FILING RECEIPT

OC000000004982118

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: ASSISTANT SECRETARY AND
COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
60/177,972	01/25/2000		150	095962	_		

KILPATRICK STOCKTON, LLP
1100 PEACHTREE STREET
SUITE 2800
ATLANTA, GA 30309

Date Mailed: 03/06/2000

Receipt is acknowledged of this provisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Customer Service Center. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Frank R. Koperda, Suwanee, GA ;

Continuing Data as Claimed by Applicant

Foreign Applications

Foreign filing license granted on 03/03/2000

Title

METHOD TO PROVIDE VIRTUAL FIREWALL FUNCTIONALITY FROM A REMOTE SERVICE PROVIDER

Preliminary Class

Data entry by : SNEED, LISA **Team :** OIPE **Date:** 03/06/2000

Entered Computer 3/12/2000
198874

Provisional Patent Application

TITLE: A Method to Provide Virtual Firewall Functionality from a Remote Service Provider

INVENTORS: Frank R. Koperda
2252 Merrymount Dr.
Suwanee, GA. 30024

Matthew M. Rosenhaft
6391 Glenridge Drive, #200
Atlanta, GA. 30328

CORRESPONDENCE ADDRESS: E-Panacea.com, LLC
100 Peachtree Street, Suite 450
Atlanta, GA 30303
(small entity status)

Date: January 19, 2000

DESCRIPTION OF DRAWINGS:

Figure 1. Equipment placement and connectivity to an ASP
Figure 2. Data path for a business using the Internet to reach the ASP
Figure 3. Direct Link between the business and the ASP
Figure 4. L2TP connection from Business to ASP through firewall to the Internet
Figure 5. Dial-in firewall protection for business traveler

BACKGROUND OF INVENTION:

As more computers have entered the small business environment, it has been difficult for firms to perform the same operations support that larger companies have attained. The adverse effects of this are that companies must either do without proper security/backup/maintenance or spend a higher percentage of their revenue on contract firms to do these functions.

One aspect of computer migration into the small business is the connectivity to the Internet that they have come to appreciate. Although the Internet has great benefit to a company, there is also great risk to the company's valuable electronic data. A common device used to isolate the company's data network from the Internet is a firewall.

The firewall requires a physical device to intercept and analyze the data to monitor communications transactions thereby keeping the company network secure. A firewall can also provide a mechanism to ensure employees are prohibited from visiting sites unrelated to their work duties. Maintaining the security on the firewall as new threats evolve and keeping the policy and prohibited site information current is difficult and resource intensive.

The cost of the firewall consists of the equipment, keeping the security features current, and knowing the inappropriate sites. It is possible to reduce these costs by moving the firewall to a more central location and having the costs of this asset shared by many companies. This invention describes the mechanism to ensure that a higher level of security can be attained by small business for a lower cost by using a Virtual Firewall at the business and implementing the actual firewall function at a central site.

PRIOR ART:

Related art includes firewall functions implemented at a corporate gateway, TCP/IP security layer IPSEC, and secure HTML communications such as SSL.

DESCRIPTION OF INVENTION:

A small business may have one or more computers connected onto a Local Area Network (LAN) which allows printer and external data links to be used by all the computers. To reduce the costs of purchasing and maintaining the

current level of a software program, a trend is emerging to have programs no longer reside on the local computer but to have it provided by a server. This server need not be located on the company premises.

A new business opportunity has emerged for companies to host programs on servers and having the maintenance costs shared by many companies. This type of company is known generically as an Application Service Provider (ASP). Current pricing allows for a single copy of a program to be maintained on the server and licenses purchased for the maximum number of concurrent users. This is significantly cheaper for a business than buying multiple retail copies of a program sufficient for all the computers in the company that might possibly need it.

Figure 1 shows the placement of equipment and possible connectivity. This figure represents one of many possible ways that such connectivity can be provided and is a useful figure for purposes of explaining the problem. It should not be construed to be the only embodiment of this invention.

