

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Larson <i>et al.</i>	
U.S. Patent No.:	7,921,211	Attorney Docket No.: 38868-0007IP3
Issue Date:	April 5, 2011	
Appl. Serial No.:	11/840,560	
Filing Date:	August 17, 2007	
Title:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS USING SECURE DOMAIN NAMES	

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Science & Engineering department at Washington University in St. Louis. I have been asked to offer technical opinions relating to U.S. Patent No. 7,921,211, and prior art references relating to its subject matter. My current curriculum vitae is attached and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure des télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) and PhD (1986) in electrical engineering from The California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at the IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I was a research staff member within the Communication Department, where I worked to design and evaluate high-speed switches and networks. From 1990 to 1991, I was a research staff member within the IBM High Performance Computing and Communications Department, where I worked to develop and deploy an integrated broadband network. From 1992 to 1997, I was the manager of Broadband Networking within IBM's Security and Networking Systems Department, where I led a group of researchers in the area of design, architecture, and analysis of broadband networks. One of the projects on which I worked, for example, led to U.S. Patent No. 5,673,318, which regards "[a]

method and system for providing data authentication, within a data communication environment, in a manner which is simple, fast, and provably secure,” and of which I am a named inventor.

See U.S. Patent No. 5,673,318, abstract. From 1997 to 1998, I was the manager of Network Control and Services within IBM’s Security and Networking Systems Department, where I led a department responsible for networking and distributed applications, including topics such as advance reservations, policy support, including for Resource Reservation Protocol (RSVP), quality of service (QoS) routing, and security, and integrated switch and scheduling designs.

4. I have been a professor of engineering for the past fifteen years. As such, but prior to becoming the chair of the Computer Science & Engineering department at Washington University in St. Louis, I was the Alfred Fitler Moore Professor of Telecommunications Networks (an honorary chair) in the Department of Electrical and Systems Engineering at the University of Pennsylvania. As a professor of engineering, I have taught many courses in networking, including Advanced Networking Protocols (TCOM 502), which addressed, among other things, virtual private networks.

5. I have authored over fifty journal publications, including “On the Feasibility and Efficacy of Protection Routing in IP Networks,” which was honored with the IEEE INFOCOM 2010 Best Paper Award. I have been named a Fellow by both the IEEE and ACM, and, from 2009 to 2012, I was the Editor-in-Chief of the IEEE/ACM Transactions on Networking. Furthermore, I am a named inventor on over thirty issued U.S. patents.

6. I am familiar with the content of U.S. Patent No. 7,921,211 (the “‘211 patent”). In addition, I have considered the various documents referenced in my declaration as well as additional background materials. I have also reviewed certain sections of the prosecution history of the ‘211 patent, the prosecution history of reexamination control numbers 95/001,789 and

95/001,856; and the claim construction orders from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:07CV80 (E.D. Tex.) and *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Docket No. 6:10cv417 (E.D. Tex.).

7. Counsel has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '211 patent at the time of the invention, and I have done so during my review of these materials. I believe one of ordinary skill as of February 15, 2000 (the earliest priority date of the '211 patent) would have a Master's degree in computer science or computer engineering, or in a related field such as electrical engineering, as well as about two years of experience in computer networking and in some aspect of security with respect to computer networks. I base this on my own personal experience, including my knowledge of colleagues and others at the time.

8. I have no financial interest in either party or in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

9. My opinions, as explained below, are based on my education, experience, and background in the fields discussed above.

10. This declaration is organized as follows:

- I. Brief Overview of the '211 Patent
- II. Terminology
- III. Provino and Combinations Based on Provino
- IV. Publication and Authenticity of Requests For Comment (RFCs)
- V. Conclusion

I. Brief Overview of the '211 Patent

11. A section of the '211 patent's specification titled "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks" describes "the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.," with reference to FIG. 26. Ex. 1001, 38:55-57. Referring to FIG. 26 below, a "user's computer 2601 includes a conventional client (e.g., a web browser) 2605 and an IP protocol stack 2606 that preferably operates in accordance with an IP hopping function 2607 as outlined above." Ex. 1001, 39:48-51. "A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610." Ex. 1001, 39:51-52. "A gatekeeper server 2603 is interposed between the modified DNS server and a secure target site [2604]." Ex. 1001, 39:52-53. "An 'unsecure' target site 2611 is also accessible via conventional IP protocols." Ex. 1001, 39:53-56.

