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

(10) **DE 698 37 201 T2** 2007.11.08

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 988 736 B1**
(21) Deutsches Aktenzeichen: **698 37 201.8**
(86) PCT-Aktenzeichen: **PCT/US98/12226**
(96) Europäisches Aktenzeichen: **98 929 021.8**
(87) PCT-Veröffentlichungs-Nr.: **WO 1998/057464**
(86) PCT-Anmeldetag: **11.06.1998**
(87) Veröffentlichungstag der PCT-Anmeldung: **17.12.1998**
(97) Erstveröffentlichung durch das EPA: **29.03.2000**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **28.02.2007**
(47) Veröffentlichungstag im Patentblatt: **08.11.2007**

(51) Int Cl.[8]: ***H04L 12/46*** (2006.01)
H04L 29/06 (2006.01)

(30) Unionspriorität:
874091 **12.06.1997** **US**

(84) Benannte Vertragsstaaten:
AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE

(73) Patentinhaber:
VPNET Technologies, Inc., San Jose, Calif., US

(72) Erfinder:
GILBRECH, Sidney A., Los Altos, CA 94024, US

(74) Vertreter:
Fiener, J., Pat.-Anw., 87719 Mindelheim

(54) Bezeichnung: **GERÄT ZUR REALISIERRUNG VON VIRTUELLEN PRIVATNETZEN**

Beschreibung

HINTERGRUND DER ERFINDUNG

1. Spezifische Information

[0001] Die vorliegende Erfindung ist auf die unter der Anmeldenummer 08/874,090 mit dem Titel „Architektur für virtuelle Privatnetze" beschriebene, auf den Rechtsnachfolger der vorliegenden Erfindung übertragene und gleichzeitig hiermit eingereichte US-Patentanmeldung bezogen, die der am 29.03.2000 veröffentlichten EP 0 988 735 A entspricht.

2. Gebiet der Erfindung

[0002] Die vorliegende Erfindung bezieht sich auf das Gebiet der Datenfernübertragung. Insbesondere bezieht sich die vorliegende Erfindung auf Verfahrenstechniken für die Einrichtung sicherer virtueller Privatnetze über öffentliche oder in anderer Hinsicht unsichere Datenübertragungsinfrastrukturen, nämlich ein Verfahren gemäß dem Oberbegriff des Anspruches 1. Ein derartiges Verfahren ist aus der WO-A-97/00471 bekannt.

3. Hintergrund

[0003] In den letzten Jahren pflegten sich Organisationen stark auf die Fähigkeit zu verlassen, elektronische Daten zwischen Mitgliedern der Organisation zu übertragen. Zu solchen Daten gehören typischerweise elektronische Post und gemeinsame Dateinutzung oder Dateitransfer. In einer zentralisierten Einzelstandortorganisation werden diese Übertragungen elektronischer Daten ganz allgemein durch ein Ortsnetz (LAN) unterstützt, das von dem einzelnen Unternehmen eingerichtet und betrieben wird.

[0004] Das Verhindern von unbefugtem Zugriff auf Daten, die das LAN eines Unternehmens durchlaufen, ist relativ einfach. Dies gilt sowohl für unbefugte Zugriffe durch Mitglieder des Unternehmens als auch noch bedeutender für Dritte von außerhalb. Solange eine intelligente Netzverwaltung gepflegt wird, sind unbefugte Zugriffe auf Daten, die das interne LAN eines Unternehmens durchlaufen, relativ leicht zu vermeiden. Erst wenn das Unternehmen Filialstandorte umspannt, werden Sicherheitsbedrohungen von außen zu einer größeren Sorge.

[0005] Für dezentralisierte Unternehmen, die die Annehmlichkeiten der oben beschriebenen elektronischen Datenübertragungen wünschen, gibt es mehrere gegenwärtig vorhandene Optionen, aber jede mit zugehörigen Nachteilen. Die erste Möglichkeit ist die gegenseitige Verbindung der Büros oder verschiedenen Standorte mit reservierten oder privaten Kommunikationsverbindungen, die oft als Standleitungen bezeichnet werden. Dies ist die herkömmliche Methode, die Organisationen benutzen, um ein Fernnetz (WAN) einzurichten. Die Nachteile der Einrichtung eines firmeneigenen und überwachten WAN sind offensichtlich: sie sind teuer, aufwendig und häufig nicht ausgelastet, wenn sie zur Verarbeitung der Spitzenkapazitätsanforderungen des Unternehmens erstellt sind. Der offensichtliche Vorteil dieser Lösung ist, dass die Leitungen für den Gebrauch durch das Unternehmen reserviert und deshalb sicher oder einigermaßen sicher vor Spionage oder Fälschung durch Zwischenvermittler sind.

[0006] Eine Alternative zur Verwendung reservierter Datenübertragungsleitungen in einem Fernnetz ist für ein Unternehmen die Handhabung der Datenverteilung zwischen den Standorten über den aufkommenden öffentlichen Netzraum. In den letzten Jahren ist das Internet von einem Werkzeug primär für Wissenschaftler und Akademiker zu einem Schaltwerk für globale Kommunikationstechnik mit weitreichender geschäftlicher Tragweite geworden. Das Internet liefert elektronische Kommunikationswege zwischen Millionen von Computern durch Verbinden der verschiedenen Netzwerke, auf denen sich diese Computer befinden. Es ist alltäglich, ja sogar Routine, für Unternehmen geworden, selbst solche auf nicht technischen Gebieten, zumindest für einen Teil der Rechner innerhalb des Unternehmens Internetzugriff bereitzustellen. Für viele Geschäftsbetriebe erleichtert dies die Kommunikation mit Kunden, potentiellen Geschäftspartnern sowie den verteilten Mitgliedern der Organisation.

[0007] Dezentralisierte Unternehmen haben herausgefunden, dass das Internet ein bequemes Werkzeug zur Bereitstellung elektronischer Kommunikation zwischen Mitgliedern des Unternehmens ist. Zum Beispiel können zwei entfernte Standorte innerhalb des Unternehmens sich jeweils über einen örtlichen Internetdienstanbieter (ISP) mit dem Internet verbinden. Dies versetzt die verschiedenen Mitglieder des Unternehmens in die Lage, mit anderen Standorten im Internet einschließlich derer innerhalb ihrer eigenen Organisation zu kommunizieren. Der einschränkende Nachteil der Benutzung des Internet für unternehmensinterne Kommunikation ist, dass das Internet ein öffentlicher Netzraum ist. Der Leitweg, auf dem der Datenaustausch von einem Punkt zum anderen stattfindet, kann auf Paketbasis variieren und ist weitgehend unbestimmt. Ferner sind die Datenprotokolle zur Übertragung von Informationen über die verschiedenen Netzwerke des Internet umfassend bekannt und machen die elektronische Kommunikationstechnik anfällig für Abfangen und Spionage mit Paketen, die an den meisten Zwischenetappen repliziert werden. Noch größere Bedenken erheben sich, wenn erkannt wird, dass Übertragungen unterwegs von Betrügern verändert oder sogar initiiert werden können. Bei diesen verwirrenden Risiken

sind die meisten Unternehmen nicht gewillt, ihre eigene und vertrauliche interne Kommunikation der Bloßlegung des öffentlichen Netzraums zu unterwerfen. Für viele Organisationen ist es heute alltäglich, nicht nur an jedem Standort Internetzugriff zur Verfügung zu haben, sondern auch die bestehenden reservierten Kommunikationswege für die interne Unternehmenskommunikation mit allen begleitenden oben beschriebenen Nachteilen beizubehalten.

[0008] Zwar wurden verschiedene Chiffrierungs- und andere Schutzmechanismen für Datenfernübertragung entwickelt, keiner davon spricht aber die erhobenen Bedenken umfassend und angemessen an, um es einem Unternehmen zu erlauben, sich für eine sichere unternehmensinterne Datenfernübertragung wirklich auf den öffentlichen Netzraum zu verlassen. Es wäre wünschenswert und ist deshalb eine Aufgabe der vorliegenden Erfindung, solche Techniken bereitzustellen, die es dem dezentralisierten Unternehmen erlauben würden, sich für unternehmensinterne Kommunikation einzig auf den öffentlichen Netzraum zu verlassen, ohne Bedenken wegen Sicherheitsrisiken, wie sie gegenwärtig bestehen.

[0009] Die WO 97/00471 offenbart eine virtuelle Privatnetzeinheit gemäß dem Oberbegriff des Anspruches 1.

WESEN DER ERFINDUNG

[0010] Aus dem Vorstehenden wird ersichtlich, dass es wünschenswert und vorteilhaft wäre, Protokolle und Architektur zu entwickeln, um es einer einzelnen Organisation oder einem einzelnen Unternehmen zu erlauben, sich für sichere organisationsinterne elektronische Datenfernübertragung auf den öffentlichen Netzraum zu verlassen. Die vorliegende Erfindung ist daher auf Protokolle und Architektur zur Implementierung sicherer virtueller Privatnetze über das Internet oder andere öffentliche Netzvorrichtungen gerichtet. Die Architektur der vorliegenden Erfindung führt eine Standort-Schutzeinrichtung oder virtuelle Privatnetz-(VPN-)Einheit ein, welche die Datenfernübertragung zwischen Mitgliedern einer definierten VPN-Gruppe moderiert. In Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung befindet sich die Standort-Schutzeinrichtung auf der WAN-Seite des Routers des Standorts oder der Leitvorrichtung, die zur Verbindung des Unternehmensstandorts mit dem Internet verwendet wird. In alternativen Ausführungsformen befindet sich die Standort-Schutzeinrichtung auf der LAN-Seite des Routers. Der wesentliche Punkt bei allen Ausführungsformen ist, dass es die Standort-Schutzeinrichtung auf dem Weg jedes einzelnen relevanten Datenverkehrs gibt.

[0011] Zur Sicherstellung einer sicheren Datenfernübertragung zwischen Mitgliedern derselben VPN-Gruppe implementiert die Standort-Schutzeinrichtung oder VPN-Einheit eine Kombination von Verfahrenstechniken zur Datenpakethandhabung, wenn Pakete zwischen Mitgliedern der Gruppe gesendet werden sollen. Die Pakethandhabungsverfahren schließen verschiedene Komprimierungs-, Chiffrierungs- und Beglaubigungskombinationen ein, deren einzelne Regeln für Mitglieder verschiedener Gruppen variieren können. Für jede als virtuelles Privatnetz definierte Gruppe werden die verschiedenen Parameter zur Definition von Komprimierung, Chiffrierung und Beglaubigung in Nachschlagetabellen in den zugeordneten VPN-Einheiten gepflegt. Die Nachschlagetabellen unterhalten Informationen nicht nur für Mitglieder der Gruppe mit fester Adresse, sondern bieten auch entfernten Klienten Unterstützung. Diese Fähigkeit gestattet es entfernten Benutzern, sich bei einem örtlichen Internetdienstanbieter einzuwählen und trotzdem die Mitgliedschaft in einer virtuellen Privatnetzgruppe für sichere Kommunikation über das Internet mit anderen Mitgliedern der Gruppe aufrechtzuerhalten. Im Falle eines entfernten Klienten kann die Standort-Schutzeinrichtung in einer Ausführungsform durch Software simuliert werden, die bei dem entfernten Klienten läuft.

[0012] Gemäß anderen Aspekten der vorliegenden Erfindung können die VPN-Einheiten oder Standort-Schutzeinrichtungen dynamisch konfiguriert sein, um der virtuellen Privatnetzgruppe Mitglieder hinzuzufügen oder davon abzuziehen oder deren Bewegung zu erkennen oder andere die Gruppe beeinflussende Parameter zu verändern. Zu verschiedenen anderen Pakethandhabungsaspekten der Erfindung gehört das Ansprechen des Problems, dass einige Datenpakete durch das Einschließen von Chiffrierungs- und Beglaubigungsinformationen zu groß werden. Ein anderer Pakethandhabungsaspekt stellt eine Einrichtung für Internetkommunikation bereit, die Informationen zur Identifizierung von Ursprung und Bestimmungsort des Datenpakets verbirgt. Gemäß diesem Aspekt der vorliegenden Erfindung werden die VPN-Einheiten als Sender und Empfänger für die Internetkommunikation-Datenpakete behandelt, wobei die VPN-Einheiten die Sender- und Empfangsadressen der Endstationen einkapseln.