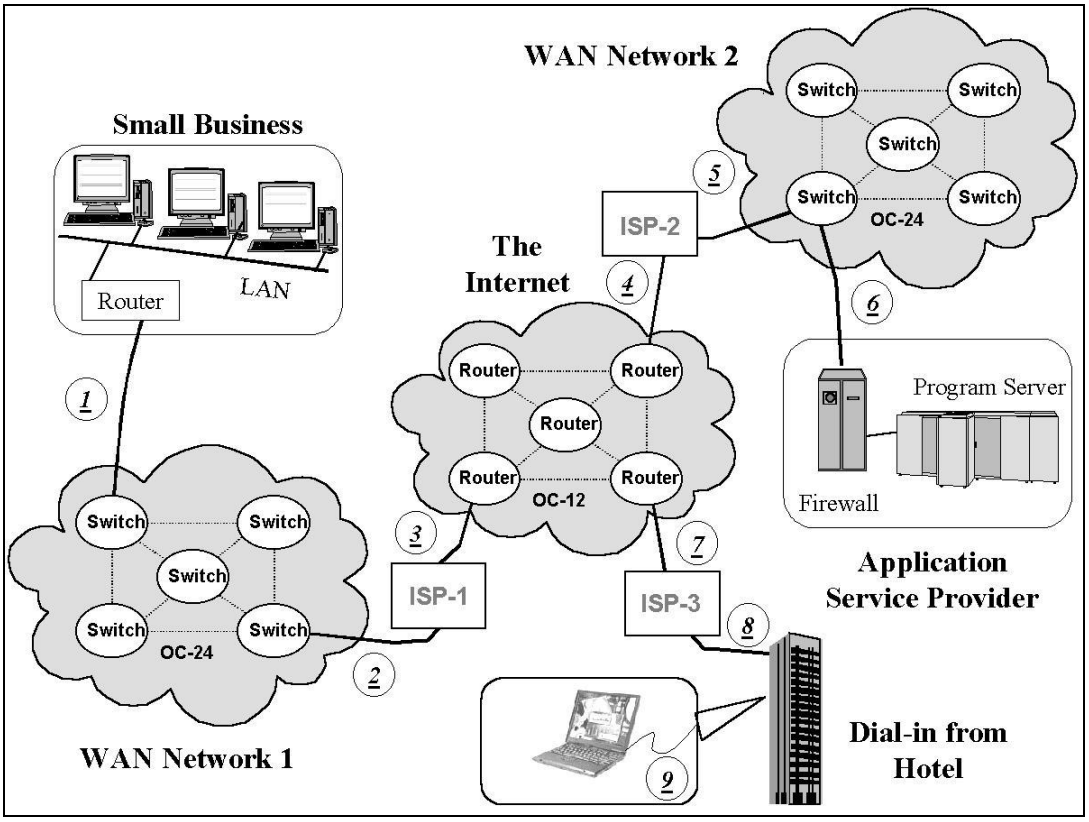

Figure 1. Equipment placement and connectivity to an ASP

The small business has various computers connected together by a Local Area network (LAN) such as Ethernet. The router located on premises decides which information needs to be remain local and which information is transmitted externally by monitoring the protocol destination addresses.

A Wide Area Network (WAN) is a network that can carry data long distances. Examples of WAN networks are Frame Relay, X.25 and ATM networks. They are directed through the various switches based on the destination address.

Access to the Internet is done by Internet Service Providers (ISPs). Only ISPs may directly connect to the Internet. The data is sent to its destination by routers that decide the path based on the destination address and by monitoring the content of header information.

The Application Service Provider (ASP) provides computing and information resources and may also provide other services where it is cost effective to share expensive resources.

Referring to Figure 2 and following Route A, when the business wishes to connect to the Internet, it connects [1] externally to WAN-1 via Frame Relay, ADSL or perhaps a cable modem. WAN-1 transports the data to ISP-1 via a high-speed link [2] and to the Internet using link [3].