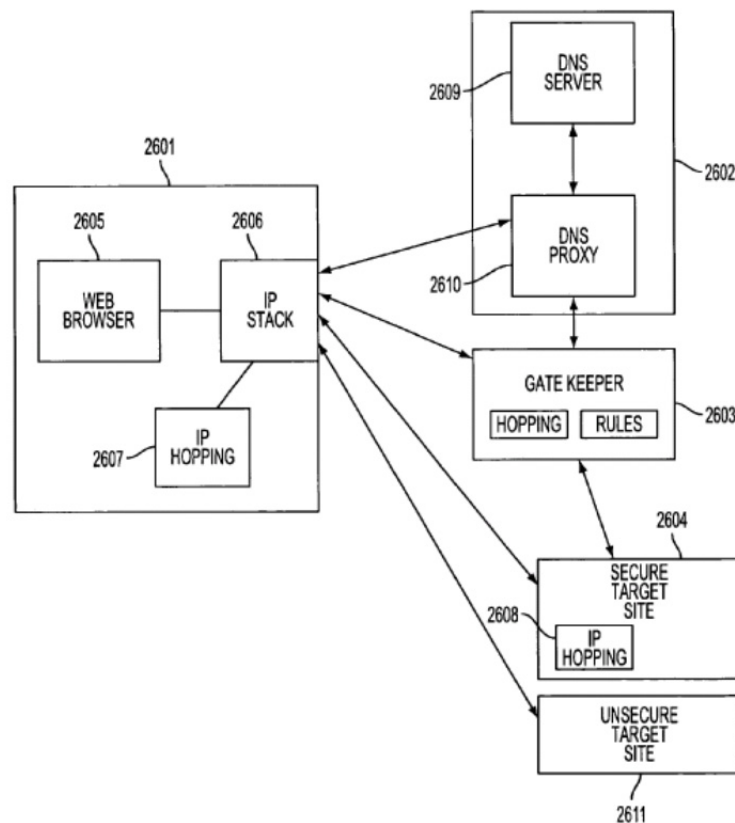


FIG. 26

12. As described by the '211 patent:

DNS proxy 2610 intercepts all DNS lookup functions from client 2605 and determines whether access to a secure site has been requested. If access to a secure site has been requested (as determined, for example, by a domain name extension, or by reference to an internal table of such sites), DNS proxy 2610 determines whether the user has sufficient security privileges to access the site. If so, DNS proxy 2610 transmits a message to gatekeeper 2603 requesting that a virtual private network be created between user computer 2601 and secure target site 2604. In one embodiment, gatekeeper 2603 creates "hopblocks" to be used by computer 2601 and secure target site 2604 for secure communication. Then, gatekeeper 2603 communicates these to user computer 2601. Thereafter, DNS proxy 2610 returns to user computer 2601 the resolved address passed to it by the gatekeeper (this address could be different from the actual target computer) 2604, preferably using a secure administrative VPN. The address that is returned need not be the actual address of the destination computer.

Had the user requested lookup of a non-secure web site such as site 2611, DNS proxy would merely pass through to conventional DNS server 2609 the look-up request, which would be handled in a conventional manner, returning the IP address of non-secure web site 2611. If the user had requested lookup of a secure web site but lacked credentials to create such a connection, DNS proxy 2610 would return a "host unknown" error to the user. In this manner, different users requesting access to the same DNS name could be provided with different look-up results.

Ex. 1001, 39:57 to 40:18.

II. Terminology

13. I have been informed that claim terminology must be given the broadest reasonable interpretation during an IPR proceeding. I have been informed that this means the claims should be interpreted as broadly as their terms reasonably allow, but that such interpretation should not be inconsistent with the patent's specification and with usage of the terms by one of ordinary skill in the art when considering the broadest reasonable construction. I have been informed that this may yield interpretations that are broader than the interpretation applied during a District Court proceeding, such as the pending *VirnetX Inc. v. Microsoft Corp.* litigation.

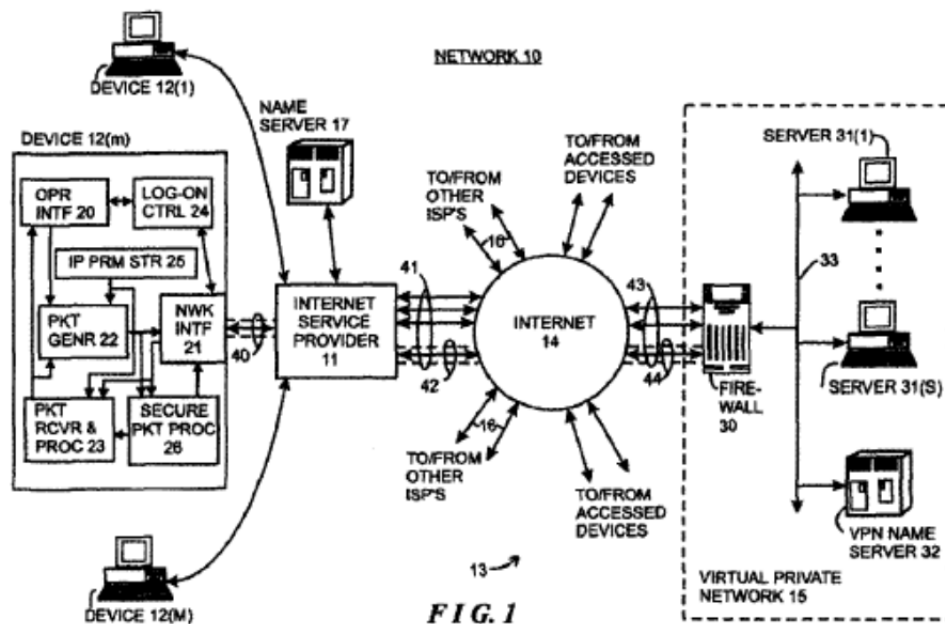
14. I have been informed that it would be useful to provide some guidance in this proceeding with respect to the term below and its corresponding construction. As part of that I considered the term's context within the claim, use within the specification, and my understanding of how one of ordinary skill in the art would understand the term around the time of the purported invention under the broadest reasonable construction standard.

15. I have considered whether a broadest reasonable interpretation of "system" would be broad enough to cover "one or more discrete computers or devices." I believe that it would, since such an interpretation is not inconsistent with the '211 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when looking for the broadest reasonable construction. For example, at col. 39, line 47 – col. 40, line 32, the '211 patent describes a system that includes a modified DNS server 2602 and a separate gatekeeper server 2603, and specifically states that "although element 2602 [(the modified DNS server)] is shown as combining the functions of two servers [(the DNS proxy 2610 and DNS server 2609)], the two servers can be made to operate independently." Ex. 1001 at col. 40:29-31.

III. Provino and Combinations Based on Provino

A. Provino

16. Provino describes “systems and methods for easing communications between devices connected to public networks such as the Internet and devices connected to private networks.” Ex. 1008 at 1:14-16. In particular, Provino describes a system that facilitates communications between a client device 12(m) connected to ISP 11 and a server 31(s) located within virtual private network (VPN) 15. *See* Ex. 1008 at 9:32 to 10:33. An example of the architecture of Provino’s system is illustrated in Figure 1 of Provino.