[0013] Es wird auch eine Hardware-Architektur und -Realisierung für eine VPN-Einheit offenbart. Diese Ausführungsform ist derart ausgelegt, dass sie ihren Platz auf der WAN-Seite des Routers eines gegebenen Standorts hat. In der dargestellten Ausführungsform ist zur Ausführung der Prozesse des VPN-Gerätes zur Komprimierung, Chiffrierung und Beglaubigung unter der Leitung eines Mikroprozessors eine Kombination aus Computer-Hardware und -Software vorgesehen.

KURZBESCHREIBUNG DER ZEICHNUNGEN

[0014] Die Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden aus der folgenden detaillierten Beschreibung offensichtlich werden, in der:

[0015] Fig. 1 eine Konfiguration des Standes der Technik für eine beispielhafte unternehmensinterne Kommunikationsarchitektur eines Unternehmens darstellt;

[0016] Fig. 2 ein Unternehmenskommunikationsszenario in Übereinstimmung mit der vorliegenden Erfindung unter Verwendung des Internet oder eines anderen öffentlichen Netzraums als Medium zur Beförderung von Nachrichten zwischen Mitgliedern eines virtuellen Privatnetzes darstellt;

[0017] Fig. 3 ein Ablaufdiagramm zur Handhabung eines Paketes darstellt, das von einem Mitglied einer virtuellen Privatnetzgruppe über das Internet zu einem anderen Mitglied übertragen wird;

[0018] Fig. 4 die Handhabung eines Datenpaketes darstellt, das von einem Mitglied einer virtuellen Privatnetzgruppe über das Internet von einem anderen Mitglied empfangen wird;

[0019] Fig. 5 die Lebensdauer eines Datenpaketes graphisch darstellt, das von einem Mitglied einer virtuellen Privatnetzgruppe über das Internet an ein anderes gesendet wird;

[0020] Fig. 6 eine alternative Lebensdauer eines Datenpaketes darstellt, das von einem Mitglied einer virtuellen Privatnetzgruppe über das Internet an ein anderes gesendet wird, wo die Sender- und Empfangsadressen der Gruppenmitglieder ebenfalls verdeckt sind;

[0021] Fig. 7 ein Architekturblockdiagramm für eine Realisierung einer virtuellen Privatnetzeinheit in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung darstellt;

[0022] Fig. 8 ein detaillierteres Blockdiagramm für eine Realisierung einer virtuellen Privatnetzeinheit in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung darstellt.

DETAILLIERTE BESCHREIBUNG DER ERFINDUNG

[0023] Es wird eine virtuelle Privatnetzeinheit zur Einrichtung sicherer virtueller Privatnetze für Unternehmenskommunikation über das Internet oder anderen öffentlichen Netzraum offenbart. Obwohl die vorliegende Erfindung vorwiegend bezogen auf die Verwendung des Internet als Kommunikationsmedium beschrieben wird, sind die Konzepte und Methoden breit genug gefasst, um die Einrichtung sicherer virtueller Privatnetze über andere öffentliche oder unsichere Kommunikationsmedien zu bewerkstelligen. Durch die ganze detaillierte Beschreibung hindurch werden zahlreiche spezifische Einzelheiten dargelegt, wie z. B. spezielle Chiffrierungs- oder Schlüsselverwaltungsprotokolle, um für ein gründliches Verständnis der vorliegenden Erfindung zu sorgen. Für den Fachmann wird jedoch verständlich sein, dass die vorliegende Erfindung ohne solche spezifische Einzelheiten ausgeführt werden kann. In anderen Beispielen sind hinlänglich bekannte Steuerstrukturen und Gerätekomponenten nicht im Einzelnen gezeigt worden, um die vorliegende Erfindung nicht zu verschleiern.

[0024] In vielen Beispielen sind durch die vorliegende Erfindung realisierte Komponenten auf einer architektonischen, funktionellen Ebene beschrieben. Viele der Elemente können unter Verwendung hinlänglich bekannter Strukturen konfiguriert werden, insbesondere jene, die als verschiedene Komprimierungs- oder Chiffrierungstechniken betreffend bezeichnet sind. Zum Einschließen von Logik in der Vorrichtung der vorliegenden Erfindung sind zusätzlich Funktionalität und Ablaufdiagramme auf eine solche Art und Weise beschrieben, dass der Durchschnittsfachmann in der Lage sein wird, die speziellen Verfahren ohne übermäßiges Experimentieren zu realisieren. Es sollte ferner verständlich sein, dass die Verfahrenstechniken der vorliegenden Erfindung unter Verwendung vieler verschiedener Technologien realisiert werden können. Zum Beispiel kann die hierin weiter zu beschreibende virtuelle Privatnetzeinheit oder Standort-Schutzeinrichtung in Software realisiert sein, die auf einer Rechnervorrichtung läuft, oder in Hardware realisiert sein, die entweder von einer Kombination von Mikroprozessoren Gebrauch macht oder von anderen speziell entworfenen, anmeldungsspezifischen integrierten Schaltkreisen, programmierbaren Logikvorrichtungen oder verschiedenen Kombinationen davon. Fachleuten wird verständlich sein, dass die vorliegende Erfindung nicht auf irgendeine spezielle Implementierungstechnik beschränkt ist, und wenn die mit diesen Komponenten auszuführende Funktionalität einmal beschrieben ist, wird der Durchschnittsfachmann in der Lage sein, die Erfindung ohne übermäßiges Experimentieren mit verschiedenen Technologien zu realisieren.

[0025] Es wird nun auf Fig. 1 Bezug genommen, wo ein herkömmliches Szenario für unternehmensinterne Datenfernübertragung für eine dezentralisierte Organisation gezeigt ist. In dieser Illustration einer beispielhaften Organisationsstruktur besteht das Unternehmen aus einem Zentralenstandort **105** mit Nebenstandorten oder Zweigstellen **110** bzw. **112**. In modernen Organisationen wie der beispielhaften Or-

ganisation gemäß Fig. 1 können der Zentralensitz **105** sowie die Zweigstellensitze **110** und **112** jeweils eine zahlreiche Belegschaft umfassen, von denen viele mit Computern oder Arbeitsstationen mit Netzzugang ausgestattet sind. Die internen Netzarchitekturen an der Zentrale für Zweigstellen können viele Formen annehmen, darunter ein oder mehrere Ortsnetze (LANs). Für die zwischenstandörtliche Kommunikation zwischen der Zentrale und den Zweigstellen können reservierte oder gemietete Kommunikationsleitungen **115** und **120** vorgesehen sein. Darüber hinaus kann ein optionaler reservierter Kommunikationsweg **125** zwischen den Zweigstellen **110** und **112** vorgesehen sein. Als Alternative zu der optionalen reservierten Kommunikationsleitung **125** zwischen den Zweigstellen können Datenpakete zwischen der Zweigstelle **110** und der Zweigstelle **112** durch die Zentralennetzeinrichtung hindurchgeleitet werden.

[0026] Neben den reservierten Kommunikationsleitungen zwischen der Zentrale und den verschiedenen Zweigstellen ist es heute alltäglich, Computerbenutzern innerhalb einer Organisation Zugriff auf das Internet für elektronische Post an externe Teilnehmer sowie zur Vornahme verschiedener Arten von Recherche über das Internet unter Verwendung solcher Instrumente wie das World Wide Web etc. zur Verfügung zu stellen. In Fig. 1 ist das übliche Szenario gezeigt, wo der Zentralensitz **105** und die Zweigstellen **110** und **112** jeweils separat mit einem Direktzugriff auf Internetdienstanbieter **130**, **133** bzw. **136** ausgestattet sind. Dies erleichtert den Benutzern an den verschiedenen Standorten den Zugriff auf das Internet für obige Zwecke. In einer alternativen Struktur kann es sein, dass nur der Zentralensitz **105** mit einem Zugriff auf einen Internetdienstanbieter **130** ausgestattet ist und dass Benutzer der Computer der Zweigstellensitze **110** und **112** über ihre reservierten Kommunikationswege **115** und **120** durch die Zentrale mit dem Internet verbunden werden. Der Nachteil dieser alternativen Konfiguration ist, dass sie die Bandbreitenauslastung auf den reservierten Leitungen erheblich steigert, vielleicht bis zum Sättigungspunkt. Ein Vorteil ist, dass nur ein Netzverbindungsrechner zum Internet für die Organisation vorgesehen sein braucht, was die Durchsetzung von Sicherheitsbeschränkungen bei Verbindungen zur Außenwelt vereinfacht.

[0027] In der beispielhaften Organisation **100** ist ferner gezeigt, dass es unter gewissen Umständen erwünscht sein kann, Kunden oder anderen Geschäftspartnern die direkte Einwahl in das Rechnernetz der Organisation zu erlauben. In Fig. 1 ist dargestellt, dass der Kunde **140** tatsächlich einen derartigen Informationsaustausch über einen Kommunikationsweg **145** ausführen kann, der eine Standleitung sein kann, die für die Annehmlichkeit des Kunden zwischen dem Kunden und der Organisation vorgesehen sein kann. Der Weg **145** kann auch eine Wählleitung sein, die der Kunde vielleicht nur sporadisch benutzt. In Einklang mit der aufkommenden Nutzung des Internet und seiner Beliebtheit ist gezeigt, dass der Kunde **140** durch ISP **148** seine eigene Internetverbindung besitzt.

[0028] Schließlich ist in Fig. 1 gezeigt, dass es für andere Mitglieder des Unternehmens, die vielleicht unterwegs sind oder von zu Hause oder an anderen entfernten Orten arbeiten, häufig wünschenswert ist, Daten mit anderen Mitgliedern des Unternehmens auszutauschen. Daher sind Fernklienten **150** und **155** gezeigt, die über Telefonfernleitungen **157** und **158** mit der Zentrale kommunizieren. Dieses Beispiel nimmt an, dass die Fernklienten sich an einem wirklich von der Zentrale entfernten Ort befinden. Die Fernklienten **150** und **155** sind ferner jeweils mit örtlichem Zugriff auf das Internet durch örtliche ISP **160** und **165** gezeigt.

[0029] Die obige Beschreibung einer Unternehmens-Datenkommunikationsarchitektur gemäß Fig. 1 stellt die im vorstehenden Abschnitt beschriebenen Nachteile dar. Diese Nachteile werden beseitigt durch Realisierung der vorliegenden Erfindung, wie mit Bezug auf Fig. 2 allgemein dargestellt. In der in Fig. 2 dargestellten Betriebsnetz-Kommunikationsarchitektur **200** sind die Zentrale **105**, erste Zweigstelle **110** und zweite Zweigstelle **112** der Organisation auf detailliertere logische Art dargestellt als in Fig. 1 präsentiert. So ist die Zentrale **105** mit drei Endstationen **201**, **202** und **203** dargestellt, die jeweils zur Übertragung von Datenpaketen über ein Ortsnetz (LAN) **205** angeschlossen sind. Gleicherweise ist der Zweigstellensitz **110** mit einer Vielzahl von Endstationen **211**, **212** und **213** gezeigt, die jeweils zur lokalen Übertragung von Daten über ein LAN **215** angeschlossen sind. Schließlich ist der zweite Zweigstellensitz **112** mit einer illustrativen Zusammenstellung von Rechnerstationen **221**, **222** und **223** gezeigt, die zur Kommunikation über ein LAN **225** verbunden sind. Der Kundensitz **140** ist in Fig. 2 ferner als eine Vielzahl von durch **331** und **332** dargestellten Computern umfassend dargestellt, die zur Kommunikation über ein LAN **235** des Kunden angeschlossen sind. Die zur Datenfernübertragung innerhalb der Zentralen-, Kunden- und Zweigstellensitze verwendeten Ortsnetze können einer breiten Vielfalt von Netzprotokollen folgen, von denen Ethernet und Token Ring die am weitesten verbreiteten sind.