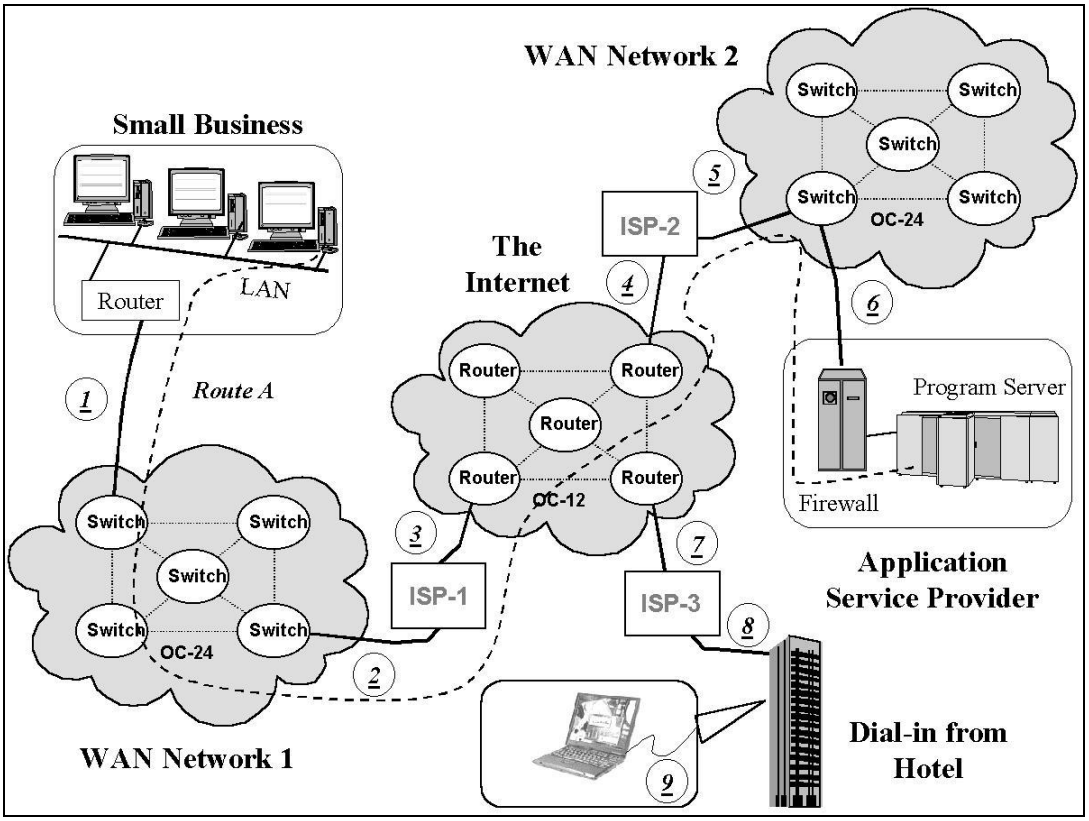

Figure 2. Data path for a business using the Internet to reach the ASP

If the business wishes to also connect to an ASP over that single connection, it would use the Internet and exit [4] to the same or different ISP (ISP-2). The data would be sent [5] to WAN-2 for local connection [6] to that ASP.

The company can also directly connect to the ASP as shown in Figure 3. Route B allows the company to use the previously mentioned link [1] to reach WAN-1. The connection flows between one or more WANs via link [10] thru connection [6] and then terminates again at the ASP.

Internet access is achieved by using the firewall of the ASP to protect all of the ASP's connections. The connection now flows over link [6] into WAN-2 to reach its ISP (ISP-2) over link [5]. The ISP communicates via link [4] to the Internet.

The advantage of this routing is that the small business needs no firewall of its own. In many instances, the link between the small business and the ASP may be considered relatively secure from interception. For enhanced security, point-to-point security methods consisting of hardware or software can be implemented.