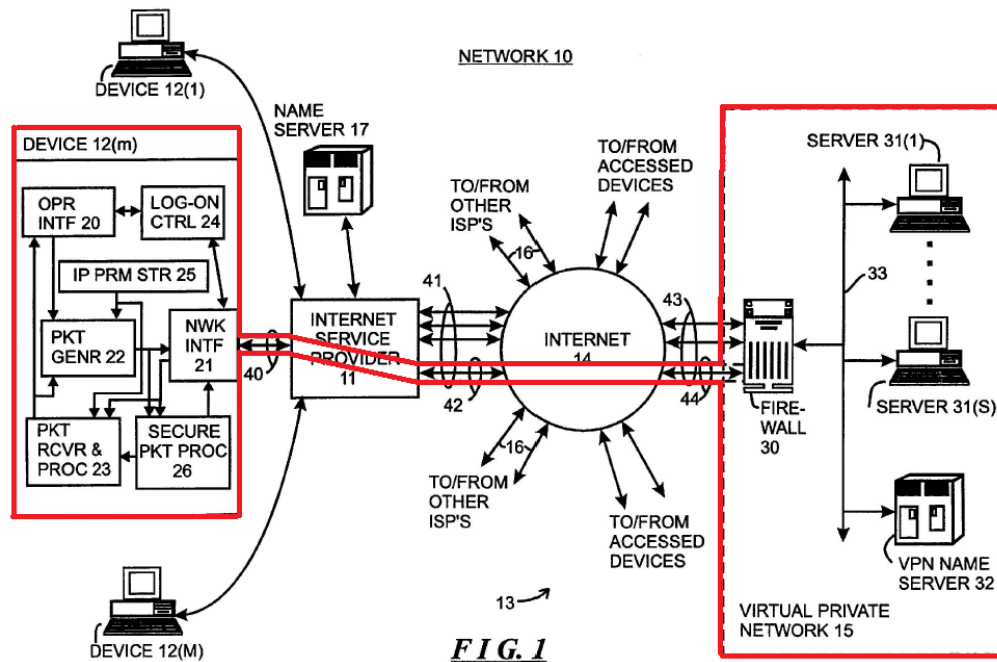
17. For a device 12(m) external to VPN 15 to communicate with a server 31(s) within VPN 15, Provino describes a two phase process for establishing communications. *See* Ex. 1008 at 12:1-2. During the first phase described by Provino, the device 12(m) establishes a secure tunnel with VPN 15, via firewall 30, and identifies a VPN name server 32 inside VPN 15. Ex. 1008 at 9:61-65, 10:58-64. In particular, during the first phase, the client device 12(m) obtains an address for the firewall 30 from standard name server 17, e.g., by initiating a request for the

address, and establishes a secure tunnel with firewall 30 by exchanging encryption/decryption information. Ex. 1008 at 12:17-36. During the second phase, the client device 12(m) uses the secure tunnel to send encrypted message packets to VPN 15, via firewall 30. Ex. 1008 at 12:8-16. In particular, during the second phase, the client device 12(m) communicates with VPN name server 32 to obtain addresses for servers (e.g., server 31(s)) inside the VPN 15, and then uses those addresses to send encrypted messages to those servers, via firewall 30. Ex. 1008 at 12:8-16.

18. Therefore, Provino's standard ISP nameserver 17 and the VPN nameserver 32 (with the assistance of firewall 30) each resolves human-readable Internet addresses (i.e., hostnames) for servers into respective integer Internet addresses (i.e., IP addresses). *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59. Further, as described above, Provino discloses that the firewall 30 and nameservers 17 and 32 establish a secure communication link between the client device 12(m) and a destination (or server) within the VPN 15.

19. Further details of the first phase are provided next. The client device 12(m) first locates the firewall 30 by obtaining "an integer Internet address for the firewall" which, in some cases, is "provided by the nameserver 17 after a human-readable Internet address [i.e., hostname] was provided by the operator or a program." Ex. 1008 at 12:20-24. After the client device 12(m) obtains the address of firewall 30, the device 12(m) sends a message packet to the firewall 30, requesting establishment of a secure tunnel. Ex. 1008 at 9:47-52. If the firewall 30 determines that the client device 12(m) is authorized to access the VPN 15, then the firewall 30 provides the device 12(m) with encryption and decryption information, such as identification of an encryption/decryption algorithm and associated encryption and decryption keys. Ex. 1008 at 9:61-65. The device 12(m) subsequently uses the encryption and decryption information to

securely communicate with the VPN 15, thus establishing a secure tunnel through the Internet 14 to the VPN 15. *See* Ex. 1008 at 12:2-4. As shown in Annotation 1 below, the creation of the secure tunnel between device 12(m) and VPN 15 effectively extends the VPN to include the device 12(m) via Internet 14. *See* Ex. 1008 at 6:10-15.



(Annotation 1)

20. Provino further discloses that, during this first phase, in addition to encryption and decryption information, the firewall 30 may also provide the device 12(m) with an identification of a VPN nameserver 32 in the VPN 15. Ex. 1008 at 10:58-64. Functionally, the VPN nameserver 32 “serves to resolve human-readable Internet addresses [i.e., hostnames] for servers 31(s) internal to the virtual private network 15 to respective integer Internet addresses.” Ex. 1008 at 9:2-5. In particular, the client device 12(m) utilizes the VPN nameserver 32 (in the subsequent second phase) to locate servers inside the VPN by obtaining “the appropriate integer Internet addresses for the human-readable Internet addresses [i.e., hostnames] which may be provided by the operator of device 12(m).” Ex. 1008 at 10:64-67. Provino describes that

