US006055575A

United States Patent [19]

Paulsen et al.

[11] **Patent Number: 6,055,575**

[45] **Date of Patent: Apr. 25, 2000**

[54] **VIRTUAL PRIVATE NETWORK SYSTEM AND METHOD**

[75] Inventors: **Gaige B. Paulsen**, Great Falls; **Amanda Walker**, Reston, both of Va.

[73] Assignee: **Ascend Communications, Inc.**, Alameda, Calif.

[21] Appl. No.: **09/013,122**

[22] Filed: **Jan. 26, 1998**

Related U.S. Application Data

[60] Provisional application No. 60/035,215, Jan. 10, 1997.

[51] **Int. Cl.**[7] **G06F 13/00**

[52] **U.S. Cl.** **709/229**; 709/228; 709/226; 709/245

[58] **Field of Search** 709/245, 229, 709/228, 226; 380/23, 30

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,416,842	5/1995	Aziz	380/30
5,548,646	8/1996	Aziz et al.	380/23
5,550,984	8/1996	Gelb	709/245
5,835,726	11/1998	Shwed et al.	709/229
5,872,849	2/1999	Sudia	380/23

FOREIGN PATENT DOCUMENTS

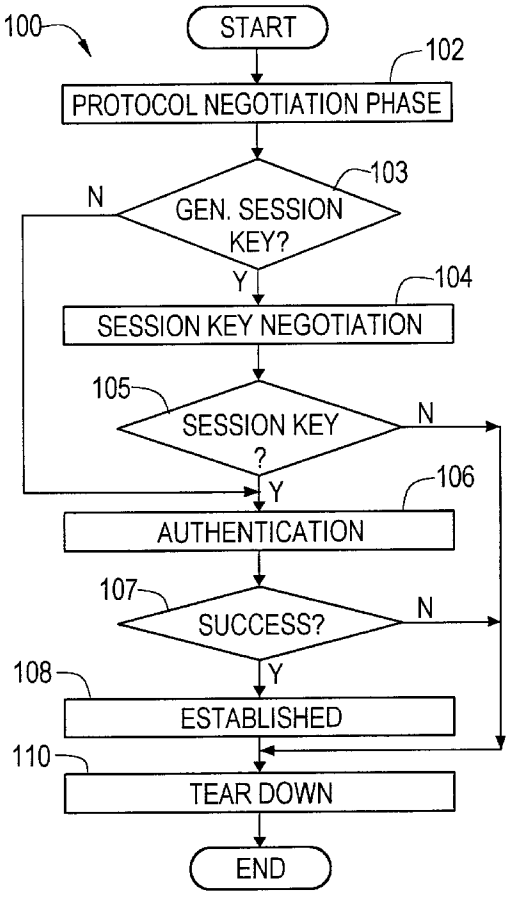
0739106A1	10/1996	European Pat. Off.	H04L 9/08

Primary Examiner—Ahmad F. Matar
Assistant Examiner—Philip B. Tran
Attorney, Agent, or Firm—Weingarten, Schurgin, Gagnebin & Hayes LLP

[57] **ABSTRACT**

A system and method for remote users to access a private network having a first communications protocol via a public network, such as any TCP/IP network having a second different communications protocol, in a secure manner so that the remote user appears to be connected directly to the private network and appears to be a node on that private network. A host connected to the private network may execute a host software application which establishes and provides a communications path for secure access of the remote client computer. An encrypted data stream may be communicated between the host and the client representing traffic and commands on the network.

28 Claims, 2 Drawing Sheets



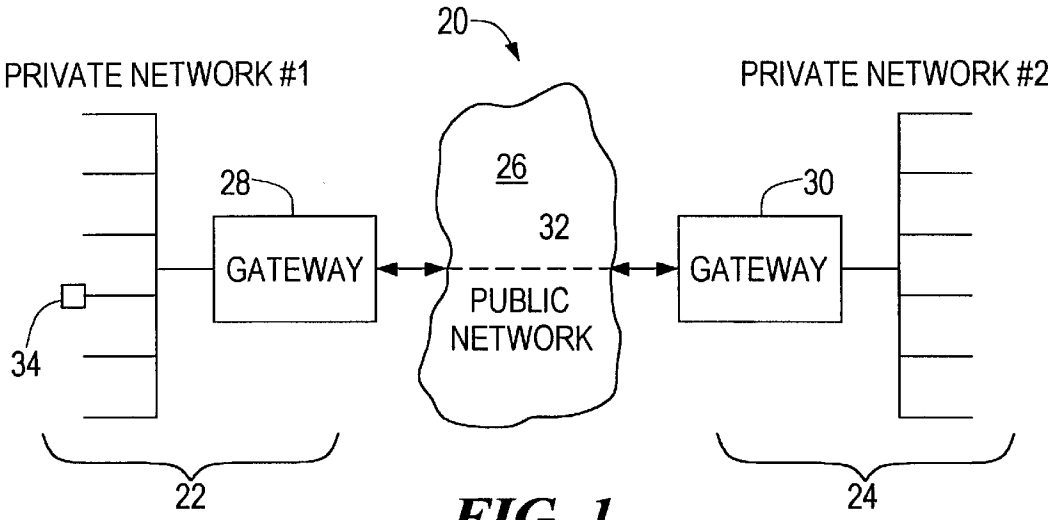


FIG. 1

PRIOR ART

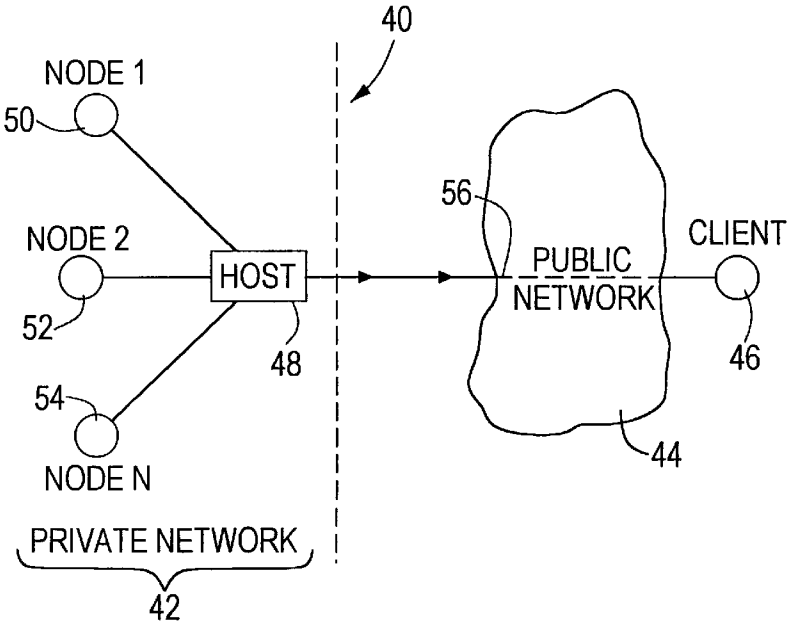


FIG. 2

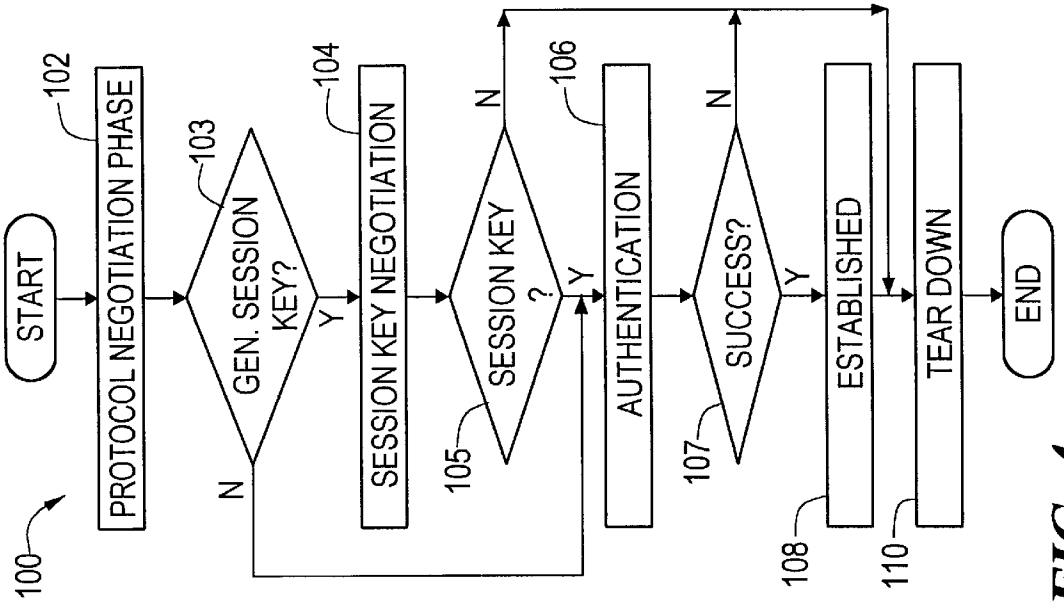


FIG. 4

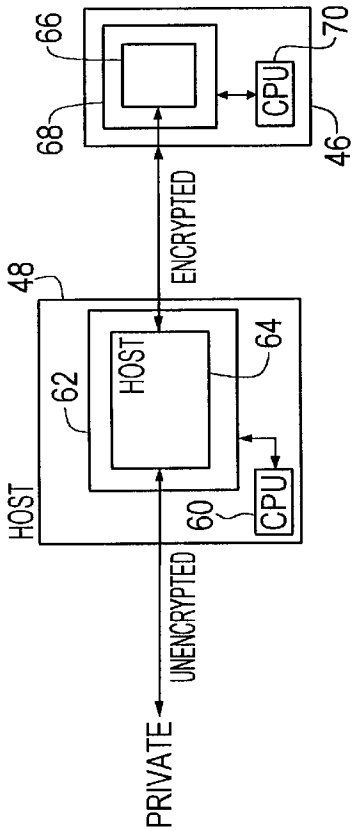


FIG. 3

VIRTUAL PRIVATE NETWORK SYSTEM AND METHOD

This application claims benefit of provisional application Ser. No. 60/035,215 filed Jan. 10, 1997.

BACKGROUND OF THE INVENTION

This invention relates generally to apparatus and methods for accessing computer networks and in particular to establishing a secure connection between a remote computer and a private computer network using a public computer network.

In the past, organizations and companies have used private (internal) computer data networks to connect its users to each other. These private networks are not accessible to the public and permit sensitive data to be transferred between users within the company. However, due to the increasing numbers of people who need access to the private computer data network and the disparate locations of these people, there are several disadvantages of these conventional private computer networks.

As the number of people in a company grows, the workforce becomes more dispersed among different locations and there are more employees who are mobile, such as salespeople who travel around a region of the United States. For example, some employees may telecommute which requires dial-up access to the private computer data network. The dispersed workforce and the mobile workforce make a private computer data network unmanageable because this mobility requires at least two network connections for each user. In addition, since cellular telephone access has also become more available, additional connections to the network for this access is needed. In addition, full-time telecommuters dramatically increase the number of permanent "remote offices" a company must interconnect which further complicates the private computer data network administration and topology. In addition, as companies increase in size, due to acquisitions, mergers and expansion, the private computer data network must support more remote offices and more network nodes. Thus, as a organization expands, the private computer data network of the organization becomes unwieldy and unmanageable.

