IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of: Larson *et al.*
U.S. Patent No.: 7,188,180 Attorney Docket No.: 38868-0002IP1
Issue Date: Mar. 6, 2007
Appl. Serial No.: 10/702,486
Filing Date: Nov. 7, 2003
Title: METHOD FOR ESTABLISHING SECURE COMMUNICATION LINK BETWEEN COMPUTERS OF VIRTUAL PRIVATE NETWORK

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. 7,188,180, 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 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 as 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. 7,188,180 (the "'180 patent"). Additionally, I have reviewed the following: U.S. Patent No. 6,557,037 to Provino ("Provino"); Alvaro Guillen *et al.*, 1993 International Conference on Network Protocols, *An Architecture for Virtual Circuit/QoS Routing* (Oct. 1993) ("Guillen"); Dave Kosiur, "Building and Managing

Virtual Private Networks" (1998) ("Kosiur"); E. Gavron, RFC 1535, *A Security Problem and Proposed Correction With Widely Deployed DNS Software* (Oct. 1993); RFC 791, *Internet Protocol* (Sep. 1981). I have also reviewed certain sections of the prosecution history of the '180 patent, the prosecution histories of reexamination control numbers 95/001,270 and 95/001,792; 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 '180 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 April 26, 2000 (the priority date of the '180 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 '180 Patent

11. The '180 patent is directed to a "method for establishing [a] secure communication link between computers of [a] virtual private network." Ex. 1001, Title. The '180 patent includes 41 claims, of which claims 1, 17, and 33 are independent.

12. A section of the '180 patent's specification titled "F. One-Click Secure On-Line Communications and Secure Domain Name Service" describes "a technique for establishing a secure communication link between a first computer and a second computer over a computer network," with reference to FIGS. 33-35. Ex. 1001, 49:57-59. Referring to Annotation A of FIG. 33 below, a computer 3301 establishes a VPN communication link with a server computer 3320, or a secure edge router for the server computer 3320. *See* Ex. 1001, 51:16-18, 52:30-33.

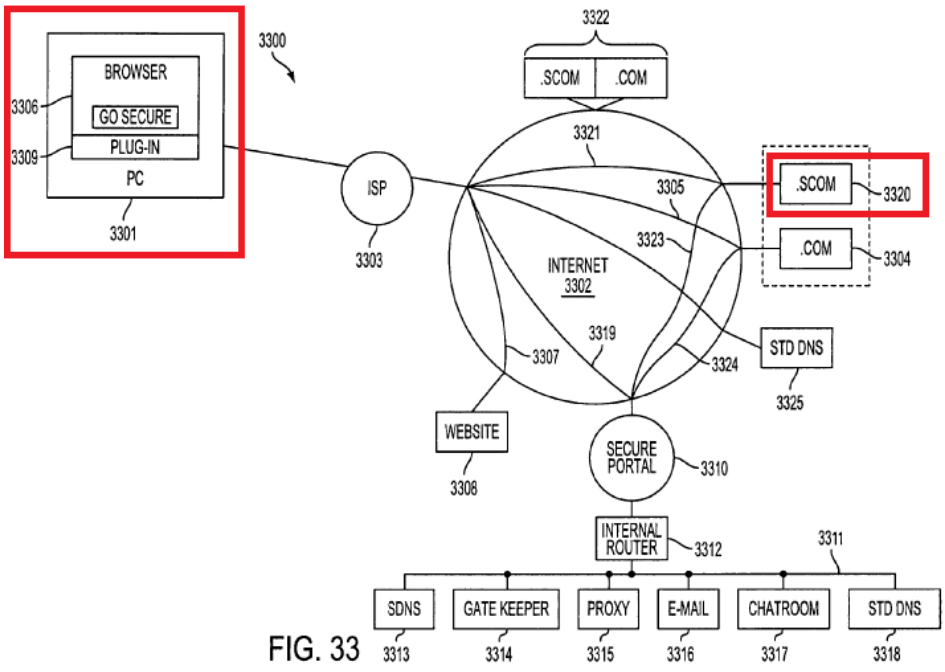

FIG. 33

Annotation A

13. The server computer 3320 is associated with a secure top-level domain name. *See* Ex. 1001, 51: 21-22. Domain names are a type of human-readable name/address for resources

on a network, such as the Internet. *See* RFC 1535, p. 1 (1993) ("Current Domain Name Server clients are designed to ease the burden of remembering IP dotted quad addresses. As such they translate human-readable names into addresses and other resource records."). Domain names are resolved by name servers into numerical addresses that are utilized for packet forwarding over networks. *See id.*; *see also* RFC 791, pp. 2, 5-6 (1981). As such, domain names may be maintained in the human-readable form, which is easier for a human operator to utilize than the numerical addresses relied upon by the networks for forwarding packets. Ex. 1003, 1:49-56.

14. With respect to the term "secure top-level domain name," the '180 patent notes that "[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." Ex. 1001, 51:29-32. Thus, in the context of the '180 patent, a secure top-level domain name is differentiated from a standard domain name in that a secure top-level domain name cannot be resolved by a standard domain name service.

15. In order to resolve the secure top-level domain name of the server computer 3320, the computer 3301 sends a query to a secure domain name service (SDNS) 3313, as illustrated in the following Annotation B of FIG. 33. *See* Ex. 1001, 51:46-50. This query to the SDNS 3313 can either be sent "in the clear" or can use a VPN communication link. *See* Ex. 1001, 52:41-43. With respect to the term "secure domain name service," the '180 patent indicates that "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses." Ex. 1001, 52:4-5. In other words, the SDNS 3313 differs from a standard name service in that it is configured to resolve secure domain names.