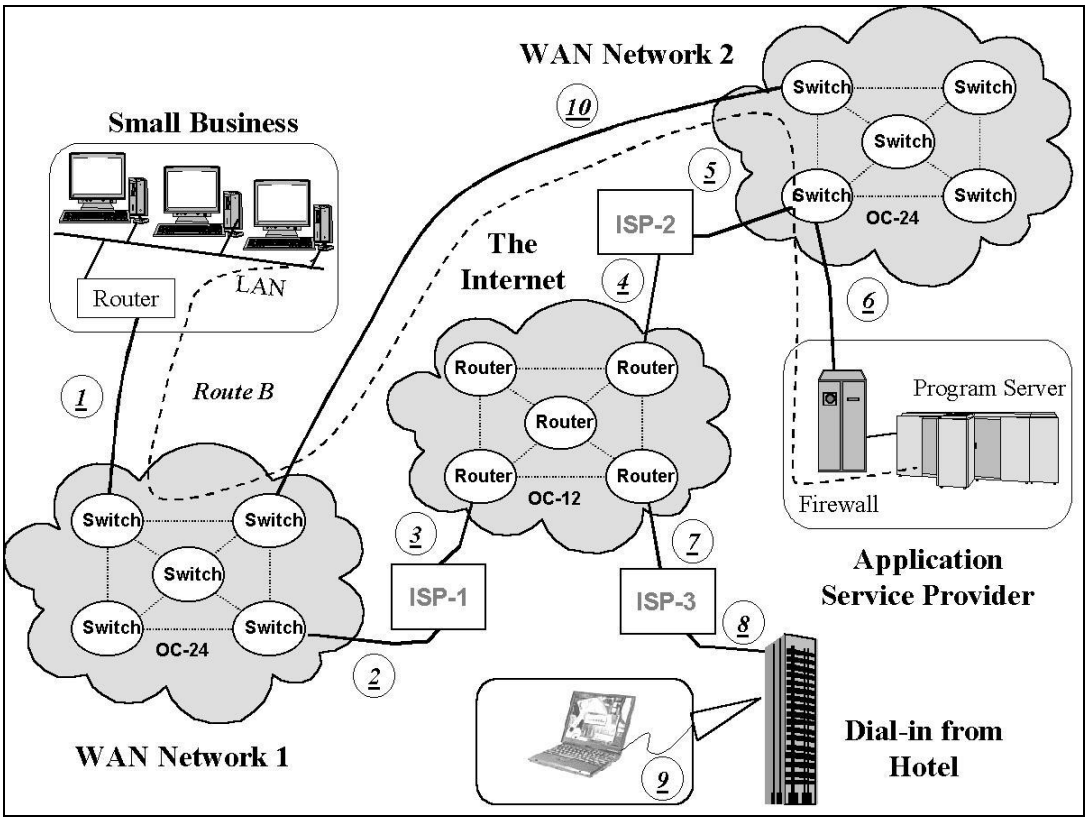

Figure 3. Direct Link between the business and the ASP

For those skilled in the art, Figure 3 should be recognized as a traditional firewall configuration with the exception that multiple companies may be using the firewall services of the same ASP. The functionality of the firewall under these circumstances enforces separate policies which is dependent on the traffic from each unique small business.

Security for Route A may employ one of many techniques for creating a secure connection between the business premisis to the ASP as shown in

Figure 4. One example of such a technique is when the local business uses the IP protocol to route the data from the business LAN to link [1] and forward it to the ASP. In this circumstance, the premisis router may incorporate a technique called Layer 2 Tunneling Protocol (L2TP) combined with IP security (IPSEC) to provide the secure protocol transport stream.

Conceptually, a computer in the business wanting to communicate with a web site would use HTTP over IP over Ethernet to reach the router. The router would recognize the destination was not local and remove the data (DATA1) from the Ethernet frame and put it into another packet (DATA2) which would be encrypted using the IPSEC protocol and then forwarded through Route A.

When the secure data reaches the ASP, DATA1 is removed from DATA2 and sent back out through the ASP firewall using the Internet policies for that business. The data follows Route D to the Internet through link[6], link[5], and link [4].

