. Solche Daten können eine mit der externen Benutzereinrichtung **40** assoziierte Identität, eine Identität einer Zwischenvorrichtung, die das SDP-Objekt A an die Unternehmensbenutzereinrichtung **28** weitergeleitet hat, einen Austausch von Verschlüsselungsschlüsseln oder einen Typ eines interaktiven WebRTC-Flusses beinhalten, wobei es sich um nicht einschränkende Beispiele handelt. Die Unternehmensrichtliniendatenablage **26** sendet reagierend auf die Abfrage die angeforderten Unternehmensrichtlinien an den Agenten für verteilte Richtlinienerzwingung **12** zurück, wie durch den Pfeil **72** in **Fig. 2** gekennzeichnet. Der Agent für verteilte Richtlinienerzwingung **12** wendet dann die Unternehmensrichtlinien auf das SDP-Objekt A an. In einigen Ausführungsformen kann das Anwenden der Unternehmensrichtlinien auf das SDP-Objekt A Folgendes umfassen: weiteres Validieren des WebRTC-Sitzungsbeschreibungsojektformats; Herstellen oder Ablehnen des Herstellens einer interaktiven WebRTC-Sitzung; Bereitstellen von Optionen für eine alternative interaktive WebRTC-Sitzung für die externe Benutzereinrichtung **40**; und/oder Abwandeln der Inhalte eines WebRTC-Sitzungsbeschreibungsojekts, wobei es sich um nicht einschränkende Beispiele handelt.

**[0038]** Angenommen, die durch den Agenten für verteilte Richtlinienerzwingung **12** angewendeten Unternehmensrichtlinien gestatten das Fortsetzen der Herstellung der interaktiven WebRTC-Sitzung, so leitet der Agent für verteilte Richtlinienerzwingung **12** als Nächstes das WebRTC-Sitzungsbeschreibungsojekt zur herkömmlichen Verarbeitung an die Skript-Engine **32**, wie durch den Pfeil **74** gekennzeichnet. Wie oben angemerkt, hat der Agent für verteilte Richtlinienerzwingung **12** beim Anwenden der Un-



ternehmensrichtlinien gegebenenfalls die Inhalte des SDP-Objekts A abgewandelt. Daher wird das an die Skript-Engine **32** weitergeleitete WebRTC-Sitzungsbeschreibungsjekt SDP-Objekt A' genannt.

**[0039]** Nachdem die Skript-Engine **32** das SDP-Objekt A' vom Agenten für verteilte Richtlinienerzwingung **12** empfangen hat, sendet die Skript-Engine **32** reagierend darauf ein WebRTC-Sitzungsbeschreibungsjekt, das als SDP-Objekt B bezeichnet wird, an den Agenten für verteilte Richtlinienerzwingung **12**, wie durch den Pfeil **76** gekennzeichnet. Das SDP-Objekt B stellt in diesem Beispiel beim WebRTC-Angebot-Antwort-Austausch die „Antwort“ dar. In einigen Ausführungsformen kann der Agent für verteilte Richtlinienerzwingung **12** Unternehmensrichtlinien anwenden, indem er einen Inhalt des SDP-Objekts B abwandelt, bevor er es an den Webanwendungsserver **38** weiterleitet. Folglich wird das durch den Agenten für verteilte Richtlinienerzwingung **12** weitergeleitete WebRTC-Sitzungsbeschreibungsjekt als SDP-Objekt B' bezeichnet. Das SDP-Objekt B' wird über eine sichere Netzverbindung an den Webanwendungsserver **38** gesendet, wie durch den Pfeil **78** gekennzeichnet. Der Webanwendungsserver **38** leitet daraufhin das SDP-Objekt B' an die externe Benutzereinrichtung **40** weiter, wie durch den Pfeil **80** dargestellt.

**[0040]** In **Fig. 2**, auf die weiter Bezug genommen wird, starten der externe Webclient **42** auf der externen Benutzereinrichtung **40** und der Unternehmens-Webclient **30** (vor allem der WebRTC-Funktionsanbieter **34**) dann das Hole Punching, um den besten Weg zur Herstellung direkter Kommunikationen zu bestimmen. Dies wird durch die in zwei Richtungen weisenden Pfeile **82** und **83** in **Fig. 2** gekennzeichnet. Hole Punching ist eine Technik, die oft Protokolle wie Interactive Connectivity Establishment (ICE) nutzt, über die beide Webclients eine Verbindung zu einem keinen Einschränkungen unterliegenden Dritt-anbieterserver (nicht gezeigt) herstellen, der externe und interne Adressinformationen zur Nutzung bei direkten Kommunikationen erkennt. In diesem Beispiel kann der Agent für verteilte Richtlinienerzwingung **12** im Rahmen von Hole Punching ausgetauschte Daten empfangen, analysieren und abwandeln. Zum Beispiel kann der Agent für verteilte Richtlinienerzwingung **12** einen Session-Traversal-Utilities-for-NAT (STUN)-Server und/oder einen Traversal-Using-Relays-around-NAT(TURN)-Server, die von der Unternehmensbenutzereinrichtung **28** für Hole Punching genutzt werden, hinzufügen oder entfernen. Auf diese Weise kann der Agent für verteilte Richtlinienerzwingung **12** Unternehmensrichtlinien auf die interaktive WebRTC-Sitzung anwenden, selbst nachdem der WebRTC-Angebot-Antwort-Austausch beendet ist.

**[0041]** Sobald das durch die Pfeile **82** und **83** gekennzeichnete Hole Punching erfolgreich ist, fangen der externe Webclient **42** und der WebRTC-Funktionsanbieter **34** des Unternehmens-Webclients **30** mit den Schlüsselaushandlungen an, um eine sichere Peerverbindung herzustellen (in zwei Richtungen weisender Pfeil **84**). Nach dem Herstellen einer sicheren Peerverbindung fangen der externe Webclient **42** und der WebRTC-Funktionsanbieter **34** des Unternehmens-Webclients **30** damit an, sichere WebRTC-Medien- oder -Datenflüsse auszutauschen, wie durch den in zwei Richtungen weisenden Pfeil **86** gezeigt.

**[0042]** Um beispielhafte Betriebsvorgänge des Agenten für verteilte Richtlinienerzwingung **12** von **Fig. 1** für eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive WebRTC-Sitzungen allgemein zu beschreiben, wird **Fig. 3** bereitgestellt. **Fig. 3** ist ein Ablaufschema, das beispielhafte Betriebsvorgänge für eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive WebRTC-Sitzungen veranschaulicht. In diesem Beispiel von **Fig. 3** fangen die Betriebsvorgänge damit an, dass der Agent für verteilte Richtlinienerzwingung **12** ein von einer Sendereinrichtung (etwa der externen Benutzereinrichtung **40**) ausgehendes und an eine Empfängereinrichtung (etwa die Unternehmensbenutzereinrichtung **28**) gerichtetes WebRTC-Sitzungsbeschreibungsjekt über eine sichere Netzverbindung empfängt (Block **88**). In einigen Ausführungsformen kann das durch den Agenten für verteilte Richtlinienerzwingung **12** empfangene WebRTC-Sitzungsbeschreibungsjekt ein „Angebot“ von der Sendereinrichtung bei einem WebRTC-Angebot-Antwort-Austausch darstellen oder eine „Antwort“ darstellen, die reagierend auf ein zuvor gesendetes Angebot gesendet wird.