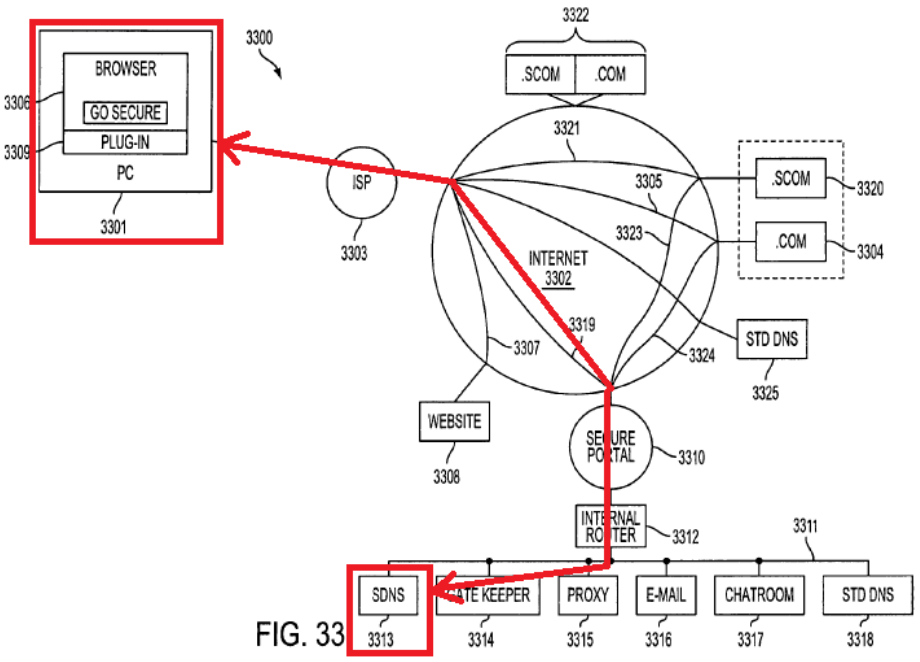

FIG. 33

Annotation B

16. Based on its cross-reference database, the SDNS 3313 responds to the query of computer 3301 with a secure network address for the server 3320. *See* Ex. 1001, 52:37-40. The secure network address is then used to establish, a VPN communication link 3321 between the computer 3301 and server 3320. *See* Ex. 1001, 52:27-54. The '180 patent describes that the SDNS 3313 and VPN gatekeeper 3314 may work together to establish a VPN communication link 3321 between computer 3301 and server 3320, or, alternatively, that the computer 3301 may establish the VPN communication link 3321 with server 3320 on its own. *See id.* Regardless of how the VPN communication link 3321 is established between computer 3301 and server 3320, the computer 3301 utilizes the secure network address it receives from SDNS 3313 to send an access request to the server 3320 over the earlier-established VPN communication link 3321, as illustrated in the following Annotation C of FIG. 33. *See* Ex. 1001, 52:55-60. In the primary embodiment described by the '180 patent, the resource accessed by computer 3301 on the server

3320 may be a secure website requested by a browser 3306 on computer 3301. *See* Ex. 1001, 52:8-26.

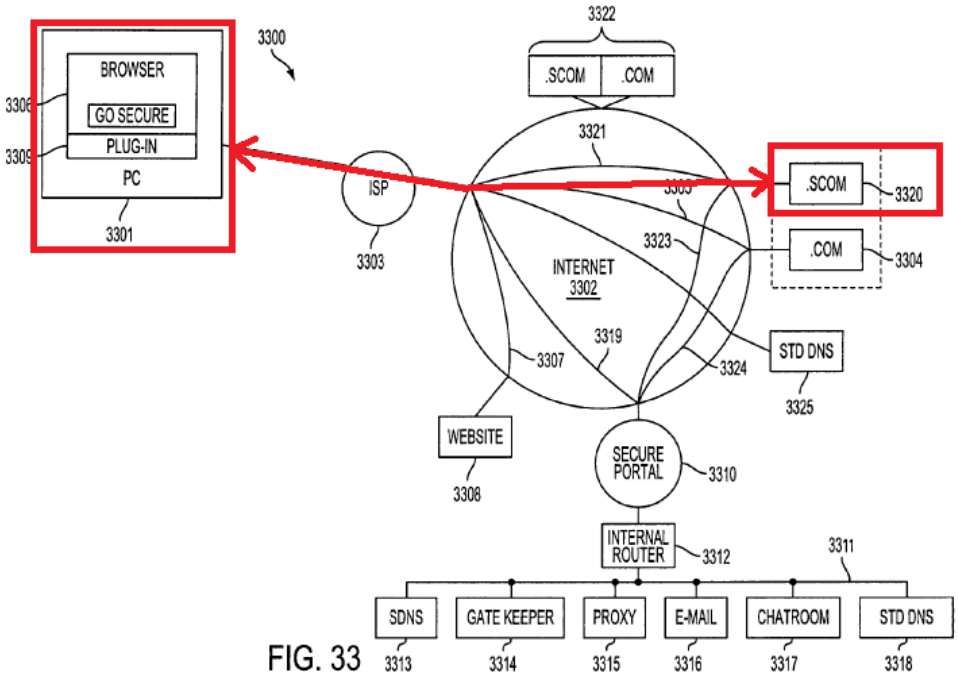

FIG. 33

Annotation C

II. Terminology

17. 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. Counsel has also informed me 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.

18. I have been informed that it would be useful to provide some guidance in this proceeding with respect to certain terms, and has asked me to consider the terms below and corresponding constructions. As part of that, for each term addressed below, I considered each

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.