[0030] Wie aus Fig. 2 ersichtlich ist, wurden die reservierten Kommunikationsleitungen zwischen dem Zentralensitz **105** und den Zweigstellensitzen **110** und **112** sowie zwischen dem Zentralensitz **105** und dem Kundensitz **140** ausgeschaltet. Stattdessen soll die Datenfernübertragung zwischen Mitgliedern der Organisation in Übereinstimmung mit der vorliegenden Erfindung über das Internet oder anderen öffentlichen Netzraum ausgeführt werden. Für die Zwecke

der vorliegenden Erfindung wird angenommen, dass es das weithin aufkommende Internet ist, das das Medium für Datenpaketübertragungen zwischen Mitgliedern der Organisation ist.

[0031] Jedes der in Fig. 2 dargestellten LANs für die einzelnen Standorte ist letztlich durch eine zugeordnete Leitweglenkungs- oder Konzentratorvorrichtung, die als Router **240**, **242**, **244** bzw. **246** gekennzeichnet sind, zum Internet **250** durchgeschaltet. Es sollte verständlich sein, dass zwischen den verschiedenen in **200** dargestellten Standorten transportierte Datenpakete in vielen Fällen auf dem Weg zwischen dem Sender- und dem Empfangsstandort für die Pakete eine Vielzahl von zusätzlichen Leitweglenkungsvorrichtungen durchlaufen. Die Techniken für Datenpaketübertragungen über das Internet sind hinlänglich bekannt und werden hierin nicht in großer Einzelheit beschrieben. Es versteht sich von selbst, dass die Datenpakete in Übereinstimmung mit dem Internetprotokoll (IP) zusammengesetzt sind und hierin als IP-Pakete bezeichnet werden, ungeachtet der gegenwärtig gültigen Version des Internetprotokolls. Im Falle der in Fig. 2 dargestellten Fernklienten **150** und **155** versteht es sich von selbst, dass diese Datenübertragungs-Software benutzen, um sich bei einem örtlichen Internetdienstanbieter einzuwählen, der selbst die notwendigen Netzverbindungsrechner für die Kommunikation über das Internet **250** bereitstellt.

[0032] Wie oben beschrieben wurde, erforderten frühere Bemühungen, das Internet für eine sichere Datenfernübertragung zu nutzen, Bewusstsein oder Realisierung von Sicherheitsüberlegungen an den Endstationen. Dies ist von Nachteil, wenn Transparenz für einen Endbenutzer erwünscht ist. Die vorliegende Erfindung ist andererseits transparent für Endbenutzer, wobei die Datenfernübertragung über das Internet genauso vor sich geht, wie sie sich vorher zeigte. Bei Benutzern, die als Mitglieder desselben virtuellen Privatnetzes identifiziert werden, wird die Datenfernübertragung jedoch auf eine Art und Weise gehandhabt, die Sicherheit und Unversehrtheit der Datenpakete gewährleistet. In Fig. 2 sind zwischen dem Internet **250** und jedem der jeweiligen Router **240**, **242**, **244** und **246** virtuelle Privatnetzeinheiten (VPN-Einheiten; VPNUs) **250**, **252**, **254** und **256** dargestellt. In Übereinstimmung mit der speziellen dargestellten Ausführungsform der vorliegenden Erfindung liegen die VPN-Einheiten zwischen einem Router des Standorts und dem Weg zum Internet. Es sollte verständlich sein, dass diese Platzierung von VPN-Einheiten in der Gesamtsystemarchitektur nur eine Unterbringungswahl repräsentiert. Aus dem noch folgenden Stoff wird deutlich werden, dass der Knackpunkt im Hinblick auf die VPNU-Platzierung darin besteht, dass sie auf dem Datenverkehrsweg liegen. In vielen Ausführungsformen kann es sich tatsächlich als wünschenswert erweisen, die VPNU auf der LAN-Seite des Routers eines Standorts unterzubringen. Wie nachstehend noch näher beschrieben wird, unterhalten die VPN-Einheiten Nachschlagetabellen zur Identifikation der Mitglieder spezifischer virtueller Privatnetzgruppen.

[0033] Wenn ein Datenpaket zwischen Sender- und Empfangsadressen gesendet wird, die beide Mitglieder derselben VPN-Gruppe sind, verarbeitet die VPN-Einheit das Datenpaket von der Sendeseite auf eine Weise, um sicherzustellen, dass es chiffriert, beglaubigt und ggf. komprimiert wurde. Gleicherweise erkennt die den Standort bedienende VPN-Einheit, wo die Empfangsadresse gelegen ist, dass ein Paket zwischen Mitgliedern derselben VPN-Gruppe übertragen wird. Die empfangende VPN-Einheit erledigt den Dechiffrierungs- und Beglaubigungsprozess des Paketes, bevor sie es zur Empfangsendstation übermittelt. Auf diese Weise wird eine sichere Datenfernübertragung zwischen Endbenutzern auf eine Art und Weise bewirkt, die für die Endbenutzer transparent ist. Im Falle von Fernklienten **150** und **155** kann die VPN-Einheit in Software simuliert werden, die in Verbindung mit der Datenübertragungs-Software operiert, um den Fernklienten mit dem zugeordneten örtlichen Internetdienstanbieter zu verbinden.

[0034] Die Funktionalität der VPN-Einheiten wird nun mit Bezug auf die folgenden Figuren beginnend mit dem Flussdiagramm von Fig. 3 beschrieben. Wenn ein Datenpaket von einer Endstation stammt, wie z. B. der Endstation **202** des LAN **205** am Standort **105**, und sein Ziel an einem entfernten Standort liegt, der ein anderer ist als der Zentralensitz **105**, wird es anfangs als gewöhnliche Internet-Datenpaketübertragung behandelt. Das Paket geht von der Endstation **202** über das LAN **205** weiter zur Leitweglenkungsvorrichtung **240**, die das Datenpaket in Übereinstimmung mit dem Internetprotokoll einkapselt und ein abgehendes IP-Paket bildet. Auf seinem Weg von dem Standort weg passiert das IP-Paket die zugeordnete VPN-Einheit für den Standort. Das in Fig. 3 dargestellte Flussdiagramm zeigt die funktionelle Wirkungsweise einer VPN-Einheit für ein abgehendes Paket, das dadurch empfangen wird. Das Paketübertragungsverfahren **300** beginnt, wenn das abgehende Datenpaket bei Schritt **310** an der VPN-Einheit empfangen wird. Am Auswahlblock **320** wird bestimmt, ob die Sender- und die Empfangsadresse für das Datenpaket beide Elemente derselben VPN-Gruppe sind oder nicht. Diese Bestimmung kann mit Bezug auf Nachschlagetabellen, die von den VPN-Einheiten unterhalten werden, oder mit Bezug auf andere Speichermechanismen vorgenommen werden. Dieser Schritt kann als Mitgliederfilterung für Datenpakete angenommen werden, die zwischen dem Einzelstandort und der diesen bedienenden VPN-Einheit übertragen werden. Wenn der Sender und die Empfangsadresse für das Datenpaket nicht beide Mitglieder derselben VPN-Gruppe sind, dann wird das Paket bei Schritt **330** als gewöhnlicher

Internetverkehr von dem Standort an das Internet übermittelt, als ob die VPN-Einheit nicht involviert wäre. In diesem Fall endet das Verfahren bei Schritt **335**. In einer alternativen Ausführungsform kann es wünschenswert sein, nicht von einem Mitglied für ein anderes einer VPN-Gruppe bestimmten Datenverkehr lieber abzulegen als ihn als unsicheren Verkehr weiterzuleiten. In einer anderen alternativen Ausführungsform kann die Bereitstellung der Option wünschenswert sein, Nicht-VPN-Gruppen-Datenverkehr entweder weiterzugeben oder abzulegen.

[0035] Wenn am Auswahlblock **320**, dem Mitgliederfilter, bestimmt wird, dass sowohl die Sender- als auch die Empfangsadresse für das Datenpaket Elemente derselben VPN-Gruppe sind, dann wird das Datenpaket bei Schritt **340** verarbeitet und verschiedenen Kombinationen von Komprimierung, Chiffrierung und Beglaubigung unterzogen. Die von der VPN-Einheit **250** und allen VPN-Einheiten gepflegten Nachschlagetabellen weisen neben der Identifizierung von Mitgliedern bestimmter VPN-Gruppen auch aus, ob zwischen Mitgliedern der bestimmten VPN-Gruppe übertragene Datenpakete komprimiert werden sollen oder nicht und wenn ja, welcher Algorithmus für die Komprimierung verwendet werden soll. Viele mögliche Komprimierungsalgorithmen sind hinlänglich bekannt, aber in einer Ausführungsform der Erfindung wird die LZW-Komprimierung ausgeführt. Die Nachschlagetabelle für die VPN-Gruppe, zu der die Sender- und die Empfangsadresse als Elemente gehören, identifiziert auch den speziellen Chiffrierungsalgorithmus, der für Datenpakete zu verwenden ist, die das Internet für diese VPN-Gruppe durchlaufen, sowie die dadurch zu verwendenden Beglaubigungs- und Schlüsselverwaltungsprotokoll-Informationen. Als Alternative zu Nachschlagetabellen kann die VPN-Einheit so programmiert sein, dass sie immer dieselben Algorithmen für alle VPN-Gruppen verwendet.

[0036] Die speziellen Paketverarbeitungsalgorithmen, die für den VPN-Verkehr zu verwenden sind, können variieren, solange die Nachschlagetabellen sowohl in der sendenden als auch der empfangenden VPN-Einheit dieselben Komprimierungs-, Chiffrierungs- und Beglaubigungsregeln anlegen und in der Lage sind, sie für Mitglieder derselben Gruppe zu implementieren und zu deimplementieren. Es sollte verständlich sein, dass eine einzelne VPN-Einheit mehrfache VPN-Gruppen bedienen kann und dass bestimmte Adressen Elemente mehrfacher Gruppen sein können. So wird bei Schritt **340** ein Paket, das von einem Mitglied der VPN-Gruppe für ein anderes bestimmt ist, gemäß den in den Tabellen der VPN-Einheit ausgewiesenen Komprimierungs-, Chiffrierungs- und Beglaubigungsregeln für diese spezielle VPN-Gruppe verarbeitet. Bei Schritt **350** wird das verarbeitete Paket dann über das Internet zur Empfangsadresse übermittelt. Der Befehlsteil der sendenden VPN-Einheit endet dann bei Schritt **355**.

[0037] Die entgegennehmende VPN-Einheit kehrt die obigen Abläufe für den VPN-Verkehr um, wie durch das Flussdiagramm gemäß Fig. 4 dargestellt. Das Paketempfangsverfahren **400** beginnt bei Schritt **410**, wenn an der entgegennehmenden VPN-Einheit ein ankommendes Datenpaket aus dem Internet empfangen wird. Am Auswahlblock **420** wird das ankommende Datenpaket geprüft, um zu bestimmen, ob die Sender- und die Empfangsadresse des Datenpaketes beide Elemente derselben VPN-Gruppe sind. Es wird angenommen, dass die von allen VPN-Einheiten gepflegten Nachschlagetabellen sowohl konsistent als auch kohärent sind. Wenn bestimmt wird, dass das ankommende Datenpaket kein VPN-Verkehr ist, dann wird das Paket bei Schritt **430** durchgelassen und zum Empfangsstandort übermittelt, als ob es normaler Internetdatenverkehr wäre. In diesem Fall endet der Prozess bei Schritt **435**. In einer alternativen Ausführungsform kann es wünschenswert sein, ankommenden Datenverkehr abzulegen, der nicht von einem identifizierten Mitglied einer VPN-Gruppe kommt, die von der VPNU unterstützt wird.