**[0043]** In **Fig. 3**, auf die weiter Bezug genommen wird, bestimmt der Agent für verteilte Richtlinienerzwingung **12** als Nächstes eine oder mehrere Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsjekt (Block **90**). In einigen Ausführungsformen können die Unternehmensrichtlinien basierend auf einem Inhalt des WebRTC-Sitzungsbeschreibungsjekts und/oder auf Daten bestimmt werden, welche durch Pakete, die das WebRTC-Sitzungsbeschreibungsjekt transportieren, bereitgestellt werden. Gemäß einigen Ausführungsformen können der Inhalt des WebRTC-Sitzungsbeschreibungsjekts und/oder Daten, welche durch Pakete, die das WebRTC-Sitzungsbeschreibungsjekt transportieren, bereitgestellt werden, eine mit der Sendereinrichtung assoziierte Identität, eine Identität einer Zwischenvorrichtung, die das WebRTC-Sitzungsbeschreibungsjekt an die Empfängereinrichtung weitergeleitet hat, einen Austausch von Verschlüsselungsschlüsseln oder einen Typ eines interaktiven WebRTC-Flusses beinhalten. Einige Ausführungsformen können vorsehen, dass der

Agent für verteilte Richtlinienerzwingung **12** die eine oder die mehreren Unternehmensrichtlinien bestimmt, indem er eine Abfrage von Unternehmensrichtlinien an eine Unternehmensrichtliniendatenablage (nicht gezeigt), etwa die Unternehmensrichtliniendatenablage **26** von **Fig. 1**, sendet.

**[0044]** In **Fig. 3**, auf die weiter Bezug genommen wird, wendet der Agent für verteilte Richtlinienerzwingung **12** die eine oder die mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsbjekt an (Block **92**). Der Agent für verteilte Richtlinienerzwingung **12** kann die Unternehmensrichtlinien durch Validieren des WebRTC-Sitzungsbeschreibungsbjektformats, durch Herstellen oder Ablehnen einer interaktiven WebRTC-Sitzung, durch Bereitstellen von Optionen für eine alternative interaktive WebRTC-Sitzung für die Sendereinrichtung, durch Abwandeln der Inhalte eines WebRTC-Sitzungsbeschreibungsbjekts und/oder durch Veranlassen, dass ein interaktiver WebRTC-Fluss umgeleitet, geklont, protokolliert oder aufgezeichnet wird, anwenden, wobei es sich um nicht einschränkende Beispiele handelt.

**[0045]** Die **Fig. 4A** und **Fig. 4B** werden bereitgestellt, um einen beispielhaften verallgemeinerten Prozess, bei dem der Agent für verteilte Richtlinienerzwingung **12** von **Fig. 1** eine verteilte Anwendung von Unternehmensrichtlinien auf interaktive WebRTC-Sitzungen bereitstellt, detaillierter zu veranschaulichen. **Fig. 4A** zeigt detailliert Betriebsvorgänge zum Empfangen und Validieren eines WebRTC-Angebot-Austausches und Bestimmen angemessener Unternehmensrichtlinien zur Anwendung auf eine interaktive WebRTC-Sitzung. **Fig. 4B** zeigt Betriebsvorgänge zum Anwenden der Unternehmensrichtlinien auf den WebRTC-Angebot-Austausch und einen resultierenden interaktiven WebRTC-Fluss. Zu Veranschaulichungszwecken beziehen sich die **Fig. 4A** und **Fig. 4B** auf Elemente des beispielhaften Systems **10** und des Agenten für verteilte Richtlinienerzwingung **12** von **Fig. 1**.

**[0046]** In **Fig. 4A**, auf die nunmehr Bezug genommen wird, empfängt der Agent für verteilte Richtlinienerzwingung **12** über eine sichere Netzverbindung (Block **94**) ein WebRTC-Sitzungsbeschreibungsbjekt, das von einer Sendereinrichtung (etwa einer externen Benutzereinrichtung **40**) ausgeht und an eine Empfängereinrichtung (etwa die Unternehmensbenutzereinrichtung **28**) gerichtet ist. Das durch den Agenten für verteilte Richtlinienerzwingung **12** empfangene WebRTC-Sitzungsbeschreibungsbjekt kann ein „Angebot“ von der Sendereinrichtung bei einem WebRTC-Angebot-Austausch darstellen oder eine „Antwort“ darstellen, die reagierend auf ein zuvor gesendetes Angebot gesendet wird. Der Agent für verteilte Richtlinienerzwingung **12** bestimmt als Nächstes, ob das We-

bRTC-Sitzungsbeschreibungsbjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsbjektformat übereinstimmt (Block **96**). Falls der Agent für verteilte Richtlinienerzwingung **12** bestimmt, dass das WebRTC-Sitzungsbeschreibungsbjekt mit einem erwarteten Format nicht übereinstimmt, kann der Agent für verteilte Richtlinienerzwingung **12** das WebRTC-Sitzungsbeschreibungsbjekt einfach verwerfen (Block **98**). Dadurch kann eine gesonderte Sicherheitsmaßnahme gegen Angriffe durch Malware und/oder Viren, die über eine interaktive WebRTC-Sitzung auf das Unternehmensnetz **14** zuzugreifen versuchen, bereitgestellt werden.

**[0047]** Falls der Agent für verteilte Richtlinienerzwingung **12** bei Block **96** von **Fig. 4A** bestimmt, dass das WebRTC-Sitzungsbeschreibungsbjekt ein angemessenes Format hat, bestimmt der Agent für verteilte Richtlinienerzwingung **12** als Nächstes eine oder mehrere zu erzwingende Unternehmensrichtlinien. In diesem Beispiel fragt der Agent für verteilte Richtlinienerzwingung **12** eine Unternehmensrichtliniendatenablage (etwa die Unternehmensrichtliniendatenablage **26** von **Fig. 1**) ab, um basierend auf dem WebRTC-Sitzungsbeschreibungsbjekt eine oder mehrere Unternehmensrichtlinien zu bestimmen (Block **100**). In einigen Ausführungsformen können die Unternehmensrichtlinien basierend auf einem Inhalt des WebRTC-Sitzungsbeschreibungsbjekts und/oder auf Daten bestimmt werden, welche durch Pakete, die das WebRTC-Sitzungsbeschreibungsbjekt transportieren, bereitgestellt werden. Der Inhalt des WebRTC-Sitzungsbeschreibungsbjekts und/oder die Daten, welche durch Pakete, die das WebRTC-Sitzungsbeschreibungsbjekt transportieren, bereitgestellt werden, können insbesondere eine mit der Sendereinrichtung assoziierte Identität, eine Identität einer Zwischenvorrichtung, die das WebRTC-Sitzungsbeschreibungsbjekt an die Empfängereinrichtung weitergeleitet hat, einen Austausch von Verschlüsselungsschlüsseln oder einen Typ eines interaktiven WebRTC-Flusses beinhalten. In einigen Ausführungsformen kann eine mit der Sendereinrichtung assoziierte Identität eine Identität der Sendereinrichtung, eine Benutzer-ID des Senders und/oder einen Namen des Senders enthalten. Der Agent für verteilte Richtlinienerzwingung **12** empfängt dann von der Unternehmensrichtliniendatenablage eine oder mehrere Unternehmensrichtlinien (Block **102**). Die Verarbeitung wird dann bei Block **104** von **Fig. 4B** fortgesetzt.