19. I have considered whether a broadest reasonable interpretation of "virtual private network" would be broad enough to cover "a network of computers that privately communicate with each other by encrypting traffic on insecure communication paths between the computers." I believe that it would, since such an interpretation is not inconsistent with the '180 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. There is not an explicit definition of "virtual private network" in the '180 patent. However, in describing the "advantages of the present invention," the '180 patent describes the VPN connection between computer 3301 and secure server 3320 as "a secure communication link between a first computer and a second computer over a computer network, such as the Internet." *See* Ex. 1001, 6:42-44.

20. Moreover, some of the VPNs described in the '180 patent rely upon encryption, and the '180 patent acknowledges that "[o]ther types of VPNs can alternatively be used" for securing communications over the Internet 3302. Ex. 1001, 44:19-24; 51:66-67. I therefore believe that a broadest reasonable interpretation of "virtual private network" would be broad enough to cover "a network of computers that privately communicate with each other by encrypting traffic on insecure communication paths between the computers."

21. I have considered whether a broadest reasonable interpretation of "virtual private network communication link" would be broad enough to cover "any communication link between two end points in a virtual private network." I believe that it would, since such an interpretation is not inconsistent with the '180 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when considering the broadest reasonable

construction. There is not an explicit definition of "communication link" in the '180 patent. Instead, the '180 specification broadly describes a virtual private network (VPN) communication link through a computer network between two end points. *See* Ex. 1001, 50:26-31. However, the use of the term "communication link" in the claims and specification of the '180 patent does not limit the recited communication link to any particular end points. Indeed, the '180 patent makes clear that the VPN communication link can be established with an edge router (e.g., a firewall). Ex. 1001, 52:30-33. I therefore believe that a broadest reasonable interpretation of "virtual private network communication link" would be broad enough to cover "any communication link between two end points in a virtual private network."

22. I have considered whether a broadest reasonable interpretation of "secure computer network address" would be broad enough to cover "a network address that requires authorization for access and is associated with a computer configured to be accessed through a virtual private network." I believe that it would, since such an interpretation is not inconsistent with the '180 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when considering the broadest reasonable construction. There is not an explicit definition of "secure computer network address" in the '180 patent. However, the '180 patent describes that secure server 3320 has a secure computer network address, and that "[s]erver 3320 can only be accessed through a VPN communication link." Ex. 1001, 52:29-30. Moreover, before providing computer 3301 with the information for the server 3320, the patent specification indicates that the SDNS 3313 may verify a user's identity, which is a form of authentication and authorization. *See* Ex. 1001, 52:22-26. I therefore believe that a broadest reasonable interpretation of "secure computer network address" would be broad enough to cover

"a network address that requires authorization for access and is associated with a computer configured to be accessed through a virtual private network."

23. I have considered whether a broadest reasonable interpretation of "secure domain name" would be broad enough to cover "a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)." I believe that it would, since such an interpretation is not inconsistent with the '180 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when considering the broadest reasonable interpretation. There is not an explicit definition of "secure domain name" in the '180 patent. However, the '180 patent describes that "[b]ecause the secure top-level domain name is a non-standard domain name, a query to a standard domain name service (DNS) will return a message indicating that the universal resource locator (URL) is unknown." Ex. 1001, 51:29-32. Usage of "secure domain name" throughout the specification is consistent with this statement. *See generally* Ex. 1001, 49:57 to 54:6. I therefore believe that a broadest reasonable interpretation of "secure domain name" would be broad enough to cover "a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional domain name service (DNS)."

24. I have considered whether a broadest reasonable interpretation of "secure domain name service" would be broad enough to cover "a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses." I believe that it would, since such an interpretation is not inconsistent with the '180 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when considering the broadest reasonable construction. There is not an explicit definition of "secure domain name service" in the '180 patent. However, the '180 patent

describes that "SDNS 3313 contains a cross-reference database of secure domain names and corresponding secure network addresses." Ex. 1001, 52:4-5. Moreover, the '180 patent describes that a standard DNS cannot resolve secure domain names. *See* Ex. 1001, 51:29-32. I therefore believe that a broadest reasonable interpretation of "secure domain name service" would be broad enough to cover "a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses."

25. I have considered whether a broadest reasonable interpretation of "provisioning information" would encompass "information that enables communication in a virtual private network." I believe that it would, since such an interpretation is not inconsistent with the '180 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when considering the broadest reasonable interpretation. There is not an explicit definition of "provisioning information" in the '180 patent. Indeed, the only part of the '180 patent that uses similar language states: "VPN gatekeeper 3314 **provisions** computer 3301 and secure web server computer 3320, or a secure edge router for server computer 3320, thereby creating the VPN." Ex. 1001, 52:30-33 (emphasis added). However, the '180 patent does not provide any more detail regarding this provisioning. I therefore believe that a broadest reasonable interpretation of "provisioning information" would be broad enough to cover "information that enables communication in a virtual private network," which could include, for example, encryption keys and/or quality of service (QoS) parameters.

III. Provino and Combinations Based on Provino

A. Provino

26. In general, Provino describes a system and method for easing communications between devices connected respectively to public networks, such as the

Internet, and to private networks by facilitating resolution of human-readable addresses. Ex. 1003, title. The network 10 described by Provino and illustrated in FIG. 1 includes a virtual private network (VPN) 15 that includes a firewall 30, a plurality of servers 31(s) and a nameserver 32, all interconnected by a communication link 33. Ex. 1003, 6:15-19. The VPN 15 is "maintained by a company, governmental agency, organization or the like, which desires to allow the servers 31(s) to access other devices outside of the virtual private network 15 and transfer information thereto over the Internet 14 . . . in a controlled manner." Ex. 1003, 9:6-13.