[0038] Bei Datenpaketen, die am Auswahlblock **420** als VPN-Verkehr bestimmt werden, verarbeitet die VPN-Einheit das ankommende Paket zur Wiederherstellung des Originaldatenpaketes, wie es von der Senderendstation bereitgestellt wurde. Die von der entgegennehmenden VPN-Einheit unterhaltene Nachschlagetabelle identifiziert dann die für die VPN-Gruppe verwendeten Komprimierungs-, Chiffrierungs- und Beglaubigungsregeln und rekonstruiert das ursprüngliche IP-Paket in Übereinstimmung mit diesen Regeln bei Schritt **440**. Bei **450** wird das rekonstruierte Paket dann zum Standort der Empfangsadresse geliefert, und bei Schritt **455** endet das Verfahren.

[0039] Fig. 5 stellt die Lebensdauer des zwischen zwei Mitgliedern derselben VPN-Gruppe gesendeten Datenpaketes graphisch dar. Das Datenpaket stammt von einem Sender **500** und breitet sich von dem Senderstandort über seinen zugeordneten Router aus, um ein IP-Datenpaket **510** zu erzeugen. Das Datenpaket **510** ist nicht dazu gedacht, alle Gebiete darzustellen, die mit einem vollständigen IP-Datenpaket verbunden sind, zeigt aber die für diese Erörterung relevanten Abschnitte einschließlich der Empfangsadresse, Senderadresse und Nutzlastinformationen des Paketes. Das Datenpaket **510** wird dann von der VPN-Einheit geprüft, die bestimmt, ob das Datenpaket Verkehr zwischen Mitgliedern einer identifizierten VPN-Gruppe ist. Die VPN-Einheit **520** verarbeitet das Paket in Übereinstimmung mit den oben im Hinblick auf Fig. 3 beschriebenen Paketverarbeitungsverfahren, wobei das resultierende Paket als Paket **530** dargestellt ist. Das Paket **530** weist immer

noch die Empfangs- und Senderadressen des Datenpaketes aus, aber der Rest des Paketes ist chiffriert und ggf. komprimiert.

[0040] Im Anschluss an die Verarbeitung durch die abgebende VPN-Einheit wird das Datenpaket über das Internet zu **550** übertragen, wobei die Empfangs- und Senderinformationen den zugeordneten Routern des Internet den Weg weisen, den das Paket letztlich nehmen sollte, um seinen Bestimmungsort zu erreichen. Das Paket taucht am Rand des Zielstandorts als Datenpaket **540** aus dem Internet auf und ist im Wesentlichen identisch mit dem Datenpaket **530**. Das Paket wird von der entgegennehmenden VPN-Einheit **550** "rückverarbeitet", die das ursprüngliche Paket in seiner Form **560** wiederherstellt, um es über den dem Empfangsstandort zugeordneten Router am Bestimmungsort **570** an den letzten Bestimmungsort zu liefern.

[0041] Wie oben beschrieben wurde, unterstützt die Lösung der vorliegenden Erfindung für virtuelle Privatnetze nicht nur eine optionale Komprimierung von Datenpaketen, sondern auch Chiffrierungs- und Beglaubigungstechniken. Ein hervortretender Standard für Schlüsselverwaltung in Verbindung mit Internetprotokoll-Datenübertragungen mit Beglaubigung wird als einfache Schlüsselverwaltung für Internetprotokolle (SKIP) bezeichnet und ist in dem auf Sun Microsystems, Inc., Mountain View, CA übertragenen US-Patent 5,588,060 beschrieben. Beglaubigte Datenübertragungen unter Verwendung von SKIP unterstützen ein Datenübertragungsverfahren, auf das als Tunnelmodus Bezug genommen wird. Die oben beschriebene Datenübertragung im Hinblick auf Fig. 5 stellt ein Transportbetriebsverfahren dar, in dem die Daten- und Senderadressen freigelegt sind, wenn das Datenpaket das Internet durchläuft. Im Tunnelmodus kann eine zusätzliche Sicherheitsmaßnahme vorgesehen sein, bei der das gesamte Datenpaket in ein anderes Paket eingekapselt wird, das die Sender- und Empfangsadressen nur für die VPN-Einheiten ausweist. Dies hält die letzten Sender- und Empfangsadressen unterwegs geheim.

[0042] Fig. 6 stellt die Lebensdauer eines Datenpaketes dar, das von einem Sender **600** unter Verwendung des Tunnelmodus zu einem Bestimmungsort **670** übertragen wird. In diesem Betriebsmodus wird das Datenpaket **610** durch eine abgebende VPN-Einheit **620** verarbeitet, die ein resultierendes Paket **630** erzeugt. Das resultierende Paket **630** chiffriert und komprimiert (ggf.) nicht nur die Datennutzlast des Paketes, sondern auch die Empfangs- und Senderadressen der Endstationen. Das eingekapselte Paket wird dann mit einer zusätzlichen Anfangskennung versehen, die ausweist, dass der Sender des Paketes die abgebende VPN-Einheit **620** ist und dass der Bestimmungsort die annehmende VPN-Einheit **650** ist. Demnach ist das Paket **640**, das aus dem Internet auftaucht, im Hinblick auf seine Sender- und Adressinformationen sowie die eingekapselte Nutzlast identisch mit dem Paket **630**. Das Paket wird von der annehmenden VPN-Einheit **650** zerlegt, um das ursprüngliche Datenpaket bei **660** zur Lieferung an den Bestimmungsort **670** zu rekonstruieren.

[0043] Die Gesamtarchitektur der vorliegenden Erfindung ist widerstandsfähig. Sie gestattet Endbenutzern die Annehmlichkeit, dass ihre ganz persönliche Datenfernübertragung über einen öffentlichen Netzraum wie das Internet vonstatten geht. Die Architektur der vorliegenden Erfindung ermöglicht ferner die Implementierung einer breiten Vielfalt von Komprimierungs-, Chiffrierungs- und Beglaubigungstechnologien, solange die VPN-Einheiten an jedem Ende der Transaktion die zugeordneten Protokolle unterstützen. Die vorliegende Erfindung ist ferner zur Zusammenarbeit mit herkömmlichen Internetsicherheitstechniken wie Firmen-Firewalls geeignet. Eine Firewall könnte in Reihe geschaltet mit der VPN-Einheit an einem gegebenen Standort in Betrieb sein oder intelligent in einem Einzelkasten mit der VPN-Einheit konfiguriert sein, um parallele Firewall- und VPN-Einheit-Sicherheitsfunktionen bereitzustellen.

Architektur für eine virtuelle Privatnetzeinheit

[0044] Die obige Erörterung bezieht sich auf die Funktionalität zur Realisierung virtueller Privatnetze. Es wird nun eine Hardware-Architektur und Realisierung für eine virtuelle Privatnetzeinheit in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung beschrieben. Es wird nun auf Fig. 7 Bezug genommen, wo ein allgemeines Blockdiagramm für eine virtuelle Privatnetzeinheit **700** dargestellt ist. Die allgemeine Architektur der VPN-Einheit **700** ist im Wesentlichen die einer maßgeschneiderten Personalcomputer-(PC-) Geräte-Architektur. Der Gesamtbetrieb der VPN-Einheit **700** wird durch eine zentrale Verarbeitungseinheit (CPU) **705** gesteuert, die zur Kommunikation mit den anderen Komponenten der Vorrichtung über einen Gerätebus **710** angeschlossen ist. In der für die VPN-Einheit **700** dargestellten allgemeinen Architektur ist die Speichervorrichtung **720** ferner als auf dem Gerätebus **710** befindlich dargestellt. Der Durchschnittsfachmann wird selbstverständlich erkennen, dass verschiedene Speicherkonfigurationen realisiert werden können, von denen einige einen reservierten Speicherbus für einen Durchsatz mit höherer Geschwindigkeit an die Speichervorrichtung **720** einschließen können.

[0045] Die VPN-Einheit **700** ist als Zwischenbaustein zwischen dem privaten Ortsnetz eines Standorts und dem Internet oder anderen öffentlichen Netzraum ausgelegt. Demzufolge ist die VPN-Einheit **700** so dargestellt, dass sie eine Ein-Ausgabe-Steuereinheit **730** zum Anschluss der VPN-Einheit **700** an

das Internet oder anderen öffentlichen Netzraum aufweist. In ähnlicher Weise ist eine Ein-Ausgabe-Steuereinheit **740** zum Anschluss der VPN-Einheit **700** an den Randrouter des Standorts vorgesehen. In Übereinstimmung mit den oben beschriebenen Funktionsvoraussetzungen befindet sich die VPN-Einheit **700** zwischen dem Router des Standorts und dem Internet. In dieser Ausführung ist die Ein-Ausgabe-Steuereinheit **740** für Datenpaketübertragungen zwischen dem Router für den Standort und der VPN-Einheit **700** verantwortlich. In einer alternativen Ausführungsform der vorliegenden Erfindung kann die VPN-Einheit **700** zwischen dem privaten Ortsnetz eines Standorts und seinem Router angeordnet sein, in welchem Fall die Ein-Ausgabe-Steuereinheit **730** für Datenpaketübertragungen zwischen der VPN-Einheit **700** und dem Router verantwortlich wäre, während die Ein-Ausgabe-Steuereinheit **740** gewissermaßen die Schnittstelle der VPN-Einheit zu dem privaten Ortsnetz wäre. In dieser alternativen Ausführungsform müssten Datenpaketübertragungen wahrscheinlich eher in Übereinstimmung mit dem Netzprotokollstandard des privaten Ortsnetzes als mit den oben beschriebenen IP-Übertragungen des öffentlichen Netzraums gehandhabt werden. In jedem Fall stellt die allgemeine Architektur für die VPN-Einheit **700** dar, dass die zwei Ein-Ausgabe-Steuereinheiten **730** und **740** zur Kommunikation über den Gerätebus **710** durch eine Ein-Ausgabe-Steuerlogik **750** angeschlossen sind. In Übereinstimmung mit dieser Architektur ist die Ein-Ausgabe-Steuerlogik **750** dafür verantwortlich, über den Zugang ankommender und abgehender Datenpakete zu dem Gerätebus zu entscheiden und den notwendigen Durchsatz für die Datenverbindungen zu gewährleisten.

[0046] Wie bereits beschrieben, erfolgt bei Erhalt eines Datenpaketes an der VPN-Einheit **700**, ob abgehend oder eingehend, eine Bestimmung durch Prüfen des Datenkopfes des Datenpaketes dahingehend, ob sowohl die Ursprungs- als auch die Empfangsadresse Mitglieder derselben VPN-Gruppe repräsentieren oder nicht. Bei einer Ausführungsform erfordert die Bestimmung die Abfrage einer Nachschlagetabelle, welche die Identitäten der verschiedenen, von der VPN-Einheit **700** verwalteten VPN-Gruppen sowie der Gruppenmitglieder und der verschiedenen Verarbeitungsparameter für Datenpakete pflegt, die zwischen Gruppenmitgliedern ausgetauscht werden. In Übereinstimmung mit der allgemeinen Architektur der VPN-Einheit **700** kann diese Abfrage von der CPU **705** mit Bezug auf Nachschlagetabellen gehandhabt werden, die in der Speichervorrichtung **720** unterhalten würden.