**[0048]** In **Fig. 4B**, auf die nunmehr Bezug genommen wird, bewertet der Agent für verteilte Richtlinienerzwingung **12**, ob das WebRTC-Sitzungsbeschreibungsbjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt (Block **104**). Die Unternehmensrichtlinien können vorgeben, welche Typen eines interaktiven WebRTC-Flusses gestattet sind, oder können interaktive WebRTC-Sit-

zungen basierend auf einer mit der Sendereinrichtung assoziierten Identität oder einer Senderdomain oder -identität ausdrücklich zulassen oder ablehnen. Falls bei Block **104** bestimmt wird, dass das WebRTC-Sitzungsbeschreibungsjekt mit der einen oder den mehreren Unternehmensrichtlinien nicht übereinstimmt, kann der Agent für verteilte Richtlinien erzwingung **12** ablehnen, dass zwischen der Sendereinrichtung und der Empfängereinrichtung ein interaktiver WebRTC-Fluss hergestellt wird (Block **106**). Der Agent für verteilte Richtlinien erzwingung **12** kann optional eine oder mehrere Optionen für einen alternativen interaktiven WebRTC-Fluss für die Sendereinrichtung bereitstellen (Block **108**).

**[0049]** Falls der Agent für verteilte Richtlinien erzwingung **12** bei Block **104** bestimmt, dass das WebRTC-Sitzungsbeschreibungsjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt, gestattet der Agent für verteilte Richtlinien erzwingung **12**, dass zwischen der Empfängereinrichtung und der Sendereinrichtung eine sichere Peer-Verbindung hergestellt wird, wie oben mit Bezug auf **Fig. 2** erörtert (Block **110**). In einigen Ausführungsformen kann das Herstellen einer sicheren Peer-Verbindung beinhalten, dass der Agent für verteilte Richtlinien erzwingung **12** ein oder mehrere beim Hole Punching genutzte ICE-Pakete basierend auf der einen oder den mehreren Unternehmensrichtlinien abwandelt. Die Empfängereinrichtung empfängt dann einen ersten interaktiven WebRTC-Fluss, der von der Sendereinrichtung ausgeht, über die sichere Peer-Verbindung, und die interaktive WebRTC-Sitzung beginnt (Block **112**).

**[0050]** In einigen Ausführungsformen kann der Agent für verteilte Richtlinien erzwingung **12** optional die eine oder die mehreren Unternehmensrichtlinien auf den ersten interaktiven WebRTC-Fluss anwenden (Block **114**). Zum Beispiel können die Unternehmensrichtlinien erfordern, dass der erste interaktive WebRTC-Fluss aufgezeichnet, protokolliert oder umgeleitet wird. Wenn der erste interaktive WebRTC-Fluss ein interaktiver Datenaustausch ist, kann das Anwenden der einen oder der mehreren Unternehmensrichtlinien das Untersuchen der Inhalte des interaktiven Datenaustausches beinhalten, um die Einhaltung der einen oder der mehreren Unternehmensrichtlinien zu festzustellen.

**[0051]** In diesem Zusammenhang veranschaulicht **Fig. 5** beispielhafte Betriebsvorgänge zum Anwenden von Unternehmensrichtlinien auf einen interaktiven WebRTC-Fluss, wie in Block **114** von **Fig. 4B** beschrieben. In **Fig. 5** beginnen die Betriebsvorgänge mit der Anforderung des Agenten für verteilte Richtlinien erzwingung **12**, dass ein zweiter interaktiver WebRTC-Fluss, der Daten aus dem ersten interaktiven WebRTC-Fluss beinhaltet, zwischen der Empfängereinrichtung und einer Unternehmensein-

richtung, etwa der Unternehmenseinrichtung **36** von **Fig. 1**, hergestellt wird (Block **116**). Reagierend auf die Anforderung wird der zweite interaktive WebRTC-Fluss an der Unternehmenseinrichtung empfangen (Block **118**). Der zweite interaktive WebRTC-Fluss wird dann gemäß der einen oder den mehreren Unternehmensrichtlinien durch die Unternehmenseinrichtung verarbeitet (Block **120**). In einigen Beispielen kann der zweite interaktive WebRTC-Fluss, wie gemäß den Unternehmensrichtlinien erforderlich, aufgezeichnet oder protokolliert oder an eine andere Einrichtung innerhalb des Unternehmens, etwa eine Media-Anchoring-Einrichtung (nicht gezeigt), umgeleitet werden.

**[0052]** Einige Ausführungsformen könne Variationen der mit Bezug auf **Fig. 5** oben beschriebenen WebRTC-Topologie vorsehen. Zum Beispiel kann der Agent für verteilte Richtlinien erzwingung **12** anfordern, dass der erste interaktive WebRTC-Fluss direkt zwischen einer externen Benutzereinrichtung und der Unternehmenseinrichtung hergestellt wird und dass der zweite interaktive WebRTC-Fluss an der Empfängereinrichtung empfangen wird. In einigen Ausführungsformen kann der Agent für verteilte Richtlinien erzwingung **12** auf die Inhalte des ersten interaktiven WebRTC-Flusses zugreifen und Unternehmensrichtlinien anwenden, indem er die Inhalte des ersten interaktiven WebRTC-Flusses direkt manipuliert, umleitet, protokolliert oder kopiert, wobei es sich um nicht einschränkende Beispiele handelt.

**[0053]** **Fig. 6** stellt eine schematische Diagramm-darstellung ein Verarbeitungssystem **122** in der beispielhaften Form eines beispielhaften Computersystems **124** dar, das angepasst ist, um Befehle zum Durchführen der hierin beschriebenen Funktionen auszuführen. In einigen Ausführungsformen kann das Verarbeitungssystem **122** Befehle zum Durchführen der Funktionen des Agenten für verteilte Richtlinien erzwingung **12** von **Fig. 1** ausführen. In diesem Zusammenhang kann das Verarbeitungssystem **122** das Computersystem **124** umfassen, innerhalb dessen ein Satz von Befehlen das Verarbeitungssystem **122** veranlassen kann, eine beliebige oder beliebige mehrere der hierin erörterten Methodiken durchzuführen. Das Verarbeitungssystem **122** kann mit anderen Maschinen in einem Local Area Network (LAN), einem Intranet, einem Extranet oder dem Internet verbunden (insbesondere etwa vernetzt) sein. Das Verarbeitungssystem **122** kann in einer Client-Server-Netzumgebung oder als gleichrangige Maschine in der Umgebung eines Peer-to-Peer-(oder verteilten) Netzes betrieben werden. Auch wenn nur ein einziges Verarbeitungssystem **122** veranschaulicht wird, können die Begriffe „Controller“ und „Server“ auch so aufgefasst werden, dass sie eine beliebige Gruppe von Maschinen beinhalten, die individuell oder gemeinsam einen Satz (oder mehrere Sätze) von Befehlen zum Durchführen einer beliebigen oder be-

liebiger mehrerer der hierin erörterten Methodiken ausführen. Das Verarbeitungssystem **122** kann ein Server, ein Personal Computer, ein Desktopcomputer, ein Laptopcomputer, ein Personal Digital Assistant (PDA), ein Computerpad, eine mobile Einrichtung oder eine beliebige andere Einrichtung sein und insbesondere einen Server oder einen Computer eines Benutzers darstellen.