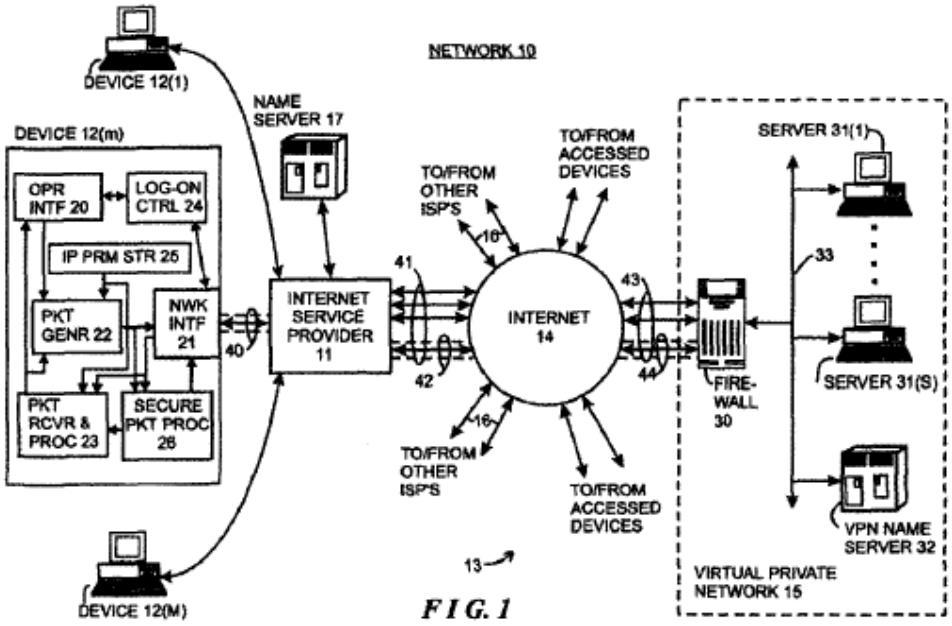

FIG. 1

27. Provino describes a process that allows a client device 12(m) to communicate with a server 31(s) inside the VPN 15. *See* Ex. 1003, 9:6-15. This process of communication proceeds in two phases. *See* Ex. 1003, 12:1-16. First, the device 12(m) and the firewall 30 negotiate to extend the VPN 15 across the Internet 14 to include the device 12(m) by establishing a secure tunnel between the device 12(m) and the firewall 30. *See* Ex. 1003, 12:17-36. Second, the device 12(m) communicates with name

server 32 to resolve the human-readable domain name of a server 31(s) into an integer Internet address that the device 12(m) uses to address its requests to the server 31(s).

28. More specifically, in the first phase, the device 12(m) requests establishment of a secure tunnel with firewall 30. Ex. 1003, 9:46-47. The firewall 30 of VPN 15 authenticates the device 12(m) by determining whether it is authorized to access a server 31(s) residing within the VPN 15. *See* Ex. 1003, 9:56-60. If the firewall 30 authenticates the device 12(m), the firewall 30 provides the encryption and decryption algorithms and keys used for establishing a secure tunnel with the device 12(m), and thus communication between the device 12(m) and the VPN 15. *See* Ex. 1003, 9:56 to 10:12. By establishing a secure tunnel with the device 12(m) over the Internet 14, the firewall 30 effectively extends the VPN 15 to include the device 12(m) via the Internet 14, as illustrated in Annotation 1 of FIG. 1. *See, e.g.*, Ex. 1006, p. 19 (describing that VPNs use "the Internet to link together a company's sites and mobile workers into one private, secure network"). In other words, after the first phase, the VPN 15 includes device 12(m).

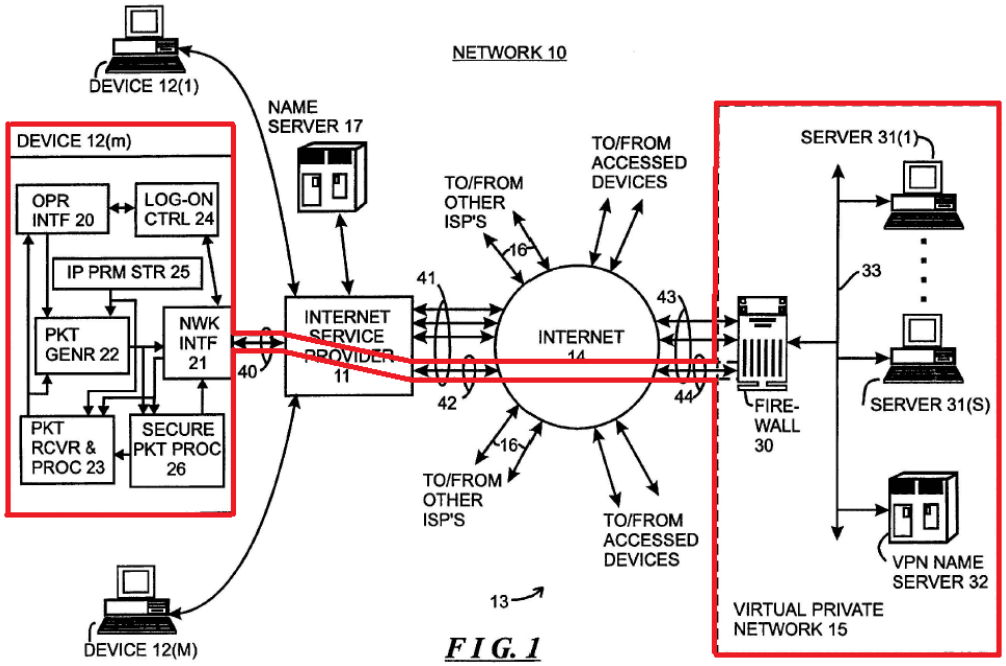

FIG. 1

Annotation 1

29. Once the secure tunnel is established between the device 12(m) and firewall 30, the device 12(m) may communicate with one or more servers 31(s) within the VPN 15. However, Provino describes that an operator of device 12(m) may provide a human-readable domain name for the server 31(s), instead of the integer Internet address that is required to communicate message packets to the server 31(s). *See* Ex. 1003, 13:26-40. Thus, after receiving the human-readable domain name from the operator, the device 12(m) must resolve the domain name into the integer Internet address of the server 31(s).