Recently, it has become necessary and desirable to permit employees of the company to interact "on-line" with customers and suppliers. This function adds a new dimension of complexity to the private computer data network since multiple private computer data networks must be interfaced together in a delicate balance of integration while maintaining some isolation due to security concerns. The individual networks that are being integrated together typically use different data transfer protocols, different software applications, different data carriers and different network management systems. Thus, interfacing these private computer data networks is a major challenge.

There is also a desire to consolidate and simplify the user interface to the computer network as well as to the software applications being executed by the computer network since it is often difficult to keep on top of each new software application. Thus, the costs of implementing and maintaining a private computer data network is high and is expected to increase in the future as the factors set forth above continue to drive up the costs of the private computer data networks. These high costs are compounded by the high costs for long distance telephone charges for leased lines and

data networks also further increases the costs to manage the private computer data networks. In addition, software applications which execute over the private network require separate backup equipment which further complicates the topology and increases the cost of the private computer data network. Thus, the costs and complexity of these private computer data networks are continuing to spiral upwards and there is no foreseeable end in sight.

A typical private computer data network may be used by a organization for some of its communications needs and may carry exclusively data traffic or a mix of voice/video and data traffic. The private computer data network may be constructed with a variety of wide area network (WAN) services that often use the public switched telephone network (PSTN) as a communications medium. A typical network may use high speed leased lines that carry voice, facsimile, video and data traffic between major facilities. These leased lines may include integrated services digital network (ISDN) lines or conventional T1 telephone lines. Because these leased lines are point-to-point connections, a mesh topology is necessary to interconnect multiple facilities. In addition, each leased line must be dedicated to a particular interconnection. A remote office may use switched services over the PSTN, such as ISDN or frame relay. For individual mobile employees, an analog modem may be the best solution for connection to the private computer data network. The private computer data network with all of these different connections, therefore, is very expensive to implement and maintain for the reasons set forth above.

A virtual private network (VPN), on the other hand, may offer the same capabilities as a private computer data network, but at a fraction of the cost. A virtual private network is a private data network that uses a public data network, instead of leased lines, to carry all of the traffic. The most accessible and less expensive public data network currently is the Internet which can be accessed worldwide with a computer and a modem. An Internet-based virtual private network (VPN) is virtual because although the Internet is freely accessible to the public, the Internet appears to the organization to be a dedicated private network. In order to accomplish this, the data traffic for the organization may be encrypted at the sender's end and then decrypted at the receiver's end so that other users of the public network can intercept the data traffic, but cannot read it due to the encryption.

A VPN can replace an existing private data network, supplement a private data network by helping relieve the load on the private data network, handle new software applications without disturbing the existing private data network or permit new locations to be easily added to the network. A typical VPN connects one or more private networks together through the Internet in which the network on each side of the Internet has a gateway and a leased line connecting the network to the Internet. In these typical VPNs, the same protocol for each private network, such as TCP/IP, is used which makes it easier to communicate data between the two networks. To create the VPN, a secure communications path between the two gateways is formed so that the two private networks may communicate with each other. In this configuration, however, each network is aware that the other network is at some other location and is connected via a router. As an example, if a company has a central private network in California and a remote office in Hong Kong, these two private networks may be connected via the VPN which reduces long distance telephone call

California, the individual must incur long distance telephone charges or, if there is a remote office in Hong Kong, then the entire private network must be connected via the VPN to the California private network to communicate data. In addition, with the conventional VPN described, the individual in Hong Kong is aware that he is connected to the Hong Kong network which is in turn connected, via the gateway and the VPN, to the network in California so that the person in Hong Kong cannot, for example, easily use the network resources of the California network, such as a printer.

Thus, a conventional VPN requires the expense of a leased line and a gateway at each end of the VPN and cannot adequately address the needs of a individual who needs access to the private network. In addition, these conventional VPNs cannot easily connect networks which have different networking protocols. In addition, these conventional VPNs cannot be easily used for connecting an individual who needs remote access to the private network since the entire network with a gateway is needed.