**[0054]** Das beispielhafte Computersystem **124** beinhaltet eine Verarbeitungseinrichtung oder einen Prozessor **126**, einen Arbeitsspeicher **128** (insbesondere ein Read Only Memory (ROM), einen Flash-Speicher, einen dynamischen Schreib-Lese-Speicher (DRAM) wie ein synchrones DRAM (SDRAM) usw.) und einen statischen Speicher **130** (insbesondere einen Flash-Speicher, einen statischen Schreib-Lese-Speicher (SRAM) usw.), die über einen Bus **132** miteinander kommunizieren können. Alternativ kann die Verarbeitungseinrichtung **126** direkt oder über irgendein anderes Konnektivitätsmittel mit dem Arbeitsspeicher **128** und/oder dem statischen Speicher **130** verbunden sein.

**[0055]** Die Verarbeitungseinrichtung **126** stellt eine oder mehrere Verarbeitungseinrichtungen wie einen Mikroprozessor, eine Zentralverarbeitungseinheit (CPU) oder dergleichen dar. Insbesondere kann die Verarbeitungseinrichtung **126** ein Mikroprozessor für Rechenvorgänge mit komplexem Befehlssatz (CISC) sein, ein Mikroprozessor für Rechenvorgänge mit reduziertem Befehlssatz (RISC), ein Mikroprozessor für überlange Befehlsörter (VLIW), ein Prozessor, der andere Befehlssätze implementiert, oder Prozessoren, die eine Kombination von Befehlssätzen implementieren. Die Verarbeitungseinrichtung **126** ist konfiguriert, um Verarbeitungslogik in Befehlen **134** und/oder gecachten Befehlen **136** auszuführen, um die hierin erörterten Betriebsvorgänge und Schritte durchzuführen.

**[0056]** Das Computersystem **124** kann ferner eine Kommunikationsschnittstelle in Form einer Netzschmittstelleneinrichtung **138** umfassen. Es kann auch eine Eingabe **140** zum Empfangen von Eingaben und Auswahloptionen, die bei der Ausführung der Befehle **134**, **136** an das Computersystem **124** zu kommunizieren sind, beinhalten. Es kann auch eine Ausgabe **142**, die unter anderem die Anzeige(n) **144** beinhaltet, beinhalten. Die Anzeige(n) **144** kann/können eine Videoanzeigeeinheit (insbesondere eine Flüssigkristallanzeige (LCD) oder eine Kathodenstrahlröhre (CRT)), eine Einrichtung für alphanumerische Eingaben (insbesondere eine Tastatur), eine Cursorsteuereinrichtung (insbesondere eine Maus) und/oder eine Touchscreen-Einrichtung (insbesondere eine Tablet-Eingabeeinrichtung oder einen Bildschirm) beinhalten.

**[0057]** Das Computersystem **124** kann eine Datenablageeinrichtung **145** beinhalten, welche die Nutzung eines Laufwerks/von Laufwerken **146** beinhaltet, um die hierin beschriebenen Funktionen in einem computerlesbaren Medium **148** abzulegen, auf dem ein oder mehrere Sätze von Befehlen **150** (z. B. Software) abgelegt sind, die eine beliebige oder beliebige mehrere der hierin beschriebenen Methodiken oder Funktionen ausführen. Die Funktionen können Verfahren und/oder andere Funktionen des Verarbeitungssystems **122**, eine Teilnehmerbenutzereinrichtung und/oder einen Lizenzierungsserver beinhalten, wobei es sich um nicht einschränkende Beispiele handelt. Der eine oder die mehreren Sätze von Befehlen **150** können während ihrer Ausführung durch das Computersystem **124** auch vollständig oder mindestens teilweise innerhalb des Arbeitsspeichers **128** und/oder innerhalb der Verarbeitungseinrichtung **126** liegen. Der Arbeitsspeicher **128** und die Verarbeitungseinrichtung **126** stellen ebenfalls für Maschinen zugängliche Ablagemedien dar. Die Befehle **134**, **136** und/oder **150** können ferner über ein Netz **152** über die Netzschmittstelleneinrichtung **138** gesendet oder empfangen werden. Das Netz **152** kann ein Intranetz oder ein Inter-Netz sein.

**[0058]** Wenngleich das computerlesbare Medium **148** in einer beispielhaften Ausführungsform als einzelnes Medium gezeigt wird, ist der Begriff „für Maschinen zugängliches Ablagemedium“ so aufzufassen, dass er ein einzelnes Medium oder mehrere Medien beinhaltet (eine zentrale oder eine verteilte Datenbank und/oder assoziierte Cache-Speicher und Server als nicht einschränkende Beispiele), die ein oder mehrere Sätze von Befehlen ablegen. Der Begriff „für Maschinen zugängliches Ablagemedium“ ist auch so aufzufassen, dass er beliebige Medien beinhaltet, die fähig sind, einen Satz von Befehlen zur Ausführung durch die Maschine abzulegen, zu codieren oder zu übertragen, und die die Maschine veranlassen, eine beliebige oder beliebige mehrere der hierin offenbarten Methodiken durchzuführen. Der Begriff „für Maschinen zugängliches Ablagemedium“ ist folglich so aufzufassen, dass er insbesondere Halbleiterspeicher, optische und magnetische Medien und Trägerwellensignale beinhaltet.

**[0059]** Die hierin offenbarten Ausführungsformen können in Hardware und in Befehlen, die in Hardware abgelegt sind, ausgeführt werden und in einem Random Access Memory (RAM), einem Flash-Speicher, einem Read Only Memory (ROM), einem Electrically Programmable ROM (EPROM), einem Electrically Erasable Programmable ROM (EEPROM), in Registern, auf einer Festplatte, einer Wechselfestplatte, einer CD-ROM oder einem computerlesbaren Medium in irgendeiner anderen aus dem Stand der Technik bekannten Form befinden, wobei es sich um nicht einschränkende Beispiele handelt. Ein beispielhaftes Ablagemedium ist an den Prozessor gekoppelt, so-

dass der Prozessor Informationen auf dem Ablagemedium lesen und das Ablagemedium mit Informationen beschreiben kann. Alternativ kann das Ablagemedium fest in den Prozessor integriert sein. Der Prozessor und das Ablagemedium können sich in einer anwendungsspezifischen integrierten Schaltung (ASIC) befinden. Die ASIC kann sich in einem entfernten Endgerät befinden. Alternativ können sich der Prozessor und das Ablagemedium als diskrete Komponenten in einem entfernten Endgerät, in einer Basisstation oder auf einem Server befinden.