30. To resolve the domain name into the integer Internet address of the server 31(s), the device 12(m) initially accesses a nameserver 17, which is a conventional DNS server associated with internet service provider 11 and external to VPN 15. *See* Ex. 1003, 7:37-43. The device 12(m) accesses the conventional nameserver 17 in an "attempt to obtain the integer Internet address associated with the human-readable Internet address." Ex. 1003, 11:5-11. But, because the nameserver 17 is outside of the VPN 15, it will not

have the information necessary to resolve the integer Internet address of server 31(s), and will send a message indicating the error. *See* 1003, 11:11-14. In response to the error message, the client 12(m) will request resolution of the human-readable domain name from the nameserver 32 that is inside the VPN 15. *See* 1003, 11:14-17. This request (1) and the subsequent response (2) from the nameserver 32 are illustrated in the following Annotation 3 of FIG. 1.

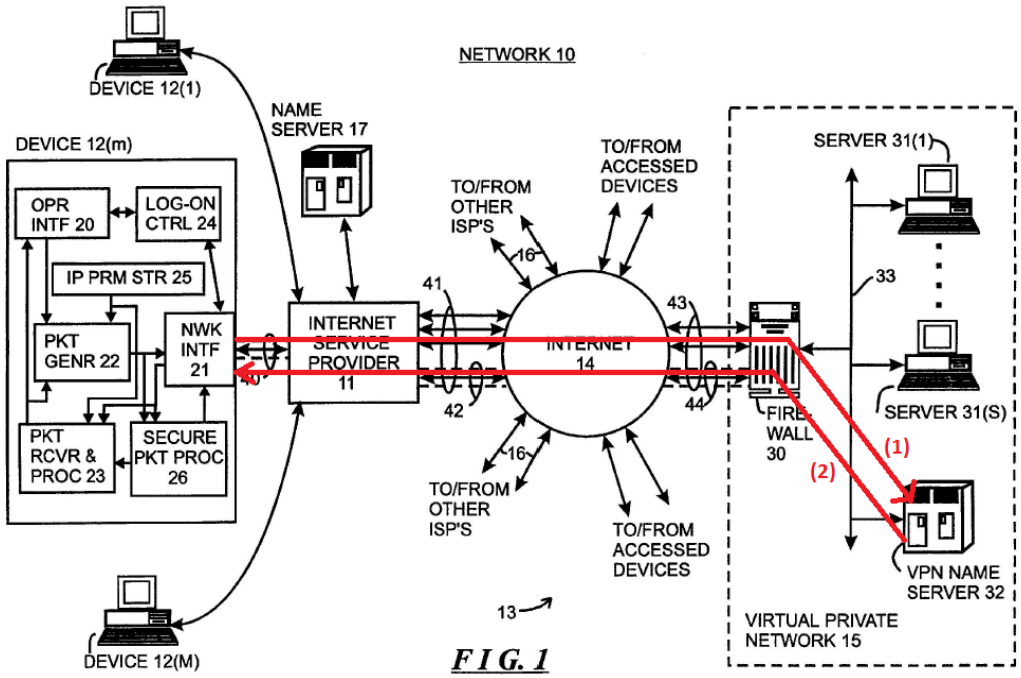

FIG. 1

Annotation 3

31. In particular, the device 12(m) sends an encrypted request message to the firewall 30 through the secure tunnel. *See* Ex. 1003, 13:63 to 14:26. The request message includes address information for the nameserver 32 and the human-readable domain name of the server 31(s). *Id.* As illustrated in the following Annotation 4 of FIG. 1, the firewall 30 decrypts the request message and transmits it over the communication link 33 to nameserver 32. *See* Ex. 1003, 14:27-34.