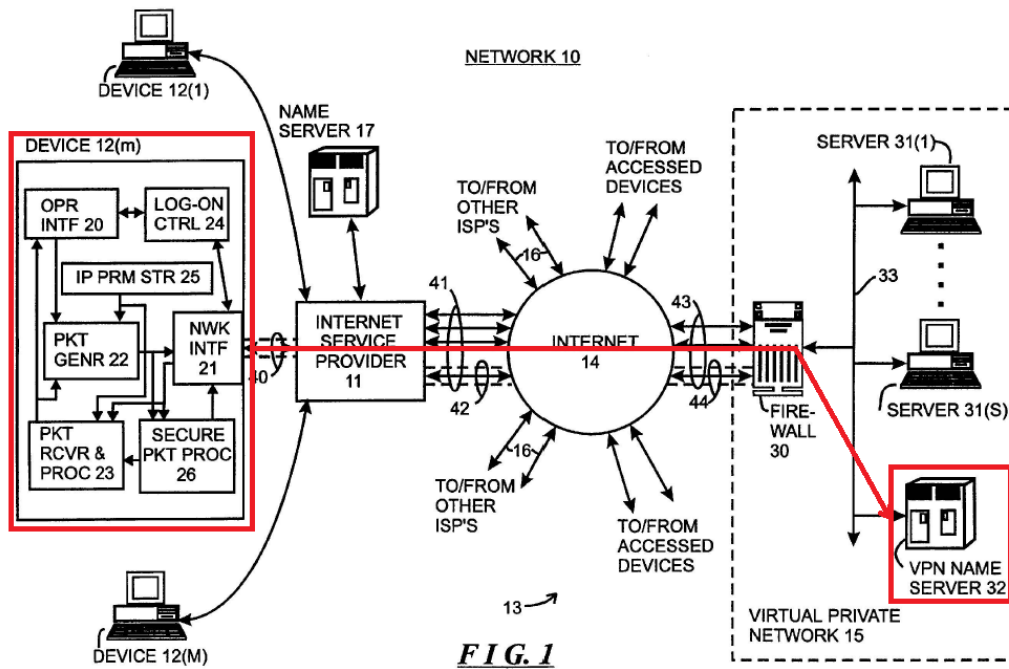
message packets transferred over the Internet “conform to that defined by the so-called Internet protocol ‘IP’” and that, in particular, the integer Internet address of a message packet is an “IP parameter.” Ex. 1008 at 3:62-65, 7:51-53. Provino also describes that the integer Internet address of the server 31(s) is “in the form of an ‘n’-bit integer (where ‘n’ may be thirty two or 128).” Ex. 1008, 1:45-47. Thirty-two and 128 are the number of bits in Internet Protocol Version 4 and 6 IP addresses, respectively. Based on these disclosures, one of ordinary skill in the art would understand that the integer Internet address of the server 31(s) is an IP address.

21. Further details of the second phase are provided next. After creating a secure tunnel to VPN 15 and identifying VPN name server 32, “the device 12(m) can use the information provided during the first phase in connection with generating and transferring message packets to one or more servers 31(s) in the virtual private network 15, in the process obtaining resolution [of] human-readable Internet addresses [i.e., hostnames] to integer Internet addresses [i.e., IP addresses] as necessary from the nameserver 32 that was identified by the firewall 30 during the first phase.” Ex. 1008 at 12:8-16.

22. In particular, in the second phase of Provino, a user of client device 12(m) may instigate communications with secure servers within VPN 15 (e.g., a server 31(s)) by using a hostname that is associated with server 31(s). *See* Ex. 1008 at 13:31-40. Provino describes that, in general, the client device 12(m) will “initially access the nameserver 17. . . to attempt to obtain the integer Internet address associated with the human-readable Internet address [i.e., hostname].” Ex. 1008 at 11:6-10. If the standard ISP nameserver 17 cannot resolve the hostname (e.g., because the requested server 31(s) is within a VPN), then the standard ISP nameserver 17 returns an error message indicating that it does not have the IP address for the hostname of server 31(s). Ex. 1008 at 11:10-15. In this case, the client device 12(m) sends a request message

packet to the VPN nameserver 32, through the firewall 30, in attempting to identify the IP address of the server 31(s). Ex. 1008 at 11:10-15.

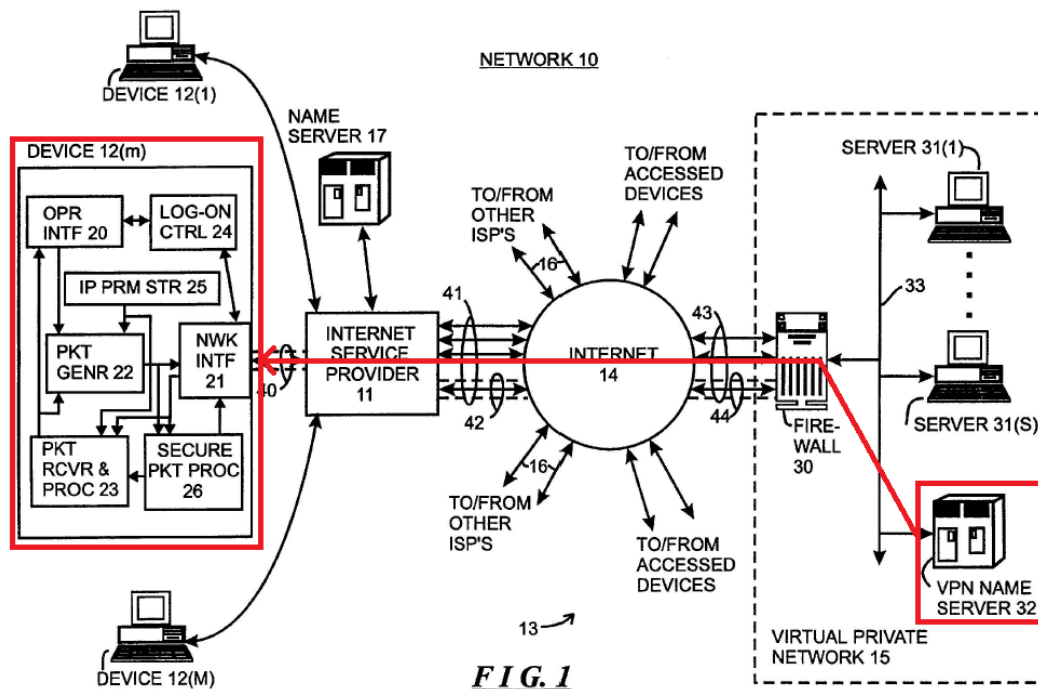
23. Below, in Annotations 2 and 3 of FIG. 1, the client's exchange with VPN nameserver 32 is highlighted. In particular, to resolve the hostname using VPN nameserver 32, the device 12(m) initiates "a request message packet for transmission to the nameserver 32 through the firewall 30 and over the secure tunnel." Ex. 1008 at 11:13-16. This request process is illustrated in Annotation 2 of FIG. 1, which shows the device 12(m) sending a request message packet to the nameserver 32 (via firewall 30) to request the IP address corresponding to the hostname of a server 31(s).