**[0060]** Es wird auch angemerkt, dass die in beliebigen der beispielhaften Ausführungsformen hierin beschriebenen Betriebsschritte Beispiele bereitstellen und eine Erörterung ermöglichen sollen. Die beschriebenen Betriebsvorgänge sind auch in zahlreichen anderen und nicht nur in den veranschaulichten Ablauffolgen durchführbar. Des Weiteren können Betriebsvorgänge, die als einzelner Betriebsschritt beschrieben werden, in Wirklichkeit auch in etlichen unterschiedlichen Schritten durchgeführt werden. Zusätzlich können ein oder mehrere in den beispielhaften Ausführungsformen erörterte Betriebsschritte auch kombiniert werden. Es sollte sich verstehen, dass die in den Ablaufdiagrammen veranschaulichten Betriebsschritte auf zahlreiche unterschiedliche Arten abgewandelt werden können, die sich für den Fachmann ohne Weiteres ergeben. Es verstünde sich für den Fachmann auch, dass Informationen und Signale unter Nutzung beliebiger einer Vielzahl unterschiedlicher Technologien und Techniken dargestellt werden können. Daten, Befehle, Kommandos, Informationen, Signale, Bits, Symbole und Chips, auf die in der obigen Beschreibung gegebenenfalls Bezug genommen wird, können durch Spannungen, Ströme, elektromagnetische Wellen, Magnetfelder oder -partikel, optische Felder oder Partikel oder beliebige Kombinationen davon dargestellt sein, wobei es sich um nicht einschränkende Beispiele handelt.

**[0061]** Die vorangehende Beschreibung der Offenbarung wird bereitgestellt, um den Fachmann zu einer Anfertigung gemäß der Offenbarung oder zu ihrer Nutzung zu befähigen. Verschiedene Abwandlungen der Offenbarung werden sich für den Fachmann ohne Weiteres ergeben, und die allgemeinen, hierin definierten Prinzipien können auf andere Variationen angewendet werden, ohne vom Gedanken oder vom Schutzbereich der Offenbarung abzuweichen. Deshalb soll die Offenbarung nicht auf die hierin beschriebenen Beispiele und Ausführungen eingeschränkt sein, sondern ihr soll der weitestmögliche Schutzbereich zukommen, der mit den Prinzipien und den Neuheitsmerkmalen, die hierin offenbart werden, vereinbar ist.

## Patentansprüche

1. Verfahren zum Anwenden einer Unternehmensrichtlinie auf eine interaktive Web-Real-Time-Communications(WebRTC)-Sitzung, das Folgendes umfasst:

Empfangen eines von einer Sendereinrichtung ausgehenden und an eine Empfängereinrichtung gerichteten WebRTC-Sitzungsbeschreibungsjekts durch einen Agenten für verteilte Richtlinienerzwingung der Empfängereinrichtung;

Bestimmen einer oder mehrerer Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsjekt durch den Agenten für verteilte Richtlinienerzwingung;

Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsjekt;

Feststellen, ob das WebRTC-Sitzungsbeschreibungsjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsjektformat übereinstimmt; und

reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsjektformat nicht übereinstimmt, Verwerfen des WebRTC-Sitzungsbeschreibungsjekts.

2. Verfahren nach Anspruch 1, wobei das Bestimmen der einen oder der mehreren Unternehmensrichtlinien Folgendes umfasst:

Abfragen einer Unternehmensrichtliniendatenablage durch den Agenten für verteilte Richtlinienerzwingung; und

reagierend auf das Abfragen Empfangen der einen oder der mehreren Unternehmensrichtlinien von der Unternehmensrichtliniendatenablage durch den Agenten für verteilte Richtlinienerzwingung.

3. Verfahren nach Anspruch 1, wobei das Bestimmen der einen oder der mehreren Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsjekt Bestimmen der einen oder der mehreren Unternehmensrichtlinien basierend auf einer mit der Sendereinrichtung assoziierten Identität, einer Identität einer Zwischenvorrichtung, die das WebRTC-Sitzungsbeschreibungsjekt an die Empfängereinrichtung weitergeleitet hat, einen Austausch von Verschlüsselungsschlüsseln oder einen Typ eines interaktiven WebRTC-Flusses oder Kombinationen davon umfasst.

4. Verfahren nach Anspruch 1, wobei das Anwenden der einen oder der mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsjekt das Feststellen umfasst, ob das WebRTC-Sitzungsbeschreibungsjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt.

5. Verfahren nach Anspruch 4, das ferner reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt, Herstellen eines ersten interaktiven WebRTC-Flusses zwischen der Sendereinrichtung und der Empfängereinrichtung umfasst.

6. Verfahren nach Anspruch 5, wobei das Herstellen des ersten interaktiven WebRTC-Flusses Folgendes umfasst:

Herstellen einer sicheren Peerverbindung zwischen der Empfängereinrichtung und der Sendereinrichtung;

Empfangen des ersten interaktiven WebRTC-Flusses, der von der Sendereinrichtung ausgeht, über die sichere Peerverbindung an der Empfängereinrichtung; und

Anwenden der einen oder der mehreren Unternehmensrichtlinien auf den ersten interaktiven WebRTC-Fluss.

7. Verfahren nach Anspruch 6, wobei der erste interaktive WebRTC-Fluss ein interaktiver Datenaustausch ist; und wobei das Anwenden der einen oder der mehreren Unternehmensrichtlinien auf den ersten interaktiven WebRTC-Fluss Untersuchen von Inhalten des interaktiven Datenaustausches umfasst, um die Einhaltung der einen oder der mehreren Unternehmensrichtlinien zu bestimmen.

8. Verfahren nach Anspruch 7, wobei das Anwenden der einen oder der mehreren Unternehmensrichtlinien auf den ersten interaktiven WebRTC-Fluss Folgendes umfasst:

Anfordern, dass ein zweiter interaktiver WebRTC-Fluss, der Daten aus dem ersten interaktiven WebRTC-Fluss beinhaltet, zwischen der Empfängereinrichtung und einer Unternehmenseinrichtung hergestellt wird, durch den Agenten für verteilte Richtlinien erzwingung;

Empfangen des zweiten interaktiven WebRTC-Flusses an der Unternehmenseinrichtung; und

Verarbeiten des zweiten interaktiven WebRTC-Flusses gemäß der einen oder den mehreren Unternehmensrichtlinien durch die Unternehmenseinrichtung.