[0047] Für Datenpakete, die als zwischen Mitgliedern einer unterstützten VPN-Gruppe gesendete Pakete zu verarbeiten sind, ist beschrieben worden, dass für solche Daten Komprimierungs- und Dekomprimierungsfunktionen sowie Chiffrierungs- und Dechiffrierungsfunktionen durchgeführt werden müssen. Demzufolge schließt die Architektur der VPN-Einheit **700** ein Komprimierungsmodul **760** ein, das zur Kommunikation mit dem Rest des Gerätes über den Gerätebus **710** angeschlossen ist, sowie ein Chiffrierungsmodul **770**, das gleichermaßen an den Gerätebus **710** angeschlossen ist. Bei Hilfsfunktionen wie die oben beschriebenen verschiedenen Schlüsselverwaltungsprotokolle, die zur Generierung von Paket-Einkapselungsdatenköpfen führen, kann die Verarbeitung von der CPU **705** ausgeführt werden, wobei Pakete in der CPU **705** oder an spezifizierten Speicherstellen in der Speichervorrichtung **720** zusammengesetzt werden. Alternativ kann die Logik in die VPN-Einheit **700** integriert sein, die speziell zur Unterstützung solcher Schlüsselverwaltungsprotokolle oder anderer Paketverarbeitungsoperationen ausgelegt ist.

[0048] Schließlich ist in der Architektur der VPN-Einheit **700** gezeigt, dass optionale Ein-Ausgabe-Vorrichtungen **780** über die Ein-Ausgabe-Steuerlogik **790** mit der VPN-Einheit **700** verbunden sein können. Dies kann die Leitung der Einheit entweder durch Zulassen des direkten Tastaturzugriffs zur Steuerung des Prozessors erleichtern oder einen Verbindungsweg für andere Kommunikationseinrichtungen bereitstellen, die vielleicht mit der VPN-Einheit **700** kommunizieren müssen.

[0049] Es wird nun auf Fig. 8 Bezug genommen, wo ein detaillierteres Blockdiagramm für eine Realisierung einer VPN-Einheit in Übereinstimmung mit einer Ausführungsform der vorliegenden Erfindung dargestellt ist. In der realisierten Ausführungsform der VPN-Einheit **800** ist eine Architektur offenbart, die durch den Mikroprozessor **805**, einen Intel **486** DX4 mit 100 MHz, gesteuert wird. Der Gerätebus für diese Konfiguration ist der VSIA-Bus **810**, an den die anderen Komponenten des Gerätes angeschlossen sind. Die Speichervorrichtung wird in diesem Fall von mehreren Modulen eines dynamischen Zwischenspeichers (DRAM) **820** beliefert. In Übereinstimmung mit dieser realisierten Ausführungsform ist zum Steuern des Gesamtbetriebs der Vorrichtung bei **825** eine PC-Chipsatzausführung von Opti Corporation vorgesehen. Der Opti-Chipsatz sowie die Bereitstellung einer Gerätesteuereinheit-Funktionalität für den Mikroprozessor **486** DX4 können ferner zur Bereitstellung einer Schnittstelle mit einem optionalen ISA-Bus **828** verwendet werden, mit dem andere periphere Geräte an die Vorrichtung angeschlossen werden können.

[0050] In der realisierten VPN-Einheit **800** sind die Ein-Ausgabe-Anschlüsse zum öffentlichen Netzraum **830** durch eine Reihe von Multiprotokoll-Sender-Empfängern mit einem 25er Datenbusstecker vorgesehen. In ähnlicher Weise sind die Anschlüsse für die Privatnetzseite der Einheit durch zusätzliche Multiprotokoll-Sender-Empfänger und einen zusätzli-

chen 25er Datenbusstecker vorgesehen. Die Ein-Ausgabe-Anschlüsse an das öffentliche und private Netz werden durch einen Doppelanschluss SCC **845** gehandhabt, der eine Vielzahl von Eingabe- und Ausgabepuffern zur Übertragung und zum Empfang von Datenpaketen an die VPN-Einheit **800** einschließt. Die Datenpaket-Ein-Ausgabe-Steuereinheit ist durch die FPGA-Steuer- und Randlogik **850** an den VSIA-Bus **810** angeschlossen.

[0051] Das Komprimierungsmodul für die realisierte VPN-Einheit **800** wird durch eine Ausführung des STAC-Komprimierungsalgorithmus unter Verwendung des Komprimierungsmoduls **860** des STAC-Chips 9710 bereitgestellt, der mit einem reservierten Modul des SRAM **865** verbunden ist, um die Verarbeitung zu unterstützen. Schließlich wird das Chiffrierungsmodul in der realisierten Ausführungsform durch ein Blockchiffrierungsmodul DES **870** bereitgestellt, das entweder in einer serienmäßig produzierten besonderen integrierten Schaltungskonfiguration oder einer zum Betrieb in Übereinstimmung mit dem Betrieb der VPN-Einheit **800** ausgelegten Konfiguration realisiert ist. In Übereinstimmung mit einer alternativen Ausführungsform der vorliegenden Erfindung ist denkbar, dass das Komprimierungsmodul und das Chiffrierungsmodul durch auf dem Mikroprozessor **805** oder einer anderen Allzweck-Verarbeitungslogik laufende Software-Routinen gehandhabt werden könnten. Andere alternative Ausführungsformen können spätere Generationen von Mikroprozessoren verwenden, die mit höheren Geschwindigkeiten arbeiten und die Realisierung eines andersartigen Gerätebusses erfordern können, wie z. B. der aufkommende PCI-Bus-Standard. Der Durchschnittsfachmann wird alternative und verschiedene Ausführungsformen erkennen, die so gestaltet werden können, dass sie sich für einen bestimmten Zweck eignen.

[0052] Es wurde also ein Protokoll und eine Architektur zur Einrichtung virtueller Privatnetze für die Benutzung eines öffentlichen Netzraums für eine sichere Privatnetz-Datenfernübertragung beschrieben. Obwohl die vorliegende Erfindung im Hinblick auf bestimmte beispielhafte und realisierte Ausführungsformen beschrieben wurde, sollte verständlich sein, dass der Durchschnittsfachmann verschiedene Alternativen zur vorliegenden Erfindung leicht einschätzen kann. Demgemäß sollte der Schutzbereich der vorliegenden Erfindung an den Ausdrücken der Ansprüche gemessen werden.

Patentansprüche

1. Virtuelle Privatnetzeinheit zur Bereitstellung von gesicherter Datenfernübertragung zwischen Mitgliedern einer virtuellen Privatnetzgruppe, umfassend:
– eine Ein-Ausgabe-(I/O-)Schaltung (**730**, **740**) zum Empfangen und Übertragen von Datenpaketen zwischen den Mitgliedern (**201**, **202**, **203**, **211**, **212**, **213**, **331**, **332**, **150**, **155**) der virtuellen Privatnetzgruppe über ein öffentliches Netz (**250**);
– einen mit der I/O-Schaltung in Verbindung stehenden Systembus (**710**) zum Transportieren von Daten zwischen Komponenten der virtuellen Privatnetzeinheit;
– ein mit dem Systembus in Verbindung stehendes Komprimierungsmodul (**760**) zum Komprimieren abgehender Datenpakete und Dekomprimieren ankommender Datenpakete;
– ein mit dem Systembus in Verbindung stehendes Chiffrierungsmodul (**770**) zum Verschlüsseln abgehender Datenpakete und Entschlüsseln ankommender Datenpakete;
– eine mit dem Systembus in Verbindung stehende zentrale Verarbeitungseinheit (CPU) (**705**) zum Steuern der Verarbeitung von Datenpaketen durch die virtuelle Privatnetzeinheit; und
– einen mit dem Systembus in Verbindung stehenden Speicher (**720**),
dadurch gekennzeichnet, dass
– der Speicher (**720**) geeignet ist, eine Liste von Mitgliedern der virtuellen Privatnetzgruppe zu pflegen und vorbestimmte Parameter zu speichern; und
– die CPU (**705**) geeignet ist, auf der Basis der Mitgliederliste zwischen gerade zwischen Mitgliedern der virtuellen Privatnetzgruppe gesendeten Datenpaketen und zwischen einem Mitglied der virtuellen Privatnetzgruppe und einem Nichtmitglied der virtuellen Privatnetzgruppe gesendeten Datenpaketen zu unterscheiden, wobei,
– wenn die Datenpakete als zwischen zwei Mitgliedern der virtuellen Privatnetzgruppe gesendete Datenpakete bestimmt werden, diese dann auf den vorbestimmten Parametern basieren, von dem Chiffrierungsmodul (**770**) verschlüsselt und ggf. von dem Komprimierungsmodul (**760**) komprimiert werden, und
– wenn die Datenpakete als nicht zwischen zwei Mitgliedern der virtuellen Privatnetzgruppe gesendete Datenpakete bestimmt werden, diese als gewöhnlicher Internetverkehr behandelt werden.

2. Virtuelle Privatnetzeinheit gemäß Anspruch 1, wobei die virtuelle Privatnetzeinheit eine erste virtuelle Privatnetzeinheit ist, und ferner umfassend:
– einen ersten Computer (**211**) an einem ersten Standort, wobei der erste Computer eine erste Netzadresse aufweist;
– einen ersten Router (**242**), der mit dem ersten Standort verbunden ist, um von dem ersten Computer stammende Datenpakete über das Netz (**250**) zu leiten;
wobei die erste virtuelle Privatnetzeinheit (**252**) zwischen dem ersten Router und dem Netzwerk angeordnet ist und die erste virtuelle Privatnetzeinheit geeignet ist, einen Datenverkehr der virtuellen Privatnetzgruppe zu identifizieren und den Datenverkehr

durch Handhaben des Datenverkehrs zu sichern;
– einen zweiten Router (**244**), der mit einem zweiten Standort verbunden ist, um den zweiten Standort an das Netzwerk anzuschließen;
– eine zweite virtuelle Privatnetzeinheit (**254**), die vom Aufbau her mit der ersten virtuellen Privatnetzeinheit identisch ist, wobei die zweite virtuelle Privatnetzeinheit zwischen dem zweiten Router und dem Netzwerk zum Abfangen des für den zweiten Standort bestimmten Netzverkehrs, der zweiten virtuellen Privatnetzeinheit zum Erkennen des virtuellen Privatnetzgruppenverkehrs und zum Wiederherstellen ursprünglicher Paketdaten angeordnet ist; und
– einen zweiten Computer (**221**) an dem zweiten Standort, wobei der zweite Computer eine zweite Netzadresse zum Empfangen der Datenpakete aufweist.

3. Virtuelle Privatnetzeinheit gemäß Anspruch 1, wobei die virtuelle Privatnetzeinheit eine erste virtuelle Privatnetzeinheit ist, und ferner umfassend:
– einen ersten Computer (**211**) an einem ersten Standort, wobei der erste Computer eine erste Netzadresse aufweist;
– einen ersten Router (**242**), der mit dem ersten Standort verbunden ist, um von dem ersten Computer stammende Datenpakete über das Netz (**250**) zu leiten;
wobei die erste virtuelle Privatnetzeinheit (**252**) zwischen dem ersten Router (**242**) und dem ersten Computer (**211**) angeordnet ist und die erste virtuelle Privatnetzeinheit geeignet ist, einen Datenverkehr der virtuellen Privatnetzgruppe zu identifizieren, und den Datenverkehr durch Handhaben des Datenverkehrs sichert;
– einen zweiten Router (**244**), der mit einem zweiten Standort verbunden ist, um den zweiten Standort an das Netzwerk anzuschließen;
– einen zweiten Computer (**221**) an dem zweiten Standort, wobei der zweite Computer eine zweite Netzadresse zum Empfangen der Datenpakete aufweist; und
– eine zweite virtuelle Privatnetzeinheit (**254**), die vom Aufbau her mit der ersten virtuellen Privatnetzeinheit identisch ist, wobei die zweite virtuelle Privatnetzeinheit zwischen dem zweiten Router (**244**) und dem zweiten Computer (**221**) zum Abfangen des für den zweiten Standort bestimmten Netzverkehrs, der zweiten virtuellen Privatnetzeinheit zum Erkennen des virtuellen Privatnetzgruppenverkehrs und zum Wiederherstellen ursprünglicher Paketdaten angeordnet ist.

4. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei der Speicher (**720**) auch geeignet ist, Mitgliedern der virtuellen Privatnetzgruppe zugeordnete Übertragungsparameter zu speichern, und wobei die Übertragungsparameter diktieren, ob eine Datenpaketübertragung zu/von einem bestimmten Mitglied der virtuellen Privatnetzgruppe eine Komprimierung/Dekomprimierung und/oder Chiffrierung/Dechiffrierung erfordert.

5. Virtuelle Privatnetzeinheit gemäß Anspruch 4, wobei das Komprimierungsmodul (**760**) und das Chiffrierungsmodul (**770**) eine Schaltung oder Software zum Generieren und Bestätigen eines abgehenden bzw. ankommenden Datenpaketen zugeordneten Beglaubigungscodes einschließen.

6. Virtuelle Privatnetzeinheit gemäß Anspruch 5, wobei die Mitgliedern der virtuellen Privatnetzgruppe zugeordneten Übertragungsparameter auch spezifizieren, ob eine Beglaubigung der übermittelten Datenpakete, die zu/von dem zugehörigen Mitglied der virtuellen Privatnetzgruppe übertragen werden, erforderlich ist oder nicht.

7. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei das Netzwerk das Internet (**250**) ist.

8. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei die I/O-Schaltung umfasst:
– einen privaten I/O-Anschluss (**740**) zum Anschließen der virtuellen Privatnetzeinheit an das Privatnetz eines Standorts;
– einen öffentlichen I/O-Anschluss (**730**) zum Anschließen der virtuellen Privatnetzeinheit an das Netz (**250**); und
– eine I/O-Steuerlogik (**750**), die mit dem Systembus (**710**) in Verbindung steht und an den privaten und den öffentlichen I/O-Anschluss angeschlossen ist, um den Datenpaketfluss zwischen der virtuellen Privatnetzeinheit und Mitgliedern der virtuellen Privatnetzgruppe zu steuern.

9. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei die CPU (**705**) Kapselungsköpfe für abgehende Datenpakete in Übereinstimmung mit einem Schlüsselverwaltungsprotokoll generiert.

10. Virtuelle Privatnetzeinheit gemäß Anspruch 9, wobei das Schlüsselverwaltungsprotokoll die einfache Schlüsselverwaltung für Internetprotokolle (SKIP) einschließt.

11. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei das Komprimierungsmodul (**760**) und das Chiffrierungsmodul (**770**) eine Schaltung oder Software zur Durchführung von Blockchiffrierung oder Dreifach-Blockchiffrierung in Übereinstimmung mit den vorbestimmten Parametern einschließen.

12. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei das Komprimierungsmodul (**760**) und das Chiffrierungsmodul (**770**)

eine Schaltung oder Software zur Durchführung von LZW-Komprimierung einschließen.

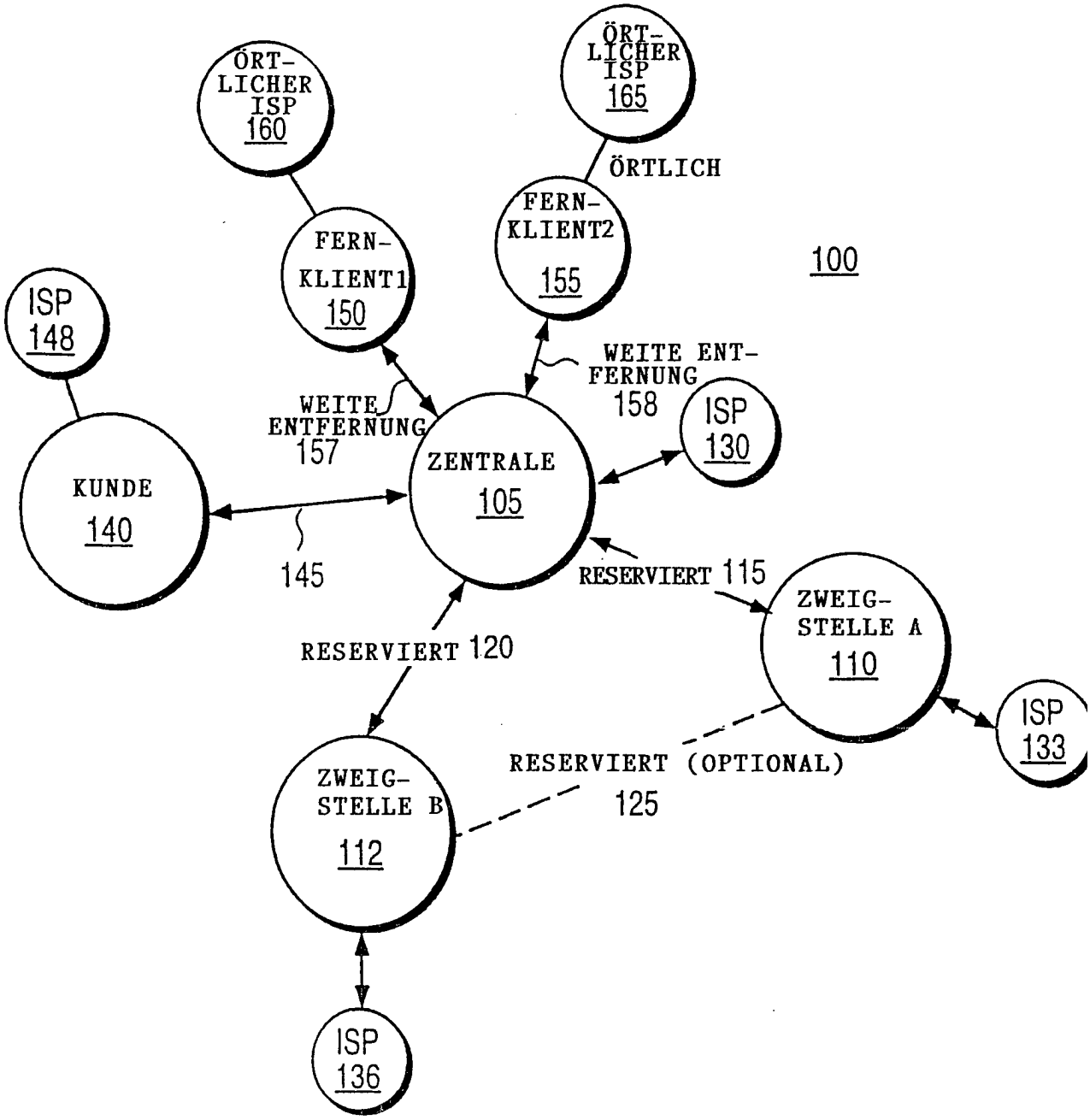
13. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei der Speicher (**720**) Nachschlagetabellen zur Identifizierung aller virtuellen Privatnetzgruppen und Mitglieder der Gruppen umfasst, wobei die Mitglieder jeweils durch eine Netzadresse identifiziert werden und eine einzige Netzadresse ein Mitglied als zu mehreren virtuellen Privatnetzgruppen gehörend identifizieren kann.

14. Virtuelle Privatnetzeinheit gemäß einem der vorhergehenden Ansprüche, wobei wenn die Datenpakete als gerade zwischen einem Mitglied der virtuellen Privatnetzgruppe und einem Nichtmitglied der virtuellen Privatnetzgruppe gesendete Datenpakete bestimmt werden, diese nicht komprimiert und nicht verschlüsselt werden.

Es folgen 7 Blatt Zeichnungen

Anhängende Zeichnungen

FIG. 1 (STAND DER TECHNIK)



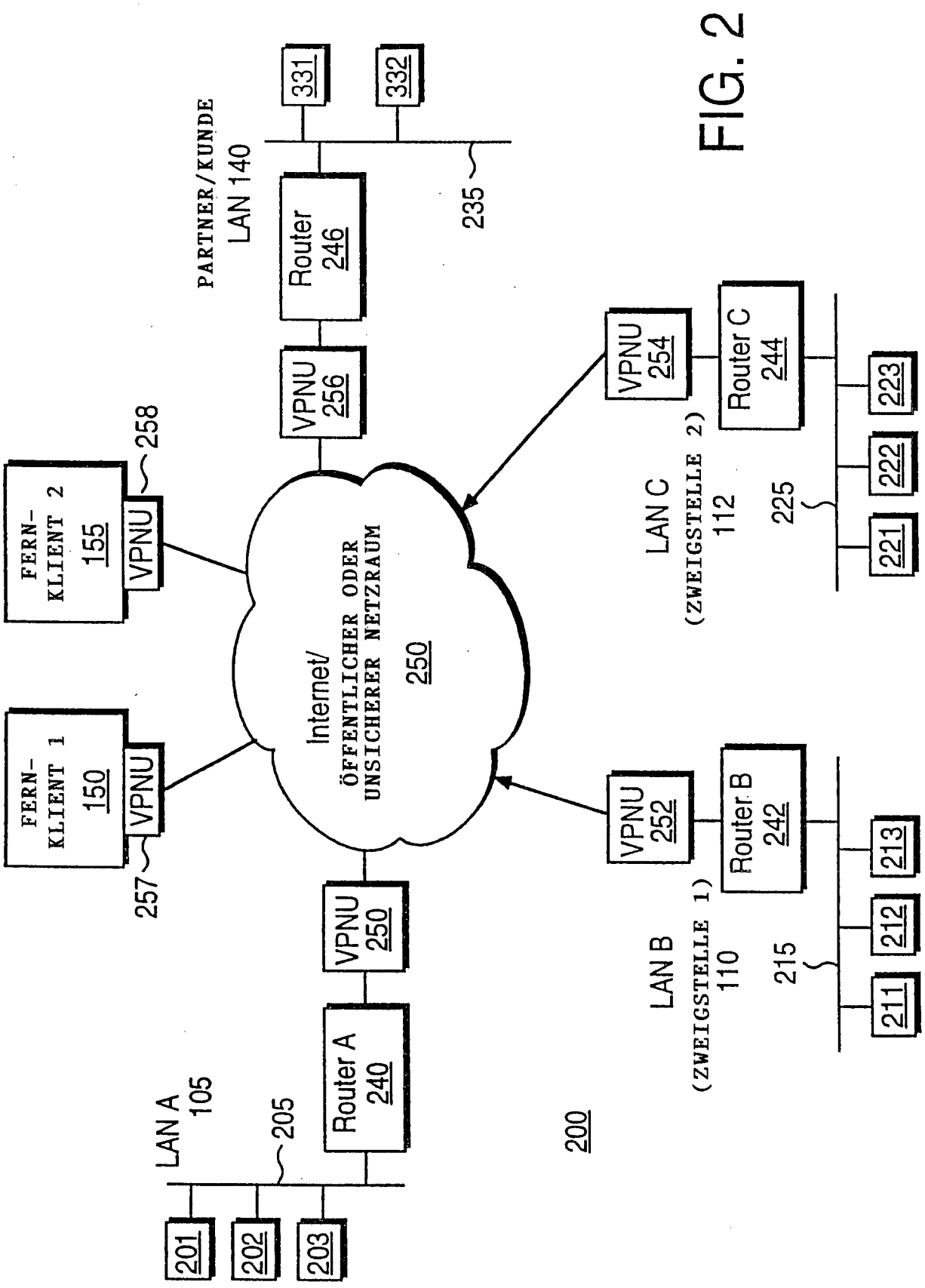

PARTNER/KUNDE
LAN 140
331
332
Router 246
235
VPNU 256
VPNU 254
Router C 244
LAN C
(ZWEIGSTELLE 2)
112
225
223
222
221
FERN-KLIENT 2
155
VPNU
258
FERN-KLIENT 1
150
VPNU
257
Internet/
ÖFFENTLICHER ODER
UNSICHERER NETZRAUM
250
VPNU 252
Router B 242
LAN B
(ZWEIGSTELLE 1)
110
215
213
212
211
VPNU 250
Router A 240
LAN A
105
205
201
202
203
200