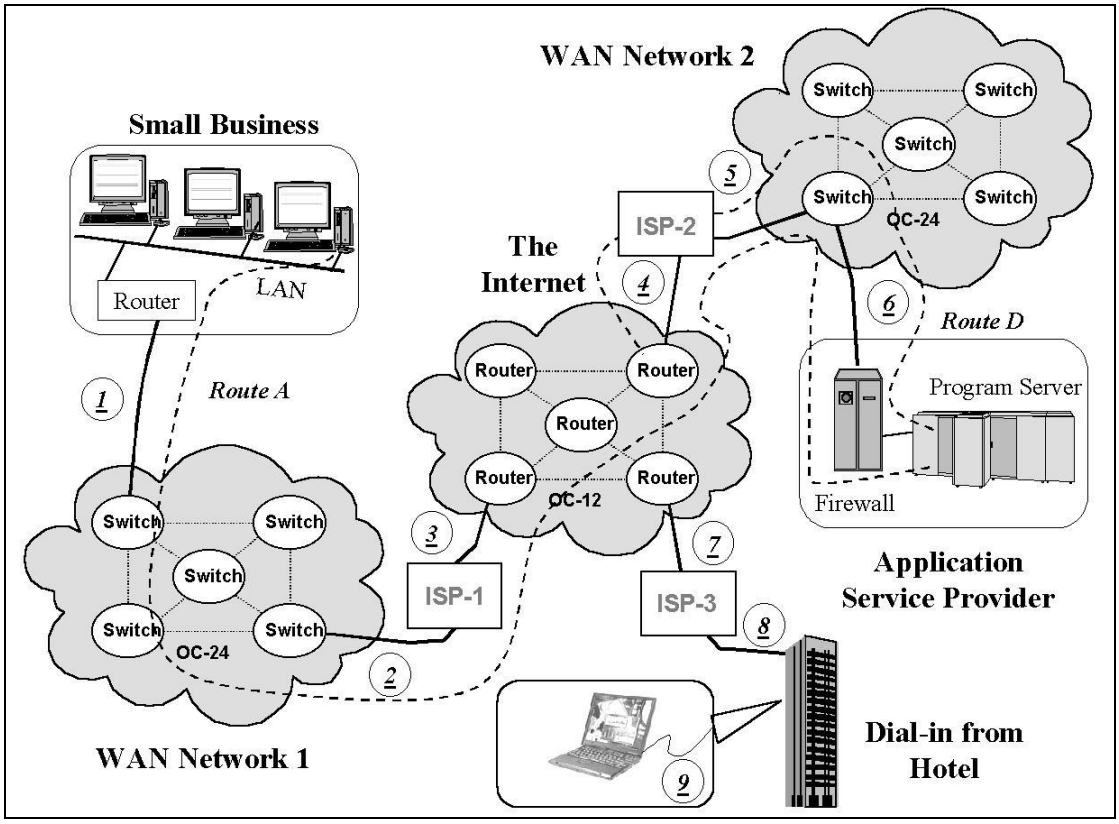

Figure 4. L2TP connection from Business to ASP through firewall to the Internet

The response (DATA3) from the Internet flows back using Route D to the ASP through the firewall. The ASP then puts DATA3 into a secure packet (DATA4) that is then forwarded along Route A back to the business.

The router at the small business strips DATA3 from DATA4, provides the decyption and then puts it into an Ethernet frame and forwarded on the LAN to the computer that originated the query.

This invention thus allows full firewall functionality for the small business without an onsite firewall. This "virtual firewall" functionality can provide the benefits of reducing capital expnediture since the actuall firewall can be amortized over many users and it reduces the maintaince cost since the ASP may distribute the support personel costs over many more users and do it with 24 hour support.

It is also possible to reduce the router operations support cost still furthur. This may optionally be done if the router is remotely configurable by the ASP or other support organizations (e.g. the ISP). This configuration information might consit of router address tables, the ASP destination address, protocol software fixes, and IPSEC key information.

Another desirable feature for business people that are traveling is to remain in contact with their corporate electronic information. Security from remote dial-in locations have been addressed in a number of ways and it is possible to incorporate these advances to bring the same level of virtual firewall protection to customers operating outside the business premises.