9. System zum Anwenden einer Unternehmensrichtlinie auf eine interaktive Web-Real-Time-Communications(WebRTC)-Sitzung, das Folgendes umfasst:

mindestens eine Kommunikationsschnittstelle; und eine Empfängereinrichtung, die mit der mindestens einen Kommunikationsschnittstelle assoziiert ist und einen Agenten für verteilte Richtlinien erzwingung umfasst, wobei der Agent für verteilte Richtlinien erzwingung konfiguriert ist, um:

ein WebRTC-Sitzungsbeschreibungsobjekt, das an die Empfängereinrichtung gerichtet ist, das von einer Sendereinrichtung ausgeht, zu empfangen;

eine oder mehrere Unternehmensrichtlinien basierend auf dem WebRTC-Sitzungsbeschreibungsobjekt zu bestimmen;

die eine oder die mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt anzuwenden;

festzustellen, ob das WebRTC-Sitzungsbeschreibungsobjekt mit einem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat übereinstimmt; und

reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit dem erwarteten WebRTC-Sitzungsbeschreibungsobjektformat nicht übereinstimmt, das WebRTC-Sitzungsbeschreibungsobjekt zu verwerfen.

10. System nach Anspruch 9, wobei der Agent für verteilte Richtlinien erzwingung konfiguriert ist, um die eine oder die mehreren Unternehmensrichtlinien durch Folgendes zu bestimmen:

Abfragen einer Unternehmensrichtliniendatenablage; und

reagierend auf das Abfragen Empfangen der einen oder der mehreren Unternehmensrichtlinien von der Unternehmensrichtliniendatenablage.

11. System nach Anspruch 9, wobei der Agent für verteilte Richtlinien erzwingung konfiguriert ist, um die eine oder die mehreren Unternehmensrichtlinien auf das WebRTC-Sitzungsbeschreibungsobjekt anzuwenden, indem er feststellt, ob das WebRTC-Sitzungsbeschreibungsobjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt.

12. System nach Anspruch 11, wobei der Agent für verteilte Richtlinien erzwingung ferner konfiguriert ist, um reagierend auf das Feststellen, dass das WebRTC-Sitzungsbeschreibungsobjekt mit der einen oder den mehreren Unternehmensrichtlinien übereinstimmt, einen ersten interaktiven WebRTC-Fluss zwischen der Sendereinrichtung und der Empfängereinrichtung herzustellen.

13. System nach Anspruch 12, wobei der Agent für verteilte Richtlinien erzwingung konfiguriert ist, um den ersten interaktiven WebRTC-Fluss durch Folgendes herzustellen:

Herstellen einer sicheren Peerverbindung zwischen der Empfängereinrichtung und der Sendereinrichtung;

Empfangen des ersten interaktiven WebRTC-Flusses, der von der Sendereinrichtung ausgeht, über die sichere Peerverbindung an der Empfängereinrichtung; und

Anwenden der einen oder der mehreren Unternehmensrichtlinien auf den ersten interaktiven WebRTC-Fluss.