FIG. 2

FIG. 3

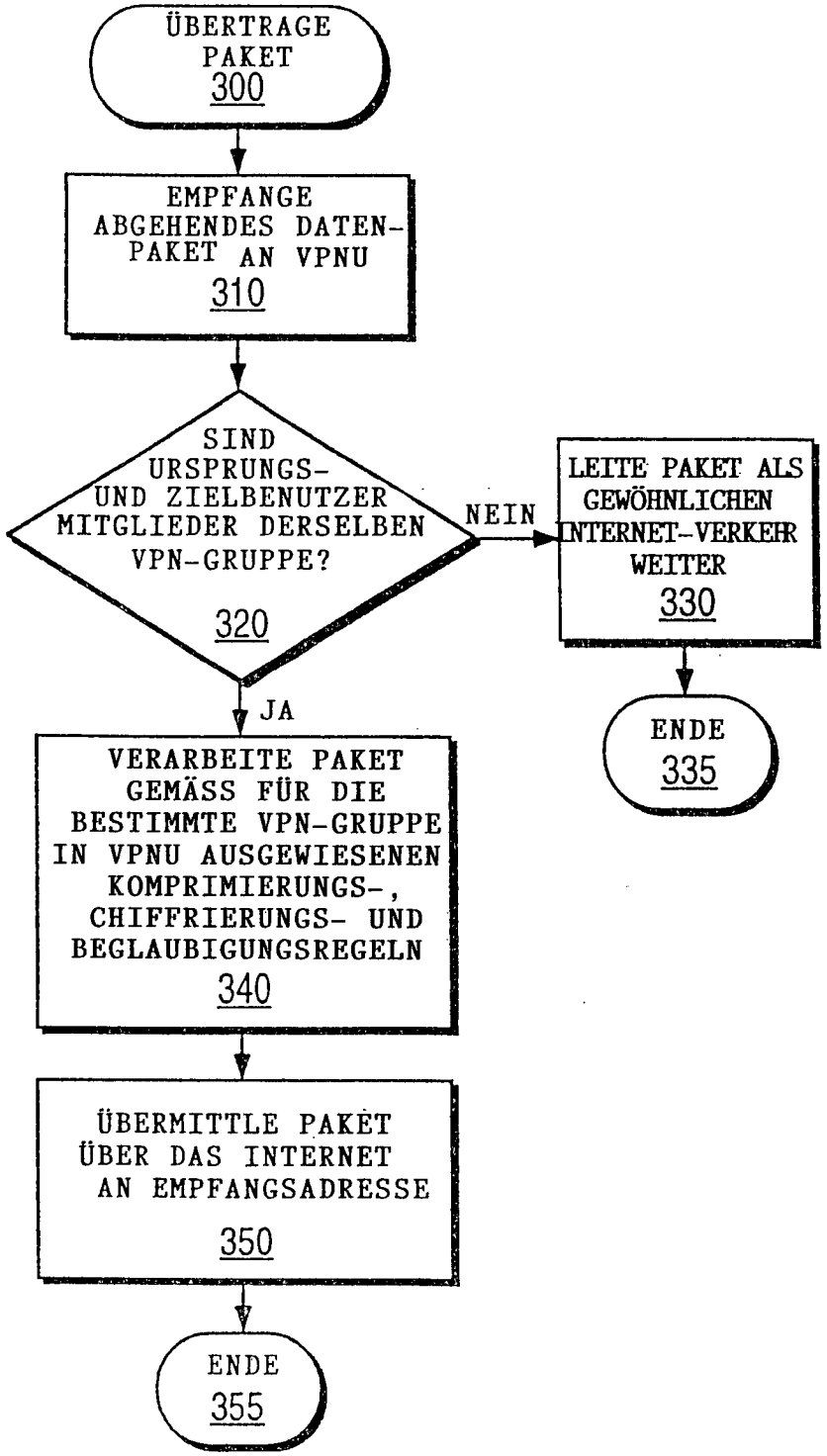

ÜBERTRAGE PAKET 300
EMPFANGE ABGEHENDES DATEN-PAKET AN VPNU 310
SIND URSPRUNGS- UND ZIELBENUTZER MITGLIEDER DERSELBEN VPN-GRUPPE? 320
NEIN
LEITE PAKET ALS GEWÖHNLICHEN INTERNET-VERKEHR WEITER 330
ENDE 335
JA
VERARBEITE PAKET GEMÄSS FÜR DIE BESTIMMTE VPN-GRUPPE IN VPNU AUSGEWIESENEN KOMPRIMIERUNGS-, CHIFFRIERUNGS- UND BEGLAUBIGUNGSREGELN 340
ÜBERMITTLE PAKET ÜBER DAS INTERNET AN EMPFANGSADRESSE 350
ENDE 355

FIG. 4

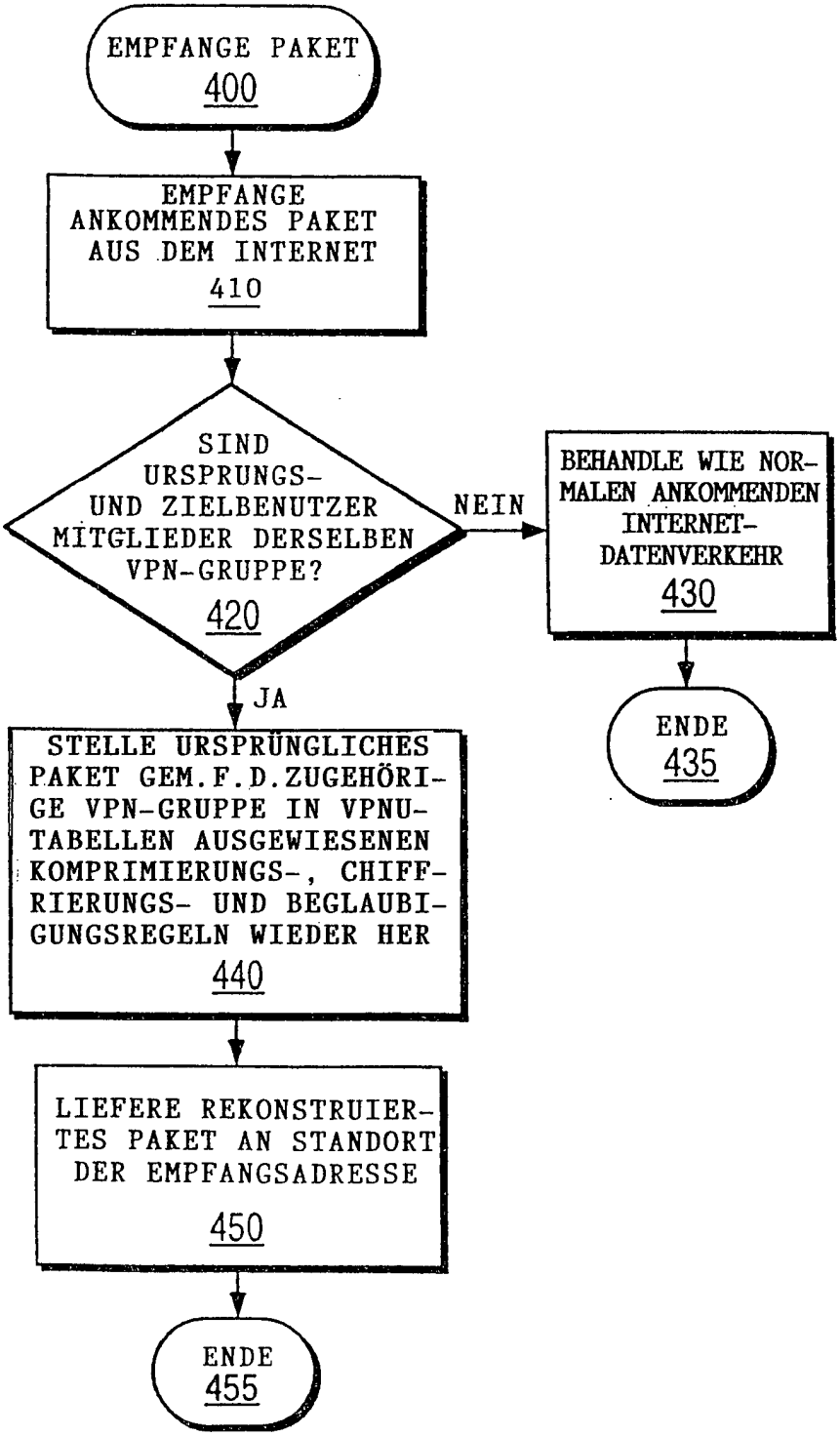

EMPFANGE PAKET
400
EMPFANGE ANKOMMENDES PAKET AUS DEM INTERNET
410
SIND URSPRUNGS- UND ZIELBENUTZER MITGLIEDER DERSELBEN VPN-GRUPPE?
420
NEIN
BEHANDLE WIE NORMALEN ANKOMMENDEN INTERNET-DATENVERKEHR
430
ENDE
435
JA
STELLE URSPRÜNGLICHES PAKET GEM. F. D. ZUGEHÖRIGE VPN-GRUPPE IN VPNU-TABELLEN AUSGEWIESENEN KOMPRIMIERUNGS-, CHIFFRIERUNGS- UND BEGLAUBIGUNGSREGELN WIEDER HER
440
LIEFERE REKONSTRUIERTES PAKET AN STANDORT DER EMPFANGSADRESSE
450
ENDE
455

FIG. 5

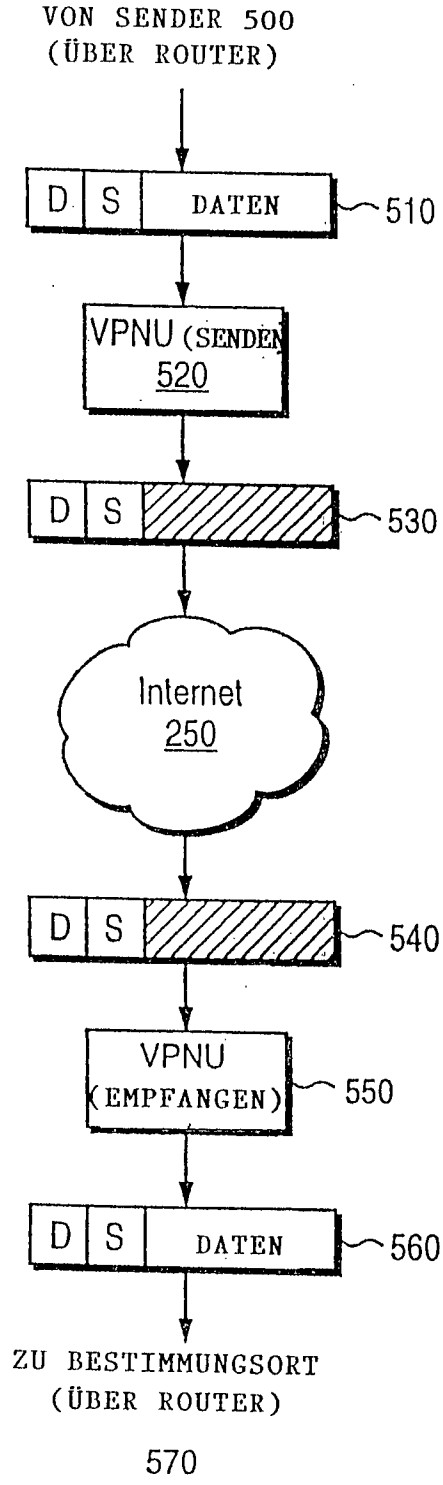
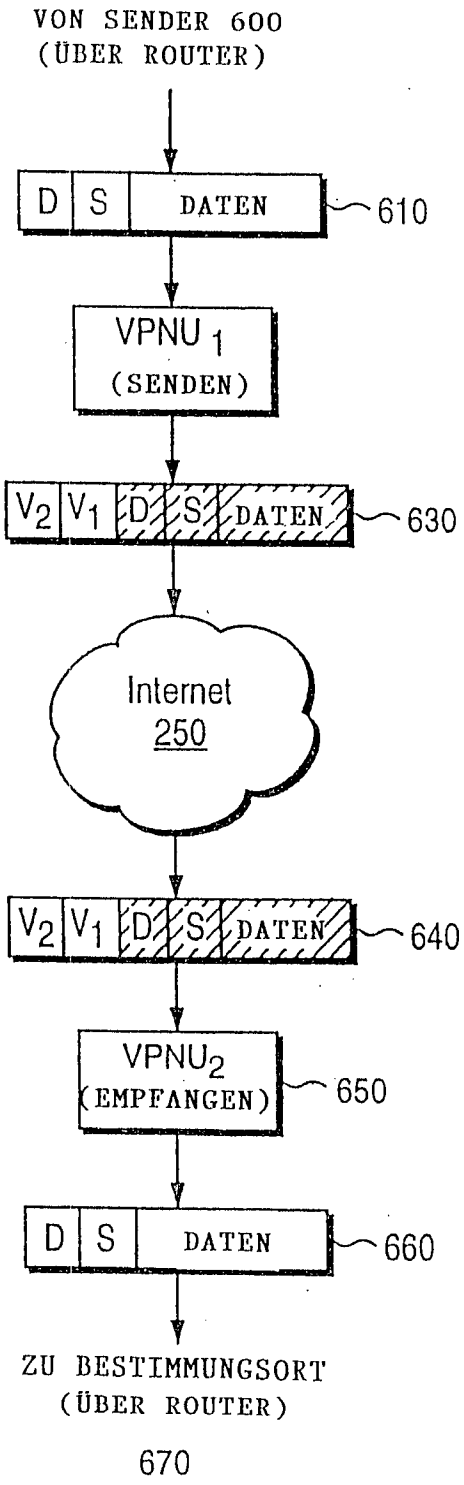