Thus, the invention provides a virtual private network (VPN) which avoids these and other problems with conventional VPNs and it is to this end that the invention is directed.

SUMMARY OF THE INVENTION

In accordance with the invention, a virtual private network system is provided which connects a private data network and a remote client which does not require expensive leased lines or gateways to establish a secure communications path. The system also permits an individual to access the private data network without incurring any long distance telephone charges. In addition, the system permits a private data network and remote client that use one communications protocol to communicate with each other over a public data network that uses a different communications protocol. The system also permits an individual to easily connect to the private date network without a remote private network and the individual appears to be a node on the private network, once connected, so that the individual may access any resources on the private data network.

In accordance with the invention, a system and method for forming a communications path between a public access network and a private access network where the two networks have substantially incompatible transmission protocols is provided. The method comprises establishing a secure communications path over the public access network between a host computer connected to the private network and a remote client computer, encrypting data and commands of the host computer and the client computer, and formatting the encrypted data and commands into a format compatible for transmission over the public access network. The formatted data and commands are then transmitted over the public access network. Once the formatted data and commands has reached its destination, it is decrypted to establish the client computer as a virtual node on the private network. In accordance with another aspect of the invention, a data structure for communicating data for a private data network having a first communications protocol over a public access network having a second communications protocol is provided.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a conventional virtual private network;

FIG. **3** is a block diagram illustrating more details of the host computer of FIG. **1**; and

FIG. **4** is a flowchart illustrating a method for establishing a virtual private network and communicating secure data over the virtual private network in accordance with the invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

The invention is particularly applicable to a system and method for providing a virtual private network which permits remote users to access a private network, such as an AppleTalk network, via a public TCP/IP network, such as the Internet, in a secure manner as if the remote user was one of the nodes on that private network. It is in this context that the invention will be described. It will be appreciated, however, that the system and method in accordance with the invention has greater utility. Before describing the invention, a brief description of a conventional virtual private network (VPN) will be provided.

FIG. **1** is a block diagram illustrating a conventional virtual private network (VPN) **20**. The VPN includes a first private network **22** and a second private network **24** connected together through a public computer network **26**, such as the Internet. The communications protocols for the first and second private networks as well as the public network may be the standard Transmission Control Protocol/Internet Protocol (TCP/IP). Thus, the communications protocols for the private networks are the same as the public network. Each private network **22**, **24** includes a gateway **28**, **30** which interfaces between the respective private network and the public network. Each gateway encrypts data traffic from the private network which is going to enter the public network and decrypts encrypted data received from the public network. In normal operation, a secure communications path **32**, referred to as a tunnel, is formed over the public network that connects the first and second private networks through the respective gateways. The combination of the two private networks and the tunnel over the public network forms the virtual private network (VPN). The VPN is virtual since it is actually using a public network for the connection, but due to the encryption both private networks believe that they have a private network over which data may be sent. For example, a node **34** of the first private network **22** may send data which is encrypted by the gateway **28** through the tunnel **32**, and the data is received by the second gateway **30** which decrypts the data and routes it to the appropriate node in the second private network. This conventional VPN, however, does not adequately provide an individual remote user with a system for remotely accessing the private network because the conventional VPN connects two networks with a tunnel and would require the individual to be connected to one of the private networks to utilize the VPN. In addition, this conventional VPN does not connect a remote individual directly to the private network so that a remote user with a VPN connection cannot directly access resources, such as a printer, connected to the private network. This conventional system also does not handle computer networks which have different communications protocols. Now, the virtual private network system in accordance with the invention will be described which overcomes these problems with a conventional VPN.

FIG. **2** is a block diagram illustrating a virtual private network (VPN) **40** in accordance with the invention. The

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.