Es folgen 7 Seiten Zeichnungen



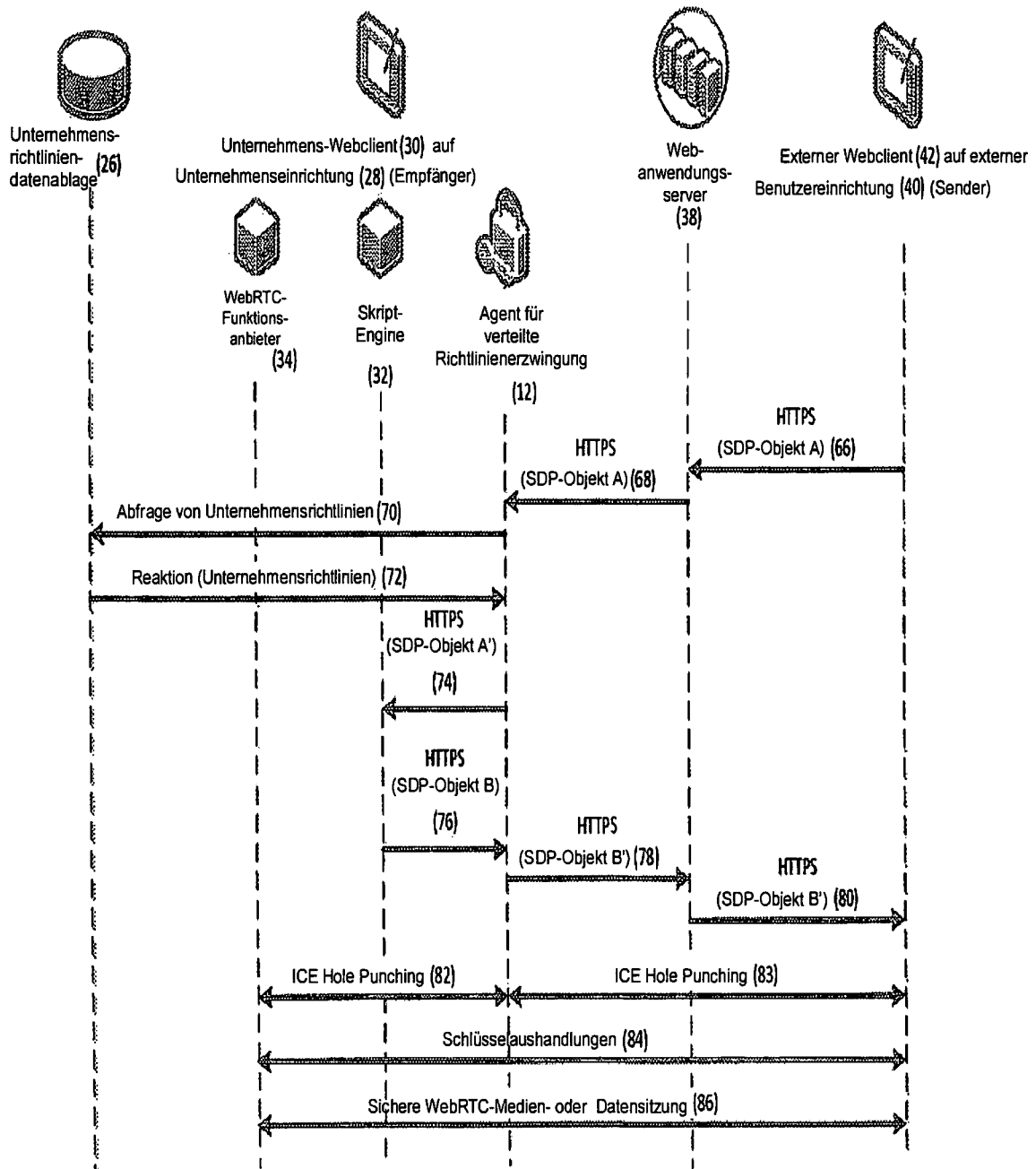


Fig. 2



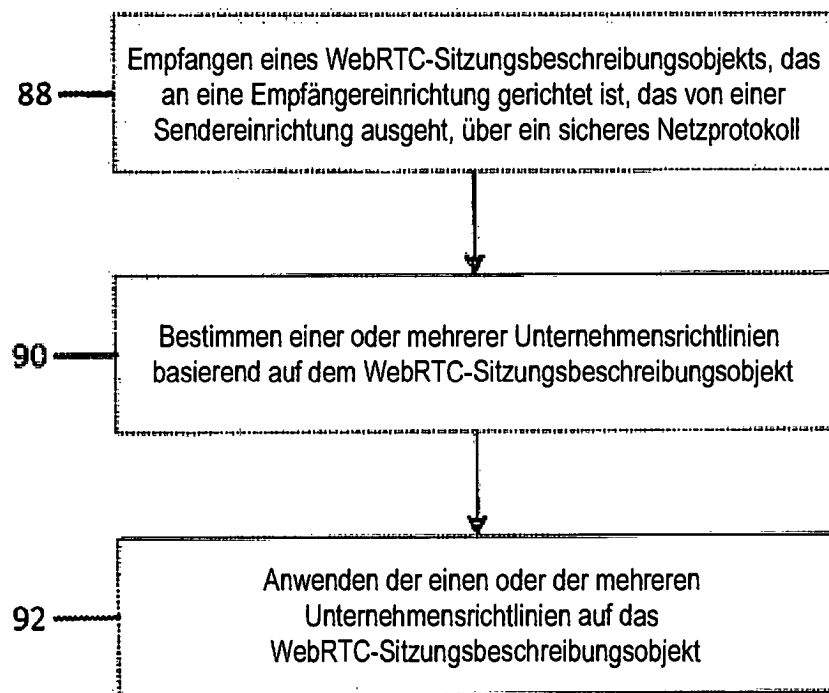


Fig. 3

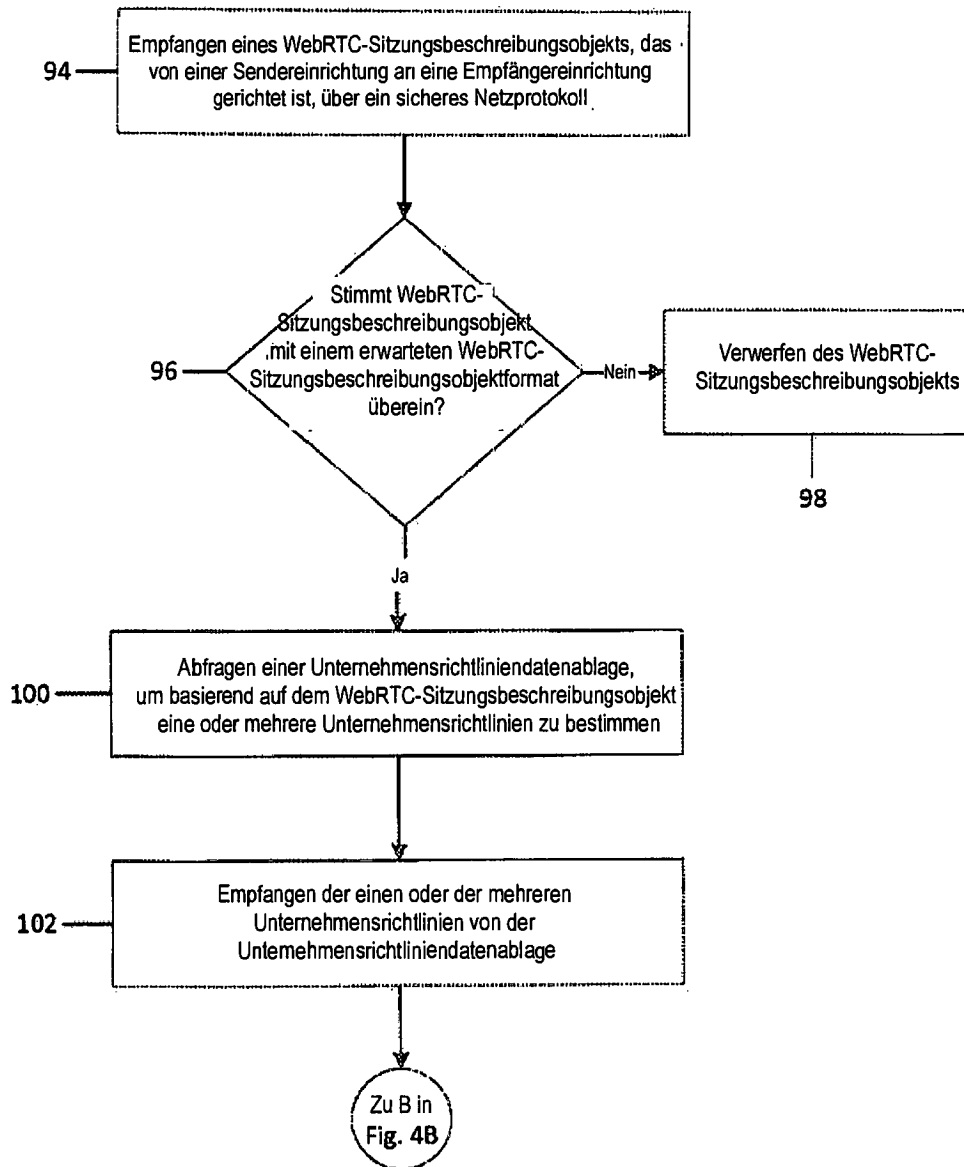