VON SENDER 500
(ÜBER ROUTER)
D
S
DATEN
510
VPNU (SENDEN
520
D
S
530
Internet
250
D
S
540
VPNU
(EMPFANGEN)
550
D
S
DATEN
560
ZU BESTIMMUNGSORT
(ÜBER ROUTER)
570

FIG. 6


VON SENDER 600
(ÜBER ROUTER)
D
S
DATEN
610
VPNU 1
(SENDEN)
V2
V1
D
S
DATEN
630
Internet
250
V2
V1
D
S
DATEN
640
VPNU2
(EMPFANGEN)
650
D
S
DATEN
660
ZU BESTIMMUNGSORT
(ÜBER ROUTER)
670

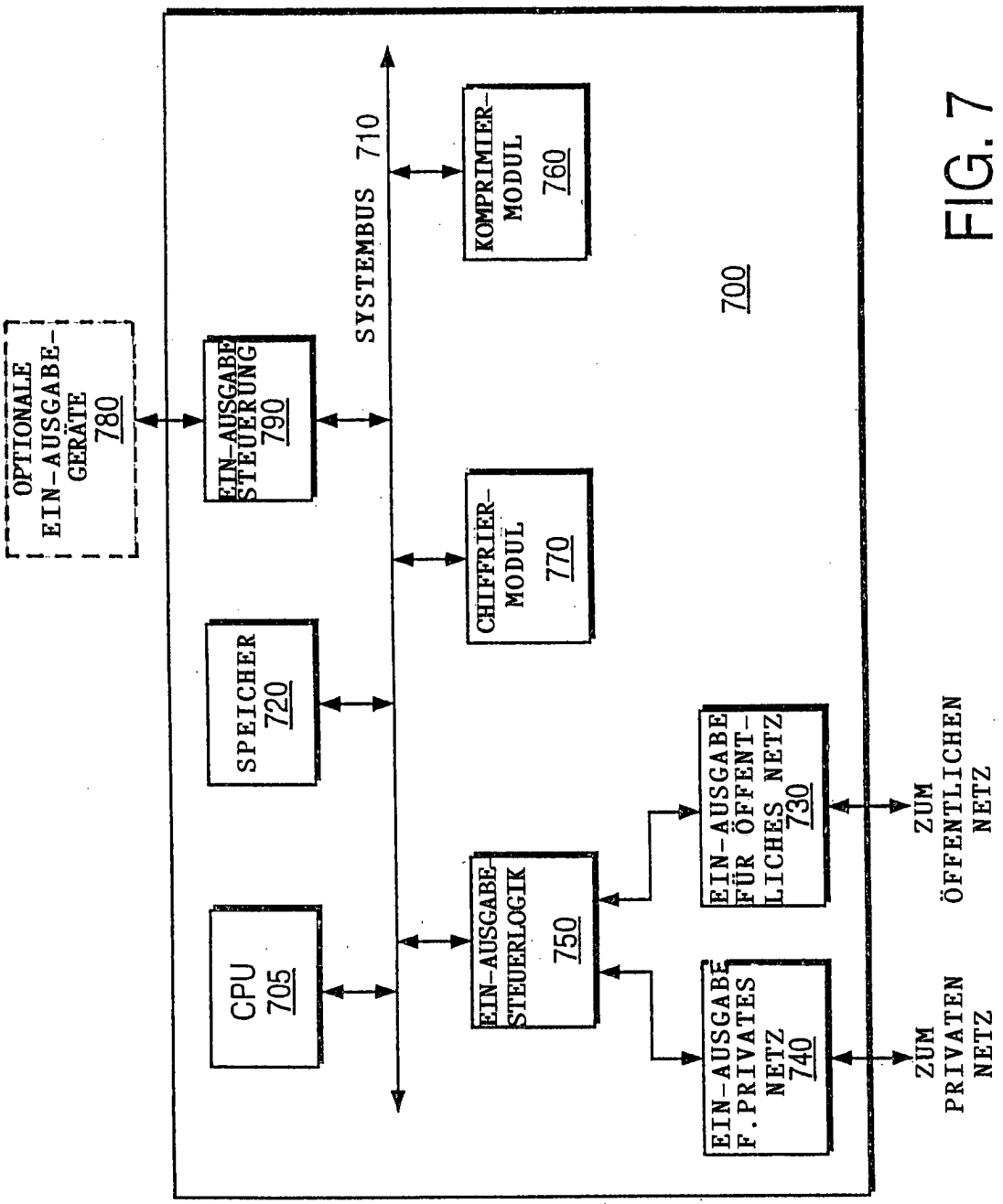

OPTIONALE EIN-AUSGABE-GERÄTE 780
EIN-AUSGABE STEUERUNG 790
SYSTEMBUS 710
KOMPRIMIER-MODUL 760
700
SPEICHER 720
CHIFFRIER-MODUL 770
CPU 705
EIN-AUSGABE-STEUERLOGIK 750
EIN-AUSGABE FÜR ÖFFENT-LICHES NETZ 730
EIN-AUSGABE F. PRIVATES NETZ 740
ZUM ÖFFENTLICHEN NETZ
ZUM PRIVATEN NETZ

FIG. 7

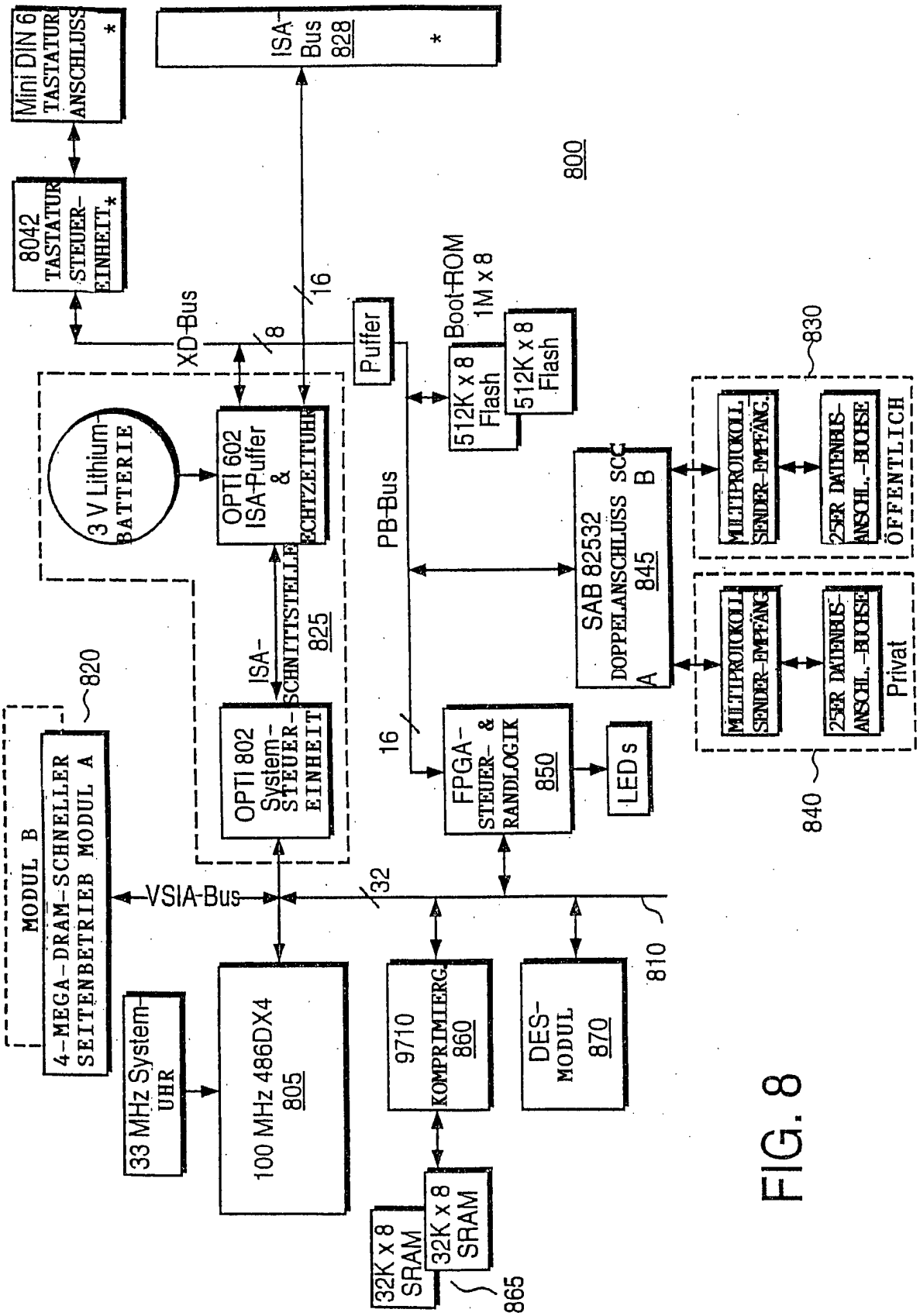

Mini DIN 6 TASTATUR ANSCHLUSS *
8042 TASTATUR STEUER-EINHEIT *
XD-Bus
8
16
ISA-Bus 828 *
800
Puffer
Boot-ROM 1M x 8
512K x 8 Flash
512K x 8 Flash
3 V Lithium-BATTERIE
OPTI 602 ISA-Puffer & ECHTZEITUHR
ISA-SCHNITTSTELLE 825
PB-Bus
SAB 82532 DOPPELANSCHLUSS SCC 845
A
B
MULTIPROTOKOLL SENDER-EMPFÄNG.
25ER DATENBUS-ANSCHL.-BUCHSE
ÖFFENTLICH
830
MULTIPROTOKOLL SENDER-EMPFÄNG.
25ER DATENBUS-ANSCHL.-BUCHSE
Privat
840
820
MODUL B
4-MEGA-DRAM-SCHNELLER SEITENBETRIEB MODUL A
OPTI 802 System-STEUER-EINHEIT
16
FPGA-STEUER- & RANDLOGIK 850
LED s
VSIA-Bus
32
810
33 MHz System-UHR
100 MHz 486DX4 805
9710 KOMPRIMIERG. 860
DES-MODUL 870
32K x 8 SRAM
32K x 8 SRAM
865

FIG. 8