(Annotation 2)

24. The VPN nameserver 32 receives the message request packet from the client device 12(m), via firewall 30, and attempts to resolve the hostname of server 31(s) into an IP address. Ex. 1008 at 11:19-21. If a corresponding IP address is found, then the VPN name server 32 returns the IP address back to the client device 12(m), via the firewall 30. Ex. 1008 at 11:21-

25. Therefore, as a result of the client device 12(m) sending a request message packet to the VPN name server 32, Provino describes that the device 12(m) receives the IP address for server 31(s) in a message packet transmitted from nameserver 32 via firewall 30, as illustrated in Annotation 3 of FIG. 1. *See* Ex. 1008 at 11:16-25.



(Annotation 3)

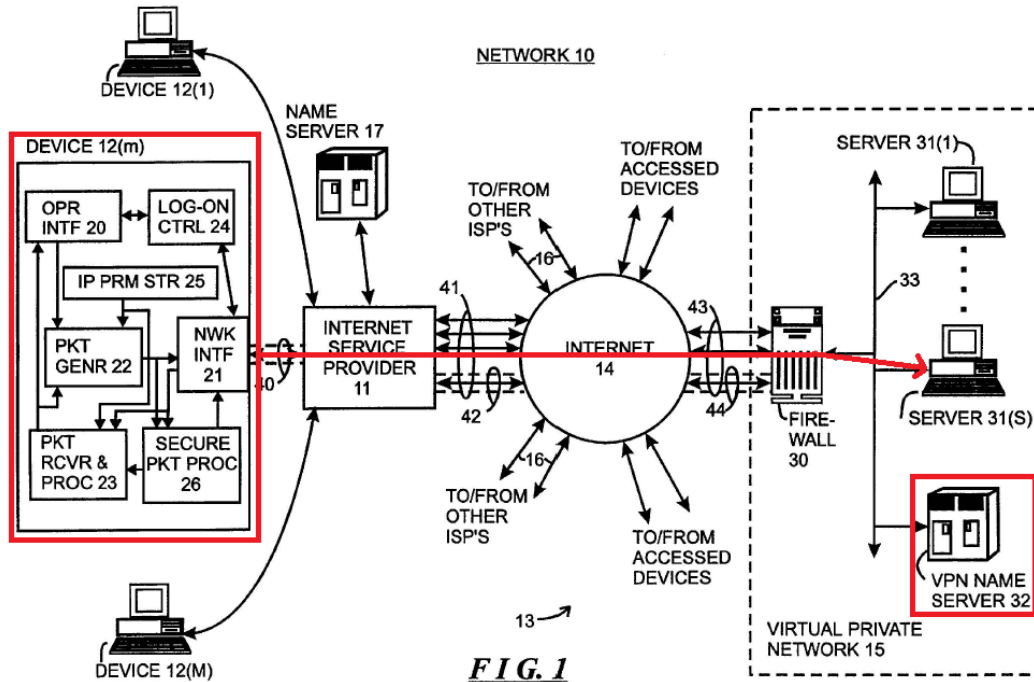
25. Otherwise, if the nameserver 32 does not have an association between the requested hostname for server 31(s) and an IP address, “the nameserver 32 can provide a response message packet so indicating.” Ex. 1008 at 11:50-54. If the client device 12(m) is unable to obtain an IP address associated with the hostname from any of the nameservers to which it has access, then the client device 12(m) “may so notify its operator or program which requested the access.” Ex. 1008 at 11:64-65.

26. Provino explains that its nameservers 17 and 32 operate as DNS servers and resolve hostnames into corresponding IP addresses. *See* Ex. 1008 at 1:56-60, 7:37-43, 12:56-59. Prior to February of 2000, one of ordinary skill in the art would understand that each of

nameservers 17 and 32 would, by their nature, contain a database to store a plurality of domain names and associated network addresses, in order to perform the function of domain name resolution described by Provino. For instance, this knowledge of a person of ordinary skill was reflected in the publically available RFC 1034 (Ex. 1010), which discloses that a domain name database is used for domain name resolution. *See* Ex. 1010 at 7, 18.

27. Furthermore, prior to February of 2000, one of ordinary skill in the art would understand that domain names handled by standard domain name servers, such as those disclosed by Provino, would contain a top-level domain, as used in the Internet, for example. For instance, this knowledge is reflected in the publically available RFC 1591 (Ex. 1011), which describes the domain name system structure and notes that in “the Domain Name System (DNS) naming of computers there . . . are a set of what are called ‘top-level domain names’ (TLDs)” Ex. 1011 at 1. Moreover, Provino describes nameservers 17 and 32 as comprising a server. *See* Ex. 1008 at 1:56-60.

28. Once the client device 12(m) receives the IP address for server 31(s) from VPN name server 32, the client device 12(m) stores the address in a local cache, “along with the association of the human readable address [i.e., hostname] thereto,” in IP parameter store 25. Ex. 1008 at 11:35-39. The client device 12(m) subsequently uses the stored IP address and associated hostname to communicate with server 31(s) by sending messages via the encrypted tunnel to firewall 30, which forwards the messages to server 31(s). Ex. 1008 at 10:28-32; 11:40-45. In particular, Provino describes that “the device [12(m)] can use that integer Internet address [i.e., IP address] in generating message packets for transmission to the server 31(s) which is associated with the human-readable Internet address [i.e., hostname].” Ex. 1008 at 15:27-30. This transmission to the server 31(s) is illustrated in Annotation 4 of FIG. 1, below.

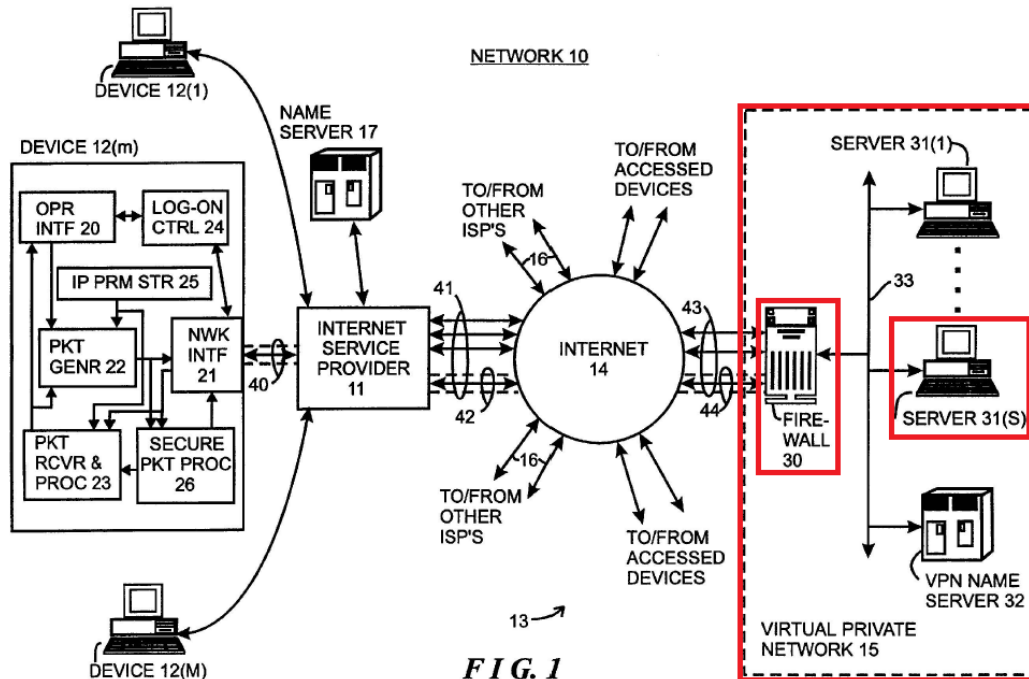


(Annotation 4)

29. Provino additionally describes the transfer of information stored on server 31(s) to device 12(m). Ex. 1008 at 9:6-13. By describing that device 12(m) generates a message packet for transmission to server 31(s) and receives information transferred from server 31(s), Provino describes that device 12(m) leverages the resolved secure computer network address (i.e., integer Internet address) to send access request messages to server 31(s) that contains a request for information stored on server 31(s). Thus, once the device 12(m) obtains the integer Internet address of server 31(s) from nameserver 32 during the second phase of establishing communications with server 31(s), the device 12(m) may send access requests to server 31(s) using the secure tunnel established with the firewall 30 in the first phase of the communication process. Ex. 1008 at 15:21-30.

30. In Annotation 5 of FIG. 1, which follows, firewall 30 is shown as limiting access to server 31(s) by computers outside of the VPN 15. See Ex. 1008 at 9:6-27. Provino describes that, the firewall 30 authenticates message requests from client device 12(m) by determining

whether the device 12(m) is authorized to access server 31(s) within the VPN 15. *See* Ex. 1008 at 9:17-27, 56-60, 12:26-32.



(Annotation 5)

31. For example, in the first phase, if the firewall 30 accepts the secure tunnel establishment request from client device 12(m), then the firewall 30 “will generate a response message packet for transmission to the device 12(m) that identifies the encryption and decryption algorithms and keys” to be used in establishing the secure tunnel. Ex. 1008 at 12:26-32

32. In addition, in the second phase, in order for the device 12(m) to access the server 31(s), the device 12(m) must be authorized to do so. Ex. 1008 at 9:20-27. In particular, if the requesting message indicates a device 12(m) that is authorized to access the server 31(s), then “firewall 30 will forward the message packet to the server 31(s).” Ex. 1008 at 9:20-23. Otherwise, if the client device 12(m) is not authorized to access server 31(s), then “the firewall 30 will not forward the message packet to the server 31(s), and may, instead, transmit a response

message packet to the source device indicating that the source was not authorized to access the server 31(s).” Ex. 1008 at 9:21-27.

33. Provino also describes that its system utilizes various services that use protocols and application programs. For example, “[e]ach device 12(m) communicates with the ISP 11 to transfer message packets thereto for transfer over the Internet 14, or to receive message packets therefrom received by the ISP 11 over the Internet 14, using any convenient protocol such as the well-known point-to-point protocol (“PPP”) if the device 12(m) is connected to the ISP 11 using a point-to-point link, any conventional multi-drop network protocol if the device 12(m) is connected to the ISP 11 over a multi-drop network such as the Ethernet.” Ex. 1008 at 4:23-35. Provino also describes that its system includes “network and/or telephony interface devices for interfacing the respective device to the ISP 11.” Ex. 1008 at 4:43-45. Provino further discloses a system that is configured to process “programs, including application programs, under control of an operating system, to generate processed data” and that a “video display unit permits the device to display processed data and processing status to the user.” Ex. 1008 at 4:44-49.

34. Provino describes a system that establishes secure tunnels between an external device and an internal device without user involvement. For example, Provino discloses when a human operator “has provided the human-readable Internet address” (i.e., hostname) to the client device 12(m), then the device 12(m) performs various operations in attempting to obtain the corresponding IP address. Ex. 1008 at 11:7-17. Provino describes that the client device 12(m) will “initially contact nameserver 17 to attempt to obtain the appropriate integer Internet address [i.e., IP address].” Ex. 1008 at 11:7-17. If unsuccessful, the device 12(m) “generates a message packet requesting establishment of a secure tunnel for transfer to the firewall 30” (assuming one has not already been established), and if authorized, receives encryption and decryption

information from the firewall that allows the client device 12(m) to establish a secure tunnel with VPN 15. Ex. 1008 at 12:16-20. Provino does not describe the steps of contacting the firewall 30 and establishing a secure tunnel with the VPN 15 as requiring user involvement. In fact, Provino describes that the IP address of firewall 30 may have, in some cases, “been provided by the device's operator or a program being processed by the device 12(m).” Ex. 1008 at 12:20-23 (emphasis added). Therefore, Provino describes a scenario in which a program, instead of a user, requests the address of the firewall 30, allowing the client device 12(m) to establish a secure tunnel with the VPN 15. Therefore, Provino discloses that a user is not required to be involved in establishing the secure tunnel.

35. Provino explains that its system uses computing devices (*i.e.*, computers, servers, firewalls, etc.) that have software running on them, which necessarily include a machine-readable medium comprising executable instructions. *See* Ex. 1008 at 4:35-49. For example, Provino’s client device 12(m) includes processing, memory, and mass storage devices and includes programs under control of an operating system to generate processed data. *Id.* Also, Provino describes that its firewall 30 and servers 31(s) also include, for example, personal computers, computer workstations, and the like, and also include mini-and mainframe computers, mass storage systems, computer servers. Ex. 1008 at 6:19-25.

B. Combination of Provino and RFC 1034

36. As explained above, Provino discloses name servers (e.g., nameservers 17 and 32) which return a corresponding IP address in response to a query for a domain name. *See* Ex. 1008 at 7:34-43, 10:62-67. As I indicated above, I believe one of ordinary skill in the art would understand that Provino’s VPN nameserver 32 and standard ISP nameserver 17 would include a domain name database to store a plurality of domain names and corresponding network

addresses, in order to perform the function of domain name resolution. Even if that were not the case, it would have been obvious to one of ordinary skill in the art to use such a database in Provino's nameservers in view of the disclosure of RFC 1034.

37. RFC 1034 discloses that each name server in the Domain Name System includes a domain name database for the zones managed by the name server: "Name servers are the repositories of information that make up the domain database" and the domain name database "is divided up into sections called zones, which are distributed among the name servers." Ex. 1016 at § 4.1. As a particular example, RFC 1034 describes a domain name database being shared by a name server and a resolver: "a resolver on the same machine as a name server might share a database consisting of the the [sic] zones managed by the nameserver and the cache managed by the resolver. Ex. 1016 at § 3.1.

38. Prior to February 2000, one of ordinary skill in the art would have been motivated to use the domain name database described by RFC 1034 in the name servers of Provino to store domain names and corresponding IP addresses, because databases store data in a structured manner that allows for fast and efficient storing and searching of the data relative to other storage structures, such as an unstructured flat text file. Because the number of domain names and IP addresses can be relatively large depending on the size of the network, having a fast and efficient storage would allow for a timely response to a query to resolve a domain name. One of ordinary skill in the art would therefore have been motivated to use the domain database of RFC 1034 in the nameservers of Provino.

C. Combination of Provino and Kosiur

39. Kosiur provides information regarding the capabilities of VPNs at or before the time of the '211 patent. In particular, Kosiur is "a book [that] aims to provide you with the

background on VPN technologies and products that you need to make appropriate business decisions about the design of a VPN and expectations for its use.” Ex. 1006, p. 9. Chapter 15 of Kosiur “covers the basics of network performance and related application requirements as well as methods for offering network services to your customers that can be differentiated on the basis of those application and/or user requirements.” Ex. 1006, p. 243.

40. In chapter 15, Kosiur describes that “a wide variety of applications can run on networks.” Ex. 1006, p. 244. In particular, Kosiur describes that, if they’re configured for differentiated services, virtual private networks can support “newer applications, such as interactive multimedia and videoconferencing.” Ex. 1006, p. 254. Kosiur describes that VPN traffic may include “file transfers, Web browsing, and e-mail,” in which case the VPN “won’t need to be concerned with QoS.” Ex. 1006, p. 249. Conversely, Kosiur describes that VPN traffic may also include “transactional traffic, interactive multimedia, and IP telephony,” in which case “you’ll need to track developments in QoS technologies.” *Id.* For example, Kosiur describes that a VPN can be configured to “utiliz[e] streaming multimedia,” which would include audio and/or video. *See* Ex. 1006, p. 244. Therefore, Kosiur describes that VPNs could be configured to support a plurality of application programs, including application programs that support interactive multimedia, file transfers, Web browsing, and e-mail.

41. Provino does not provide many specific details about the types of applications and services that are supported by VPN 15. However, Provino notes that the device 12(m) may be operated by an “employee of a particular company or governmental agency.” Ex. 1003, 3:54-56. It would have been obvious to one of ordinary skill in the art to configure the VPN 15 described by Provino to support the applications and services described by Kosiur, as these applications

and services would increase the mobility and productivity of the employees operating devices 12(m).

42. In particular, Kosiur recognizes the increasing mobility of the modern workforce in which business persons require productivity applications, such as videoconferencing. *See* Ex. 1006, p. 13. As of 1998, Kosiur tells us that VPNs were commonly configured to support various services and applications, such as videoconferencing. *See* Ex. 1006, p. 254. Provino provides no contrary position, as it does not explicitly or implicitly describe any limitations on the services or applications that Provino's VPN 15 may be configured to support. Indeed, Provino describes that the devices in its system are capable of supporting numerous applications and services using various transfer methods. *See* Ex. 1003, 6:10-50. Moreover, Provino describes the maintenance of its VPN 15 "by a company, governmental agency, organization or the like." Ex. 1003, 9:6-7. Prior to 2000, it was common for companies or similar organizations to have their employees use interactive multimedia, videoconferencing, file transfers, Web browsing, and e-mail as part of their daily routine to increase the employees' productivity and mobility. *See* Ex. 1006, p. 13. A company or other similar organization would find it desirable to make those resources available to remotely located employees through the VPN 15 so as to similarly increase the productivity of those remote employees.

D. Combination of Provino and RFC 2660

43. As explained above, Provino discloses a secure tunnel that is provided between a client device 12(m) and a firewall 30 in a VPN. *See, e.g.*, Ex. 1008 at 9:32-:32-38. In addition to the secure tunnel, one of skill in the art, based on Provino and an early draft of RFC 2660 (hereinafter "RFC 2660"), would have been motivated to employ end-to-end encryption between

the client device 12(m) and the secure server 31(s), and would have found doing so to be a straightforward and obvious design choice.

44. In particular, a person of ordinary skill would have considered it obvious to configure Provino's client device 12(m) and the secure server 31(s) to implement end-to-end encryption using the Secure HTTP (S-HTTP) protocol. Prior to February of 2000, a motivation for encrypting communications within each VPN would be to screen certain communications from others within the private network. For example, certain user information (e.g., confidential employment information) may need to be encrypted even within a private network, securing the communications from third parties without authorization to view the user information, such as network administrators.

45. RFC 2660 discloses the use of encryption between clients and servers: "Secure HTTP (S-HTTP) provides secure communication mechanisms between an HTTP client-server pair in order to enable spontaneous commercial transactions for a wide range of applications." Ex. 1029 at § 1. In particular, RFC 2660 describes that "Secure HTTP provides a variety of security mechanisms to HTTP clients and servers" and that "[s]everal cryptographic message format standards may be incorporated into S-HTTP clients and servers." Ex. 1029 at § 1.1. "S-HTTP provides full flexibility of cryptographic algorithms, modes and parameters." Ex. 1029 at § 1.1.

46. The combination of Provino and RFC 2660 would result in encrypted communications between the client device 12(m) and secure server 31(s) using S-HTTP messages instead of standard HTTP messages. In this way, the use of S-HTTP could simply replace HTTP within the secure tunneling scheme described by Provino. Thus, the exchange of the S-HTTP messages would ensure end-to-end encryption between the client device 12(m) and

secure server 31(s). Moreover, RFC 2660 describes that the client 12(m), modified to utilize S-HTTP, would still be capable of communicating with a non-secure server that does not implement S-HTTP. *See* Ex. 1029 at § 1.1 (“S-HTTP supports interoperation among a variety of implementations, and is compatible with HTTP. S-HTTP aware clients can communicate with S-HTTP oblivious servers and vice-versa, although such transactions obviously would not use S-HTTP security features.”).

47. Therefore, it would have been an obvious design choice to one of ordinary skill in the art to incorporate the cryptography provided by Secure HTTP, as taught by RFC 2660, into Provino’s client device 12(m) and secure server 31(s), in order to provide end-to-end encryption. Therefore, Provino (which discloses a secure tunnel between the client device 12(m) and the firewall 30) in view of RFC 2660 (which discloses encrypted/secure end-to-end communications between a client and server) discloses a secure communication link that starts at the client device 12(m) and ends at the secure server 31(s).

IV. Publication and Authenticity of Requests For Comment (RFCs)

48. There are a number of publications that I discuss in this report that are “Request For Comment” documents or “RFCs.” These publications are prepared and distributed under a formalized publication process overseen by the Internet Engineering Task Force (IETF).

49. The way IETF RFC publications are prepared and released to the public in a formalized and structured process. In fact, the RFC development and publication process itself is described in an RFC – RFC 2026, dated October 1996. That RFC explains that RFC publications and “Internet-Drafts” are widely disseminated on the Internet. For example, § 2.1 of RFC 2026 explains: Each distinct version of an Internet standards-related specification is published as part of the “Request for Comments” (RFC) document series. This archival series is the official publication channel for Internet standards documents and other publications of the

IESG, IAB, and Internet community. RFCs can be obtained from a number of Internet hosts using anonymous FTP, gopher, World Wide Web, and other Internet document-retrieval systems. Ex. 1041 at 5.

50. RFC 2026 explains that once a standard is adopted, it will be formally published. *See* Ex. 1041 at § 6.1.3 (“If a standards action is approved, notification is sent to the RFC Editor and copied to the IETF with instructions to publish the specification as an RFC.”) Draft IETF standards-track and other documents are also formally published and widely distributed. *See also id.* at 7 (§ 2.2) (“During the development of a specification, draft versions of the document are made available for informal review and comment by placing them in the IETF’s “Internet-Drafts” directory, which is replicated on a number of Internet hosts. This makes an evolving working document readily available to a wide audience, facilitating the process of review and revision.”).

51. RFC documents are published on a specific date, which starts a period for others to provide comments on the document. Ex.1041 at 19-120 (§ 6.2) (“These minimum periods are intended to ensure adequate opportunity for community review without severely impacting timeliness. These intervals shall be measured from the date of publication of the corresponding RFC(s)...”). The publication date of each RFC is contained in the RFC, typically in the top right corner of the first page of the document. This is the date it was released for public distribution on the Internet.

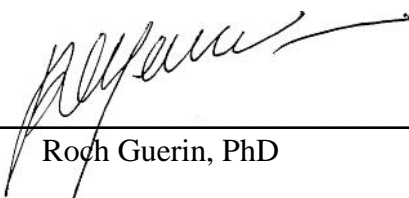
52. Each RFC document is uniquely numbered. If it becomes necessary to make a substantive change (e.g., other than a minor typographical error), the RFC will be republished with a different number. *See e.g.*, Ex. 1041 at 19-20 (§ 6.2) (“... the IESG or RFC Editor may be asked to republish the RFC (with a new number) with corrections...”).

53. The formalized process of preparing, publishing and widely distributing RFC documents is a very important part of the Internet culture, which works to develop standards in an open and transparent process. It is also important to the adoption of these standards, and the stability and functionality of the Internet for developers to adhere to standards and evolving “best practices.”

54. Because RFC documents and the IETF’s “Internet-Drafts” are published and widely distributed, they are printed publications as of the date printed on their front page. As such, I understand the RFCs and Internet-Drafts relied upon herein and submitted for this proceeding are authentic.

V. Conclusion

55. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Signature: _____
Roch Guerin, PhD

Date: April 11th, 2014