Fig. 4A

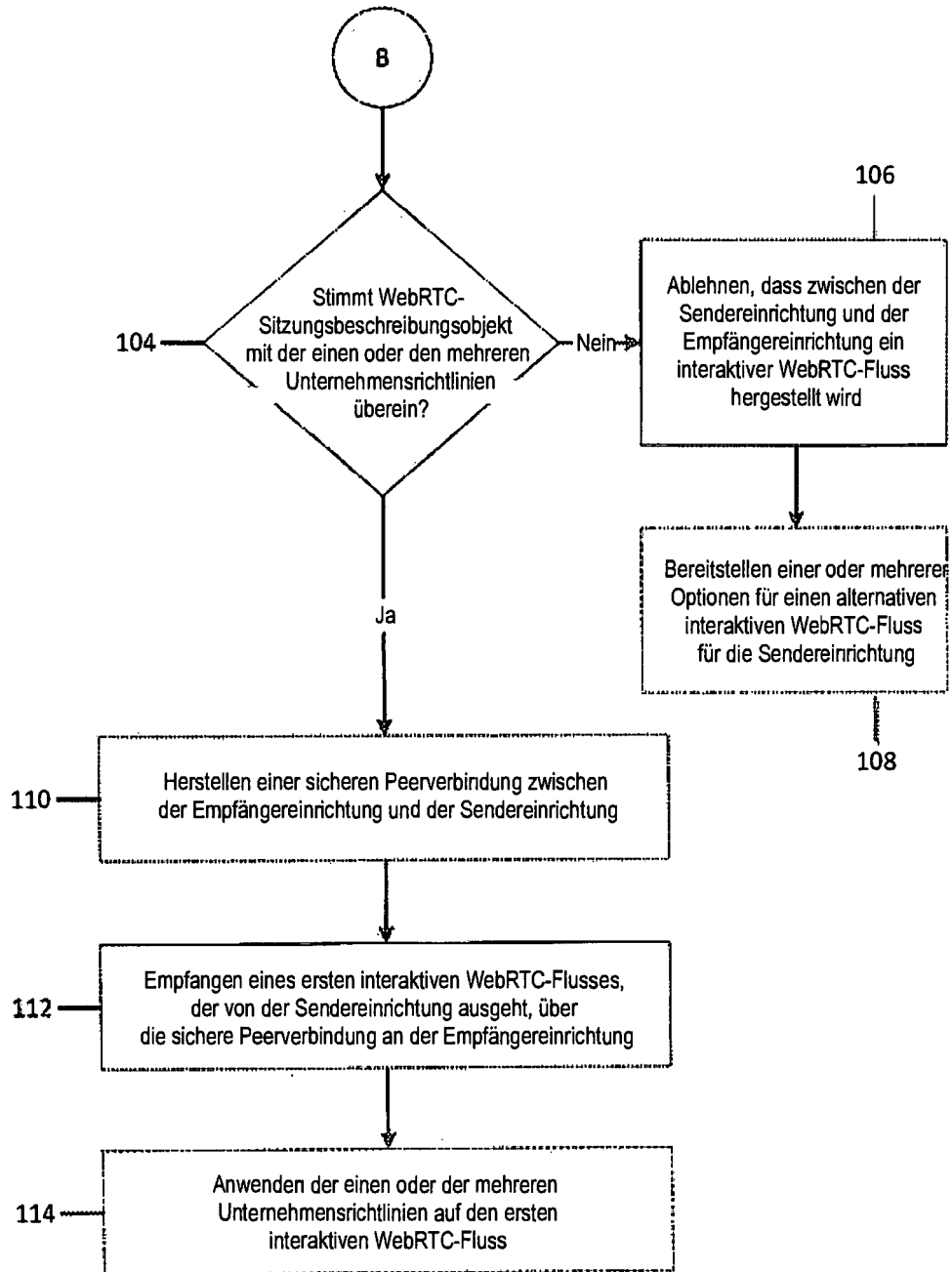


Fig. 4B

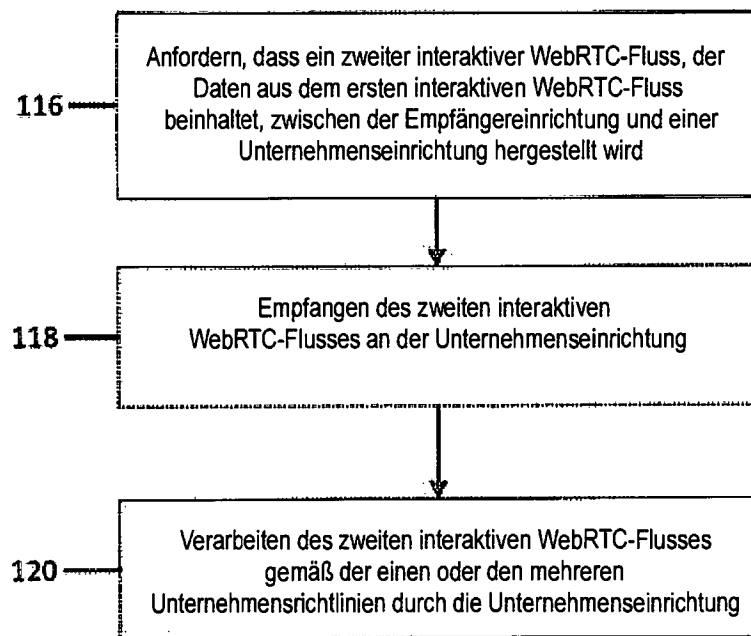


Fig. 5

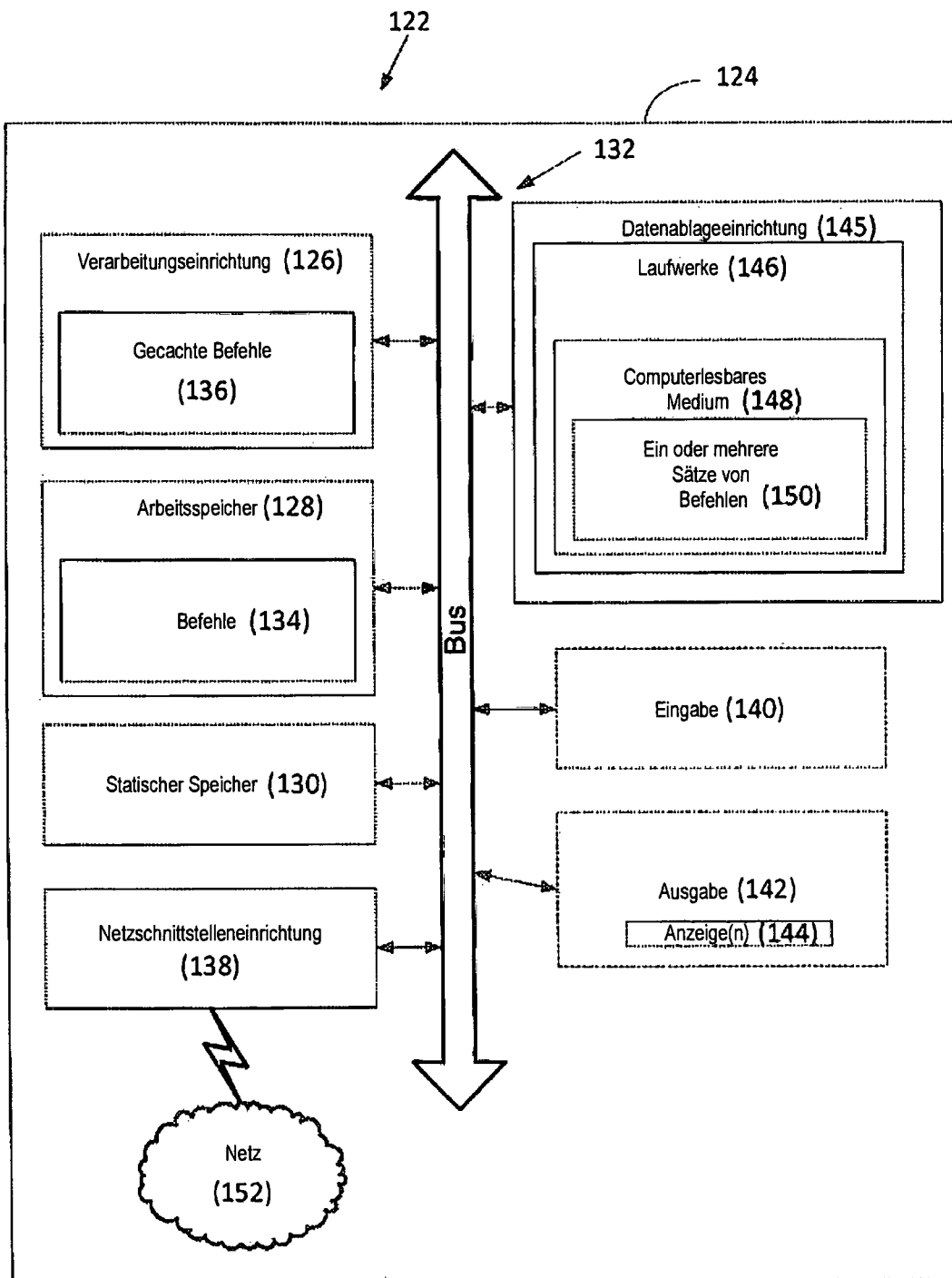


Fig. 6