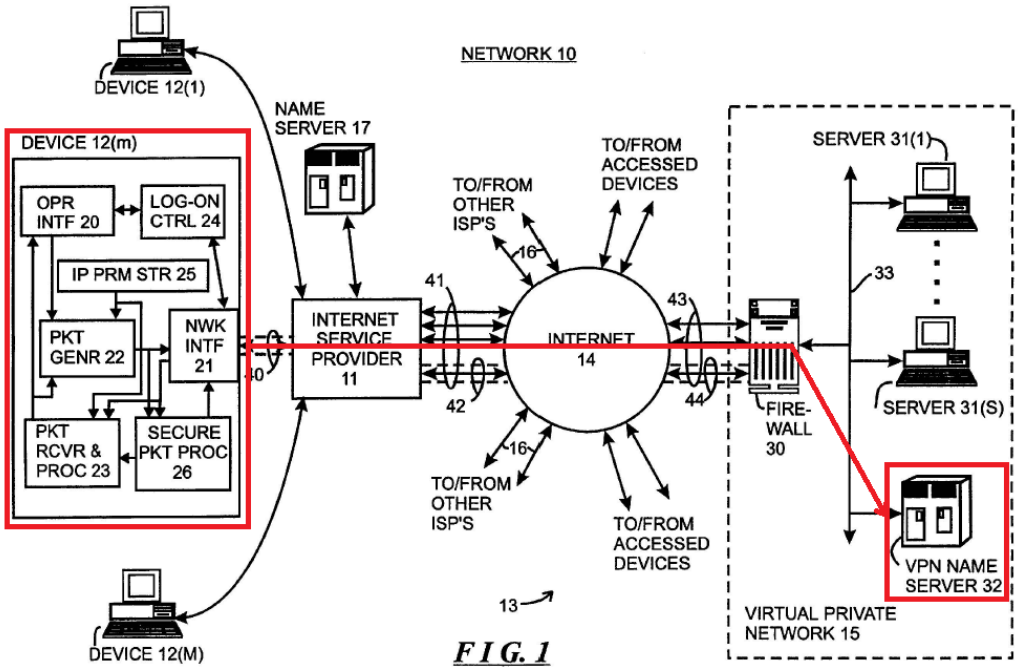

FIG. 1

Annotation 4

32. If the nameserver 32 has an integer Internet address associated with the human-readable Internet address in the request message provided by the device 12(m), it will generate a response message including the integer Internet address. Ex. 1003, 14:42-46. One of ordinary skill in the art would understand that, by determining whether it has an integer Internet address, the nameserver 32 determines whether the human-readable Internet address has been registered, because this process leverages the registration of an association between a human-readable Internet address and an integer Internet address would have to be recorded at the nameserver 32. Moreover, only if the human-readable Internet address was registered before the query (i.e., the nameserver 32 has an associated integer Internet address) does the nameserver 32 return an integer Internet address to the client 12(m). As illustrated in the following Annotation 5 of FIG. 1, the response message is passed to the firewall 30, which sends the response message to the device 12(m) over the secure tunnel.

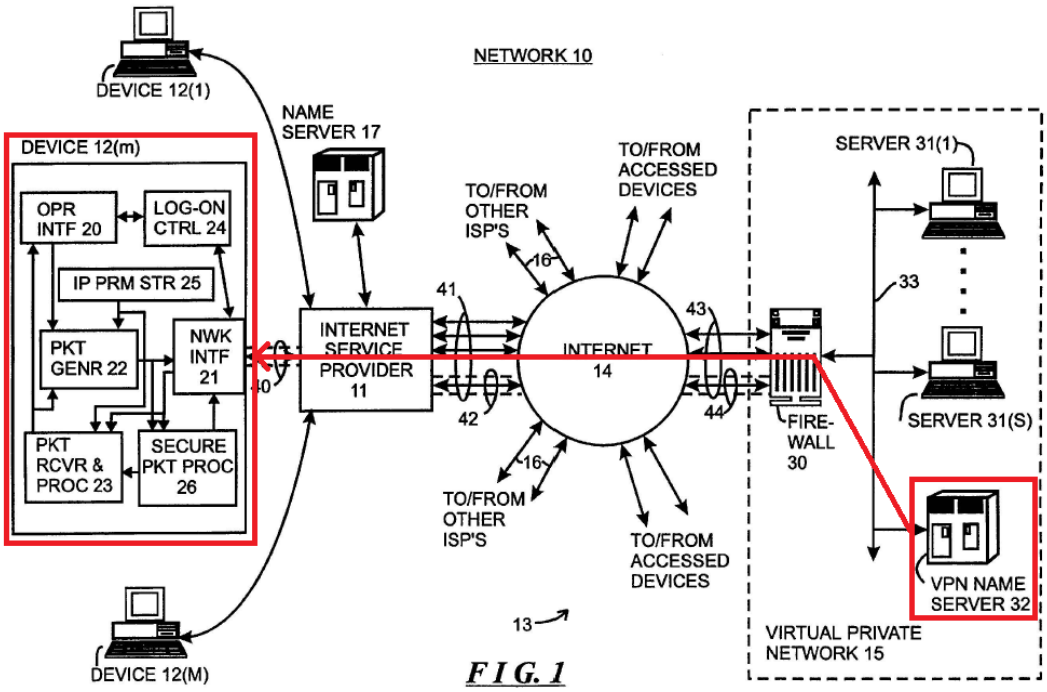

FIG. 1

Annotation 5

33. Provino describes that the integer Internet address of the server 31(s) is an IP address. As explained above, before creation of the secure tunnel, the firewall 30 must authenticate the device 12(m). *See* Ex. 1003, 9:56-60. Thus, in order for the device 12(m) to access the server 31(s), the device 12(m) must be authorized to do so. Accordingly, the integer Internet address of the server 31(s) is a network address that requires authorization for access and is associated with a computer (i.e., server 31(s)) configured to be accessed through a virtual private network. Moreover, Provino 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)," which are the number of bits in Internet Protocol Version 4 and 6 IP addresses, respectively. Ex. 1003, 1:45-47. Therefore, it is clear that the integer Internet address of the server 31(s) is an IP address.

34. Provino describes that the human readable domain name of the server 31(s) may be a non-standard domain name that corresponds to a secure computer network address (i.e., integer Internet address of the server 31(s)) and cannot be resolved by a conventional domain

name service (DNS). In particular, Provino describes that the human readable domain name of the server 31(s) may be "any form of secondary or informal network address arrangement." Ex. 1003, 16:12-17. In other words, the VPN 15 described by Provino is configured to support non-standard human readable domain names. Moreover, as described above, conventional nameserver 17 cannot resolve the human-readable domain names of the servers 31(s) internal to the VPN 15. *See* Ex. 1003, 11:11-14.

35. Provino describes that the nameserver 32 is a service that can resolve secure computer network addresses for a secure domain name for which a conventional domain name service cannot resolve addresses. In particular, as highlighted in Annotation 6 of FIG. 1 below, the nameserver 32 is behind firewall 30, within VPN 15 and specifically configured to resolve the human-readable domain names of the servers 31(s) internal to the VPN 15. *See* Ex. 1003, 8:67 to 9:5. As described above, conventional nameserver 17 cannot resolve the human-readable domain names of the servers 31(s) internal to the VPN 15. *See* Ex. 1003, 11:11-14.

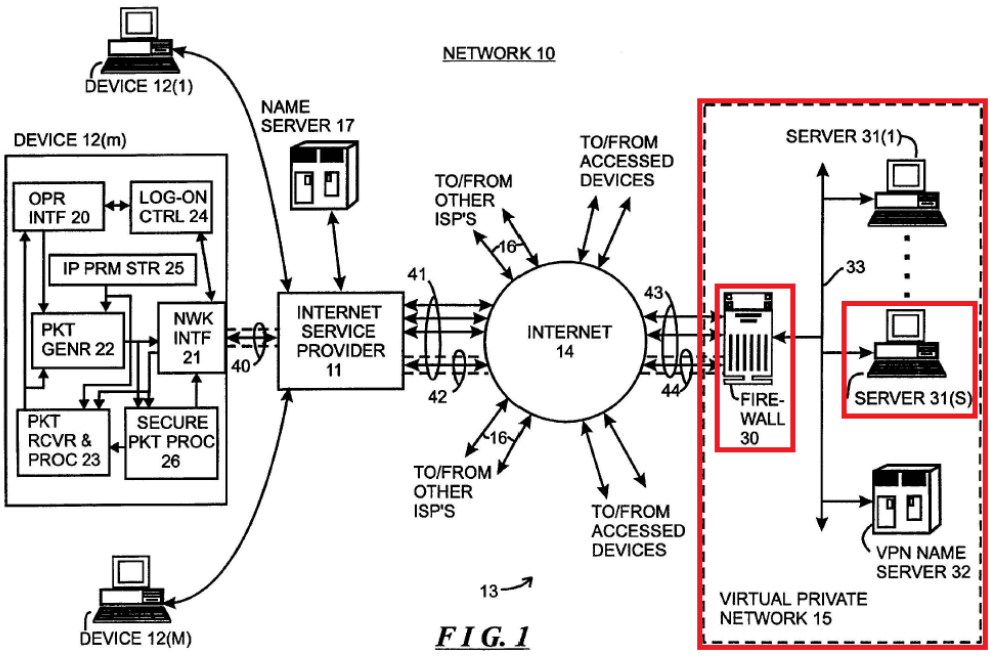

FIG. 1

Annotation 6

36. The firewall 33 encrypts the integer Internet address of the server 31(s) when forwarding the response message to the client device 12(m). In particular, Provino describes that the response message including the integer Internet address that is sent by the nameserver 32 is initially forwarded to the firewall 30 over the communication link 33. *See* Ex. 1003, 14:42-46. The firewall 33 will then "encrypt the response message packet received from the nameserver 32." Ex. 1003, 14:59-61. Because the response message includes the integer Internet address of the server 31(s), the firewall 33 necessarily encrypts the integer Internet address of the server 31(s) as part of encrypting the response message. *See id.*

37. Also as part of forwarding the response message from the nameserver 32 to the client device 12(m), the firewall 30 is configured, where necessary, to encapsulate the encrypted response packet in a message packet that "conform[s] to the protocol of Internet 14." *See* Ex. 1003, 14:57 to 15:19. In particular, the firewall 30 "generate[s] a message packet for transmission to the device 12(m) including the encrypted response message packet." Ex. 1003, 14:61-63. In other words, the firewall encapsulates the encrypted response message packet in another message packet for transmission over the secure tunnel. "In addition, depending on the protocol for transmission of message packets over the communication link 33, the firewall 30 may need to process and/or modify the message packet to conform to the protocol of Internet 14." Ex. 1003, 15:16-19. Thus, the VPN 15 (through firewall 30) encapsulates a first packet of a first protocol (i.e. the packet received from the nameserver 32) in a second packet of a second protocol (i.e., the packet transmitted from the firewall 30 to the computer 12(m)).

38. After receiving the encrypted response message from the firewall 30, the device 12(m) "decrypt[s] the encrypted portion of the message packet to obtain the integer Internet address associated with the human-readable Internet 25 address." Ex. 1003, 15:20-27. Because

the integer Internet address was encrypted as part of the response message, as described above, the device 12(m) decrypts the integer Internet address as part of decrypting the response message. With the decrypted integer Internet address, the device 12(m) may communicate directly with the server 31(s), as illustrated in the following Annotation 7 of FIG. 1. *See* Ex. 1003, 15:27-30.

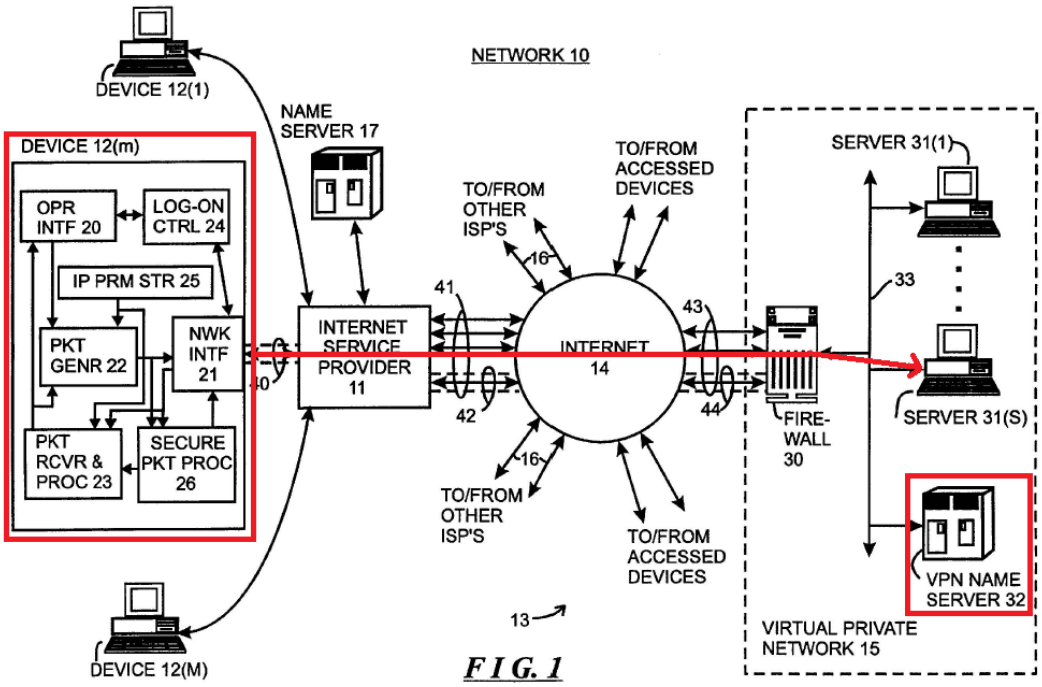

FIG. 1

Annotation 7

39. 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. *See* Ex. 1003, 15:21-30. In particular, Provino describes that the server 31(s) may be a "storage server" that provides information that is requested by a client. *See* Ex. 1003, 6:19-50. As a consequence, the requests sent to server 31(s) by device 12(m) may be requests for information stored at the server 31(s). 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 contain requests for access to information stored on server 31(s).

B. Provino in view of Guillen and Kosiur

40. Guillen describes the use of Quality of Service (QoS) parameters in a network to ensure that characteristics of communications over the network "correspond to the needs of [any] application that will be used" by a user on the network. Ex. 1005, § 2.1, p. 81. "With the emergence of multimedia applications, networks have to provide more and more bandwidth and should guarantee the quality of the communication between users." Ex. 1005, p. 80, Abstract. In this context, the term QoS "is used to refer to the parameters allowing . . . control [of] the characteristics of the data transmission." Ex. 1005, § 2.3, p. 82. By implementing a QoS system, devices in a network can control the characteristics of the data transmission related to a given multimedia application such that the service requirements of that multimedia application are met, and the multimedia application can properly function. *See* Ex. 1005, §§ 2.3 and 2.4, pp. 81-82.

41. The clients within a network must have a means to determine the QoS parameters necessary for a given connection and application. *See* Ex. 1005, § 2.3, p. 82. One way to provide a client with QoS parameters is through the use of a DNS directory service. *See id.* Recognizing that applications rely upon DNS directory services for address resolution, Guillen proposes that the DNS directory services also store values of QoS parameters that are related to connections to the destination for which an address is being resolved. *See id.* Through this proposal, a user is able to obtain "an indication of what [QoS-level] is feasible" at the point of address resolution.

42. Though Guillen describes QoS parameters in the context of a Virtual Circuit model such as Asynchronous Transfer Mode (ATM), it was well known at the time of the'180 patent that QoS parameters were equally applicable in any network architecture supporting multimedia applications, including VPNs. *See, e.g.*, Kosiur, pp. 243-254. In the context of VPNs, it was well known that, "to support the different latency and bandwidth requirements of multimedia and other real-time applications, networks can use QoS parameters to accept an application's network traffic and prioritize traffic relative to other QoS requests from other applications." *See, e.g.*, Kosiur, p. 159. Thus, the benefits of QoS described by Guillen in the context of ATM communications were known by those of ordinary skill in the art to be equally applicable to VPNs. Moreover, Provino relies upon DNS servers to perform address resolution in the context of VPNs in the same manner as Guillen describes their use in the context of ATM communications. *See* Ex. 1003, 10:45-67. Therefore, it would have been obvious to one of ordinary skill in the art to modify the VPN 15 described by Provino to utilize QoS parameters in the manner described by Guillen so that Provino's VPN could support the "the different latency and bandwidth requirements of multimedia and other real-time applications" used by the device 12(m) and the servers 31(S).

43. In particular, a person of ordinary skill in the art would have modified the VPN name server 32 of Provino to store, in part, topology dependent QoS parameters, as described by Guillen. Such a modified VPN name server 32 would be configured to respond to requests by device 12(m) to resolve the human-readable network addresses of servers 31(S) with both the integer Internet address of the servers 31(S) and the QoS parameters for the servers 31(S). As described by Guillen, the device 12(m) would insert these QoS parameters into a field of the packets transmitted from the device 12(m) to the servers 31(S), indicating the level of service for

these packets ("such as 'high - medium –low'"). *See* Guillen, § 2.3, p. 82; § 3.9, p. 86. To accommodate these QoS parameters, the network devices that handle communications over the VPN 15 would rely upon these QoS parameters to control characteristics of data transmissions between the device 12(m) and the servers 31(S). *See* Guillen, § 2.3, p. 82. As implemented in the proposed modification, the QoS parameters are a type of provisioning information for the VPN 15, because the devices of the VPN 15 rely upon the QoS parameters to control the characteristics of data transmission over the VPN 15.

IV. Conclusion

44. 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: _____ Date: January 10, 2014
Roch Guerin, PhD