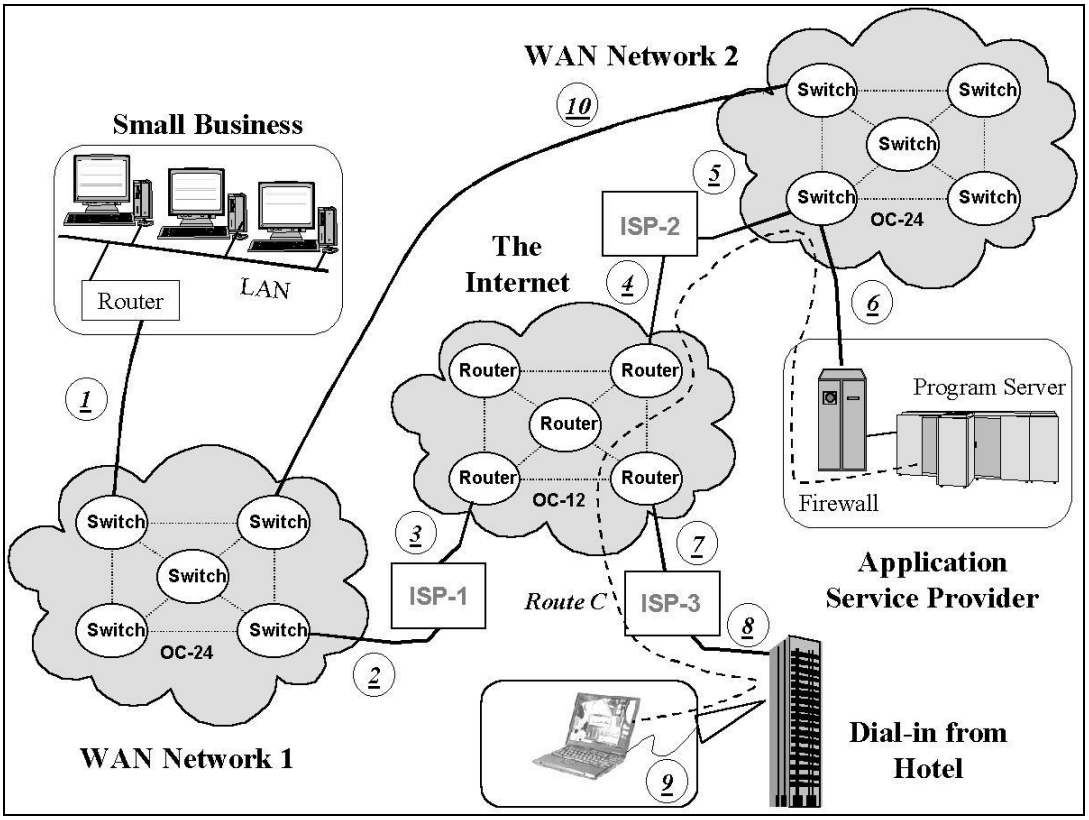

Figure 5. Dial-in firewall protection for business traveler

Figure 5 shows the path through the Internet to reach the ASP. Route C begins at the business traveler's hotel where it connects via a suitable connection [9] such as an analog phone line, hotel LAN, or other physical connection. The hotel uses link [8] to gain access to ISP-3 to access the

Internet via link [7]. The connection exits the Internet through link [4] into WAN-2 via link [5] and finally reaches the ASP on link [6].

For the business travel, this connection to the internet provides no firewall protection on its path. This invention overcomes that problem by having a secure connection with the ASP and then back through the firewall to the Internet. Route C may be protected by one of several security protocols that create a secure point-to-point connection.

One method, but not the only method embodied in the invention, is to use the technique from shopping sites by activiating the Secure Socket Layer (SSL) of many web browsers. This technique uses public/private key technology to encrypt with a public key known to all. The ASP will decrytpt the information with its own private key.

The business traveler now has a secure path (Route C) to the ASP and the ASP has a secure route to the business premises (Route A). The business traveler also has protected access to the Internet through Route C and Route D.

INVENTORS

_____ _____

Frank R. Koperda Date:

_____ _____

Matthew M. Rosenhaft Date: