2. Requester's assertion that He and Fortinsky are directed to using ticket-based security architecture to control users' access to application servers on the network (e.g., network resources).

Requester and the Examiner accurately describe He and Fortinsky as a "ticket based *security architecture*." However as described above, the ticket based security architecture requires that the "ticket" contain information regarding the user identity, user authority, user privileges and the identity of a network server to be accessed. This ticket information is communicated over the network before any access control occurs. The access processing must therefore occur at the network element after the ticket information is transmitted over the network to the network server. By contrast, the '118 patent uses a rule set that includes "elements or conditions" programmed into a redirection sever to control access to the network itself. He and Fortinsky and Admitted Prior Art do not teach controlling access to the network, but rather, access to information on an identified network server where access is allowed or denied based on processing of the ticket data at the network server *after access to the network itself has been allowed without restriction.* The cited references, alone or in any possible combination, therefore do not suggest, disclose or provide any motivation for controlling access to the network itself, and indeed, *teach just the opposite* -- the absence of any filter or control of access to the network itself.

3. Requester's assertion that Fortinsky uses a "gateway server" to allow a ticket to access external network elements.

Requester argued, and the Examiner adopted, the position that Fortinsky uses a "gateway server" and therefore, it would have been obvious to use a gateway server in He. However, Requester misperceives the purpose and function of the "gateway server" of Fortinsky. Specifically, the "gateway server" is a server that modifies the ticket information to be readable by a network server, that is, a server external to the private network so that the external server can process the ticket information and either allow or deny access to the information on that external server. The "gateway server" does not allow or deny access to any network including the external network, as required by the '118 patent. As with He, the ticket data of Fortinsky is transmitted on the network without pre-processing or restriction, which is contrary to the requirements of the ‘118 patent where access control, essential to enable the ‘118 patent system to perform its intended function, is to the network itself. Furthermore, the only processing taught by He and Fortinsky is done *at the destination server*, whether on the private network or an external network, using data from the ticket transmitted to the destination sever. As such, Fortinsky *actually teaches away* from the ‘118 patent system.

4. Requester’s assertion that one of ordinary skill in the art would have considered placing a redirection server between the user and the network because there would be a “a reasonable expectation of success in controlling a user’s access to the public network by locating the redirect server … between the user’s dial-up network server and the public network.”

He, Fortinsky and the Admitted Prior Art each teach processing ticket information *at a destination server after the ticket information has been transmitted without restriction over the network*. Processing at the destination server is essential to be able to perform the security function and protect the security of the information on that destination server. If the ticket information processing was done at the user side merely to give access to the network, as claimed by ‘118 patent, the user would either be indiscriminately blocked or given access to any destination server on the network, and the security purpose of the references could not be achieved.

The specific claim language that supports the above analysis is now discussed.

D. Processing Before Network Access is Allowed.

The processing of data before access to the network (public or private) is permitted is a requirement of each of the claims of the ‘118 patent. Self-evident is the fact that control over access to a network (e.g., so that access services can be billed to a customer), necessarily requires that the control processing must be performed *<u>before</u> access is granted.* If access were granted first, any subsequent control would obviously be useless in achieving the purpose of the ‘118 patent. The ‘118 patent network access control is not based on processing data at the destination server, nor is it to protect information stored on a destination server, as required by He and Fortinsky. Zenchelsky does teach a firewall that is arguably at the user side of a network. However, Zenchelsky still teaches controlling access to identified network elements based on the content of those network elements, albeit at the user side of the network.

The ‘118 patent is not concerned with the content of network elements, only with controlling access to the network itself to enable a provider to be able to charge a fee for granting that access.

E. User’s Credentials Do Not Meet the Definition of “Rule Set” From The ‘118 Patent.

Requester argues that the user “credentials” of He; the privilege attribute certificate (PAC) of Fortinsky; and the individualized rules of Zenchelsky are the same as the “rule sets” taught by the ‘118 patent. However, both Requester and the Examiner have again failed to articulate any basis for this conclusion. Furthermore, as set forth in, e.g., Sections IV – X above, there are no grounds for this rejection because there is no teaching in any of the prior art, alone or in combination, of the “rule set” defined and claimed in the ‘118 patent as incorporating “elements or conditions” programmed into a redirection server for processing data packets from a user during a user session, or a “rule set” that enables the redirection server to modify the rule set during a user session.

A finding of obviousness requires that the rejection articulate the reasons why the references teach, disclose or would motivate one skilled in the art to incorporate a rule set that incorporates “elements or conditions,” where the rule set is programmed into a redirection sever and the redirection server thereafter processes data packets from a user during a user session according to the rule set, and to enable the redirection server to modify the rule set during a user session. Having failed to articulate *any* basis for this obviousness rejection based on the meaning of rule set defined and taught only in the ‘118 patent, this obviousness rejection must be withdrawn.

F. Redirection

Reference is made to, e.g., Sections IV(B), V(D), VII(D) and IX(B). For the same reasons set forth in those Sections, none of the prior art teach redirection by a redirection server into which a rule set is programmed where the programmed rule set itself includes a “redirect” action to be performed on data packets passing through the redirection server from a user computer at the user side of the network. Accordingly, Patent Owner respectfully requests withdrawal of the rejections of the claims based on He, Zenchelsky and Forinsky and the Admitted Prior Art.

G. Modification of "Rule Set"

Reference is made to, e.g., Sections IV(C), V(E), VII(C) and IX(C). For the same reasons set forth in those Sections, none of the prior art teach modification of the rule set by the redirection server during a user session, or that the modification is effected by the programming of the rule set in response to an "element or condition" which are part of the rule set. Accordingly, Patent Owner courteously requests withdrawal of the rejections of the claims based on He, Zenchelsky and Forinsky and the Admitted Prior Art.

XII. Conclusion.

For all of the above reasons, the Examiner is respectfully requested to withdraw the rejections of all claims and issue a Reexamination Certificate allowing all claims, or withdraw the grant of this Reexamination and issue a denial of the Request.

The Examiner is invited to direct any questions regarding this matter to the undersigned at the below-listed contact numbers and addresses.

Respectfully submitted,
Koichiro Ikudome et al.

/Abe Hershkovitz/
Abraham Hershkovitz
Reg. No. 45,294

Date: January 17, 2013

HERSHKOVITZ & ASSOCIATES, LLC
2845 Duke Street
Alexandria, VA 22314
TEL: (703) 370-4800
FAX: (703) 370-4809
E-MAIL: patent@hershkovitz.net

R1341006F.A02; AH/pjj

CERTIFICATE OF SERVICE

It is hereby certified that the attached RESPONSE TO OFFICE ACTION UNDER 37 CFR §1.945, COPY OF RESPONSE AND AMENDMENT UNDER 37 CFR §1.111 AFTER BOARD DECISION IN PROCEEDING NO. 90/009,301 and this Certificate of Service **are being served on January 17, 2013 by first class mail** on the third party requester at the third party requestor's address:

IP Section
HAYNES & BOONE
2323 Victory Avenue, Suite 700
Dallas, TX 75219

/Abe Hershkovitz/
Abraham Hershkovitz

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Koichiro Ikudome, et al.	Art Unit: 3992
Reexamination Proceeding: 90/009,301 (based on U.S. Patent No. 6,779,118)	Confirmation No.: 6609
Reexamination Filed: December 17, 2008	Examiner: Sam Rimell

For: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

RESPONSE UNDER 37 CFR 1.111
AND PROPOSED AMENDMENT UNDER 37 CFR 1.530

Attn: Mail Stop "Ex Parte Reexamination"
August 20, 2010
Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, Virginia 23313-1450

Dear Commissioner:

This Response is in reply to the Board of Appeals Decision ("Decision") mailed on August 23, 2011, and the Personal Interview held on October 3, 2011 and subsequent follow-up telephone interview in the above-identified *ex-parte* reexamination proceeding. The due date for filing a Response is October 24, 2011 (because October 23, 2011 falls on a Sunday). Accordingly, this Response is timely filed. A Statement of Substance of Interview is being submitted concurrently.

Please amend the present claims as proposed below and consider the detailed traversal below, wherein:

The Status of claims is listed on page 2 of this paper.

Amendments to the Claims begin on page 3 of this paper.

Remarks/Arguments begin on page 18 of this paper.

Evidence of Service of this Response on the 3rd party requester is found after the last page of this paper.

STATUS OF CLAIMS

Claims 1-47 are subject to reexamination. According to the Decision:

- the Examiner's rejection of claims 32, 37, 42, and 47 is affirmed;
- claims 1, 8, 15, and 25 are rejected under a new grounds of rejection; and
- the rejection of all other claims (2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46) is reversed.

In response to the Decision, the following amendments are made, resulting in pending claims 2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46, and 48-94.

AMENDMENTS TO THE CLAIMS

Per 37 CFR 1.530(i) and MPEP 2250, these amendments are made relative to the patent as of the date of filing the request for examination. This Amendment does not introduce new matter. Accordingly, entry of this Amendment is appropriate and is urged.

Rejected claims 1, 8, 15, 25, 32, 37, 42, and 47 are canceled. Claims 16-23 and 38-41 are placed in independent form.

Additionally, a new set of claims is provided (48-94) which corresponds to the claim set that was appealed, and which further clarifies the location of the redirection server. Specifically, new independent claims 48, 60, 72, and 87 correspond to independent claims 1, 8, 15, and 25 respectively, with additional terms to clarify the "between" location of the redirection server. These clarifications were discussed with the Examiners at the Personal Interview held on October 3, 2011, and follow-up telephone interviews with the Examiner and the Examiner stated that such clarifications would overcome the applied art and make these claims patentable.

Similarly, new dependent claims 49-59, 61-71, 73-86, and 88-94 depend from allowable independent claims 48, 60, 72, and 87, respectively, and generally correspond respectively, to dependent claims 2-7, 28-32, 9-14, 33-37, 16-24, 38-42, 26-27 and 43-47, depending from independent claims 1, 8, 15, and 25.

Claims 2-7, 9-14, 16-24, 26-31, 33-36, 38-41 and 43-46, as to which the Board overturned all prior rejections, as well as new claims 48-94 are pending.

1. (Canceled)

2-7. (Original)

8. (Canceled)

9-14. (Original)

15. (Canceled)

16. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

18. (Thrice Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses. [access.]

19. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. (Thrice Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses. [access.]

22. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses. [access.]

23. (Amended) [The system of claim 15,] A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

24. (Original)

25. (Canceled)

26. (Twice Amended) The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses. [access.]

27. (Twice Amended) The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and [the] a location or locations the user accesses. [access.]

28. (New) The system of claim 1, wherein the individualized rule set includes at least one

rule as a function of a type of IP (Internet Protocol) service.

29. (New) The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

30. (New) The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

31. (New) The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

32. (Canceled)

33. (New) The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

34. (New) The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

35. (New) The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

36. (New) The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

37. (Canceled)

38. (New) A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

39. (New) A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

40. (New) A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

41. (New) A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

42. (Canceled)

43. (New) The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

44. (New) The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

45. (New) The method of claim 25, wherein the modified rule set includes at least one rule

allowing access based on a request type and a destination address.

46. (New) The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

47. (Canceled)

48. (New) A system comprising:

a database with entries correlating each of a plurality of user IDs with an individualized rule set;

a dial-up network server that receives user IDs from users' computers;

a redirection server connected between the dial-up network server and a public network, and

an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

49. (New) The system of claim 48, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

50. (New) The system of claim 48, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

51. (New) The system of claim 48, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

52. (New) The system of claim 48, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

53. (New) The system of claim 48, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

54. (New) The system of claim 48, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

55. (New) The system of claim 48, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

56. (New) The system of claim 48, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

57. (New) The system of claim 48, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

58. (New) The system of claim 48, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

59. (New) The system of claim 48, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule

set.

60. (New) In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server, a method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

61. (New) The method of claim 60, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

62. (New) The method of claim 60, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

63. (New) The method of claim 60, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

64. (New) The method of claim 60, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

65. (New) The method of claim 60, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

66. (New) The method of claim 60, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

67. (New) The method of claim 60, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

68. (New) The method of claim 60, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

69. (New) The method of claim 60, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

70. (New) The method of claim 60, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

71. (New) The method of claim 60, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

72. (New) A system comprising:

a redirection server connected between a user computer and a public network, the redirection server programmed with a user's rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.

73. (New) The system of claim 72, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

74. (New) The system of claim 72, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

75. (New) The system of claim 72, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

76. (New) The system of claim 72, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

77. (New) The system of claim 72, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

78. (New) The system of claim 72, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

79. (New) The system of claim 72, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

80. (New) The system of claim 72, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

81. (New) The system of claim 80 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

82. (New) The system of claim 72, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

83. (New) The system of claim 72, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

84. (New) The system of claim 72, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

85. (New) The system of claim 72, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

86. (New) The system of claim 72, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

87. (New) In a system comprising a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a

plurality of functions used to control data passing between the user and a public network; a method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and

wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

88. (New) The method of claim 87, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

89. (New) The method of claim 87, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.

90. (New) The method of claim 87, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

91. (New) The method of claim 87, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

92. (New) The method of claim 87, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

93. (New) The method of claim 87, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

94. (New) The method of claim 87, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.

REMARKS

I. Introduction and Discussion of Preliminary Issues

Patent Owner appreciates the courtesies and helpful suggestions by the Examiners at the Personal Interview of October 3, 2011 and follow-up telephone interviews. The Examiners stated that if the independent claims were amended to clarify the location of the redirection server, then such clarification would overcome the applied art.

Patent Owner asserts that the location of the redirection server is already clear in independent claims 1, 8, 15, and 25. Indeed, in the co-pending litigation, the district court judge has already issued a claim construction consistent with Patent Owner's argument. However, in the interests of compact prosecution and special dispatch, Patent Owner has added new independent claims 48, 60, 72, and 87 (corresponding to canceled independent claims 1, 8, 15, and 25 respectively) with additional terms to clarify the "between" location of the redirection server. Patent Owner notes that these new claims do not add new matter nor do they alter the scope of the original claims.

Thus, Patent Owner respectfully submits that the new claims 48-94 (independent claims 48, 60, 72, and 87 plus their dependent claims) are patentable for, at a minimum, the clarified "between" location of the redirection server, in addition to the reasons discussed below regarding corresponding canceled claims.

For the convenience of the Examiner, a list is provided below explaining the history of all pending claims. The Examiner is invited to confirm the history. The term "amended original claim" refers to a claim from the issued patent which has been amended during this reexamination. The **independent claims in the left hand column are bolded** for convenience.

TABLE 1: HISTORY OF CLAIMS 1-47

CLAIM	HISTORY OF CLAIM
1	Canceled original independent claim
2-7	Original claims, depending from canceled original independent claim 1
8	Canceled original independent claim
9-14	Original claims, depending from canceled original independent claim 8

15	Canceled amended original independent claim
16-23	Amended original claims, originally dependent upon original independent claim 15, placed into independent form by incorporating all features of amended original independent claim 15.
24	Original claim, depending from claim 23.
25	Canceled original independent claim.
26	Amended original claim, depending from canceled original independent claim 25.
27	Amended original claim, depending from canceled original independent claim 25.
28-31	New claims, depending from canceled original independent claim 1
32	Canceled new claim, previously depending from original independent claim 1
33-36	New claims, depending from canceled original independent claim 8
37	Canceled new claim, previously depending from original independent claim 8.
38-41	New independent claims, previously dependent upon amended original independent claim 15, placed into independent form by incorporating all features of amended original independent claim 15.
42	Canceled new claim, previously depending from amended original independent claim 15
43-46	New claims, depending from canceled original independent claim 25
47	Canceled new claim, previously depending from original independent claim 25.

TABLE 2: CORRESPONDENCE OF NEW CLAIMS 48-94

CLAIM	CORRESPONDENCE
48	**Canceled original independent 1 (with location of redirection server clarified)**
49	Original 2
50	Original 3
51	Original 4
52	Original 5
53	Original 6
54	Original 7

55	New 28
56	New 29
57	New 30
58	New 31
59	Canceled new 32
60	**Canceled original independent 8 (with location of redirection server clarified)**
61	Original 9
62	Original 10
63	Original 11
64	Original 12
65	Original 13
66	Original 14
67	New 33
68	New 34
69	New 35
70	New 36
71	Canceled new 37
72	**Canceled amended original independent 15 (with location of redirection server clarified)**
73	Original 16
74	Original 17
75	Original 18
76	Original 19
77	Original 20
78	Original 21
79	Original 22
80	Original 23
81	Original 24
82	New 38
83	New 39

84	New 40
85	New 41
86	Canceled new 42
87	**Canceled original independent claim 25, (with location of redirection server clarified)**
88	Amended original 26
89	Amended original 27
90	New 43
91	New 44
92	New 45
93	New 46
94	Canceled new 47

II. Rejections reversed (2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46)

In the interests of compact prosecution and special dispatch, all claims rejected by the Decision are hereby canceled (1, 8, 15, 25, 32, 37, 42, and 47).

The rejections of the remaining claims (2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46) were reversed by the Decision. Thus, these claims (2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46) remain as appealed except that claims 16-23 and 38-41 are placed into independent form (because base independent claim 15 was previously amended). Patent Owner respectfully submits that, following the Decision reversing the rejection of these claims, and absent any new grounds of rejection by the Board, the status of these claims (2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46) is now allowable.

Patent Owner respectfully requests that the Examiner confirm the status of these claims as being allowable.

III. Additional new claims clarifying location of redirection server

New independent claims 48, 60, 72, and 87 have been added, and correspond to canceled independent claims 1, 8, 15, and 25 respectively while clarifying the location of the redirection server. The requested clarification is consistent with the Patent Owner's argument during this reexamination. The clarification also is consistent with the claim construction of "redirection server" provided by the district court judge in the co-pending litigation: "a server logically located between the user's computer and the network that controls the user's access to the network." The Examiner agreed during the above-mentioned interviews that these claims were allowable.

IV. Canceled claims 1, 8, 15 and 25 – Redirection Server

Patent Owner has canceled claims 1, 8, 15, and 25 in the interests of special dispatch. However, to keep the record clear, Patent Owner does not agree or acquiesce to the Board's position and maintains that canceled claims 1, 8, 15, and 25 should have been confirmed over the applied art.

On appeal, the Board reversed the Examiner's obviousness rejection holding that the "examiner's construction of 'redirection server' was overbroad in view of the underlying disclosure" and that HE did not teach or suggest redirecting, alone or in combination with Zenchelsky. However, the Board also reiterated that "[d]uring reexamination, a claim ... is accorded the broadest construction that is reasonable in view of the specification..." Relying on this principle, the Board stated that representative claim 1 "does not exclude communications between a user and a control server via a public network." In view of this interpretation of representative claim 1, the Board, asserted that the background section of the Present Patent's specification (patent 6,779,118, hereinafter referred to as "the '118 patent") disclosed redirection by web-servers where the redirection URL was supplied by the web server over a public network. The Board, combining HE, Zenchelsky, and the web-server redirection taught by the '118 background section, entered its new obviousness rejection of representative claim 1 (and by extension claims 8, 15 and 25). This rejection was essentially based on its broad interpretation of the independent claims as encompassing web-servers because those claims did not explicitly recite the redirection server as being *between* the user computer and point of access to the public network

This new rejection was entered over Patent Owner's consistent position during the reexamination proceeding, including the appeal to the Board, and during the prosecution of the original application, that claims 1, 8, 15 and 25, properly understood and interpreted in light of the specification, precluded communication between a user and a web-server via a public network to control access to the public network for two reasons. First, the language of the claims themselves require the redirection server to be between the user computer and the public network. Second, the claims must be interpreted in light of the specification, which explicitly teaches that "the redirection server 208 is logically located *between* the user's computer 100 and the network, and controls the user's access to the network (emphasis added)" ('118 at Col. 4, lines 50-52). The Board's "broadest" possible construction therefore contradicts the intrinsic evidence. Patent Owner also argued that the Board's interpretation (allowing access to the public network before processing by the redirection server) would defeat an essential purpose of the' 118 patent, that is, controlling access to the public network.

Patent Owner further submits that other features of the independent claims were not addressed by the Board (or by previous rejections), and therefore the rejections are improper. Examples of these other features are discussed below in a separate section.

Notwithstanding Patent Owner's disagreement with the Board's decision and rationale, in the interests of compact prosecution and special dispatch, Patent Owner has canceled claims 1, 8, 15, and 25, and has added corresponding new claims 48, 60, 72, and 87 (which have been clarified regarding the "between" location of the redirection server). For example, claim 72 includes the words "connected between a user computer and a public network" to clarify the location of the redirection server. The clarification is consistent with the claim construction of "redirection server" provided by the district court judge in the co-pending litigation: "a server logically located between the user's computer and the network that controls the user's access to the network."

V. Claim 1: Other features (regarding individualized rule set)

In addition to the Board's overbroad interpretation of redirection server discussed above, Patent Owner also submits independent claim 1 was confirmable over the cited art for the following additional reasons:

First, claim 1 requires that the redirection server process data "according to the individualized rule set." No such individualized rule set or processing is disclosed by the cited art, including the '118 background section.

Second, claim 1 requires that "the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server." No such authentication accounting server feature is disclosed by the cited art, including the ‘118 background section.

For at least these additional reasons, independent claim 1 was confirmable over the cited art. The above arguments regarding canceled claim 1 apply to corresponding new claim 48 (which has been clarified regarding the “between” location of the redirection server).

VI. Claim 8: Other features (regarding individualized rule set)

In addition to the Board's overbroad interpretation of redirection server discussed above, Patent Owner also submits that independent claim 8 is was confirmable over the cited art for the following additional reasons:

First, claim 8 requires “communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server.” No such communication is disclosed by the cited art.

Second, claim 8 requires processing data “according to the individualized rule set.” No such individualized rule set or processing is disclosed by the cited art, including the ‘118 background section.

For at least these additional reasons, canceled independent claim 8 was confirmable over the cited art. The above arguments regarding canceled claim 8 apply to corresponding new claim 60 (which has been clarified regarding the “between” location of the redirection server).

VII. Claim 15: Other features (Rule Modification and Temporary Network Address Correlation Limitations)

In addition to the Board's overbroad interpretation of redirection server discussed above, the Board also failed to consider other features of claim 15 that are not disclosed or suggested by HE, Zenchelsky or the ‘118 background section whether singly or in combination. Specifically, Claim 15 recites “a redirection server ... correlated to a temporarily assigned network address ... configured to allow ... modification of at least a portion of the rule set rule ... ” HE teaches just the opposite – that the “ticket” information (equated by the Board and examiner to the rule set) must remain unchanged for the duration of a user session. (See e.g., HE Col. 18, lines 14-23.) The ‘118 background section disclosing web server redirection does not mention (much less disclose or suggest) altering the redirection protocol (rule set) during a user session (during which the redirection server is correlated to a temporarily assigned network address). Finally, Zenchelsky teaches only the assignment of a network address and does not teach any redirection.

Accordingly none of the references cited by the Board teach or disclose a changeable rule set *while a temporary network address is assigned.*

For at least this additional reason, canceled independent claim 15 was confirmable over the cited art. The above arguments regarding canceled claim 15 apply to corresponding new claim 72 (which has been clarified regarding the "between" location of the redirection server).

VIII. Original Claim 25: Other features (Rule Set Modification *During* a User Session, i.e, While a Temporary Network Address Is Assigned)

In addition to the Board's overbroad interpretation of redirection server discussed above, the Board stated in its opinion that "LWT has not shown prejudicial error in the examiner's rejection of claim 25 beyond the misconstruction of 'redirection server.'" This statement is incorrect. The Board did not consider the argument raised by Patent Owner that the cited art does not disclose modification of the rule set during a user session while a temporary network address is assigned as recited in claim 25. This requirement is set out in the first method step of claim 25, which states:

> "*modifying* at least a portion of the user's rule set *while the user's rule set remains correlated to the temporarily assigned network address* in the redirection server"

For the same reasons discussed above in connection with claim 15, the modification of the rule set during a user session (that is, while the user computer is "correlated to the temporarily assigned network address") is not disclosed or suggested in HE, Zenchelsky or the web based redirection disclosed in the '118 background section. Significantly, although this feature of claim 15 and 25 were the subject of argument in Patent Owner's appeal brief, the examiner in the Examiner's Appeal Brief also failed to address this issue and neither cited any prior art that would preclude patentability based on this feature.

For at least this additional reason, independent claim 25 was confirmable over the cited prior art. The above arguments regarding canceled claim 25 apply to corresponding new claim 87 (which has been clarified regarding the "between" location of the redirection server).

IX. Conclusion

For at least the above reasons, it is respectfully submitted that claims 2-7, 9-14, 16-24, 26-31, 33-36, 38-41, 43-46, and 48-94 are patentably distinguished over the applied prior art. Thus, reconsideration and confirmation of the patentability of claims 2-7, 9-14, 16-24, and 26-27 and a determination of patentability of new claims 28-31, 33-36, 38-41, 43-46, and 48-94, and an early Notice of Intent to Issue a Reexamination Certificate are respectfully solicited.

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Fees for additional claims are submitted herewith. However, should any additional fee or fees be necessary for consideration of the papers filed herein, please charge any such fee or fees and refund any excess payments to Deposit Account No. 50-2929, referencing docket no. R1341006.

Should the Examiner have any questions or comments regarding this matter, the undersigned may be contacted at the below-listed telephone number.

Respectfully submitted,
Koichiro Ikudome et al.

Abraham Hershkovitz
Reg. No. 45,294

October 24, 2010

HERSHKOVITZ & ASSOCIATES, LLC
2845 Duke Street
Alexandria, VA 22314
TEL: (703) 370-4800
FAX: (703) 370-4809
E-MAIL: patent@hershkovitz.net

R1341006.A17; AH/EG

CERTIFICATE OF SERVICE

It is hereby certified that the attached Response Under 37 CFR 1.111 and Proposed Amendment under 37 CFR 1.530 is being **served by first class mail on October 25, 2011** on the third party requester at the third party requestor's address:

JERRY TURNER SEWELL
P.O. BOX 10999
NEWPORT BEACH, CA 92658-5015

Abe Hershkovitz

Electronic Acknowledgement Receipt

EFS ID:	14730743
Application Number:	95002035
International Application Number:	
Confirmation Number:	1745
Title of Invention:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
First Named Inventor/Applicant Name:	6779118
Customer Number:	40401
Filer:	Abraham Hershkovitz
Filer Authorized By:	
Attorney Docket Number:	RI1341006F
Receipt Date:	17-JAN-2013
Filing Date:	12-SEP-2012
Time Stamp:	22:35:28
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Trans Letter filing of a response in a reexam	R1341006F-A02_Transmittal-of-Response.pdf	156859 db54e88ff5a31a06909e64668e422315eb0e2a1a	no	1

Warnings:

Information:

2		R1341006F-A02_Response-and-CertofSrvc.pdf	301812 c2cdedd313d548c183417ff6d3ca61b04b704e9e	yes	31

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response after non-final action-owner timely	1	30
	Reexam Certificate of Service	31	31

Warnings:

Information:

3	Patent Owner Response after Board Decision	R1341006_Copy-of-Resp-and-Amdt-After-Board-Decision.pdf	1200677 bf2d185562b991fe4dfc0791da6eb3765f8ad60c	no	28

Warnings:

Information:

Total Files Size (in bytes):	1659348

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/002,035	09/12/2012	6779118	RI1341006F	1745

40401 7590 12/13/2012
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

EXAMINER	
WORJLOH, JALATEE	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
12/13/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patents and Trademark Office
P.O.Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS
David L. McCombs
HAYNES & BOONE, LLP, IP Section
2323 Victory Ave., Suite 700
Dallas, TX 75219

Date:

EX PARTE REEXAMINATION COMMUNICATION TRANSMITTAL FORM

REEXAMINATION CONTROL NO. : 95002035
PATENT NO. : 6779118
ART UNIT : 3993

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above identified ex parte reexamination proceeding (37 CFR 1.550(f)).

Where this copy is supplied after the reply by requester, 37 CFR 1.535, or the time for filing a reply has passed, no submission on behalf of the ex parte reexamination requester will be acknowledged or considered (37 CFR 1.550(g)).

Decision on Petition for Extension of Time in Reexamination	Control No.: 95/002,035

1. THIS IS A DECISION ON THE PETITION FILED 6 December 2012.

2. THIS DECISION IS ISSUED PURSUANT TO:
   A. □ 37 CFR 1.550(c) – The time for taking any action by a patent owner in an *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   B. ☒ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
   The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS
   Patent owner requests that the period for responding to the Office action mailed on 19 October 2012, which sets a two (2) month period for filing a response thereto, be extended by one (1) month.

   A. ☒ Petition fee per 37 CFR §1.17(g)):
      i. □ Petition includes authorization to debit a deposit account.
      ii. □ Petition includes authorization to charge a credit card account.
      iii. □ Other: ______________.
   B. ☒ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
   C. ☒ Petition was timely filed.
   D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
   A. ☒ Granted or □ Granted-in-part for one (1) month, because petitioner provided a factual accounting that established sufficient cause. (See 37 CFR 1.550(c) and 37 CFR 1.956).
      □ Other/comment: ____.
   B. □ Dismissed because:
      i. □ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).
      ii. □ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
      iii. □ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
      iv. □ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
      v. □ The petition is moot.
      vi. □ Other/comment: ____.

5. CONCLUSION

   Telephone inquiries with regard to this decision should be directed to Daniel Ryman at (571)272-3152. In his/her absence, calls may be directed to Sudhanshu Pathak at (571)272-5509 in the Central Reexamination Unit.

/Daniel Ryman/	Supervisory Patent Examiner
[*Signature*]	(Title)

U.S. Patent and Trademark Office
PTO-2293 (Rev. 09-2010)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/002,035	09/12/2012	6779118	43614.61	1745

40401 7590 12/06/2012
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

EXAMINER	
WORJLOH, JALATEE	

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
12/06/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

David L. McCombs
HAYNES & BOONE, LLP - IP SECTION
2323 VICTORY AVENUE, SUITE 700
DALLAS, TX 75219

Transmittal of Communication to Third Party Requester *Inter Partes* Reexamination

REEXAMINATION CONTROL NUMBER *95/002,035*.

PATENT NUMBER *6,779,118*.

TECHNOLOGY CENTER *3999*.

ART UNIT *3993*.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

Decision on Petition for Extension of Time in Reexamination	Control No.: 95/002,035

1. THIS IS A DECISION ON THE PETITION FILED 3 December 2012.

2. THIS DECISION IS ISSUED PURSUANT TO:
A. □ 37 CFR 1.550(c) – The time for taking any action by a patent owner in an *ex parte* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
B. ☒ 37 CFR 1.956 – The time for taking any action by a patent owner in an *inter partes* reexamination proceeding will be extended only for sufficient cause and for a reasonable time specified.
The petition is before the Central Reexamination Unit for consideration.

3. FORMAL MATTERS
Patent owner requests that the period for responding to the Office action mailed on 19 October 2012, which sets a two (2) month period for filing a response thereto, be extended by one (1) month.

A. ☒ Petition fee per 37 CFR §1.17(g)):
i. □ Petition includes authorization to debit a deposit account.
ii. □ Petition includes authorization to charge a credit card account.
iii. □ Other: ______________.
B. □ Proper certificate of service was provided. (Not required in reexamination where patent owner is requester.)
C. ☒ Petition was timely filed.
D. ☒ Petition properly signed.

4. DECISION (See MPEP 2265 and 2665)
A. □ Granted or □ Granted-in-part for ______________, because petitioner provided a factual accounting that established sufficient cause. (See 37 CFR 1.550(c) and 37 CFR 1.956).
□ Other/comment: ____.
B. ☒ Dismissed because:
i. ☒ Formal matters (See unchecked box(es) (A, B, C and/or D) in section 4 above).
ii. □ Petitioner failed to provide a factual accounting of reasonably diligent behavior by all those responsible for preparing a response to the outstanding Office action within the statutory time period.
iii. □ Petitioner failed to explain why, in spite of the action taken thus far, the requested additional time is needed.
iv. □ The statements provided fail to establish sufficient cause to warrant extension of the time for taking action (See attached).
v. □ The petition is moot.
vi. ☒ Other/comment: Patent Owner served this request for an extension of time on Jerry Turner Sewell at P.O. Box 10999 in Newport Beach, California. Third Party Requester is represented by Haynes & Boone, LLP at 2323 Victory Ave, Suite 700 in Dallas, Texas.

5. CONCLUSION

Telephone inquiries with regard to this decision should be directed to Daniel Ryman at (571)272-3152. In his/her absence, calls may be directed to Sudhanshu Pathak at (571)272-5509 in the Central Reexamination Unit.

/Daniel Ryman/	Supervisory Patent Examiner
[*Signature*]	(Title)

HERSHKOVITZ & ASSOCIATES, LLC
PATENT AGENCY
2845 DUKE STREET, ALEXANDRIA, VA 22314
TEL. 703-370-4800 ~ FACSIMILE 703-370-4809
patent@hershkovitz.net ~ www.hershkovitz.net

Inventor: Koichiro Ikudome et al. Art Unit: 3992

Reexamination Proceeding: 95/002,035
(based on U.S. Patent No. 6,779,118)
Confirmation No.: 1745

Reexamination Filed: September 12, 2012 Examiner: Jalatee Worjloh

For: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Mail Stop "*inter partes* Reexam"
Attn.: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, Virginia 23313-1450

Dear Commissioner:

Transmitted herewith are a RESUBMISSION OF PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956 and a Certificate of Service in connection with the above-captioned Proceeding.

The fee has been calculated as shown below:

Claims After Amendment	No. of Claims Previously Paid	Present Extra	Small Entity		Large Entity	
			Rate	Fee	Rate	Fee
*Total Claims:			x 30=	$	x 60=	$
**Indep. Claims:			x125=	$	x250=	$
Extension Fee for Months				$		$
Other:				$		$
		Total:		$	Total:	$

___ Fee Payment made through EFS.
___ Payment is made herewith by Credit Card (see attached Form PTO-2038).
_X_ The Director is hereby authorized to charge all fees, including those under 37 CFR §§1.16 and 1.17, which are required for entry of the papers submitted herewith, and any fees which may be required to maintain pendency of this Proceeding, to Deposit Account No. 50-2929.
___ The Director is hereby authorized to charge all fees under 37 CFR § 1.18 which may be required to complete issuance of this application to Deposit Account No. 50-2929.

Respectfully submitted,

Date: December 6, 2012

/Abe Hershkovitz/
Abraham Hershkovitz
Registration No. 45,294

R1341006F.A01; AH/DXN/pjj

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Koichiro Ikudome et al.

Art Unit: 3992

Reexamination Proceeding: 95/002,035
(based on U.S. Patent No. 6,779,118)

Confirmation No.: 1745

Examiner: Jalatee Worjloh

Reexamination Filed: September 12, 2012

For: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

RESUBMISSION OF PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956

Mail Stop "*inter partes* Reexam"
Attn.: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, Virginia 23313-1450

Dear Commissioner:

Patent Owner respectfully petitions for an extension of time for filing a Response to the outstanding Office Action mailed on October 19, 2012 in the above-identified Proceeding.

A Petition for Extension of Time with a Certificate of Service and Petition fee were submitted to the Office on December 3, 2012. On December 6, 2012, the Office mailed a Decision dismissing the Petition based on the informality that, by clerical error only, the Certificate of Service indicated an erroneous address for service on third party requester. However, the actual service letter for the filing of the Petition that was sent to third party requester was directed to the IP Section of IP Section of Haynes & Boone, 2323 Victory Avenue, Suite 700, Dallas, TX 75219. This Resubmission of Petition for Extension of Time is corrected in showing the proper mailing address of third party requester.

Consideration of this Resubmitted Petition is respectfully requested.

As required by 37 CFR §1.956, a Petition for an extension of time in *inter partes* Reexamination must (1) be filed before the due date for the response with sufficient time to grant the Petition, (2) include the Petition fee under 37 CFR §1.17(g), (3) be for cause, i.e., fully state the reasons for the extension that include (a) a statement of what action Patent Owner has taken to provide a response as of the date the Petition is submitted, and (b) why, in spite of the action taken thus far, the requested additional time is necessary, and (4) be for a reasonable amount of time.

This Petition is being filed prior to the due date for response of December 19, 2012 with ample time to be granted prior to the due date, and is therefore timely.

The sequence of events in the prosecution of this Proceeding is as follows:

on July 12, 2012, third party requester filed a defective Request for *inter partes* Reexamination;

on September 6, 2012, the Office vacated the filing date of the defective Request;

on September 15, 2012, third party requester filed an alleged "corrected" Request for *inter partes* Reexamination, which was accepted by the Office; and

on October 19, 2012, an Order granting *inter partes* Reexamination and an Office Action were mailed in connection with this Proceeding.

The Order indicates that claims 2-7, 9-14, 16-24 and 26-90 are subject to reexamination, and makes general statements about which of the proposed issues raised in the Request are taught or not taught by the combination of various ones of the references.

The Office Action also indicates that claims 2-7, 9-14, 16-24 and 26-90 are subject to reexamination, and rejects all 86 claims under various references. Patent Owner points out that the reason for the extension is to be able to complete the review of the Request and all of the 30 exhibits filed with the Request and 30 exhibits which it cites, a total of **2600** pages, is presently being studied to determine the validity, if any, of the proposed rejections of 86 claims, and arguments over the references are being prepared. However, in spite of Patent Owner studying the Request and references, **because no specific rejection or discussion of references was made in the Office Action, and the whole of the Request was merely incorporated**, it is necessary for Patent Owner to have more time to analyze and identify all of the exhibits and issues that will require treatment in Patent Owner's response only from requester's claim charts and references, specifically so far, nine (9) independent references cited in various combinations in eight (8) independent grounds of rejection for various combinations in the rejection of 86 claims.

Over the last six weeks since issuance of the Order and the Office Action, Patent Owner's representative has spent approximately 84 hours so far analyzing much of the prior art, four claim charts of 112, 104, 47 and 55 pages in length, many of the arguments of requestor in both the Request and claims charts, and the Examiner's comments in the Order. Patent Owner's representative has prepared some of the initial arguments to rebut and overcome requestor's remarks, and these arguments have been submitted to the inventor for review, with the consequent revisions of these drafts being received from the inventor with further comments and changes. It is likely that at least several more weeks of work will be required to complete the Response for review by the inventor and other counsel, which also may result in even further revisions required.

Patent Owner courteously points out that it is not possible to review the massive amount of exhibits and claim charts, and to complete arguments over the issues in the time set for response to the Action. Patent Owner also notes that a complete and *bona fide* response to the Action must as well include remarks directed to rebuttal of every other issue raised in the Request which Patent Owner intends to contest.

Accordingly, Patent Owner respectfully petitions the Office for a reasonable amount of time, i.e., one (1) month in extension of the period for response set by the Office Action, up to and including January 19, 2013.

Patent Owner submitted the fee for the original Petition under 37 CFR §1.17(g) on December 3, 2012, which Petition was dismissed. Accordingly, it is respectfully requested that the previously-submitted fee be accepted for this filing, and it is believed that no other fee is required. If any other fee is required, please charge such fee (and refund any excess payments) to Deposit Account No. 50-2929, for Docket no. R1341006F.

Evidence of Service of this Petition on 3rd party requester is found after the last page of this paper.

All of the requirements under 37 CFR §1.956 are met in this Petition.

The Examiner is invited to direct any questions regarding this matter to the undersigned at the below-listed contact numbers and addresses.

Respectfully submitted,
Koichiro Ikudome et al.

Date: December 6, 2012

/Abe Hershkovitz/
Abraham Hershkovitz
Reg. No. 45,294

HERSHKOVITZ & ASSOCIATES, LLC
2845 Duke Street
Alexandria, VA 22314
TEL: (703) 370-4800
FAX: (703) 370-4809
E-MAIL: patent@hershkovitz.net
R1341006F.A01; AH/pjj

CERTIFICATE OF SERVICE

It is hereby certified that the attached RESUBMISSION OF PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956 and this Certificate of Service **are being served on December 6, 2012 by first class mail** on the third party requester at the third party requestor's address:

IP Section
HAYNES & BOONE
2323 Victory Avenue, Suite 700
Dallas, TX 75219

/Abe Hershkovitz/
Abraham Hershkovitz

Electronic Acknowledgement Receipt

EFS ID:	14406408
Application Number:	95002035
International Application Number:	
Confirmation Number:	1745
Title of Invention:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
First Named Inventor/Applicant Name:	6779118
Customer Number:	40401
Filer:	Abraham Hershkovitz
Filer Authorized By:	
Attorney Docket Number:	RI1341006F
Receipt Date:	06-DEC-2012
Filing Date:	12-SEP-2012
Time Stamp:	19:06:11
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Trans Letter filing of a response in a reexam	R1341006F-A01_Transmittal-of-Resubmission-of-Pet-for-EoT.pdf	156751 1d9f6247350fb7f710b9d6e991a9adcabefaa070	no	1

Warnings:

Information:

2		R1341006F-A01_Resubission-of-Pet-for-EoT.pdf	134115 44c393a672e09ca7f003ce23cb152e548b37843a	yes	4

Multipart Description/PDF files in .zip description

Document Description	Start	End
Reexam Request for Extension of Time	1	3
Reexam Certificate of Service	4	4

Warnings:

Information:

Total Files Size (in bytes):	290866

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Koichiro Ikudome et al.	Art Unit: 3992
Reexamination Proceeding: 95/002,035 (based on U.S. Patent No. 6,779,118)	Confirmation No.: 1745
	Examiner: Jalatee Worjloh
Reexamination Filed: September 12, 2012	

For: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956

Mail Stop "*inter partes* Reexam"
Attn.: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, Virginia 23313-1450

Dear Commissioner:

Patent Owner respectfully petitions for an extension of time for filing a Response to the outstanding Office Action mailed on October 19, 2012 in the above-identified Proceeding.

As required by 37 CFR §1.956, a Petition for an extension of time in *inter partes* Reexamination must (1) be filed before the due date for the response with sufficient time to grant the Petition, (2) include the Petition fee under 37 CFR §1.17(g), (3) be for cause, i.e., fully state the reasons for the extension that include (a) a statement of what action Patent Owner has taken to provide a response as of the date the Petition is submitted, and (b) why, in spite of the action taken thus far, the requested additional time is necessary, and (4) be for a reasonable amount of time.

This Petition is being filed prior to the due date for response of December 19, 2012 with ample time to be granted prior to the due date, and is therefore timely.

The sequence of events in the prosecution of this Proceeding is as follows:

on July 12, 2012, third party requester filed a defective Request for *inter partes* Reexamination;

on September 6, 2012, the Office vacated the filing date of the defective Request;

on September 15, 2012, third party requester filed an alleged “corrected” Request for *inter partes* Reexamination, which was accepted by the Office; and

on October 19, 2012, an Order granting *inter partes* Reexamination and an Office Action were mailed in connection with this Proceeding.

The Order indicates that claims 2-7, 9-14, 16-24 and 26-90 are subject to reexamination, and makes general statements about which of the proposed issues raised in the Request are taught or not taught by the combination of various ones of the references.

The Office Action also indicates that claims 2-7, 9-14, 16-24 and 26-90 are subject to reexamination, and rejects all 86 claims under various references. Patent Owner points out that the reason for the extension is to be able to complete the review of the Request and all of the 30 exhibits filed with the Request and 30 exhibits which it cites, a total of **2600** pages, is presently being studied to determine the validity, if any, of the proposed rejections of 86 claims, and arguments over the references are being prepared. However, in spite of Patent Owner studying the Request and references, **because no specific rejection or discussion of references was made in the Office Action, and the whole of the Request was merely incorporated**, it is necessary for Patent Owner to have more time to analyze and identify all of the exhibits and issues that will require treatment in Patent Owner’s response only from requester’s claim charts and references, specifically so far, nine (9) independent references cited in various combinations in eight (8) independent grounds of rejection for various combinations in the rejection of 86 claims.

Over the last six weeks since issuance of the Order and the Office Action, Patent Owner’s representative has spent approximately 84 hours so far analyzing much of the prior art, four claim charts of 112, 104, 47 and 55 pages in length, many of the arguments of requestor in both the Request and claims charts, and the Examiner’s comments in the Order. Patent Owner’s representative has prepared some of the initial arguments to rebut and overcome requestor’s remarks, and these arguments have been submitted to the inventor for review, with the consequent revisions of these drafts being received from the inventor with further comments and changes. It is likely that at least several more weeks of work will be required to complete the Response for review by the inventor and other counsel, which also may result in even further revisions required.

Patent Owner courteously points out that it is not possible to review the massive amount of exhibits and claim charts, and to complete arguments over the issues in the time set for response to the Action. Patent Owner also notes that a complete and *bona fide* response to the Action must as well include remarks directed to rebuttal of every other issue raised in the Request which Patent Owner intends to contest.

Accordingly, Patent Owner respectfully petitions the Office for a reasonable amount of time, i.e., one (1) month in extension of the period for response set by the Office Action, up to and including January 19, 2013.

Patent Owner has submitted herewith the fee for this Petition under 37 CFR §1.17(g). It is believed that no other fee is required. However, should any additional fee be necessary for consideration of this Petition, please charge such fee (and refund any excess payments) to Deposit Account No. 50-2929, referencing Docket no. R1341006F.

Evidence of Service of this Petition on 3rd party requester is found after the last page of this paper.

All of the requirements under 37 CFR §1.956 are met in this Petition.

The Examiner is invited to direct any questions regarding this matter to the undersigned at the below-listed contact numbers and addresses.

Respectfully submitted,
Koichiro Ikudome et al.

/Abe Hershkovitz/
Abraham Hershkovitz
Reg. No. 45,294

Date: December 3, 2010

HERSHKOVITZ & ASSOCIATES, LLC
2845 Duke Street
Alexandria, VA 22314
TEL: (703) 370-4800
FAX: (703) 370-4809
E-MAIL: patent@hershkovitz.net

R1341006F.A01; AH/pjj

CERTIFICATE OF SERVICE

It is hereby certified that the attached PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956 and this Certificate of Service **are being served on December 3, 2012 by first class mail** on the third party requester at the third party requestor's address:

JERRY TURNER SEWELL
P.O. BOX 10999
NEWPORT BEACH, CA 92658-5015

/Abe Hershkovitz/
Abraham Hershkovitz

Electronic Patent Application Fee Transmittal

Application Number:	95002035
Filing Date:	12-Sep-2012
Title of Invention:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
First Named Inventor/Applicant Name:	6779118
Filer:	Abraham Hershkovitz
Attorney Docket Number:	43614.61

Filed as Small Entity

inter partes reexam Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Petition fee- 37 CFR 1.17(g) (Group II)	1463	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
	Total in USD ($)			**200**

Electronic Acknowledgement Receipt

EFS ID:	14372547
Application Number:	95002035
International Application Number:	
Confirmation Number:	1745
Title of Invention:	USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM
First Named Inventor/Applicant Name:	6779118
Customer Number:	40401
Filer:	Abraham Hershkovitz
Filer Authorized By:	
Attorney Docket Number:	43614.61
Receipt Date:	03-DEC-2012
Filing Date:	12-SEP-2012
Time Stamp:	22:36:32
Application Type:	inter partes reexam

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$200
RAM confirmation Number	8081
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part/.zip	Pages (if appl.)

1	Trans Letter filing of a response in a reexam	R1341006F-A01_Transmittal-for-Pet-for-EoT.pdf	159185 3793a7f5a71447022880ca0c4941011bfaa140d8	no	1
Warnings:					
Information:					
2		R1341006F-A01_Pet-for-EoT.pdf	133070 fddd27cd745d3b70aad022f5e01b5e7d5e386451	yes	4
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Receipt of Petition in a Reexam		1	3	
	Reexam Certificate of Service		4	4	
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30265 dd1819ddb026f7d4bf75979740063b934190c99a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	322520		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

HERSHKOVITZ & ASSOCIATES, LLC
PATENT AGENCY
2845 DUKE STREET, ALEXANDRIA, VA 22314
TEL. 703-370-4800 ~ FACSIMILE 703-370-4809
patent@hershkovitz.net ~ www.hershkovitz.net

Inventor: Koichiro Ikudome et al. Art Unit: 3992

Reexamination Proceeding: 95/002,035 Confirmation No.: 1745
(based on U.S. Patent No. 6,779,118)

Reexamination Filed: September 12, 2012 Examiner: Jalatee Worjloh

For: USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

Mail Stop "*inter partes* Reexam"
Attn.: Central Reexamination Unit
Commissioner for Patents
United States Patent & Trademark Office
P.O. Box 1450
Alexandria, Virginia 23313-1450

Dear Commissioner:

Transmitted herewith are a PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.956 and a Certificate of Service in connection with the above-captioned Proceeding.

The fee has been calculated as shown below:

Claims After Amendment	No. of Claims Previously Paid	Present Extra	Small Entity		Large Entity	
			Rate	Fee	Rate	Fee
*Total Claims:			x 30=	$	x 60=	$
**Indep. Claims:			x125=	$	x250=	$
Extension Fee for Months				$		$
Other: Petition Fee Under 37 CFR §1.17(g)				$		**$200.00**
			Total:	$	**Total:**	**$200.00**

X Fee Payment made through EFS.
___ Payment is made herewith by Credit Card (see attached Form PTO-2038).
X The Director is hereby authorized to charge all fees, including those under 37 CFR §§1.16 and 1.17, which are required for entry of the papers submitted herewith, and any fees which may be required to maintain pendency of this application, to Deposit Account No. 50-2929.
___ The Director is hereby authorized to charge all fees under 37 CFR § 1.18 which may be required to complete issuance of this application to Deposit Account No. 50-2929.

Respectfully submitted,

Date: December 3, 2012

/Abe Hershkovitz/
Abraham Hershkovitz
Registration No. 45,294

R1341006F.A01; AH/DXN/pjj

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/002,035	09/12/2012	6779118	43614.61	1745

40401 7590 10/19/2012
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

EXAMINER
WORJLOH, JALATEE

ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/19/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

David L. McCombs
HAYNES & BOONE, LLP, IP Section
2323 Victory Ave., Suite 700
Dallas, TX 75219

Transmittal of Communication to Third Party Requester *Inter Partes* Reexamination

REEXAMINATION CONTROL NUMBER *95/002,035*.

PATENT NUMBER *6,779,118*.

TECHNOLOGY CENTER *3999*.

ART UNIT *3992*.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

ORDER GRANTING/DENYING REQUEST FOR* INTER PARTES *REEXAMINATION	**Control No.** 95/002,035	**Patent Under Reexamination** 6779118
	Examiner Jalatee Worjloh	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

The request for *inter partes* reexamination has been considered. Identification of the claims, the references relied on, and the rationale supporting the determination are attached.

Attachment(s): □ PTO-892 ☒ PTO/SB/08 □Other: _____

1. ☒ The request for *inter partes* reexamination is GRANTED.

☒ An Office action is attached with this order.

□ An Office action will follow in due course.

2. □ The request for *inter partes* reexamination is DENIED.

This decision is not appealable. 35 U.S.C. 312(c). Requester may seek review of a denial by petition to the Director of the USPTO within ONE MONTH from the mailing date hereof. 37 CFR 1.927. EXTENSIONS OF TIME ONLY UNDER 37 CFR 1.183. In due course, a refund under 37 CFR 1.26(c) will be made to requester.

All correspondence relating to this *inter partes* reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Order.

Transmittal of Communication to Third Party Requester Inter Partes Reexamination

Control No. 95/002,035	**Patent Under Reexamination** 6779118
Examiner Jalatee Worjloh	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

DETAILED ACTION

Decision on Request

The present request for *inter partes* reexamination establishes a reasonable likelihood that requester will prevail with respect to claims 2-7, 9-14, 16-24, and 26-90 of U.S. Patent No. 6,779, 118 to Ikudome et al. ("Ikudome").

Extensions of time under 37 CFR 1.136(a) will not be permitted in *inter partes* reexamination proceedings because the provisions of 37 CFR 1.136 apply only to "an applicant" and not to the patent owner in a reexamination proceeding. Additionally, 35 U.S.C. 314(c) requires that *inter partes* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in *inter partes* reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

References cited in Request

The Examiner considers a reasonable likelihood that the requester will prevail has been raised by at least certain of the following prior art references:

- U.S. Patent No. 5835727 to Wong et al. ("Wong '727");
- U.S. Patent No. 6073178 to Wong et al. ("Wong '178");
- U.S. Patent No. 5950195 to Stockwell et al. ("Stockwell");
- U.S. Patent No. 5889958 to Willens;
- U.S. Patent No. 5848233 to Radia et al. ("Radia");

- Request for Comments 2138, Internet Engineering Task Force, April 1997 (RFC 2138);
- U.S. Patent No. 6088451 to He et al. ("He");
- U.S. Patent No. 6233686 to Zenchelsky et al. ("Zenchelsky"); and
- U.S. Patent No. 5815574 to Fortinsky.

Identification of Every Claim for which Reexamination is Requested

The references cited above are discussed in the Request and asserted to render unpatentable claims 2-7, 9-14, 16-24, and 26-90 of Ikudome patent. Claim charts AA-DD of the Request include explanations that seek to establish a reasonable likelihood that the requester will prevail with respect to at least one of the patent claims in light of the references cited. The explanations in the Request are addressed below under subheadings designation each one as a numbered "Issue".

Reasonable Likelihood to Prevail (RLP) on the Issue of Patentability

The claims for which reexamination is requested will be utilized to show whether the above-cited references, taken together with the explanation provided by requester, are found to establish, or not to establish, that there is a reasonable likelihood that the requester will prevail with respect to at least one of the patent claims.

Issue(s) Raised by Request

Issue 1: Willens in view of RFC 2138 and Stockwell

Willens, RFC 2138, and Stockwell predate the effective filing date of Ikudome patent.

Willens

Willens is directed to a network access control system and process. One object of the system is to use an extension of firewall filtering to implement content monitoring (see col. 2, lines 59-61). Willens teaches utilizing a user's profile to authenticate the user upon logging into a communications server. The user's profile also identifies the filter that controls access to Internet sites (see col. 5, lines 9-25).

RFC 2138

RFC 2138 is directed to remote authentication dial in user service (RADIUS). The reference "describes a protocol for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate links and a shared Authentication Server " (see page 1).

Stockwell

Stockwell teaches "a system and method for regulating the flow of internetwork connections through a firewall having a network protocol stack which includes an Internet Protocol (IP) layer" (see abstract). The references disclose an access control list that includes a plurality of rules (see col. 3, lines 35-37), "that regulate the flow of

Internet connections through a firewall. These rules control how a firewall's servers and proxies will react to connection attempts" (see col. 5, lines 17-22).

Hence, it is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90.

However, it is not found that the Requester has shown a reasonable likelihood of success with respect to claims 19, 20, and 73. Particularly, the claims recite "wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user." The Request relies on Willens for teaching this limitation. (See pages 26 & 27 of Exhibit AA). It is noted in the Request that Willens discloses modifying the list of sites a user is permitted to access. The reference states that "the subsystem 12 provides for a central, server based permit list that can be easily updated on a daily or hourly basis." Also, "Willens teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as password." See page 21 of Exhibit AA.

Although Willens teaches updating the permit list, the update does not necessarily include "removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claims 21 and 74, it is not found that the Requester has shown a reasonable likelihood of success with respect to these claims. Particularly, the claims recite "wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses." The Request relies on Willens for teaching this limitation. (See pages 22, 26, and 28 of Exhibit AA). It is noted in the Request that Willens discloses "modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses." The reference states that "based on the result, the server 14 either permits or denies access and updates it's local cache" See page 22 of Exhibit AA.

Although Willens teaches "updating it's local cache", the update does not necessarily include "removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claims 22, 75, and 85, it is not found that the Requester has shown a reasonable likelihood of success with respect to these claims. Particularly, the claims recite "wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses." The Request relies on Willens for teaching this limitation. (See Exhibit AA). It is noted in the Request that Willens discloses "modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses." The reference states that "based on the result, the server 14 either permits or denies access and updates it's local cache" See page 22 of Exhibit AA. Also, Willens teaches "the subsystem 12 provides for a central, server based permit list that can be easily updated on a daily or hourly basis" and "modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as password." See page 21 of Exhibit AA.

Although Willens teaches "updating it's local cache" and a permit list, the update does not necessarily include "removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claim 72, it is not found that the Requester has shown a reasonable likelihood of success with respect to this claim (see claim 19's rationale above).

Further, it is found that Willens in view of RFC 2138 and Stockwell establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90 as evidenced by the accompanying Office Action rejecting these claims.

It is not found that Willens in view of RFC 2138 and Stockwell establish that there is a reasonable likelihood that the requester will prevail with respect to claims 19-22, 72-75, and 85.

Issue 2: Willens in view of RFC 2138 and Admitted Prior Art

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90.

However, it is not found that the Requester has shown a reasonable likelihood of success with respect to claims 19, 20, and 73. Particularly, the claims recite "wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user." The Request relies on Willens for teaching this limitation. (See Exhibit AA). It is noted in the Request that Willens discloses modifying the list of sites a user is permitted to access. The reference states that "the subsystem 12 provides for a central, server based permit list that can be easily updated on a daily or hourly basis" Also, "Willens teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as password." See page 21 of Exhibit AA.

Although Willens teaches updating the permit list, the update does not necessarily include “removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claims 21 and 74, it is not found that the Requester has shown a reasonable likelihood of success with respect to these claims. Particularly, the claims recite “wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.” The Request relies on Willens for teaching this limitation. (See pages 22, 26, and 28 of Exhibit AA). It is noted in the Request that Willens discloses “modifying a user’s filtering rules based on a user’s accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses.” The reference states that “based on the result, the server 14 either permits or denies access and updates it’s local cache” See page 22 of Exhibit AA.

Although Willens teaches “updating it’s local cache”, the update does not necessarily include “removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claims 22, 75, and 85, it is not found that the Requester has shown a reasonable likelihood of success with respect to these claims. Particularly, the claims recite "wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses." The Request relies on Willens for teaching this limitation. (See Exhibit AA). It is noted in the Request that Willens discloses "modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses." The reference states that "based on the result, the server 14 either permits or denies access and updates it's local cache" See page 22 of Exhibit AA. Also, Willens teaches "the subsystem 12 provides for a central, server based permit list that can be easily updated on a daily or hourly basis" and "modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as password." See page 21 of Exhibit AA.

Although Willens teaches "updating it's local cache" and a permit list, the update does not necessarily include "removal or reinstatement" of a portion of the rule set. The process of updating requires making information current; thus, the action of deleting or restoring data is not compulsory. That is, updating could include inserting new data. Willens does not expressly define updating as reinstating data or removing data. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

As per claim 72, it is not found that the Requester has shown a reasonable likelihood of success with respect to this claim (see claim 19's rationale above).

Further, it is found that Willens in view of RFC 2138 and Admitted Prior Art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90 as evidenced by the accompanying Office Action rejecting these claims.

It is not found that Willens in view of RFC 2138 and Admitted Prior Art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 19-22, 72-75, and 85.

Issue 3: Radia in view of Wong '727 in further in view of Stockwell

Radia

Radia discloses "a method and apparatus for filtering IP packets based on events within a computer network" (see abstract). In the system, when a user logs in, his/hers filter profile is retrieved by SMS from a filtering profile database. The profile is downloaded to an access network control server (ANCS) then the network components are reconfigured (see fig. 9 and related text).

Wong '727

Wong '727 is directed to a method and apparatus for controlling access to services within a computer network. The system includes a services management system (SMS), an access network control server (ANCS), and router. The "SMS maintains a profile of filtering rule." In Wong '727, once the user accesses the network, the SMS downloads the user's filtering profiles to the ANCS, which uses the profiles to reconfigure the router. The router uses the rules to forward IP packets originating from the user's host system and directed at the network services. See abstract.

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90.

Further, it is found that Radia in view of Wong '727 in further in view of Stockwell establish that there is a reasonable likelihood that the requester will prevail with respect to claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 as evidenced by the accompanying Office Action rejecting these claims.

Issue 4: Radia in of Wong '727 and Stockwell and further in view of Wong '178

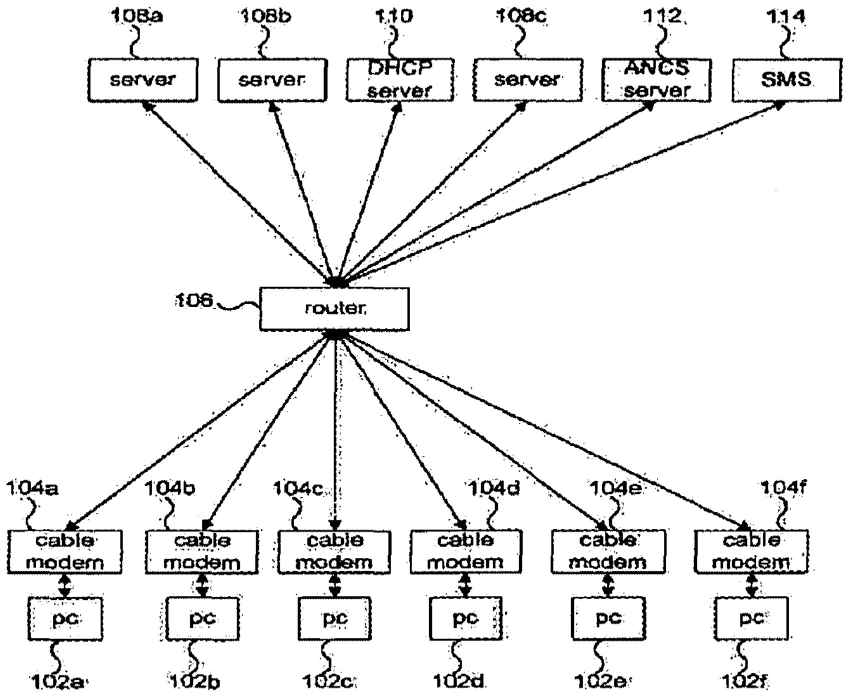
It is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-5, 9-12, 45-48, and 57-60.

Further, it is found that Radia in view of Wong '727 and Stockwell in view of Wong '178 establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-5, 9-12, 45-48, and 57-60 as evidenced by the accompanying Office Action rejecting these claims.

Issue 5: Radia in view of Wong '727 in further view of Admitted Prior Art

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 7, 14, 16-24, 50-56, and 62-90.

However, it is not found that the Requester has shown a reasonable likelihood of success with respect to claims 6, 13, 49, and 61. Specifically, the claims recite "wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set." The request asserts that "Radia illustrates in Fig. 1 that there are multiple potential destinations (servers 108) for a user's network requests:



RADIA FIG. 1

The servers 108 “are intended to represent the broad range of server systems that may be found within computer networks.” (Radia, 5:23-28). It would have been obvious for a filtering rule to redirect a user to any one or more of the servers 108.” See page 65 of Exhibit BB.

However, the Request does not explain why it is obvious for a user to be redirected to multiple destinations. Also, Fig. 1 and col. 5, lines 23-28 does not expressly teach “the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set” as required by the claims. Therefore, the Request and claim chart mapping, considered to the extent explained/analyzed by the Requester, do not clearly provide rationale to support a conclusion of obviousness with regard to these claims.

Hence, it is found that Radia in view of Wong '727 in further view of Admitted Prior Art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 7, 14, 16-24, 26-44, 50-56, and 62-90.

However, it is not found that Radia in view of Wong '727 in further view of Admitted Prior art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 6, 13, 49, and 61.

Issue 6: Radia in view of Wong '727 and Admitted Prior Art in further view of Wong '178

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-5, 9-12, 45-48, and 57-60.

Further, it is found that Radia in view of Wong '727 in further in Wong '178 establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-5, 9-12, 45-48, and 57-60 as evidenced by the accompanying Office Action rejecting these claims.

Issue 7: He in view of Zenchelsky and further in view of Admitted Prior Art

He

He is directed to a security system and method for network element access. "The network security mechanisms include: an authentication server responsible for authentication of the network users to network elements, a credential server responsible for controlling the network user credentials or privileges, and a network element access server responsible for controlling of access to the network elements by the user elements." See abstract.

Zenchelsky

Zenchelsky is directed to a system and method for providing peer level access control on a network. Zenchelsky discloses "a filter that efficiently stores, implements and maintains access rules specific to an individual computer on a network with rapidly changing configurations and security needs." See col. 4, lines 55-58. In the system, upon a network access request, each individual peer is authenticated. "The peer's local rule base is then loaded into the filter of the present invention, either from the peer itself, or from another user, host or peer. When the peer is no longer authenticated to the POP (e.g., the peer loses connectivity or logs off from the POP), the peer's local rule base is ejected (deleted) from the filter." See col. 5, lines 17-24.

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-7, 9-14, 16-24, 26-54, 56, 60-66, 68-81, and 83-89.

Further, it is found that He in view of Zenchelsky and further in view of Admitted Prior Art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-7, 9-14, 16-24, 26-54, 56, 60-66, 68-81, and 83-89 as evidenced by the accompanying Office Action rejecting these claims.

Issue 8: He in view of Zenchelsky, Fortinsky, and the Admitted Prior Art

Fortinsky

Fortinsky teaches a security ticket that includes a client's identity and privilege attributes, which controls the user's access to resources. The system aims "to implement a ticket based security system within a computing environment in which privilege authorization certificates or an equivalent data element included in tickets issued to a client to access resources can be extended where necessary to include identity and privilege data necessary for the client to access a resource accessible from the environment but utilizing a security system incompatible with the conventional authorization package." See col. 3, lines 39-48.

It is found that the Requester has shown a reasonable likelihood of success with respect to claims 2-7, 9-14, 16-24, 26-54, and 56-89.

Further, it is found that He in view of Zenchelsky, Fortinsky and the Admitted Prior Art establish that there is a reasonable likelihood that the requester will prevail with respect to claims 2-7, 9-14, 16-24, and 26-90 as evidenced by the accompanying Office Action rejecting these claims.

Summary

It is found that the requester has shown that there is a reasonable likelihood that the Requester will prevail with respect to claims 2-7, 9-14, 16-24, and 26-90. Thus, claims 2-7, 9-14, 16-24, and 26-90 of Ikudome patent will be reexamined as requested.

Conclusion

The patent owner is reminded of the continuing responsibility under 37 CFR 1.985(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent 6,779,118 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §2686 and 2686.04.

Any paper filed with the USPTO, i.e., any submission made, by either the Patent Owner or the Third Party Requester must be served on every other party in the reexamination proceedings, including any other third party requester that is part of the proceeding due to merger of the proceedings. As proof of service, the party submitting the paper to the Office must attach a Certificate of Service to paper which sets forth the name and address of the party served and the method of service. Papers filed without the required Certificate of Service may be denied consideration. 37 CFR 1.903; MPEP 2666.06.

All correspondence relating to this *inter partes* reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:
Mail Stop *Inter Partes* Reexam
ATTN: Central Reexamination Unit Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:
(571) 273-9900
Central Reexamination Unit

By Hand:
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to the Central Reexamination Unit at telephone number (571)272-7705.

/Jalatee Worjloh/
Primary Examiner, Art Unit 3992

Conferees:

/C. S./

MB

MATTHEW L. BROOKS
Supervisory Patent Reexamination Specialist
CRU -- Art Unit 3992

In place of PTO-1449 Form

U. S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

SHEET	1	OF	1

Complete if Known	
Application Number	*Inter Partes* Reexamination of U.S. Patent No. 6,779,118
Filing Date	July 12, 2012
Real Parties in Interest	Cisco Systems, Inc.
Art Unit	TBD
Examiner Name	TBD
Attorney Docket Number	43614.61

U. S. PATENTS

Examiner's Initials	Cite No.	Document Number	Issue Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	Exhibit E	5848233	12-08-1998	Radia et al.
	Exhibit F	5835727	11-10-1998	Wong et al.
	Exhibit G	5950195	09-07-1999	Stockwell et al.
	Exhibit H	6073178	06-06-2000	Wong et al.
	Exhibit I	5889958	03-30-1999	Willens
	Exhibit K	6233686	05-15-2001	Zenchelsky et al.
	Exhibit L	6088451	07-11-2000	He et al.
	Exhibit M	5815574	09-29-1998	Fortinsky

U. S. PATENT APPLICATION PUBLICATIONS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	Exhibit J	Request for Comments 2138, Internet Engineering Task Force, April 1997 ("RFC 2138").

Examiner Signature	/Jalatee Worjloh/	Date Considered	08/16/2012

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.W./

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
95/002,035	09/12/2012	6779118	43614.61	1745

40401 7590 10/19/2012
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

EXAMINER	
WORJLOH, JALATEE	
ART UNIT	PAPER NUMBER
3992	

MAIL DATE	DELIVERY MODE
10/19/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

DO NOT USE IN PALM PRINTER

(THIRD PARTY REQUESTER'S CORRESPONDENCE ADDRESS)

David L. McCombs
HAYNES & BOONE, LLP, IP Section
2323 Victory Ave., Suite 700
Dallas, TX 75219

Transmittal of Communication to Third Party Requester
Inter Partes Reexamination

REEXAMINATION CONTROL NUMBER 95/002,035.

PATENT NUMBER 6,779,118.

TECHNOLOGY CENTER 3999.

ART UNIT 3992.

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

PTOL-2070 (Rev.07-04)

Transmittal of Communication to Third Party Requester Inter Partes Reexamination	Control No.	Patent Under Reexamination
	95/002,035	6779118
	Examiner	Art Unit
	Jalatee Worjloh	3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified reexamination proceeding. 37 CFR 1.903.

Prior to the filing of a Notice of Appeal, each time the patent owner responds to this communication, the third party requester of the *inter partes* reexamination may once file written comments within a period of 30 days from the date of service of the patent owner's response. This 30-day time period is statutory (35 U.S.C. 314(b)(2)), and, as such, it cannot be extended. See also 37 CFR 1.947.

If an *ex parte* reexamination has been merged with the *inter partes* reexamination, no responsive submission by any *ex parte* third party requester is permitted.

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of the communication enclosed with this transmittal.

OFFICE ACTION IN* INTER PARTES *REEXAMINATION	**Control No.** 95/002,035	**Patent Under Reexamination** 6779118
	Examiner Jalatee Worjloh	**Art Unit** 3992

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

Responsive to the communication(s) filed by:
Patent Owner on _____
Third Party(ies) on 12 July, 2012

RESPONSE TIMES ARE SET TO EXPIRE AS FOLLOWS:

For Patent Owner's Response:
2 MONTH(S) from the mailing date of this action. 37 CFR 1.945. EXTENSIONS OF TIME ARE GOVERNED BY 37 CFR 1.956.
For Third Party Requester's Comments on the Patent Owner Response:
30 DAYS from the date of service of any patent owner's response. 37 CFR 1.947. NO EXTENSIONS OF TIME ARE PERMITTED. 35 U.S.C. 314(b)(2).

All correspondence relating to this inter partes reexamination proceeding should be directed to the **Central Reexamination Unit** at the mail, FAX, or hand-carry addresses given at the end of this Office action.

This action is not an Action Closing Prosecution under 37 CFR 1.949, nor is it a Right of Appeal Notice under 37 CFR 1.953.

PART I. THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1.□ Notice of References Cited by Examiner, PTO-892
2.□ Information Disclosure Citation, PTO/SB/08
3.□ _____

PART II. SUMMARY OF ACTION:

1a. ☒ Claims 2-7,9-14,16-24 and 26-90 are subject to reexamination.
1b. □ Claims _____ are not subject to reexamination.
2. □ Claims _____ have been canceled.
3. □ Claims _____ are confirmed. [Unamended patent claims]
4. □ Claims _____ are patentable. [Amended or new claims]
5. ☒ Claims 2-7, 9-14, 16-24, and 26-90 are rejected.
6. □ Claims _____ are objected to.
7. □ The drawings filed on _____ □ are acceptable □ are not acceptable.
8. □ The drawing correction request filed on _____ is: □ approved. □ disapproved.
9. □ Acknowledgment is made of the claim for priority under 35 U.S.C. 119 (a)-(d). The certified copy has:
□ been received. □ not been received. □ been filed in Application/Control No _____.
10. □ Other _____

DETAILED ACTION

Summary

This Office Action addresses claims 2-7, 9-14, 16-24, and 26-90 of U.S. Patent No. 6,779,118 to Ikudome et al. ("Ikudome") for which reexamination has been requested and a reasonable likelihood that requester will prevail with respect to the claims challenged in the present reexamination has determined to exist for at least one of the patented claims.

Claims 2-7, 9-14, 16-24, and 26-90 are rejected.

References cited in Request

The Examiner considers a reasonable likelihood that the requester will prevail has been raised by at least certain of the following prior art references:

- U.S. Patent No. 5835727 to Wong et al. ("Wong '727");
- U.S. Patent No. 6073178 to Wong et al. ("Wong '178");
- U.S. Patent No. 5950195 to Stockwell et al. ("Stockwell");
- U.S. Patent No. 5889958 to Willens;
- U.S. Patent No. 5848233 to Radia et al. ("Radia");
- Request for Comments 2138, Internet Engineering Task Force, April 1997 (RFC 2138);
- U.S. Patent No. 6088451 to He et al. ("He");
- U.S. Patent No. 6233686 to Zenchelsky et al. ("Zenchelsky"); and
- U.S. Patent No. 5815574 to Fortinsky.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-7, 9-14, 16-18, 23, 24, and 26-71, 76-84, and 86-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over RFC 2138 and Stockwell.

The proposed rejection of claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84 and 86-90 (see Exhibit AA, pages 2-55) of the request is hereby incorporated by reference.

Claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90 are rejected under 35 U.S. C. 103(a) as being unpatentable over Willens in view of RFC 2138 and Admitted Prior Art.

The proposed rejection of claims 2-7, 9-14, 16-18, 23, 24, 26-71, 76-84, and 86-90 (see Exhibit AA, page 56-112) of the request is hereby incorporated by reference.

Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radia in view of Wong '727 and further in view of Stockwell.

The proposed rejection of claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 (see Exhibit BB, pages 2-47) of the request is hereby incorporated by reference.

Claims 2-5, 9-12, 45-48, and 57-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radia in of Wong '727 and Stockwell and further in view of Wong '178.

The proposed rejection of claims 2-5, 9-12, 45-48, and 57-60 (see Exhibit BB, pages 48-53) of the request is hereby incorporated by reference.

Claims 7, 14, 16-24, 50-56, and 62-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radia in view of Wong '727 and further in view of Admitted Prior Art under 35 U.S.C. 103(a).

The proposed rejection of claims 7, 14, 16-24, 50-54, 56, and 62-90 (see Exhibit BB, pages 54-102) of the request is hereby incorporated by reference.

Claims 2-5, 9-12, 45-48, and 57-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radia in view of Wong '727 and Admitted Prior art and further in view of Wong '178.

The proposed rejection of claims 2-5, 9-12, 45-48, and 57-60 (see Exhibit BB, pages 103-109) of the request is hereby incorporated by reference.

Claims 2-7, 9-14, 16-24, 26-54, 56, 60-66, 68-81, and 83-89 are rejected under 35 U.S.C. 103(a) as being unpatentable over He, Zenchelsky, and the Admitted Prior Art.

The proposed rejection of 2-7, 9-14, 16-24, 26-54, 56, 60-66, 68-81, and 83-89 (see Exhibit CC) of the request is hereby incorporated by reference with **modifications**.

The modification is to include an additional motivation to combine the references. The Examiner notes, as illustrated by the Board (see Board decision of 90/009,301 mailed August 23, 2011, page 10), "since redirection would have been an obvious extension of blocking, it follows that the combination of He and Zenchelsky in view of Ikudome's admission would have made redirection based on the same bases obvious as well."

Claims 2-7, 9-14, 16-24, and 26-90 are rejected under 35 U.S.C. 103(a) as being unpatentable over He in view of Zenchelsky, Fortinsky, and the Admitted Prior Art.

The proposed rejection of claims 2-7, 9-14, 16-24, 26-89 (see Exhibit DD) of the request is hereby incorporated by reference.

Conclusion

In order to ensure full consideration of any amendments, affidavits or declarations, or other documents as evidence of patentability, such documents must be submitted in response to this Office action. Submissions after the next Office action, which is intended to be an Action Closing Prosecution (ACP), will be governed by 37 CFR 1.116(b) and (d), which will be strictly enforced.

Any paper filed with the Office, i.e., any submission made, by either the patent owner or the third party requester must be served on every other party in the reexamination proceeding including any other third party requester that is part of the proceeding due to merger of reexamination proceedings. As proof of service, the party submitting the paper to the Office must attach a certificate of service to the paper. It is required that the certificate of service set forth the name and address of the party served and the method of service. Papers filed without the required Certificate of Service may be denied consideration. 37 CFR 1.902; MPEP § 2666.06.

Any proposed amendment to the specification and/or claims in this reexamination proceeding must comply with 37 CFT 1.530(d)-(j), must be formally presented pursuant to 37 CFR 1.52(a) and (b), and must contain any fees required by 37 CFR 1.20(c). Amendments in an inter partes reexamination proceeding are made in the same manner that amendments in an ex parte reexamination proceeding are made. MPEP § 2666.01. See MPEP § 2250 for guidance as to the manner of making amendments in reexamination proceedings.

Extensions of time under 37 CFR 1.136(a) will not be permitted in *inter partes* reexamination proceedings because the provisions of 37 CFR 1.136 apply on to "an applicant" and not the patent owner in a reexamination proceedings. Additionally, 35 U.S.C. 314(c) requires that *inter partes* reexamination proceedings "will be conducted with special dispatch" (37 CFR 1.937). Patent owner extensions of time in *inter partes* reexamination proceedings are provided for in 37 CFR 1.956. Extensions of time are not available for third party requester comments, because a comment period of 30 days from service of patent owner's response is set by statute. 35 U.S.C. 314(b)(3).

The patent owner is reminded of the continuing responsibility under 37 CFR 1.985(a), to apprise the Office of any litigation activity, or other prior or concurrent proceeding, involving Patent 6,779,118 throughout the course of this reexamination proceeding. The third party requester is also reminded of the ability to similarly apprise the Office of any such activity or proceeding throughout the course of this reexamination proceeding. See MPEP §2686 and 2686.04.

Any paper filed with the USPTO, i.e., any submission made, by either the Patent Owner or the Third Party Requester must be served on every other party in the reexamination proceedings, including any other third party requester that is part of the proceeding due to merger of the proceedings. As proof of service, the party submitting the paper to the Office must attach a Certificate of Service to paper which sets forth the name and address of the party served and the method of service. Papers filed without the required Certificate of Service may be denied consideration. 37 CFR 1.903; MPEP 2666.06.

All correspondence relating to this *inter partes* reexamination proceeding should be directed as follows:

By U.S. Postal Service Mail to:
Mail Stop *Inter Partes* Reexam
ATTN: Central Reexamination Unit Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

By FAX to:
(571) 273-9900
Central Reexamination Unit

By Hand:
Customer Service Window
Randolph Building

401 Dulany Street
Alexandria, VA 22314

By EFS-Web:

Registered users of EFS-Web may alternatively submit such correspondence via the electronic filing system EFS-Web, at

https://efs.uspto.gov/efile/myportal/efs-registered

EFS-Web offers the benefit of quick submission to the particular area of the Office that needs to act on the correspondence. Also, EFS-Web submissions are "soft scanned" (i.e., electronically uploaded) directly into the official file for the reexamination proceeding, which offers parties the opportunity to review the content of their submissions after the "soft scanning" process is complete.

Any inquiry concerning this communication should be directed to the Central Reexamination Unit at telephone number (571)272-7705.

/Jalatee Worjloh/
Primary Examiner, Art Unit 3992

Conferees:

/C. S./

MB

MATTHEW L. BROOKS
Supervisory Patent Reexamination Specialist
CRU -- Art Unit 3992

Search Notes	**Application/Control No.** 95002035	**Applicant(s)/Patent Under Reexamination** 6779118
	Examiner JALATEE WORJLOH	**Art Unit** 3992

SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES

Search Notes	Date	Examiner
review of patented file's prosecution history	10/3/2012	J.W.

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Reexamination	**Application/Control No.** 95/002,035	**Applicant(s)/Patent Under Reexamination** 6779118
	Certificate Date	**Certificate Number**

Requester Correspondence Address: □ **Patent Owner** ☒ **Third Party**

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

LITIGATION REVIEW ☒	/J.W./ (examiner initials)	**10/3/2012** (date)

Case Name	Director Initials
(OPEN) 8:12cv522, Linksmart Wireless Technology Llc v. T-Mobile USA, Inc. et al., U.S District-California Central (Southern Division)	MB for IY
(CLOSED) 2:10cv277, Linksmart Wireless Technology Llc vs. TJ Hospitality Ltd. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:09cv26, Linksmart Wireless Technology Llc. v. Six Continents Hotels Inc. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv385, Linksmart Wireless Technology, Llc. V. Sbc Internet Services Inc., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv304, Linksmart Wireless Technology, Llc. V. Cisco Systems, Inc. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv264, Linksmart Wireless Technology, Llc. v. T-Mobile USA, Inc. et al., U.S District- Texas Eastern (Marshall)	MB for IY

COPENDING OFFICE PROCEEDINGS

TYPE OF PROCEEDING	**NUMBER**
Ex Parte reexamination	90/012342
Ex Parte reexamination	90/012378

Reexamination	**Application/Control No.**	**Applicant(s)/Patent Under Reexamination**
	Certificate Date	**Certificate Number**

Requester Correspondence Address: ☐ **Patent Owner** ☒ **Third Party**

David L. McCombs
Haynes and Boone, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219

LITIGATION REVIEW ☒	/J.W./ (examiner initials)	10/3/2012 (date)

Case Name	Director Initials
(OPEN) 8:12cv522, Linksmart Wireless Technology Llc v. T-Mobile USA, Inc. et al., U.S District-California Central (Southern Division)	MB for IY
(CLOSED) 2:10cv277, Linksmart Wireless Technology Llc vs. TJ Hospitality Ltd. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:09cv26, Linksmart Wireless Technology Llc. v. Six Continents Hotels Inc. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv385, Linksmart Wireless Technology, Llc. V. Sbc Internet Services Inc., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv304, Linksmart Wireless Technology, Llc. V. Cisco Systems, Inc. et al., U.S District- Texas Eastern (Marshall)	
(CLOSED) 2:08cv264, Linksmart Wireless Technology, Llc. v. T-Mobile USA, Inc. et al., U.S District- Texas Eastern (Marshall)	MB for IY

COPENDING OFFICE PROCEEDINGS

TYPE OF PROCEEDING	**NUMBER**

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/002,035	09/12/2012	6779118

CONFIRMATION NO. 1745

REEXAM ASSIGNMENT NOTICE

HAYNES AND BOONE, LLP IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

OC000000056563783

Date Mailed: 09/17/2012

NOTICE OF *INTER PARTES* REEXAMINATION REQUEST FILING DATE

Requester is hereby notified that the filing date of the request for *inter partes* reexamination is 09/12/2012, the date that the filing requirements of 37 CFR § 1.915 were received.

A decision on the request for *inter partes* reexamination will be mailed within three months from the filing date of the request for *inter partes* reexamination. (See 37 CFR 1.923.)

A copy of this Notice is being sent to the person identified by the requestor as the patent owner. Further patent owner correspondence will be with the latest attorney or agent of record in the patent file. (See 37 CFR 1.33.) Any paper filed should include a reference to the present request for *inter partes* reexamination (by Reexamination Control Number) and should be addressed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

cc: Patent Owner
40401
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

REEXAM CONTROL NUMBER	FILING OR 371 (c) DATE	PATENT NUMBER
95/002,035	09/12/2012	6779118

CONFIRMATION NO. 1745

ASSIGNMENT NOTICE

40401
Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria, VA 22314

OC000000056563784

Date Mailed: 09/17/2012

NOTICE OF ASSIGNMENT OF *INTER PARTES* REEXAMINATION REQUEST

The above-identified request for *inter partes* reexamination has been assigned to Art Unit 3992. All future correspondence in this proceeding should be identified by the control number listed above and directed to: Mail Stop Inter Partes Reexam, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

A copy of this Notice is being sent to the latest attorney or agent of record in the patent file or, if none is of record, to all owners of record. (See 37 CFR 1.33(c).) If the addressee is not, or does not represent, the current owner, he or she is required to forward all communications regarding this proceeding to the current owner(s)

(MPEP 2222). An attorney or agent receiving this communication who does not represent the current owner(s) may wish to seek to withdraw pursuant to 37 CFR 1.36 in order to avoid receiving future communications. If the address of the current owner(s) is unknown, this communication should be returned with the request to withdraw pursuant to Section 1.36.

cc: Third Party Requester
HAYNES AND BOONE, LLP IP SECTION
2323 VICTORY AVENUE
SUITE 700
DALLAS, TX 75219

/rbell/

Legal Instruments Examiner
Central Reexamination Unit 571-272-7705; FAX No. 571-273-9900

In place of PTO-1449 Form	U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	*Complete if Known*	
		Application Number	*Inter Partes* Reexamination of U.S. Patent No. 6,779,118
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*		Filing Date	September 12, 2012
		Real Parties in Interest	Cisco Systems, Inc.
		Art Unit	TBD
		Examiner Name	TBD
SHEET 1	OF 1	Attorney Docket Number	43614.61

U. S. PATENTS

Examiner's Initials	Cite No.	Document Number	Issue Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document
	Exhibit E	5848233	12-08-1998	Radia et al.
	Exhibit F	5835727	11-10-1998	Wong et al.
	Exhibit G	5950195	09-07-1999	Stockwell et al.
	Exhibit H	6073178	06-06-2000	Wong et al.
	Exhibit I	5889958	03-30-1999	Willens
	Exhibit K	6233686	05-15-2001	Zenchelsky et al.
	Exhibit L	6088451	07-11-2000	He et al.
	Exhibit M	5815574	09-29-1998	Fortinsky

U. S. PATENT APPLICATION PUBLICATIONS

Examiner's Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document

FOREIGN PATENT DOCUMENTS

Examiner's Initials	Cite No.	Foreign Patent Document (Country Code – Number – Kind)	Publication Date MM-DD-YYYY	Patentee or Applicant of Cited Document	Translation Y/N

NON-PATENT LITERATURE DOCUMENTS

Examiner's Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article, title of the item, date, page(s), volume-issue number(s), publisher, city/country where published
	Exhibit J	Request for Comments 2138, Internet Engineering Task Force, April 1997 ("RFC 2138").

Examiner Signature		Date Considered	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include a copy of this form with next communication to applicant.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of Koichiro Ikudome, et al.

U.S. Patent No. 6,779,118

Filed: April 21, 1999
CPA Filed: July 19, 2000

Issued: Aug. 17, 2004

Title: User Specific Automatic Data
Redirection System

REQUEST FOR *Inter Partes*
REEXAMINATION

Attorney Docket No.: 43614.61

Customer No.: 27683

Real Party in Interest:
Cisco Systems, Inc.

(CORRECTED) REQUEST FOR INTER PARTES REEXAMINATION

Mail Stop *Inter Partes* Reexam
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Decision Sua Sponte Vacating Filing Date mailed Sept. 6, 2012, David L. McCombs ("Requester") submits this corrected request for *inter partes* reexamination of claims 2-7, 9-14, 16-24, and 26-90 (all of the non-canceled claims) of U.S. Patent No. 6,779,118 ("the '118 patent," Exhibit A) issued August 17, 2004, to Ikudome, et al., resulting from a Continued Prosecution Application filed July 19, 2000 on a patent application filed on April 21, 1999 and including the Reexamination Certificate No. 8926 issued on March 27, 2012.

In accordance with 37 C.F.R. 1.915(b)(7), Cisco Systems, Inc. certifies that the estoppel provisions of 37 C.F.R. 1.907 do not prohibit this request for *inter partes* reexamination.

The Requester submits that this Request presents prior art references and analysis that are better than, and non-cumulative of, the prior art that was before the Examiner during the original prosecution of the '118 patent and the recent ex parte reexamination. Claims 2-7, 9-14, 16-24, and 26-90 are invalid over these references. Requester requests that the Patent Office initiate a reexamination proceeding to ultimately conclude with the issuance of a reexamination certificate cancelling all remaining claims.

TABLE OF CONTENTS

I. BACKGROUND

The '118 patent issued from a Continued Prosecution Application (CPA) filed July 19, 2000. Thus, the '118 patent is eligible for *inter partes* reexamination.[1]

The '118 patent is currently the subject of litigation, *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., et al.*, Case No. 8-12-cv-00522, in the Central District of California (filed Apr. 5, 2012). The litigation was previously pending in the Eastern District of Texas as Case Nos. 2:08-cv-00264, 2:08-cv-00304, 2:08-cv-00385, and 2:09-cv-00026, but the parties dismissed those cases without prejudice in favor of the California action. Before the change of venue, the Eastern District of Texas court issued an order construing the claims of the '118 patent (attached as Exhibit C).

The '118 patent was also the subject of a recently concluded ex parte reexamination, Control No. 90/009,301 (the "first reexamination of the '118 patent"). In that proceeding, the patent owner canceled claims 1, 8, 15, and 25, amended claims 16-23 and 26-27, and added new claims 28-90.

II. REASONABLE LIKELIHOOD THAT REQUESTER WILL PREVAIL WITH RESPECT TO AT LEAST ONE OF THE CLAIMS OF THE '118 PATENT

This request establishes that there is a reasonable likelihood that Requester will prevail with respect to at least one of the claims of the '118 patent. Further, the information presented in this request shows that there is a reasonable likelihood that the Requester will prevail with respect to all of the claims of the '118 patent.

1. Brief Overview of the '118 Patent and its Prosecution

The '118 patent relates to systems and methods that dynamically filter and redirect traffic using a database of filtering rules. The '118 patent is based on an application that was filed on April 21, 1999 and claims priority to a provisional application filed on May 4, 1998. The '118 patent ultimately issued from a continued prosecution application (CPA) filed on July 19, 2000.

[1] *See* MPEP 2611 ("An inter partes reexamination can be filed for a patent issued from an original application filed on or after November 29, 1999. ... The phrase 'original application' is interpreted to encompass ... continued prosecution applications (CPAs)....").

Claim 1, which is representative of the original independent claims (now all canceled), generally recites the following limitations:

- a database with entries correlating each of a plurality of user IDs with an individualized rule set;
- a dial-up network server that receives user IDs from users' computers;
- a redirection server connected to the dial-up network server and a public network;
- an authentication accounting server connected to the database, the dial-up network server and the redirection server;
- wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;
- wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and
- wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

2. Prior Art Presented In This Request Teaches a Redirection Server for Redirecting Data

During the first reexamination proceeding, claim 1 and the other independent claims were canceled while claims 2-7, 9-14, 16-24, and 26–27 were confirmed as patentable in a decision by the Board of Patent Appeals and Interferences. Claims 28-43, added during the first reexamination proceeding, were also before the Board. The Board reversed all of the Examiner's rejections because the prior art relied on by the Examiner did not teach a "redirection server," and instead taught a server "providing the control functions of blocking and allowing."[2] However, the Board found that redirection was in the admitted prior art, and that redirecting a request was an obvious variation on blocking the request outright.[3] On that basis, the Board entered a new ground of rejection against only the independent claims.[4] The Board's decision did not consider whether the same new ground of rejection should be applied to claims 2-7, 9-14, 16-24, and 26–43.

In contrast to the art relied on during the previous ex parte reexamination of the '118 patent, the present request presents and applies prior art that squarely teaches redirecting a user's request to an alternate destination. For example, US 5950195 to Stockwell teaches a rule that "intercepts all incoming connections that go the external side of the local Sidewinder (192.168.1.192) and *redirects* them to shade.sctc.com (172.17.192.48)."[5]

Additionally, the applicant's admitted prior art teaches a web page that "contains html code instructing the browser to request some other WWW page—hence the *redirection* of the user begins."[6] The applicant also admitted that "*redirection* of Internet traffic is most often done with World Wide Web (WWW) traffic."[7] Thus, the prior art presented in this request teaches the "redirection" limitations recited in the claims.

3. Prior Art Presented In This Request Teaches a Redirection Server Connected Between the Dial-Up Network Server and the Public Network

Also during the first reexamination proceeding, new claims 44-90 were added. The added claims are not allowed to broaden the scope of any existing claim. New claims 44-90 generally correspond to the claims 1-43, but with the additional limitation that the redirection server is connected *between* the dial-up network server and the public network (independent

[2] *See* Ex. B-3, Decision on Appeal, Reexamination Control No. 90/009,301, at 6 (Aug. 23, 2011).
[3] *See id.* at 9 ("[R]edirection is an obvious extension of the use of a control to block the user.").
[4] *See id.* at 10.
[5] Stockwell, 2:29-31 (emphasis added).
[6] '118 Patent, 1:55-57 (emphasis added). Although the admitted prior art was relied on to invalidate claims 1, 8, 15, and 25, the admitted prior art was never considered in the previous reexamination with respect to the remaining claims.
[7] '118 Patent, 1:38-39 (emphasis added).

claims 44 and 56) or *between* the user computer and the public network (independent claims 68 and 83).[8]

Claims 44-90 were added after the Board decision in the previous ex parte reexamination. The Examiner confirmed these claims because they recite the additional "between" limitation regarding the location of the redirection server.

In contrast to the art cited by the Examiner during the previous ex parte reexamination of the '118 patent, the present request presents and applies prior art teaching a redirection server connected *between* a dial-up network server and a public network.

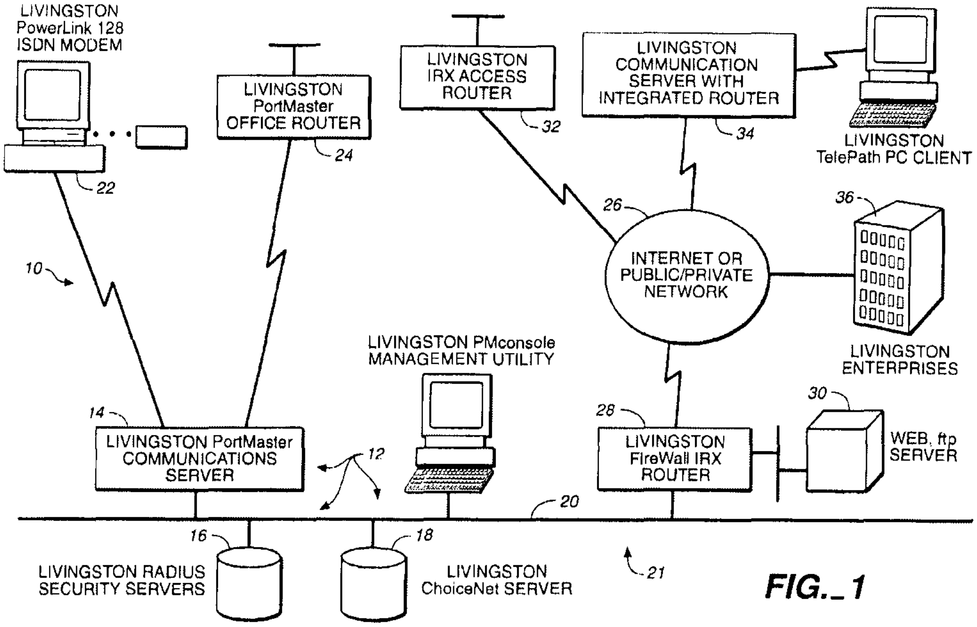
(i) Willens

Willens (Exhibit I) teaches a system for controlling users' access to a network. In one example, the Willens system can be implemented in a school setting to monitor content accessed from the Internet over the school's Local Area Network (LAN). Filters are associated with users so that, for example, a user's request for an Internet resource can be allowed or blocked at the packet level. Willens' communications server 14 provides the packet blocking function. It would have been obvious to add a redirection feature (as was already known in the prior art) to a device capable of blocking a user's access requests.[9] Therefore, the communications server 14 corresponds to the claimed redirection server. Willens illustrates in Fig. 1 that the communications server 14 is between a dial-up network server (such as the Livingston PowerLink 128 ISDN Modem or router 24[10]) and the Internet 26. Willens further illustrates in Fig. 1 an embodiment in which the blocking functionality of the communications server can be implemented in an integrated router 34 that is placed between Livingston TelePath PC Client (a user computer) and the Internet.

[8] *See* Ex. B-3, Notice of Intent to Issue Ex Parte Reexamination Certificate, at 4, Reexam Control No. 90/009301 (Jan. 6, 2012).

[9] Requester notes that the Board agreed in the previous reexamination that it would have been obvious to add a redirection feature to a device capable of blocking a user's access requests. *See* Ex. B-3, Decision on Appeal, Reexamination Control No. 90/009,301, at 9 (Aug. 23, 2011).

[10] The Patent Owner asserts that a router is a "dial-up network server." *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.


LIVINGSTON PowerLink 128 ISDN MODEM
22
LIVINGSTON PortMaster OFFICE ROUTER
24
LIVINGSTON IRX ACCESS ROUTER
32
LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER
34
LIVINGSTON TelePath PC CLIENT
36
10
26
INTERNET OR PUBLIC/PRIVATE NETWORK
LIVINGSTON ENTERPRISES
LIVINGSTON PMconsole MANAGEMENT UTILITY
14
LIVINGSTON PortMaster COMMUNICATIONS SERVER
12
28
LIVINGSTON FireWall IRX ROUTER
30
WEB, ftp SERVER
20
16
18
LIVINGSTON RADIUS SECURITY SERVERS
LIVINGSTON ChoiceNet SERVER
21
FIG._1

WILLENS FIG. 1

Willens further illustrates in Fig. 3 an example in which the dial-up network server (a "Remote Authentication and Dial In User Service," or RADIUS, client) and redirection server (ChoiceNet Client) are both provided by the disclosed communications server 14.[11] It would have been obvious to one of ordinary skill in the art that when both servers are combined into a single device, the dial-up network server provides immediate communication with the end user. Thus, the user's communications flow through the dial-up network server component before being processed by the redirection server component, so the redirection server is between the dial-up network server and the public network.

[11] The Patent Owner asserts that the dial-up network server and the redirection server limitations may be met by a single device. *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9 ("For example, the network server can be the router running the SSG or ISG software.") and at 18 ("In these configurations, the SSG is the redirection server.").

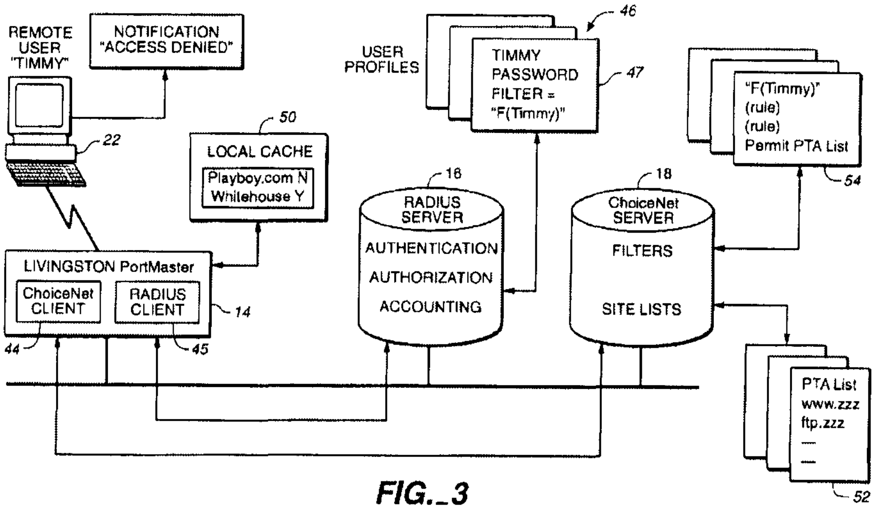


FIG._3

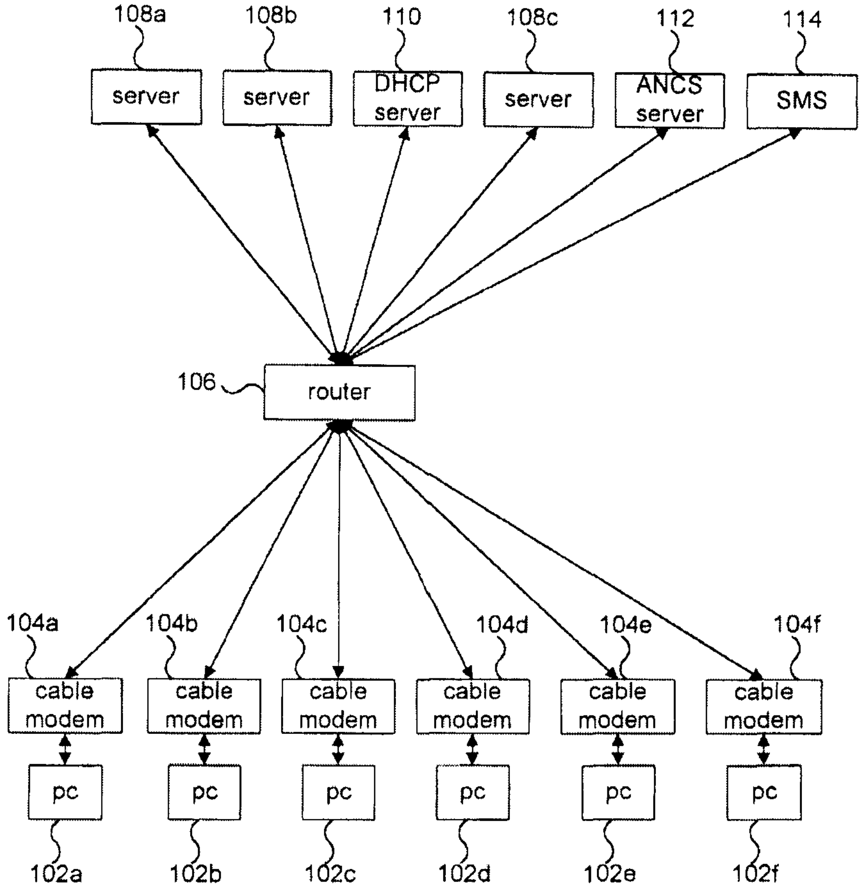
WILLENS FIG. 3

Accordingly, Willens provides multiple disclosures of the specific feature that purportedly distinguished claims 44-90 over the Board's new ground of rejection: the redirection server is connected *between* the dial-up network server and the public network. Requester shows in Exhibit AA that this feature, as well as the other features of the remaining, non-canceled claims, are disclosed by the cited combinations of art that include Willens.

(ii) Radia

Radia (Exhibit E) teaches a computer network that controls users' access to a network by applying filtering rules from a filtering profile database to network access requests made by users. An access network control server (ANCS) 112 configures a router 106 to filter packets to and from each user according to each user's filter profile. In one aspect, the router and the ANCS together act as a redirection server.[12] Radia illustrates in Fig. 1 that the access network control server (ANCS) 112 and router 106 are connected between a user's cable modem 104 (a "dial-up network server") and servers 108, which generally represent the broad range of server systems found in computer networks such as the public Internet.

[12] The Patent Owner asserts that the "redirection server" limitation may be met by a combination of multiple hardware or software components. *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 18 ("In the alternative the redirection server can be a combination of the SSG and SESM. The redirection server may also be embodied by a different combination of hardware and software.").



RADIA FIG. 1

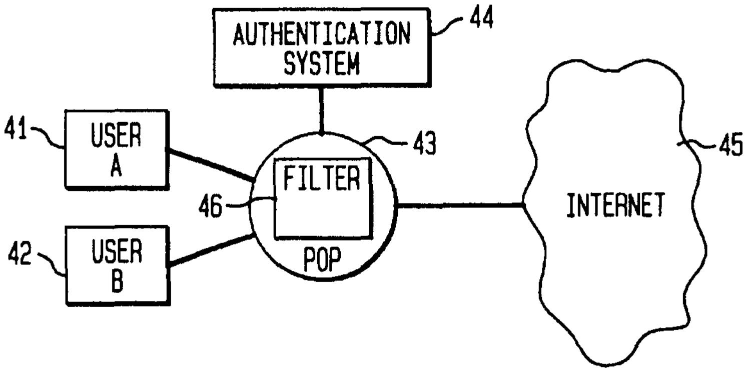
Accordingly, Radia teaches the specific feature that purportedly distinguished claims 44-90 over the Board's new ground of rejection: the redirection server is connected *between* the dial-up network server and the public network. Requester shows in Exhibit BB that this feature, as well as the other features of the remaining, non-canceled claims, are disclosed by the cited combinations of art that include Radia.

(iii) He, Zenchelsky, & Admitted Prior Art

As noted above, the Patent Owner canceled claims 1, 8, 15, and 25 (all of the original independent claims) during the previous reexamination because these claims were invalid as obvious over the prior art cited by the Board, specifically, He in view of Zenchelsky and the admitted prior art. The Board's decision did not considered whether this combination of prior art likewise invalidates the originally-issued dependent claims. It does.

For example, claim 2 recites that "the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set." Each of He, Zenchelsky, and the Admitted Prior Art teach controlling a user's access to network resources by controlling data to and from the user's computer. He teaches that the credential server (the "redirection server") controls the data a user may access as a function of the user's credentials. Zenchelsky teaches a filter rule base that provides detailed control over each user's data, allowing or blocking a user's communications on a per-user and per-destination basis. The Admitted Prior Art similarly teaches using packet filters at the Internet Protocol (IP) layer to control users' access to Internet destinations. Thus, claim 2 is not distinguishable from the prior art combination that was found to invalidate claim 1. Requester shows in Exhibit CC that the other features of the remaining original dependent claims are similarly disclosed by the combination of He, Zenchelsky, and the Admitted Prior Art.

Regarding claims 44-90 added during the previous reexamination, the Examiner found that the "between" limitation recited in the new claims distinguished over the network structure of He. But the Examiner did not consider the relevant teachings of Zenchelsky and the Admitted Prior Art.[13] For example, Zenchelsky teaches providing a filter 46 between a user and the Internet for restricting a user's access to resources on the Internet:



ZENCHELSKY FIG. 4.

Zenchelsky further describes using the filter to regulate access to the network and notes the importance of positioning the filter *between* a source and destination:

[13] *See* Notice of Intent to Issue Reexamination Certificate at 4.

> A security policy rule base is implemented on a network using a device called a filter comprising hardware and software. The rule base is loaded into the filter, which receives packets en route (***between their source and destination***) and checks the identifier of each packet against the identifier contained in each rule of the rule base for a match, i.e., if the packet corresponds to the rule. A packet corresponds to a rule if the rule applies to the packet.... If the PASS action is carried out, the packet is allowed to pass through the filter. If the DROP action is carried out, the packet is eliminated.[14]

One of ordinary skill in the art would have understood that the connection from user 41 to Internet Service Provider Point of Presence (POP) 43 includes a dial-up network server. For example, the Admitted Prior Art discloses that the dial-up network server is the physical terminus for a communication link from the user's computer:

> In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a ***physical connection between their computer 100 and a dial-up networking server 102***, the user provides to the dial-up networking server their user ID and password.[15]

Accordingly, one of ordinary skill in the art would understand that Zenchelsky's connection between the user 41 to Point of Presence (POP) 43 includes a dial-up network server. Zenchelsky's filter for controlling the user's access to the public Internet—located within the Point of Presence (POP)—is therefore *between* the dial-up network server and the public Internet. Requester shows in Exhibit CC that this feature, as well as the other features of the remaining, non-canceled claims, are disclosed by the cited combinations of art that include Zenchelsky.

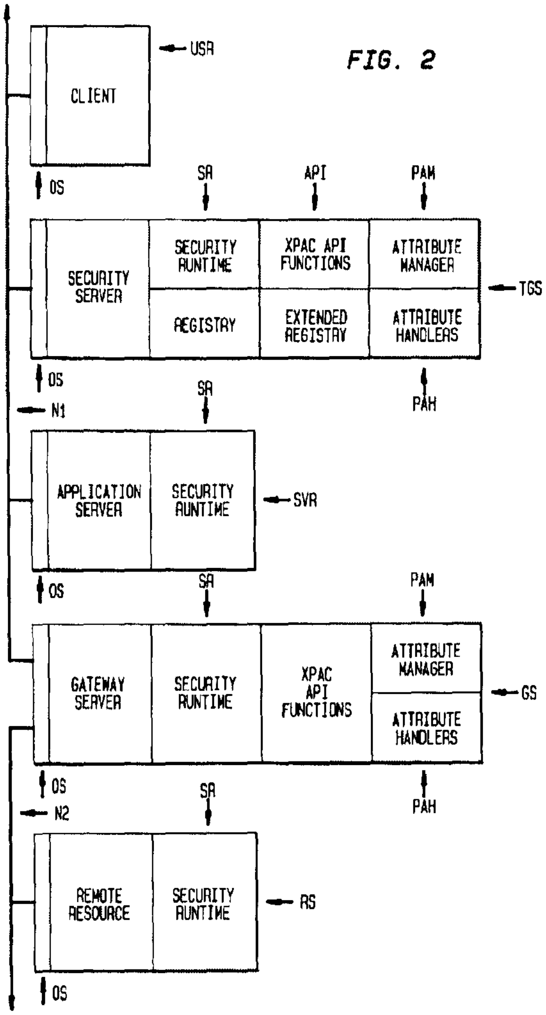
(iv) Fortinsky

Providing further support to the teachings of He, Zenchelsky, and the Admitted Prior Art is Fortinsky (Exhibit M). Fortinsky teaches a network architecture using the same authentication and security technology as He, specifically, the Kerberos authentication system

[14] Zenchelsky, 2:26-41 (emphasis added).
[15] '118 Patent, 16-21.

developed by the Massachusetts Institute of Technology. Fortinsky's network further includes a gateway server "GS" that provides controlled access to a remote resource "RS":

> The extensions provided by the present invention are described further below, in the context of a network N1 as shown diagrammatically in FIG. 2, in which a DCE network also includes a ***gateway server GS through which is accessible a non-DEC server RS, possibly by a secondary non-DEC network N2*** as shown or possibly located in the same machine.[16]



FORTINSKY, FIG. 2

[16] Fortinsky, 5:14-20 (emphasis added).

Notably, Fortinsky's gateway server is located *between* the user's connection to network N1 and the remote resource RS on network N2. Thus, Fortinsky provides a further teaching that renders obvious connecting a redirection server (such as the gateway server GS) *between* a dial-up network server and an external network. Requester shows in Exhibit DD that this feature, as well as the other features of the remaining, non-canceled claims, are disclosed by the cited combinations of art that include Fortinsky.

4. Claim Charts Presented In This Request Render Obvious All Claims Of The '118 Patent

Exhibits AA–DD present multiple reasons to combine the cited prior art references to render the claims invalid as obvious the claims of the '118 Patent.

Exhibit AA: Proposed Rejections based on Willens

Proposed Rejection #1: Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Stockwell under 35 U.S.C. § 103(a).

Proposed Rejection #2: Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Admitted Prior Art under 35 U.S.C. § 103(a).

Exhibit BB: Proposed Rejections based on Radia/Wong Family

Proposed Rejection #3: Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Stockwell under 35 U.S.C. § 103(a).

Proposed Rejection #4: Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Stockwell and further in view of Wong '178 under 35 U.S.C. § 103(a).

Proposed Rejection #5: Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Admitted Prior Art under 35 U.S.C. § 103(a).

Proposed Rejection #6: Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Admitted Prior Art and further in view of Wong '178 under 35 U.S.C. § 103(a).

Exhibit CC: Proposed Rejections based on He, Zenchelsky, and the Admitted Prior Art

Proposed Rejection #7: Claims 2-7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky and further in view of the Admitted Prior Art under 35 U.S.C. § 103(a).

Exhibit DD: Proposed Rejections based on He, Zenchelsky, Fortinsky and the Admitted Prior Art

Proposed Rejection #8: Claims 2-7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky, Fortinsky, and the Admitted Prior Art under 35 U.S.C. § 103(a).

III. CITATION OF PRIOR ART PATENTS AND PRINTED PUBLICATIONS

Reexamination of claims 2-7, 9-14, 16-24, and 26-90 (all of the non-canceled claims) of the '118 patent is requested in view of the following references:

Exhibit A	Applicants' Admitted Prior Art, U.S. Patent 6,779,118, including Fig. 1 & cols. 1-2.
Exhibit E	United States Patent No. 5,848,233 ("Radia").
Exhibit F	United States Patent No. 5,835,727 ("Wong '727").
Exhibit G	United States Patent No. 5,950,195 ("Stockwell").
Exhibit H	United States Patent No. 6,073,178 ("Wong '178").
Exhibit I	United States Patent No. 5,889,958 ("Willens").
Exhibit J	Request for Comments 2138, Internet Engineering Task Force, April 1997 ("RFC 2138").
Exhibit K	United States Patent No. 6,233,686 ("Zenchelsky").
Exhibit L	United States Patent No. 6,088,451 ("He").
Exhibit M	United States Patent No. 5,815,574 ("Fortinsky").

RFC 2138 qualifies as prior art under 35 U.S.C. § 102(b); Radia, Wong '727, Wong '178, Stockwell, Willens, Zenchelsky, He, and Fortinsky qualify as prior art under 35 U.S.C. § 102(e).

Radia, Wong '727, Stockwell, and Willens were among 104 prior art documents submitted by the Patent Owner on an Informational Disclosure Statement during the previous ex parte reexamination proceeding.[17] However, the substance of their teachings was never discussed or addressed by the Examiner.

RFC 2138 was cited by Requester Sewell in the request that initiated the first reexamination proceeding, but the Examiner did not discuss the reference except in the decision granting the request for reexamination.

He and Zenchelsky were considered during the previous ex parte reexamination and, in combination with the admitted prior art, held to invalidate the original independent claims (now canceled). The combination of He, Zenchelsky, and admitted prior art was never considered with respect to the remaining claims of the '118 Patent.

Requester failed to locate any citation to Wong '178 or Fortinsky anywhere in the prosecution history of the '118 Patent or in the file history of the previous ex parte reexamination proceeding.

IV. DETAILED EXPLANATION OF THE PERTINENCY AND MANNER OF APPLYING THE PRIOR ART REFERENCES TO EVERY CLAIM FOR WHICH REEXAMINATION IS REQUESTED

A discussion of the patent, the prosecution history, and the prior art is provided below, followed by a listing of proposed rejections and a detailed explanation and manner of applying these references to every claim for which reexamination is requested.

1. Overview of the '118 Patent and its Prosecution

The '118 patent is entitled "USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM." The '118 patent was granted on August 17, 2004 on an application filed on July 19, 2000 as a Continued Prosecution Application of application number 09/295,966 filed on April 21, 1999. The '118 patent is directed to a data redirection system that redirects a user's request based on a stored rule set. In this way, the system can control a user's access to resources on a network. The '118 patent abstract recites:

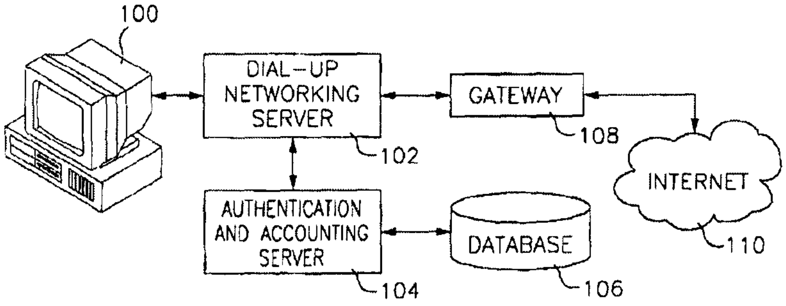
[17] *See* Ex. B-3, Information Disclosure Statement, Reexamination Control No. 90/009301 (signed by Examiner Jul. 15, 2010, mailed Aug. 2, 2010).

> A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.

('118 Patent, Abstract.)

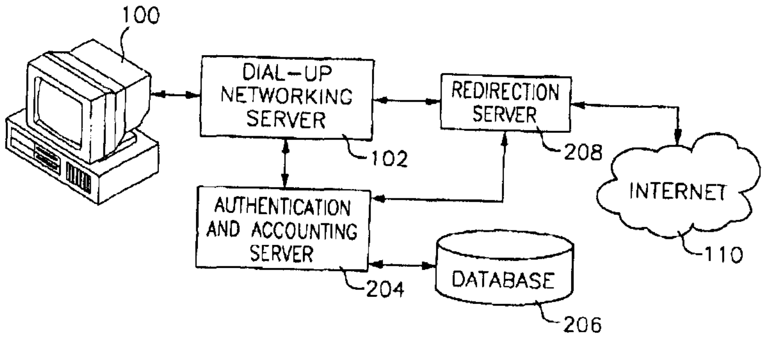
Fig. 1 of the '118 patent (below) illustrates a prior art system for a "typical Internet Service Provider environment." ('118 Patent, 3:36-37.)

FIG. 1


100
DIAL-UP NETWORKING SERVER
102
GATEWAY
108
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
104
DATABASE
106

'118 PATENT FIG. 1 (ADMITTED PRIOR ART)

Fig. 2 of the '118 patent (below) shows "a block diagram of an embodiment of an Internet Service Provider environment with integrated redirection system." ('118 Patent, 3:38-40.)


100
DIAL-UP NETWORKING SERVER
102
REDIRECTION SERVER
208
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
204
DATABASE
206

'118 PATENT FIG. 2

The '118 patent describes the functionality of the system as follows:

> The redirection server 208 is logically located between the user's computer 100 and the network, and controls the user's access to the network. The redirection server 208 performs all the central tasks of the system. The redirection server 208 receives information regarding newly established sessions from the authentication accounting server 204. The Auto-Navi component of the authentication accounting server 204 queries the database for the rule set to apply to each new session, and forwards the rule set and the currently assigned IP address to the redirection server 208. The redirection server 208 receives the IP address and rule set, and is programed to implement the rule set for the IP address, as well as other attendant logical decisions such as: checking data packets and blocking or allowing the packets as a function of the rule sets, performing the physical redirection of data packets based on the rule sets, and dynamically changing the rule sets based on conditions.

('118 Patent, 4:50-66.)

Of the 27 originally issued claims in the '118 patent, all of the independent claims (1, 8, 15, and 25) have been cancelled. Claim 44, added during the previous reexamination and based on the original claim 1, is an exemplary system claim:

> 44. A system comprising:
>
> a database with entries correlating each of a plurality of user IDs with an individualized rule set;

> a dial-up network server that receives user IDs from users' computers;
>
> a redirection server connected between the dial-up network server and a public network, and
>
> an authentication accounting server connected to the database, the dial-up network server and the redirection server;
>
> wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;
>
> wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and
>
> wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

(Ex. A, Reexamination Certificate No. 8926, 5:41-63.)

This architecture for controlling network access was already known in the prior art, as shown in the detailed analysis of this request.

2. Prosecution History and Reasons for Allowance of the '118 Patent

Requester provides a description of the prosecution history of the '118 patent for completeness, although the prosecution history of the first reexamination is generally more germane to the issues in this Request.

The '118 patent issued from U.S. App. 09/295,966, filed on Apr. 21, 1999 with 29 claims. On July 19, 2000, the applicants filed a Continued Prosecution Application (CPA).

In an Office Action dated January 30, 2001, claims 1-29 were rejected as being anticipated by WO 96/05549 to Horowitz.

In a response dated July 30, 2001, the applicants amended the independent claim 1 to further recite these additional limitations:

1) that the redirection server is connected to "a public network";

2) that the first user ID is "for one of the users' computers"; and

3) that "data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set."

(Amendment of July 30, 2001 at 8.) Claim 8 was similarly amended.

The applicants argued that claims 1 and 8 were distinguishable over the Horowitz disclosure by noting that "the filters used in Horowitz are based upon predetermined resources on the local computer network." (*Id.* at 6.) The applicants stated that because "the resources on the public network are virtually limitless, … filtering based only on predetermined resources is not effective." (*Id.* at 6–7.)

The applicants also amended claim 15 to further recite:

1) that "a plurality of functions used to control passing between the user and a public network," and

2) that "the redirection server is configured to allow automated modification of at least a portion of the rule set."

(*Id.* at 9.)

The applicants argued that claims 15 and 26 were distinguishable over Horowitz because Horowitz did not disclose "allowing modification of a portion of a rule set … and, particularly, allowing the automated modification of at least a portion of a rule set." (*Id.* at 7.) The applicants also argued that Horowitz did not disclose "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server, as set forth in claim 26." (*Id.*)

In a Final Office Action dated October 12, 2001, the examiner again rejected claims 1-29 as anticipated by Horowitz. On April 12, 2002, the applicants filed a Notice of Appeal.

On October 10, 2002, the applicants conducted an examiner interview. The Examiner's summary of the interview states that the parties "discussed the claimed invention." (Interview Summary of Oct. 10, 2002.)

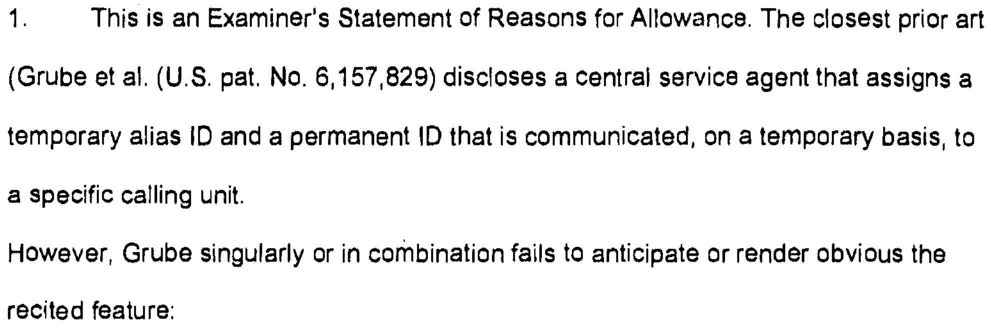
On October 22, 2002, the applicants filed a response to the October 12, 2001 Office Action. The applicants argued that Horowitz disclosed only limiting access to resources on a private network and did not disclose "anything about a system that controls a user's access to a public network, such as the Internet." (Response to Final Action of Oct. 22, 2002 at 1.) The applicants also argued that "Horowitz does not disclose any server that redirects data, but rather only passively blocks or allows data." (*Id.* at 3.) The applicants clarified that "Redirection involves the server 'directing' the user to another area of the network." (*Id.*)

In an Advisory Action dated November 8, 2002, the Examiner indicated that the response did not put the application in condition for allowance. The Advisory Action also stated that the period for reply had expired 3 months from the mailing date of the final rejection of October 12, 2001 (more than one year earlier). A Notice of Abandonment issued on March 24, 2003, but was subsequently withdrawn without explanation on April 23, 2003.

On November 22, 2002—approximately 13 months after the final rejection—the applicants filed an Appeal Brief. The applicants generally reiterated their arguments from prosecution. (See Appellant's Brief generally.) On May 13, 2003, the Examiner filed an Examiner's Answer, which reiterated the rejections. On June 30, 2003, the applicants filed a Reply Brief reiterating their arguments.

On September 8, 2003, the examiner reopened prosecution by mailing an Office Action rejecting claims 1-29 under 35 U.S.C. § 103(a) as obvious over Horowitz in view of U.S. Pat. 6,157,829 to Grube. The applicants did not file a response to the Office Action.[18]

On February 19, 2004, the examiner issued a Notice of Allowance. The Notice included an Examiner's Amendment cancelling claims 19 and 29, and incorporating their limitations into 15 and 26, respectively. The Examiner provided the following reasons for allowance:



1. This is an Examiner's Statement of Reasons for Allowance. The closest prior art (Grube et al. (U.S. pat. No. 6,157,829) discloses a central service agent that assigns a temporary alias ID and a permanent ID that is communicated, on a temporary basis, to a specific calling unit.

However, Grube singularly or in combination fails to anticipate or render obvious the recited feature:

[18] The copy of the file history for the '118 patent obtained by the present Requester provides no indication as to why the examiner rejected the claims and then mailed a Notice of Allowance. However, the file history summary in the first reexamination indicates that an examiner interview was held on November 20, 2003. *See* Ex. B-3, Amended Request for Ex Parte Reexamination at 6 (Dec. 17, 2008).

> As per claims 1 and 8" wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set".

> As per claims 1 and 8" wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server, and wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set".

> As per claim 26 " modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server, and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server".

(Notice of Allowance at 2-3.)

3. Prosecution History of the First Reexamination of the '118 Patent

On October 10, 2008, Third Party Requester, Jerry Turner Sewell, (hereinafter, Requester Sewell) filed a first Request for Ex Parte Reexamination, which was assigned serial number 90/009,301 and afforded a filing date of October 10, 2008.[19] The USPTO subsequently vacated that filing date and notified Requester Sewell that Requester Sewell had 30 days to fix various issues with the first Request for Ex Parte Reexamination. (Notice of Incomplete Ex Parte Reexamination Request at 2-8). The available file history does not include the first Request for Ex Parte Reexamination, and the first Request for Ex Parte Reexamination will not be discussed

[19] The present Requester is different from Requester Sewell.

further.

Requester Sewell filed a corrected Request for Ex Parte Reexamination (hereinafter, the Ex Parte Request) on December 17, 2008. Requester Sewell proposed numerous alternative rejections of all claims over the references:

(i) Request for Comments 2138 (hereinafter, RFC 2138),

(ii) U.S. Patent No. 6,233,686 (hereinafter, Zenchelsky),

(iii) U.S. Patent No. 5,987,611 (hereinafter, Freund),

(iv) U.S. Patent No. 5,696,898 (hereinafter, Baker) and

(v) U.S. Patent No. 6,466,976 (hereinafter, Alles).

(Response to November 17, 2008 Office Communication Accompanying Amended Request for Ex Parte Reexamination at 2-16).

The USPTO ordered reexamination on February 27, 2009 and issued a first Office Action on September 15, 2009. The Office Action of September 15, 2009 rejected all of the issued claims 1-27. However, the Office Action did not address any of Requester Sewell's proposed rejections. Instead, the Office Action rejected the claims as obvious over U.S. Patent No. 6,088,451 (hereinafter, He) in view of Zenchelsky. He had not been cited by Requester Sewell.

The Examiner issued an Interview Summary on November 9, 2009 to acknowledge an examiner interview with the Patent Owner. The Examiner indicated that some proposed amendments had been discussed, but the proposed amendments were not indentified. Also, the Examiner stated:

> Patent owner's representatives asserted that He et al was directed more to function of "stopping" or "allowing" as opposed to redirecting. Examiners indicated that such "stopping" or "allowing" could be viewed as "redirecting", although examiners would consider any arguments addressed to this point, and indications in specification where the redirecting function was discussed.

(Interview Summary of November 9, 2009 at continuation sheet.)

Patent Owner filed a response to the first reexamination Office Action on November 14, 2009. The response amended claims 15, 18, 21, 26, and 27 and added proposed new claims 28-47. (Response of November 14, 2009 at 1-7.) With respect to the rejection of claim 1 over He and Zenchelsky, the Patent Owner asserted that He teaches a response message that is sent back to the user rather than "the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server." (Response of November 14, 2009 at 11 (emphasis added).) Patent Owner made a similar argument with respect to claim 8 and its limitation, "accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server." (Response of November 14, 2009 at 14-15.)

With respect to independent claim 15, the Patent Owner argued that He does not teach that "the redirection server is configured to allow automated modification of at least a portion of the rule set . . . as a function of some combination of time, data transmitted to or from the user, or a location that the user attempts to access." (Response of November 14, 2009 at 17-19.) Specifically, the Patent Owner stated that 1) He teaches changes by an administrator, not automated modification; 2) He teaches a maximum lifetime of authentication rather than a modification of a rule set as a function of time; and 3) He teaches does not teach modification of a rule set as a function of some combination of time, data transmitted to or from a user, or a location the user attempts to access. (Response of November 14, 2009 at 17-19.)

With respect to independent claim 25, the Patent Owner argued that He does not teach "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server," because "He []merely modifies, but does not teach or suggest when this modification occurs." (Response of November 14, 2009 at 20.) Patent Owner also gave brief explanations of the added claims but did not argue them with any detail over the cited art.

On December 10, 2009, the Patent Owner filed an Examiner Interview Summary that generally reiterated the arguments presented in the Response of November 14, 2009.

On May 24, 2010, the Patent Owner filed a Supplemental Response to the Office Action of September 15, 2009, amending claims 15, 18, 21, 26, and 27 relative to the response of November 14, 2009. (Supplemental Response of May 24, 2010 at 2.) However, the Supplemental Response was refused entry as being non-compliant, according to the Final Office Action discussed immediately below.

The Examiner issued a Final Office Action on August 2, 2010 rejecting all claims (including the added claims 28-47). The Examiner rebutted all of the Patent Owner's assertions by specific reference to the claim language and to the cited art, He.

Another Examiner interview was held on September 22, 2010, and Patent Owner reiterated its arguments for patentability. For instance, Patent Owner argued that the redirection server of claim 1 must, at a minimum, be capable of redirecting. (Interview Summary of October 2, 2010 at 3-4.)

Patent Owner filed a response to the Final Office Action on October 4, 2010, in which Patent Owner made some minor amendments to the claims. (After Final Response of October 4, 2010 at 3-6.) Patent Owner also argued, *inter alia*, that the redirection server must be capable at least of redirecting, and that the cited feature of He was not so capable. (After Final Response of October 4, 2010 at 8-9.) On November 15, 2010, the Examiner issued an Advisory Action rebutting the Patent Owner's assertions.

The Patent Owner went to appeal in front of the Board of Patent Appeals and Interferences, and both the Patent Owner and the Examiner briefed their respective positions, and the briefs reiterated the positions of each party during prosecution. The Board issued a decision on August 23, 2011 affirming-in-part and reversing-in-part the Examiner. The Board Decision discussed and resolved the following points:

- The redirection server of the claims requires redirecting. (Board Decision at 4-6.)
- However, redirection is "an obvious extension of the use of a control to block the user." (Board Decision at 8-10.)
- Redirection was in the prior art. For example, redirecting by replacing a first destination address in an IP packet header by a second destination address as a function of a rule set is obvious based at least on the admitted prior art discussed in the background of the '118 Patent. The admissions make clear that "those in the art were familiar with redirection (and how to do it) at least in a world-wide web context." (Board Decision at 8-9.)
- Redirecting a user and modifying "the rule set as a function of time, data transmitted to or from the user, or location the user accesses" is obvious because it is obvious to block a website based on these factors. For instance, it would be obvious to block "a site for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work." (Board Decision at 9-10.)

- "[D]ata directed toward the public network" and "processed by the redirection server" does not exclude a scenario wherein the user communicates with the redirection server over a public network. (Board Decision at 6.)
- Automated modification of the rule set is satisfied by a tool in a computer context, even if there is human intervention. (Board Decision at 7.)

Having found that the "redirection server" must be capable of redirecting a user to an alternate destination, the Board reversed all of the Examiner's rejections that were based solely on He and Zenchelsky. But having also found that "redirection" was known in the prior art and an obvious variation of known techniques for blocking a user's access request, the Board affirmed the rejection of four dependent claims that the Examiner had rejected as obvious over He, Zenchelsky, and the applicants' admitted prior art. Since the four dependent claims could not be rejected as invalid if their parent dependent claims were found patentable, the Board entered a new ground of rejection for the four corresponding independent claims (1, 8, 15, and 25) as obvious over He, Zenchelsky, and the applicants' admitted prior art. The Board did not discuss the remaining claims, whose rejections were reversed without comment. Thus, the Board did not comment on whether the remaining claims would likewise be obvious over He, Zenchelsky, and the applicants' admitted prior art.

Patent Owner filed a response to the Board Decision on October 21, 2011 cancelling the claims rejected by the Board and placing claims 16-23 and 38-41 in independent form. The Patent Owner also added new claims 48-94. (Response after BPAI Decision at 3.) New claims 48-94 (renumbered in the reexamination certificate as claims 44-90) have "additional terms to clarify the 'between' location of the redirection server." (Response after BPAI Decision at 3.) The added claims 48-94 specify that the redirection server is <u>between</u> the dial up network server and the public network in an effort to distinguish over the combination of He and Zenchelsky. (Interview Summary of October 24, 2011 at 3.)

The claims were numbered 1-90, and the non-canceled claims were issued in their present form by the Reexamination Certificate No. 8926. Claims 44-90 were confirmed at least because they specify that the redirection server is <u>between</u> the dial up network server and the public network. (Notice of Intent to Issue a Reexamination Certificate at 4.) Issued claims 2-7, 9-14, 16-24, and 26-43 were allowed because the Board reversed the rejections of those claims. (Notice of Intent to Issue a Reexamination Certificate at 2-4.) As mentioned above, there was no discussion by the Board indicating any feature in claims 2-7, 9-14, 16-24, and 26-43 that might distinguish over the prior art used to reject the independent claims. Similarly, the Examiner did not provide any reasons for allowing the claims over the prior art submitted and analyzed by the Requester Sewell.

4. Other Reexamination Requests for the '118 Patent

On February 11, 2011, Donald D. Min filed a request for ex parte reexamination of the '118 Patent, assigned to Control No. 90/011,485. The file history of this case is attached as Exhibit B-4. Little information about this reexamination is available to the public. On May 31, 2011, the reexamination was terminated without explanation. The file history indicates that an examiner interview occurred prior to the decision to terminate the reexamination, but the summary of their discussions has not been made available to the public.[20] The Patent Owner did not file a statement of the interview.[21]

On February 17, 2012, Requester Sewell filed a request for ex parte reexamination of the '118 Patent, assigned to Control No. 90/012,149. The file history of this case is attached as Exhibit B-5. The request was denied on March 30, 2012 because the request had been filed before the issuance of the reexamination certificate from the first reexamination proceeding.[22] Requester Sewell filed a petition for reconsideration on April 19, 2012. The petition was subsequently denied on July 18, 2012.

On June 8, 2012, James Wong filed a request for ex parte reexamination of the '118 Patent, assigned to Control No. 90/012,342. The file history of this case is attached as Exhibit B-6. No decision has yet been made on this request.

[20] *See* Ex. B-4, Control Information for 90/011485. Note that MPEP 2281 indicates that an examiner interview "will be permitted prior to the first Office action *only* where the examiner initiates the interview for the purpose of providing an amendment which will make the claims patentable and the patent owner's role is passive. The patent owner's role (or patent owner's attorney or agent) is limited to agreeing to the change or not." MPEP 2281. The file history of Control No. 90/011,485 does not indicate what claim amendment, if any, the examiner proposed. As the proceeding was immediately terminated, no amendment was ever entered.

[21] *See* 37 C.F.R. § 1.560(b).

[22] Ex. B-5, Order Denying Ex Parte Reexamination at 2, Reexamination Control No. 90/012149 (Mar. 20, 2012).

5. Summary of the Cited Prior Art

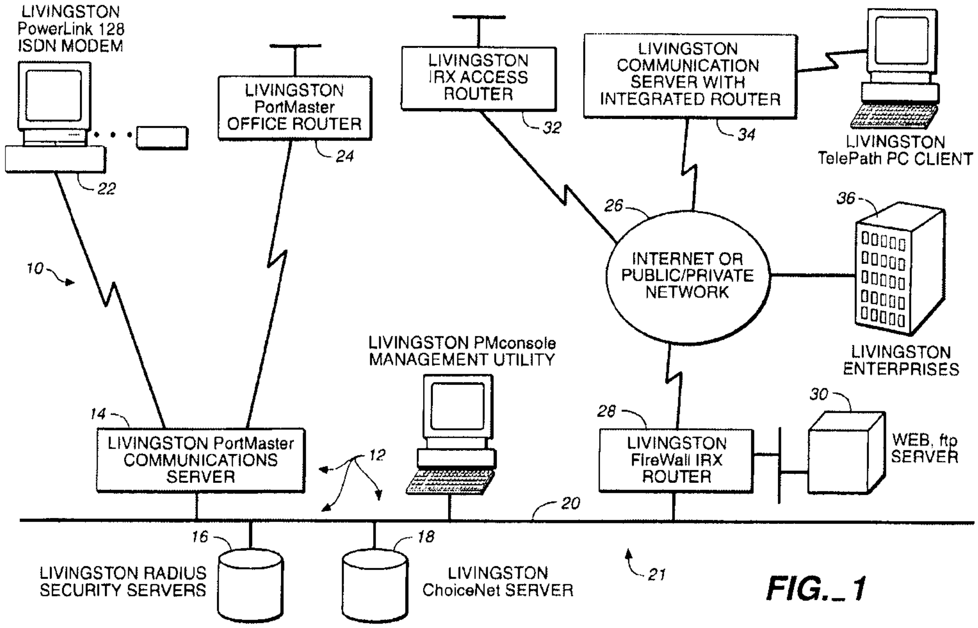
Inter partes reexamination of claims 2-7, 9-14, 16-24, and 26-90 (all of the non-canceled claims) of the '118 patent is requested in view of the following references:

Exhibit A	Applicants' Admitted Prior Art, U.S. Patent 6,779,118, including Fig. 1 & cols. 1-2.
Exhibit E	United States Patent No. 5,848,233 ("Radia").
Exhibit F	United States Patent No. 5,835,727 ("Wong '727").
Exhibit G	United States Patent No. 5,950,195 ("Stockwell").
Exhibit H	United States Patent No. 6,073,178 ("Wong '178").
Exhibit I	United States Patent No. 5,889,958 ("Willens").
Exhibit J	Request for Comments 2138, Internet Engineering Task Force, April 1997 ("RFC 2138").
Exhibit K	United States Patent No. 6,233,686 ("Zenchelsky").
Exhibit L	United States Patent No. 6,088,451 ("He").
Exhibit M	United States Patent No. 5,815,574 ("Fortinsky").

(i) Willens

Previously unconsidered U.S. Patent 5,889,958 to Willens, filed on December 20, 1996 and issued on March 30, 1999, is prior art under §102(a) and §102(e).

Willens teaches a system for controlling users' access to a public network such as the Internet. In one example, the Willens system can be implemented in a school setting to monitor content accessed from the Internet over the school's Local Area Network (LAN). The overall system is illustrated in Fig. 1 below.


LIVINGSTON PowerLink 128 ISDN MODEM
22
LIVINGSTON PortMaster OFFICE ROUTER
24
LIVINGSTON IRX ACCESS ROUTER
32
LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER
34
LIVINGSTON TelePath PC CLIENT
36
26
INTERNET OR PUBLIC/PRIVATE NETWORK
LIVINGSTON ENTERPRISES
10
LIVINGSTON PMconsole MANAGEMENT UTILITY
14
LIVINGSTON PortMaster COMMUNICATIONS SERVER
12
28
LIVINGSTON FireWall IRX ROUTER
30
WEB, ftp SERVER
20
16
18
LIVINGSTON RADIUS SECURITY SERVERS
LIVINGSTON ChoiceNet SERVER
21
FIG._1

WILLENS FIG. 1

Filters are associated with users so that, for example, a user's request for an Internet resource can be allowed or blocked at the packet level. Willens' communications server 14 includes client software 44 (shown in Fig. 3, below) that provides the packet blocking function using users' individualized filters 46 provided from authentication and accounting server 16. For example, dial-up user "TIMMY" is illustrated in Fig. 5 to have the user-specific filter "F(Timmy)." Timmy's request to access the Whitehouse is permitted, while access to Playboy is denied.

It would have been obvious to add a redirection feature (as was already known in the admitted prior art[23]) to a device capable of blocking a user's access requests. For example, redirection could be used to provide information to the user regarding *why* the request was not allowed or to direct the user to a potential substitute or alternative resource.[24] Therefore, the client software 44 on communications server 14 corresponds to the claimed redirection server. Willens illustrates in Fig. 1 that the communications server 14 is between a dial-up network

[23] *See* '118 Patent, 1:38-63.
[24] *See also* Ex. B-3, Decision on Appeal, Reexamination Control No. 90/009,301, at 6 (Aug. 23, 2011).

server (such as the Livingston PowerLink 128 ISDN Modem or router 24[25]) and the Internet 26. Willens further illustrates in Fig. 1 an embodiment in which the blocking functionality of the communications server can be implemented in an integrated router 34 that is placed between Livingston TelePath PC Client (a user computer) and the Internet.

Willens further illustrates in Fig. 3 an example in which the dial-up network server (a "Remote Authentication and Dial In User Service," or RADIUS, client) and redirection server (ChoiceNet Client 44) are both provided by the disclosed communications server 14.[26] It would have been obvious to one of ordinary skill in the art that when both servers are combined into a single device, the dial-up network server provides immediate communication with the end user. Thus, the user's communications flow through the dial-up network server component before being processed by the redirection server component, so the redirection server is between the dial-up network server and the public network.

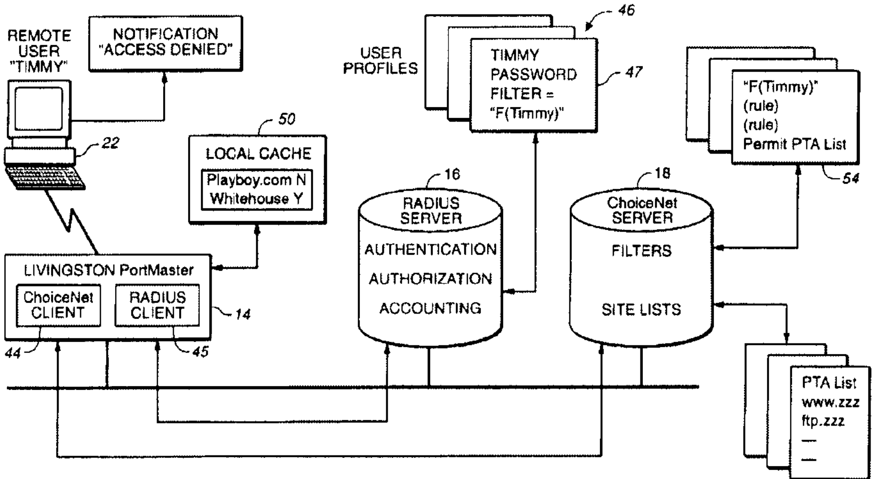


FIG._3

WILLENS FIG. 3

Accordingly, Willens discloses:

[25] The Patent Owner asserts that a router is a "dial-up network server." *See, e.g.*, Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.

[26] The Patent Owner asserts that the dial-up network server and the redirection server limitations may be met by a single device. *See, e.g.*, Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9 ("For example, the network server can be the router running the SSG or ISG software.") and at 18 ("In these configurations, the SSG is the redirection server.").

- a redirection server (client software 44) connected between a dial-up network server (such as RADIUS client 45 or router 24) and the a public network (the Internet);
- communicating a user's individualized rule set (profile 46 and filter rules 54) to the redirection server; and
- processing data directed toward a public network according to the individualized rule set.

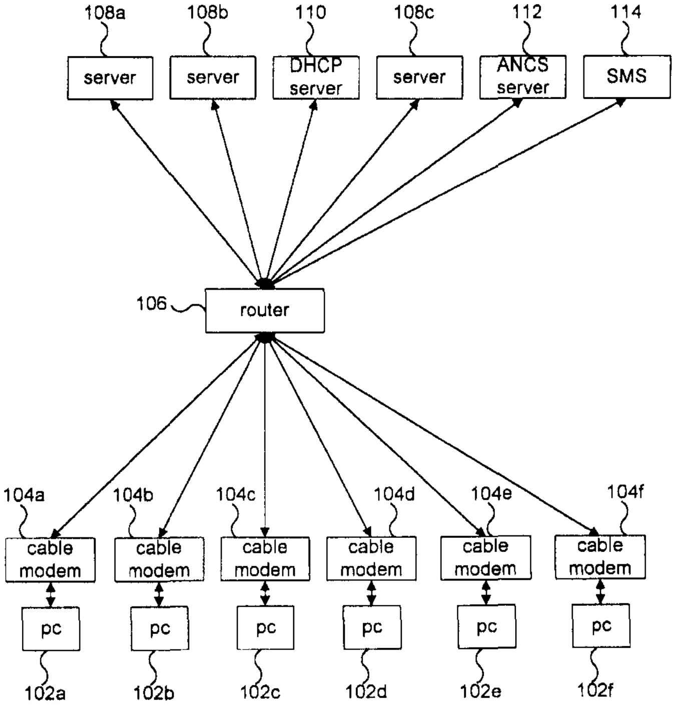
In contrast to the art considered during the first reexamination of the '118 patent, Willens discloses a redirection server that is connected between the dial-up network server and the public network. Requester shows in Exhibit AA that this feature, as well as the other features of the remaining, non-canceled claims, are disclosed by the cited combinations of art that include Willens.

(ii) Radia/Wong Patent family

Previously unconsidered U.S. Pat. 5,848,233 to Radia, filed Dec. 9, 1996 and issued Dec. 8, 1998, is prior art under §102(a) and §102(e). Radia is part of a family of closely related patents with overlapping inventors, all filed the same day and all incorporating each other by reference. Two related patents are U.S. 5,835,727 to Wong ("Wong '727") and U.S. 6,073,178 to Wong ("Wong '178"), both of which are incorporated by reference into the Radia disclosure. (*See* Radia 1:5-45.) Requester refers to Radia and the two Wong patents collectively as the "Radia/Wong Patent Family."

The Radia/Wong Patent Family discloses a system for controlling a user's access to servers on the public Internet. Specifically, Radia discloses that an "internet service provider (ISP) may have users who connect, login, logoff and disconnect to its network over time," and the "ISP would like to control access to this dynamically changing set of users." (Radia 2:45-49.) The ISP provides access to the public Internet network.

Radia illustrates in Fig. 1 (below) that a user at a PC 102 accesses the network through a cable modem 104 and router 106. When a user's PC 102 connects to the network, it receives a temporary internet protocol (IP) address from the Dynamic Host Configuration Protocol (DHCP) server 110. (Radia, 5:28-36.) The user then logs into a system management server 114, which loads the user's filtering profile from a database and sends the filtering profile, along with the user's IP address, to an access network control server (ANCS) 112. The ANCS configures the router 106 to implement the user's filtering profile, allowing or denying access to servers on the network based on the user's filtering profile. (Radia, 9:60–10:7.) Thus, the ANCS 112 and router 106 block access to network resources and it would have been obvious to extend this blocking feature to further include redirection to an alternate destination, as was known in the prior art. (*See* '118 Patent, 1:38-63; see also the discussion of Stockwell below.) For example, through redirection the user can be provided with further information about why access to network resources is not allowed or provided with information on potentially substitute or alternative network resources that would be allowed.[27]



RADIA FIG. 1

Accordingly, Radia discloses:

- a redirection server (the router 106 and the ANCS server 112, collectively) located between a public network (the servers 108 are on the public network) and a dial-up network server (cable modem 104);
- communicating a user's individualized rule set and temporarily assigned network

[27] *See also* Ex. B-3, Decision on Appeal, Reexamination Control No. 90/009,301, at 6 (Aug. 23, 2011).

address to the redirection server; and

- processing data directed toward the public network according to the individualized rule set.

In contrast to the art considered during the first reexamination of the '118 patent, Radia discloses a redirection server that is connected between the dial-up network server and the public network. Thus, Radia provides a better disclosure than (and is not cumulative of) the references previously considered by the Examiner.

(iii) Stockwell

Previously unconsidered U.S. Patent 5,950,195 to Stockwell filed on September 18, 1996 and issued on September 7, 1999, is prior art under §102(e).

Stockwell discloses a generalized security management system that uses a user-specific access control list to control access to network resources. The access control list is a "list of rules that regulate the flow of Internet connections through a firewall." (Stockwell, 5:17-19.) Stockwell discloses that the "rules determine whether the connection is allowed or denied." (Stockwell, 5:24-25.) Another "common side effect is to redirect the destination IP address to an alternate machine." (Stockwell, 5:28-29.) For example, a rule may "intercept[] all incoming connections that go [to] the external side of the local Sidewinder [firewall] (192.168.1.192) and redirects them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31.)

Accordingly, in contrast to the references considered during prosecution of the first reexamination proceeding, Stockwell discloses:

- controlling a user's access to a public network (the Internet); and
- redirecting a user's Internet access request to an alternate server.

(iv) RFC 2138

RFC 2138 is a publication by the Internet Engineering Task Force (IETF) from April 1997 and is prior art under §102(b). RFC 2138 was used in proposed rejections in the first reexamination of the '118 patent at the request stage but was not applied in a rejection or discussed by the Examiner.

RFC 2138 describes features of the Remote Authentication Dial-In User Service (RADIUS) standard. Willens (described above), provides embodiments using the RADIUS standard. Accordingly, Willens and RFC 2138 are directed to the same, or at least very similar, subject matter and overlap to a significant degree. Proposed rejections use RCF 2138 to complement features disclosed by Willens.

(v) He

U.S. Patent 6,088,451 to He, filed June 28, 1996 and issued July 11, 2000, is prior art under 35 U.S.C. § 102(e).

He discloses a system for securing access to network resources. He's system includes a authentication server for verifying user's identities and a credential server for controlling users' access to network resources. As shown more specifically by the proposed rejections in Exhibits CC and DD, He teaches nearly all of the limitations recited in the '118 Patent claims.

(vi) Zenchelsky

U.S. Patent 6,233,686 to Zenchelsky, filed January 17, 1997 and issued May 15, 2001, is prior art under 35 U.S.C. § 102(e).

Zenchelsky discloses a system for securing access to network resources. Zenchelsky discloses that such systems can be implemented in Internet Protocol (IP) networks in which a user's network address is temporarily assigned. As shown more specifically by the proposed rejections in Exhibits CC and DD, these teachings are relevant to the limitations recited in the '118 Patent claims.

(vii) Fortinsky

U.S. Patent 5,815,574 to Fortinsky, filed November 28, 1995 and issued September 29, 1998 is prior art under 35 U.S.C. § 102(e).

Fortinsky teaches a system for securing access to network resources, and more particularly, for controlling access to external resources on a separate network reachable through a gateway server. Fortinsky's teachings are in the context of the same authentication and security technology as He, specifically, MIT's Kerberos authentication system. Fortinsky illustrates in Fig. 2 that the gateway server GS connects a client's network N1 to an external network N2. Through the gateway server, the client can obtain access to a remote server RS:

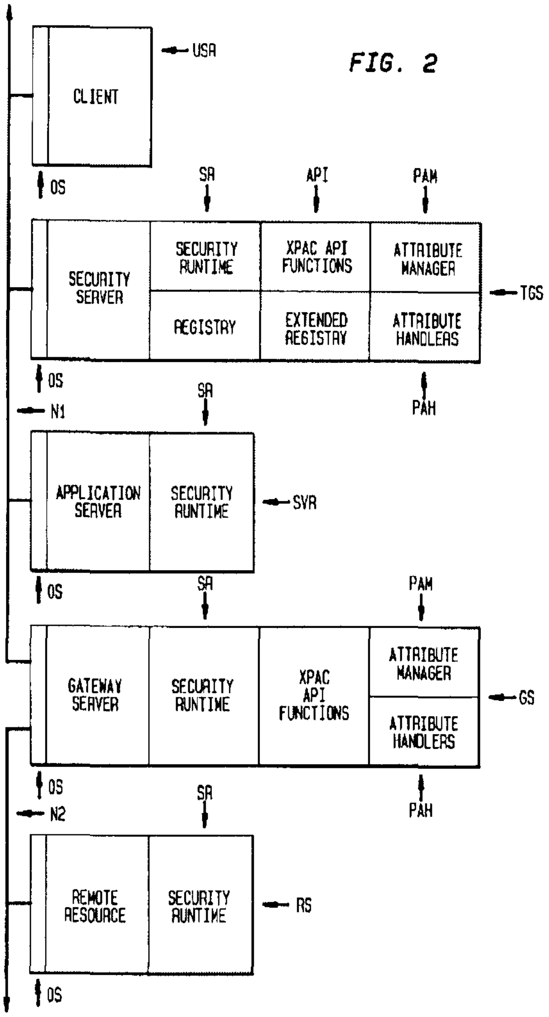


FIG. 2

FORTINSKY, FIG. 2

Accordingly, in contrast to the prior art analysis from the previous reexamination, Fortinsky teaches a redirection server (such as the gateway server GS) located *between* a dial-up network server (providing the client's connect to network N1) and an external network (N2). Thus, Fortinsky provides a better disclosure than (and is not cumulative of) the references previously considered by the Examiner.

(viii) Admitted Prior Art

The specification of the '118 Patent describes various prior art systems and technologies for providing controlled access to network resources. For example, the background describes the well-known concept of providing dial-up Internet access using temporarily-assigned network addresses. ('118 Patent, 16-36.) The background also describes using the well-known concept of redirection to redirect a user to a different destination than the user originally requested. ('118 Patent, 1:38-67.) The background further describes using a packet filter to control a user's access to network resources, and placing the packet filter so that it can process all traffic between a local network and the Internet. ('118 Patent, 2:1-44.) For example, the packet filter can allow access to a destination when it "simply forwards packets between the local user and the remote server outside the firewall." ('118 Patent, 2:40-42.)

Accordingly, the Admitted Prior Art discloses:

- a packet filter located between a user's dial-up network server and a public network, such as the Internet;
- redirecting a user's request to an alternate destination; and
- controlling a user's access to network resources by processing data directed toward the public network.

In the previous reexamination proceeding, the Examiner and the Board agreed that these teachings were relevant to the original independent claims of the '118 Patent. However, as discussed above in the summary of file history, neither the Board nor the Examiner addressed the teachings of the Admitted Prior Art with respect to the original dependent claims and the claims added during reexamination. Requester respectfully submits that the Admitted Prior Art is equally relevant to the original dependent claims and the claims added during reexamination.

V. PROPOSED REJECTIONS OF THE CLAIMS

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.*

Patentability shall not be negatived by the manner in which the invention was made.

Exhibit AA: Proposed Rejections based on Willens

Proposed Rejection #1: Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Stockwell under 35 U.S.C. § 103(a).

Proposed Rejection #2: Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Admitted Prior Art under 35 U.S.C. § 103(a).

Exhibit BB: Proposed Rejections based on Radia/Wong Family

Proposed Rejection #3: Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Stockwell under 35 U.S.C. § 103(a).

Proposed Rejection #4: Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Stockwell and further in view of Wong '178 under 35 U.S.C. § 103(a).

Proposed Rejection #5: Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Admitted Prior Art under 35 U.S.C. § 103(a).

Proposed Rejection #6: Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Admitted Prior Art and further in view of Wong '178 under 35 U.S.C. § 103(a).

Exhibit CC: Proposed Rejections based on He, Zenchelsky, and the Admitted Prior Art

Proposed Rejection #7: Claims 2-7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky and further in view of the Admitted Prior Art under 35 U.S.C. § 103(a).

Exhibit DD: Proposed Rejections based on He, Zenchelsky, Fortinsky and the Admitted Prior Art

Proposed Rejection #8: Claims 2-7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky, Fortinsky, and the Admitted Prior Art under 35 U.S.C. § 103(a).

VI. CLAIM CONSTRUCTION

"During patent examination, the pending claims must be 'given their broadest reasonable interpretation consistent with the specification.'" (MPEP § 2111). As mentioned previously, the '118 patent is the subject of litigations in Texas and California.[28] In the Texas litigation, the court made certain rulings regarding claim construction that are attached as Exhibit C. However, the standards of claim interpretation that must be used by the courts in patent litigation are different than the claim interpretation standard that must be used in the Office in claim examination proceedings (including reexamination). Therefore, any claim interpretations submitted herein for the purpose of demonstrating a reasonable likelihood of prevailing are not binding upon any of the defendants in any litigation related to the '118 patent, nor do such claim interpretations necessarily correspond to the construction of claims under the legal standards that are mandated to be used by the courts in litigation. (*See* MPEP at § 2686.04.II (determination of a substantial new question of patentability is made independently of court's decision on validity because of different standards of proof and claim interpretation employed by the District Courts and the Office); *see also, In re Zletz*, 893 F.2d 319, 322, 13 USPQ2d 1320,1322 (Fed. Cir. 1989); 35 U.S.C. §305).

The Patent Owner advocated certain constructions as evidenced in the Patent Owner's claim construction brief attached as Exhibit D-1 and infringement contentions attached as Exhibit D-2. Although the Requester does not admit or acquiesce to the correctness of the Patent Owner's constructions, the present request nonetheless presents the following claim analysis in a manner that is consistent with the Patent Owner's asserted constructions. MPEP § 2617.III states: "Admissions by the Patent Owner as to any matter affecting patentability may be utilized to determine the scope and content of the prior art in conjunction with patents and printed publications, whether such admissions are found in patents or printed publications or in some other source."

[28] *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc., et al.*, Case No. 8-12-cv-00522, (C.D. Cal. Apr. 5, 2012); *Linksmart Wireless Tech., LLC v. T-Mobile USA, Inc.*, No. 2:08-cv-00264-TJW-CE (E.D. Tex.); *Linksmart Wireless Tech., LLC v. Cisco Systems, Inc.*, No. 2:08-cv-00304-DF-CE (E.D. Tex.).

LIST OF EXHIBITS

Exhibit A	United States Patent No. 6,779,118 (the "'118 patent"), including Reexamination Certificate No. 8926 issued Mar. 27, 2012.
Exhibit B-1	File History of United States Patent No. 6,779,118
Exhibit B-2	File History of U.S. Provisional Application No. 60/084,014
Exhibit B-3	File History of Ex Parte Reexamination Control No. 90/009301
Exhibit B-4	File History of Ex Parte Reexamination Control No. 90/011485
Exhibit B-5	File History of Ex Parte Reexamination Control No. 90/012149
Exhibit B-6	File History of Ex Parte Reexamination Control No. 90/012342
Exhibit C	Claim Construction Order, *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc.*, No. 2:08-cv-264-df-ce (E.D. Tex. Jun. 30, 2010).
Exhibit D-1	Plaintiff's [Patent Owner's] Opening Claim Construction Brief, *Linksmart Wireless Technology, LLC v. T-Mobile USA, Inc.*, No. 2:08-cv-264-df-ce (E.D. Tex. Mar. 19, 2010).
Exhibit D-2	Linksmart Infringement Contentions Against Cisco IOS.
Exhibit E	United States Patent No. 5,848,233 ("Radia").
Exhibit F	United States Patent No. 5,835,727 ("Wong '727").
Exhibit G	United States Patent No. 5,950,195 ("Stockwell").
Exhibit H	United States Patent No. 6,073,178 ("Wong '178").
Exhibit I	United States Patent No. 5,889,958 ("Willens").
Exhibit J	Request for Comments 2138, Internet Engineering Task Force, April 1997 ("RFC 2138").
Exhibit K	United States Patent No. 6,233,686 ("Zenchelsky").
Exhibit L	United States Patent No. 6,088,451 ("He").
Exhibit M	United States Patent No. 5,815,574 ("Fortinsky").
Exhibit AA	Claim Charts with respect to Willens for Obviousness

Exhibit BB	Claim Charts with respect to Radia for Obviousness
Exhibit CC	Claim Charts with respect to He, Zenchelsky, and the Admitted Prior Art for Obviousness
Exhibit DD	Claim Charts with respect to He, Zenchelsky, Fortinsky and the Admitted Prior Art for Obviousness

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

//

VII. CONCLUSION

For the reasons set forth above, it is clear that Requester has established a reasonable likelihood of prevailing with respect to at least one claim of the '118 patent. Indeed, Requester has established a reasonable likelihood of prevailing with respect to all of the non-canceled claims of the '118 patent, since claims 2-7, 9-14, 16-24, and 26-90 are rendered obvious in view of the above-listed references. Therefore, Requester asks that the Patent Office order reexamination of the '118 patent and ultimately conclude by issuing a reexamination certificate cancelling claims 2-7, 9-14, 16-24, and 26-90.

As identified in the attached Certificate of Service and in accordance with 37 C.F.R. §§ 1.33(c) and 1.915(b)(6), a copy of the present request, in its entirety, is being served to the address of the attorney or agent of record.

Please direct all correspondence in this matter to the undersigned.

Respectfully submitted,

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Dated: September 12, 2012
HAYNES AND BOONE, LLP
Customer No. 27683
Telephone: 214/651-5116
Facsimile: 214/200-0808
Attorney Docket No.: 43614.61
R-296889_3.DOC

CERTIFICATE OF SERVICE

I hereby certify that this correspondence, all attachments, and any corresponding filing fee is being transmitted via the Electronic Filing System (EFS) Web with the United States Patent and Trademark Office on September 12, 2012.

Theresa O'Conn

Theresa O'Connor

VIII. CERTIFICATE OF SERVICE

The undersigned certifies that copies of the following,

(1) Request for *Inter Partes* Reexamination Transmittal Form;

(2) PTO 1449 Modified Form;

(3) Request for *Inter Partes* Reexamination; and

(4) Exhibits A-M and Exhibits AA-DD

in their entirety were served by first class mail addressed to:

Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria VA 22314

the attorney of record for the assignee of U.S. Patent No. 6,779,118, in accordance with 37 C.F.R. § 1.915(b)(6), on the 12th day of September, 2012.

/David L. McCombs/

David L. McCombs
Registration No. 32,271

Exhibit A

United States Patent No. 6,779,118 (the "'118 patent"), including Reexamination Certificate No. 8926 issued Mar. 27, 2012.

US006779118B1

(12) **United States Patent**
Ikudome et al.

(10) **Patent No.: US 6,779,118 B1**
(45) **Date of Patent: Aug. 17, 2004**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US); **Moon Tai Yeung**, Alhambra, CA (US)

(73) Assignee: **Auriq Systems, Inc.**, Pasadena, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/295,966**

(22) Filed: **Apr. 21, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) **Int. Cl.**^{7} **G06F 12/14**

(52) **U.S. Cl.** **713/201**

(58) **Field of Search** 713/200, 201, 713/202, 165, 168, 193; 709/229; 380/200, 201, 230; 340/825.31, 825.34; 705/57, 58

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,696,898 A		12/1997	Baker et al.	395/187.01
6,157,829 A	*	12/2000	Grube et al.	455/414.1
6,233,686 B1		5/2001	Dutta	

FOREIGN PATENT DOCUMENTS

CA	2226814		3/2003
EP	0 854 621		7/1998
EP	0854621 A	*	7/1998
WO	WO 96/05549		2/1996
WO	WO9605549	*	2/1996
WO	WO98/03927		1/1998
WO	WO9826548	*	6/1998
WO	WO 98/26548		6/1998
WO	WO 99/57660		11/1999
WO	WO 00/16529		3/2000

* cited by examiner

Primary Examiner—Pierre Elisca
(74) *Attorney, Agent, or Firm*—Christie, Parker & Hale, LLP

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authentication and accounting server, and a database. Prior to using the system, users authenticate with the authentication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.

27 Claims, 1 Drawing Sheet

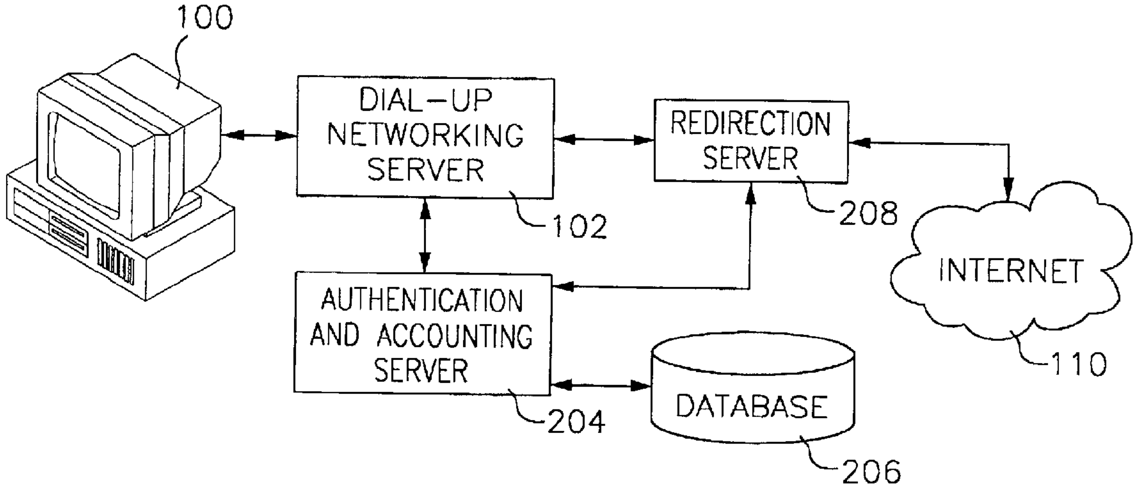

100
DIAL-UP NETWORKING SERVER
102
REDIRECTION SERVER
208
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
204
DATABASE
206

FIG. 1

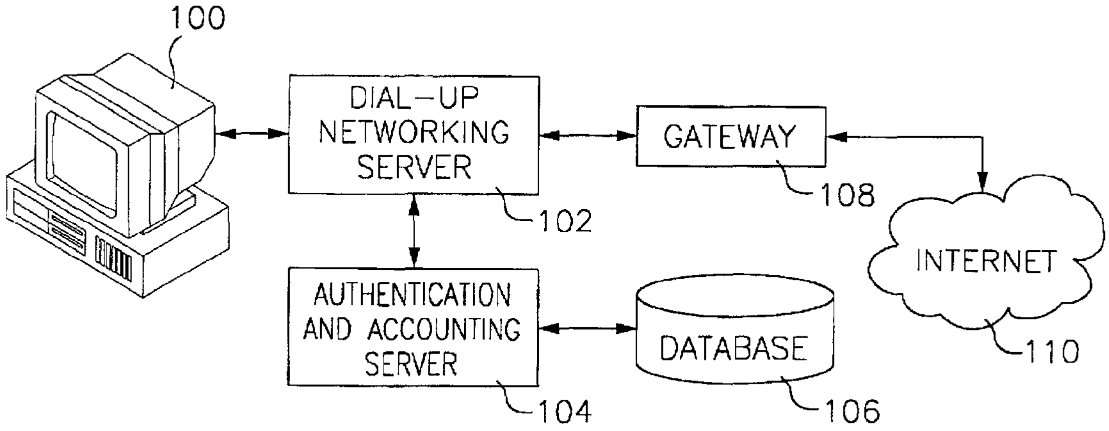
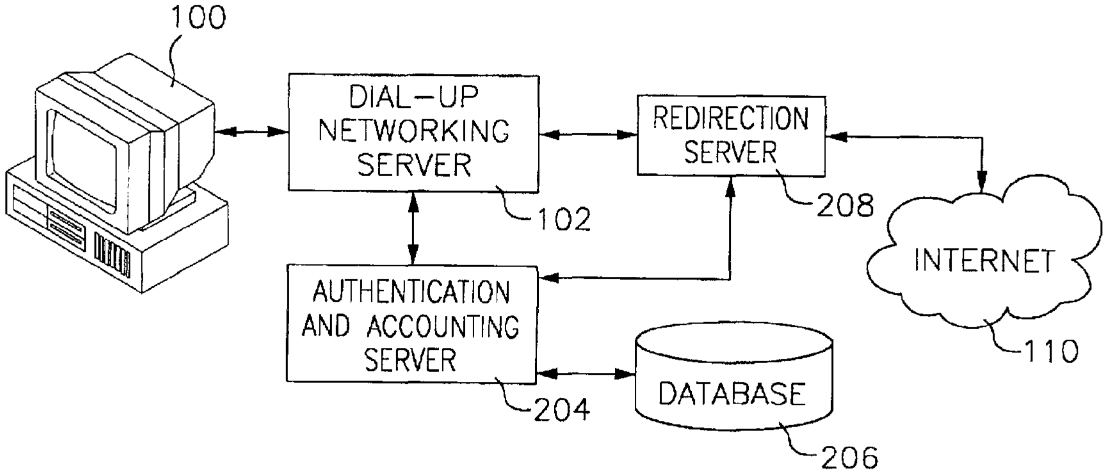

100
DIAL-UP NETWORKING SERVER
102
GATEWAY
108
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
104
DATABASE
106

FIG. 2


100
DIAL-UP NETWORKING SERVER
102
REDIRECTION SERVER
208
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
204
DATABASE
206

USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM

RELATED APPLICATION

This application claims priority of U.S. Provisional Application No. 60/084,014 filed May 4, 1998, the disclosure of which is incorporated fully herein by reference.

FIELD OF THE INVENTION

This invention relates to the field of Internet communications, more particularly, to a database system for use in dynamically redirecting and filtering Internet traffic.

BACKGROUND OF THE INVENTION

In prior art systems as shown in FIG. **1** when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a physical connection between their computer **100** and a dial-up networking server **102**, the user provides to the dial-up networking server their user ID and password. The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server **104**. A detailed description of the IP communications protocol is discussed in *Internetworking with TCP/IP*, 3rd ed., Douglas Comer, Prentice Hall, 1995, which is fully incorporated herein by reference. The authentication and accounting server, upon verification of the user ID and password using a database **106** would send an authorization message to the dial-up networking server **102** to allow the user to use the temporary IP address assigned to that user by the dial-up networking server and then logs the connection and assigned IP address. For the duration of that session, whenever the user would make a request to the Internet **110** via a gateway **108**, the end user would be identified by the temporarily assigned IP address.

The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page—hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. Alternately, redirection can also be accomplished by coding the page such that it instructs the browser to run a program, like a Java applet or the like, which then redirects the browser. One disadvantage with current redirection technology is that control of the redirection is at the remote end, or WWW server end—and not the local, or user end. That is to say that the redirection is performed by the remote server, not the user's local gateway.

Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, they can filter outgoing packets sent from users to a specific destination as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. For example, the packet filter can determine if the packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. Service identification is achieved by identifying the terminating port number contained within each IP packet header. Port numbers are standard within the industry to allow for interoperability between equipment. Packet filtering devices allow network administrators to filter packets based on the source and/or destination information, as well as on the type of service being transmitted within each IP packet. Unlike redirection technology, packet filtering technology allows control at the local end of the network connection, typically by the network administrator. However, packet filtering is very limited because it is static. Once packet filtering rule sets are programed into a firewall or other packet filter device, the rule set can only be changed by manually reprogramming the device.

Packet filter devices are often used with proxy server systems, which provide access control to the Internet and are most often used to control access to the world wide web. In a typical configuration, a firewall or other packet filtering device filters all WWW requests to the Internet from a local network, except for packets from the proxy server. That is to say that a packet filter or firewall blocks all traffic originating from within the local network which is destined for connection to a remote server on port **80** (the standard WWW port number). However, the packet filter or firewall permits such traffic to and from the proxy server. Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. When the proxy server receives a packet, the destination is checked against a database for approval. If the destination is allowed, the proxy server simply forwards packets between the local user and the remote server outside the firewall. However, proxy servers are limited to either blocking or allowing specific system terminals access to remote databases.

A recent system is disclosed in U.S. Pat. No. 5,696,898. This patent discloses a system, similar to a proxy server, that allows network administrators to restrict specific IP addresses inside a firewall from accessing information from certain public or otherwise uncontrolled databases (i.e., the WWW/Internet). According to the disclosure, the system has a relational database which allows network administrators to restrict specific terminals, or groups of terminals, from accessing certain locations. Similarly limited as a proxy server, this invention can only block or allow terminals' access to remote sites. This system is also static in that rules programmed into the database need to be reprogramming in order to change which locations specific terminals may access.

SUMMARY OF THE INVENTION

The present invention allows for creating and implementing dynamically changing rules, to allow the redirection, blocking, or allowing, of specific data traffic for specific users, as a function of database entries and the user's activity. In certain embodiments according to the present invention, when the user connects to the local network, as in the prior art system, the user's ID and password are sent to the authentication accounting server. The user ID and password are checked against information in an authentication database. The database also contains personalized filtering and redirection information for the particular user ID. During the connection process, the dial-up network server provides the authentication accounting server with the IP address that is going to be temporarily assigned to the user. The authentication accounting server then sends both the user's temporary IP address and all of the particular user's filter and redirection information to a redirection server. The IP address temporarily assigned to the end user is then sent back to the end user for use in connecting to the network.

Once connected to the network, all data packets sent to, or received by, the user include the user's temporary IP address in the IP packet header. The redirection server uses the filter and redirection information supplied by the authentication accounting server, for that particular IP address, to either allow packets to pass through the redirection server unmolested, block the request all together, or modify the request according to the redirection information.

When the user terminates the connection with the network, the dial-up network server informs the authentication accounting server, which in turn, sends a message to the redirection server telling it to remove any remaining filtering and redirection information for the terminated user's temporary IP address. This then allows the dial-up network to reassign that IP address to another user. In such a case, the authentication accounting server retrieves the new user's filter and redirection information from the database and passes it, with the same IP address which is now being used by a different user, to the redirection server. This new user's filter may be different from the first user's filter.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a typical Internet Service Provider environment.

FIG. **2** is a block diagram of an embodiment of an Internet Service Provider environment with integrated redirection system.

DETAILED DESCRIPTION OF THE INVENTION

In the following embodiments of the invention, common reference numerals are used to represent the same components. If the features of an embodiment are incorporated into a single system, these components can be shared and perform all the functions of the described embodiments.

FIG. **2**. shows a typical Internet Service Provider (ISP) environment with integrated user specific automatic data redirection system. In a typical use of the system, a user employs a personal computer (PC) **100**, which connects to the network. The system employs: a dial-up network server **102**, an authentication accounting server **204**, a database **206** and a redirection server **208**.

The PC **100** first connects to the dial-up network server **102**. The connection is typically created using a computer modem, however a local area network (LAN) or other communications link can be employed. The dial-up network server **102** is used to establish a communications link with the user's PC **100** using a standard communications protocol. In the preferred embodiment Point to Point Protocol (PPP) is used to establish the physical link between the PC **100** and the dial-up network server **102**, and to dynamically assign the PC **100** an IP address from a list of available addresses. However, other embodiments may employ different communications protocols, and the IP address may also be permanently assigned to the PC **100**. Dial-up network servers **102**, PPP and dynamic IP address assignment are well known in the art.

An authentication accounting server with Auto-Navi component (hereinafter, authentication accounting server) **204** is used to authenticate user ID and permit, or deny, access to the network. The authentication accounting server **204** queries the database **206** to determine if the user ID is authorized to access the network. If the authentication accounting server **204** determines the user ID is authorized, the authentication accounting server **204** signals the dial-up network server **102** to assign the PC **100** an IP address, and the Auto-Navi component of the authentication accounting server **204** sends the redirection server **208** **(1)** the filter and redirection information stored in database **206** for that user ID and **(2)** the temporarily assigned IP address for the session. One example of an authentication accounting server is discussed in U.S. Pat. No. 5,845,070, which is fully incorporated here by reference. Other types of authentication accounting servers are known in the art. However, these authentication accounting servers lack an Auto-Navi component.

The system described herein operates based on user Id's supplied to it by a computer. Thus the system does not "know" who the human being "user" is at the keyboard of the computer that supplies a user ID. However, for the purposes of this detailed description, "user" will often be used as a short hand expression for "the person supplying inputs to a computer that is supplying the system with a particular user ID."

The database **206** is a relational database which stores the system data. FIG. **3** shows one embodiment of the database structure. The database, in the preferred embodiment, includes the following fields: a user account number, the services allowed or denied each user (for example: e-mail, Telnet, FTP, WWW), and the locations each user is allowed to access.

Rule sets are employed by the system and are unique for each user ID, or a group of user ID's. The rule sets specify elements or conditions about the user's session. Rule sets may contain data about a type of service which may or may not be accessed, a location which may or may not be accessed, how long to keep the rule set active, under what conditions the rule set should be removed, when and how to modify the rule set during a session, and the like. Rule sets may also have a preconfigured maximum lifetime to ensure their removal from the system.

The redirection server **208** is logically located between the user's computer **100** and the network, and controls the user's access to the network. The redirection server **208** performs all the central tasks of the system. The redirection server **208** receives information regarding newly established sessions from the authentication accounting server **204**. The Auto-Navi component of the authentication accounting server **204** queries the database for the rule set to apply to each new session, and forwards the rule set and the currently assigned IP address to the redirection server **208**. The redirection server **208** receives the IP address and rule set, and is programed to implement the rule set for the IP address, as well as other attendant logical decisions such as: checking data packets and blocking or allowing the packets as a function of the rule sets, performing the physical redirection of data packets based on the rule sets, and dynamically changing the rule sets based on conditions. When the redirection server **208** receives information regarding a terminated session from the authentication accounting server **204**, the redirection server **208** removes any outstanding rule sets and information associated with the session. The redirection server **208** also checks for and removes expired rule sets from time to time.

In an alternate embodiment, the redirection server **208** reports all or some selection of session information to the database **206**. This information may then be used for reporting, or additional rule set generation.

System Features Overview

In the present embodiment, each specific user may be limited to, or allowed, specific IP services, such as WWW, FTP and Telnet. This allows a user, for example, WWW access, but not FTP access or Telnet access. A user's access can be dynamically changed by editing the user's database record and commanding the Auto-Navi component of the authentication accounting server **204** to transmit the user's new rule set and current IP address to the redirection server **208**.

A user's access can be "locked" to only allow access to one location, or a set of locations, without affecting other users' access. Each time a locked user attempts to access another location, the redirection server **208** redirects the user to a default location. In such a case, the redirection server **208** acts either as proxy for the destination address, or in the case of WWW traffic the redirection server **208** replies to the user's request with a page containing a redirection command.

A user may also be periodically redirected to a location, based on a period of time or some other condition. For example, the user will first be redirected to a location regardless of what location the user attempts to reach, then permitted to access other locations, but every ten minutes the user is automatically redirected to the first location. The redirection server **208** accomplishes such a rule set by setting an initial temporary rule set to redirect all traffic; after the user accesses the redirected location, the redirection server then either replaces the temporary rule set with the user's standard rule set or removes the rule set altogether from the redirection server **208**. After a certain or variable time period, such as ten minutes, the redirection server **208** reinstates the rule set again.

The following steps describe details of a typical user session:

A user connects to the dial-up network server **102** through computer **100**.

The user inputs user ID and password to the dial-up network server **102** using computer **100** which forwards the information to the authentication accounting server **204**

The authentication accounting server **204** queries database **206** and performs validation check of user ID and password.

Upon a successful user authentication, the dial-up network server **102** completes the negotiation and assigns an IP address to the user. Typically, the authentication accounting server **204** logs the connection in the database **206**.

The Auto-Navi component of the authentication accounting server **204** then sends both the user's rule set (contained in database **206**) and the user's IP address (assigned by the dial-up network server **102**) in real time to the redirection server **208** so that it can filter the user's IP packets.

The redirection server **208** programs the rule set and IP address so as to control (filter, block, redirect, and the like) the user's data as a function of the rule set.

The following is an example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-2) was such as to only allow that user to access the web site www.us.com, and permit Telnet services, and redirect all web access from any server at xyz.com to www.us.com, then the logic would be as follows:

The database **206** would contain the following record for user UserID-2:

```
ID                      UserID-2
Password:               secret
################
### Rule Sets ###
################
#service     rule                              expire
http         www.us.com                        0
http         *.xyz.com=>www.us.com             0
```

the user initiates a session, and sends the correct user ID and password (UserID-2 and secret) to the dial-up network server **102**. As both the user ID and password are correct, the authentication accounting server **204** authorizes the dial-up network server **102** to establish a session. The dial-up network server **102** assigns UserID-2 an IP address (for example, **10.0.0.1**) to the user and passes the IP address to the authentication accounting server **204**.

The Auto-Navi component of the authentication accounting server **204** sends both the user's rule set and the user's IP address (**10.0.0.1**) to the redirection server **208**.

The redirection server **208** programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server **208** to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
    ( ((request type=HTTP) AND (destination address=
        www.us.com) ) OR (request type=Telnet)
    ) THEN ok.
IF source IP-address=10.0.0.1 AND
    ( (request type=HTTP) AND (destination address=
        *.xyz.com)
    ) THEN (redirect=www.us.com)
```

The redirection server **208** monitors all the IP packets, checking each against the rule set. In this situation, if IP address **10.0.0.1** (the address assigned to user ID UserID-2) attempts to send a packet containing HTTP data (i.e., attempts to connect to port **80** on any machine within the xyz.com domain) the traffic is redirected by the redirection server **208** to www.us.com. Similarly, if the user attempts to connect to any service other then HTTP at www.us.com or Telnet anywhere, the packet will simply be blocked by the redirection server **208**.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

The following is another example of a typical user's rule set, attendant logic and operation:

If the rule set for a particular user (i.e., user UserID-3) was to force the user to visit the web site www.widgetsell.com, first, then to have unfettered access to other web sites, then the logic would be as follows:

The database **206** would contain the following record for user UserID-3;

```
ID                  UserID-3
Password:           top-secret
################
### Rule Sets ###
################
#service    rule                          expire
http        *=>www.widgetsell.com         1x
```

the user initiates a session, and sends the correct user ID and password (UserID-3 and top-secret) to the dial-up network server **102**. As both the user ID and password are correct, the authentication accounting server **204** authorizes the dial-up network server **102** to establish a session. The dial-up network server **102** assigns user ID 3 an IP address (for example, **10.0.0.1**) to the user and passes the IP address to the authentication accounting server **204**.

The Auto-Navi component of the authentication accounting server **204** sends both the user's rule set and the user's IP address (**10.0.0.1**) to the redirection server **208**.

The redirection server **208** programs the rule set and IP address so as to filter and redirect the user's packets according to the rule set. The logic employed by the redirection server **208** to implement the rule set is as follows:

```
IF source IP-address=10.0.0.1 AND
    (request type=HTTP) THEN (redirect=
    www.widgetsell.com)
THEN SET NEW RULE
IF source IP-address=10.0.0.1 AND
    (request type=HTTP) THEN ok.
```

The redirection server **208** monitors all the IP packets, checking each against the rule set. In this situation, if IP address **10.0.0.1** (the address assigned to user ID UserID-3) attempts to send a packet containing HTTP data (i.e., attempts to connect to port **80** on any machine) the traffic is redirected by the redirection server **208** to www.widgetsell.com. Once this is done, the redirection server **208** will remove the rule set and the user if free to use the web unmolested.

When the user logs out or disconnects from the system, the redirection server will remove all remaining rule sets.

In an alternate embodiment a user may be periodically redirected to a location, based on the number of other factors, such as the number of locations accessed, the time spent at a location, the types of locations accessed, and other such factors.

A user's account can also be disabled after the user has exceeded a length of time. The authentication accounting server **204** keeps track of user's time online. Prepaid use subscriptions can thus be easily managed by the authentication accounting Server **204**.

In yet another embodiment, signals from the Internet **110** side of redirection server **208** can be used to modify rule sets being used by the redirection server. Preferably, encryption and/or authentication are used to verify that the server or other computer on the Internet **110** side of redirection server **208** is authorized to modify the rule set or rule sets that are being attempted to be modified. An example of this embodiment is where it is desired that a user be redirected to a particular web site until the fill out a questionnaire or satisfy some other requirement on such a web site. In this example, the redirection server redirects a user to a particular web site that includes a questionnaire. After this web site receives acceptable data in all required fields, the web site then sends an authorization to the redirection server that deletes the redirection to the questionnaire web site from the rule set for the user who successfully completed the questionnaire. Of course, the type of modification an outside server can make to a rule set on the redirection server is not limited to deleting a redirection rule, but can include any other type of modification to the rule set that is supported by the redirection server as discussed above.

It will be clear to one skilled in the art that the invention may be implemented to control (block, allow and redirect) any type of service, such as Telnet, FTP, WWW and the like. The invention is easily programmed to accommodate new services or networks and is not limited to those services and networks (e.g., the Internet) now know in the art.

It will also be clear that the invention may be implemented on a non-IP based networks which implement other addressing schemes, such as IPX, MAC addresses and the like. While the operational environment detailed in the preferred embodiment is that of an ISP connecting users to the Internet, it will be clear to one skilled in the art that the invention may be implemented in any application where control over users' access to a network or network resources is needed, such as a local area network, wide area network and the like. Accordingly, neither the environment nor the communications protocols are limited to those discussed.

What is claimed is:

1. A system comprising:

a database with entries correlating each of a plurality of user IDs with an individualized rule set;

a dial-up network server that receives user IDs from users' computers;

a redirection server connected to the dial-up network server and a public network, and

an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

2. The system of claim **1**, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

3. The system of claim **1**, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

4. The system of claim **1**, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

5. The system of claim **1**, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

6. The system of claim **1**, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

7. The system of claim **1**, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

8. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server, the method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

9. The method of claim **8**, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

10. The method of claim **8**, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

11. The method of claim **8**, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

12. The method of claim **8**, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

13. The method of claim **8**, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

14. The method of claim **8**, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

15. A system comprising:

a redirection server programed with a user's rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access.

16. The system of claim **15**, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. The system of claim **15**, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

18. The system of claim **15**, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user access.

19. The system of claim **15**, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. The system of claim **15**, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. The system of claim **15**, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user access.

22. The system of claim **15**, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user access.

23. The system of claim **15**, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

24. The system of claim **23** wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

25. In a system comprising a redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; the method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

26. The method of claim **25**, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user access.

27. The method of claim **25**, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and the location or locations the user access.

* * * * *

US006779118C1

(12) EX PARTE REEXAMINATION CERTIFICATE (8926th)

United States Patent

Ikudome et al.

(10) **Number: US 6,779,118 C1**

(45) **Certificate Issued: Mar. 27, 2012**

(54) **USER SPECIFIC AUTOMATIC DATA REDIRECTION SYSTEM**

(75) Inventors: **Koichiro Ikudome**, Arcadia, CA (US); **Moon Tai Yeung**, Alhambra, CA (US)

(73) Assignee: **Linksmart Wireless Technology, LLC**, Pasadena, CA (US)

Reexamination Request:
No. 90/009,301, Dec. 17, 2008

Reexamination Certificate for:

Patent No.:	**6,779,118**
Issued:	**Aug. 17, 2004**
Appl. No.:	**09/295,966**
Filed:	**Apr. 21, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/084,014, filed on May 4, 1998.

(51) **Int. Cl.**

H04L 29/06	(2006.01)
H04L 29/00	(2006.01)

(52) **U.S. Cl.** **726/7**; 726/14

(58) **Field of Classification Search** 726/8
See application file for complete search history.

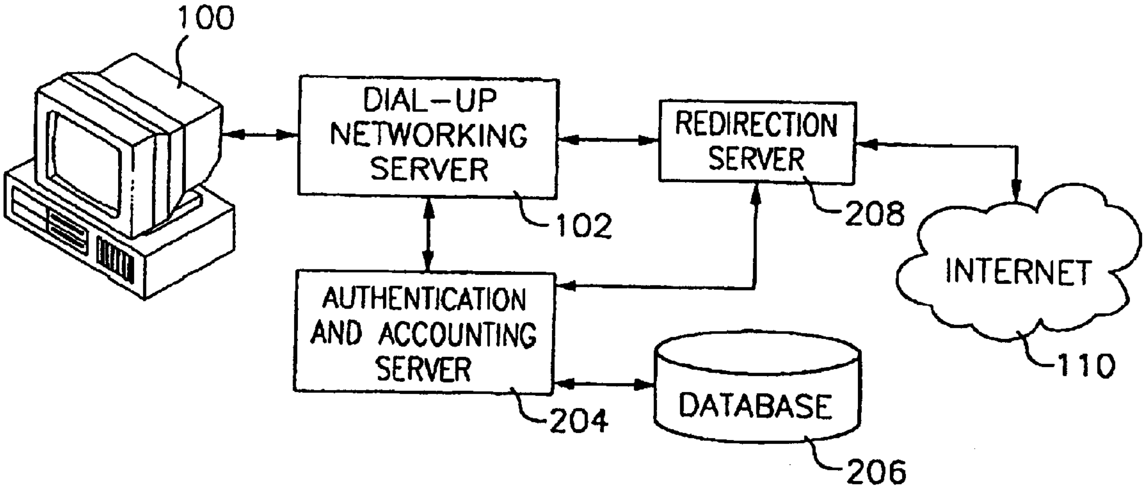
(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/009,301, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner—Samuel Rimell

(57) **ABSTRACT**

A data redirection system for redirecting user's data based on a stored rule set. The redirection of data is performed by a redirection server, which receives the redirection rule sets for each user from an authenication and accounting server, and a database. Prior to using the system, users authenticate with the authenication and accounting server, and receive a network address. The authentication and accounting server retrieves the proper rule set for the user, and communicates the rule set and the user's address to the redirection server. The redirection server then implements the redirection rule set for the user's address. Rule sets are removed from the redirection server either when the user disconnects, or based on some predetermined event. New rule sets are added to the redirection server either when a user connects, or based on some predetermined event.


100
DIAL-UP NETWORKING SERVER
102
REDIRECTION SERVER
208
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
204
DATABASE
206

EX PARTE REEXAMINATION CERTIFICATE ISSUED UNDER 35 U.S.C. 307

THE PATENT IS HEREBY AMENDED AS INDICATED BELOW.

Matter enclosed in heavy brackets [ ] appeared in the patent, but has been deleted and is no longer a part of the patent; matter printed in italics indicates additions made to the patent.

AS A RESULT OF REEXAMINATION, IT HAS BEEN DETERMINED THAT:

The patentability of claims **2-7** and **9-14** is confirmed.

Claims **1**, **8**, **15** and **25** are cancelled.

Claims **16-23** and **26-27** are determined to be patentable as amended.

Claim **24**, dependent on an amended claim, is determined to be patentable.

New claims **28-90** are added and determined to be patentable.

16. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

17. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

18. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user [access] *accesses*.

19. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

20. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

21. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatment of at least a portion of the rule set as a function of the location or locations the user [access]*accesses*.

22. [The system of claim **15**.] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user [access] *accesses*.

23. [The system of claim **15**,] *A system comprising:*

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

26. The method of claim **25**, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user [access] *accesses*.

27. The method of claim **25**, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and [the] *a* location or locations the user [access] *accesses*.

28. The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

29. The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

30. The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

31. The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

32. The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

33. The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

34. The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

35. The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

36. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

37. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

38. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

39. A system comprising:

a redirection server programmed with a user's rule set correlated to a temporarily assigned network address; wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and

wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

40. The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

41. The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

42. The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

43. The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

44. A system comprising:

a database with entries correlating each of a plurality of user IDs with an individualized rule set;

a dial-up network server that receives user IDs from users' computers;

a redirection server connected between the dial-up network server and a public network, and

an authentication accounting server connected to the database, the dial-up network server and the redirection server;

wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;

wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and

wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.

45. The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.

46. The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.

47. The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.

48. The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.

49. The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.

50. The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.

51. The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

52. The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

53. The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

54. The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

55. The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

56. In a system comprising a database with entries correlating each of a plurality of user IDs with an individualized rule set; a dial-up network server that receives user IDs from users' computers; a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection servers, a method comprising the steps of:

communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;

communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;

and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.

57. The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.

58. The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.

59. The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.

60. The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.

61. The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.

62. The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.

63. The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

64. The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an intial period of time and to thereafter utilize the standard rule set.

65. The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.

66. The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

67. The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.

68. A system comprising:

a redirection server connected between a user computer and a public network, the redirection server programmed with a users' rule set correlated to a temporarily assigned network address;

wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and

wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.

69. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.

70. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.

71. The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.

72. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.

73. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.

74. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.

75. The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.

76. The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.

77. The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.

78. The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

79. The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

80. The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

81. The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

82. The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.

83. In a system comprising a redirection server connected between a user computer and a public network, the redirection server containing a user's rule set correlated to a temporarily assigned network address wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network; a method comprising the step of:

modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and

wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and

wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.

84. The method of claim 83, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.

85. The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.

86. The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.

87. The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule *set, and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.*

88. The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.

89. The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

90. The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.

* * * * *

Exhibit AA

Claim Charts with respect to Willens for Obviousness

(Corrected) Request for *Inter Partes* Reexamination
U.S. Patent No. 6,779,118

Exhibit AA

Contents

References
Willens (Exhibit I, U.S. 5889958)
RFC 2138 (Exhibit J)
Stockwell (Exhibit G, U.S. 5950195)
Admitted Prior Art

Requester provides canceled claims 1, 8, and 25 in the claim charts below because other claims depend from those canceled claims or include the same features as those canceled claims. Requester does not propose new rejections for canceled claims 1, 8, and 25.

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

(Corrected) Request for *Inter Partes* Reexamination
U.S. Patent No. 6,779,118

Exhibit AA

Proposed Rejection #1. **Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Stockwell under 35 U.S.C. § 103(a).**

Reasons to Combine Willens, RFC 2138, and Stockwell

Willens describes a system for controlling users' access to a public network using Remote Authentication Dial In User Service (RADIUS). A RADIUS client communicates with a RADIUS server. RFC 2138 defines the standard protocol for these RADIUS communications. Thus, Willens and RFC 2138 include overlapping and complementary material regarding the same subject matter. Indeed, Steven Willens, the sole named inventor of the Willens patent, is a co-author of RFC 2138. A person of ordinary skill in the art would have viewed the relationship between Willens and RFC 2138 as an explicit suggestion to combine the teachings of the two references. For example, it would have been obvious to one of ordinary skill in the art in reviewing Willens, to refer to RFC 2138 for further details regarding the communications between Willens' RADIUS client and RADIUS server.

Willens and Stockwell are both directed to providing a configurable network device that provides IP packet filtering. Stockwell includes a teaching that a network device, such as a firewall, can redirect a communication to an alternate destination. It would have been obvious to incorporate this redirection feature into the packet filter of Willens. The redirection feature would improve a similar device (the packet filter of Willens) in the same way. The combination is also obvious because it requires only applying a known technique (redirection) to a known device (the packet filter of Willens) to yield predictable results (a packet filter with the ability to redirect packets). (*See* MPEP § 2143, *citing KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1395-97 (2007).)

Furthermore, redirection is an obvious extension of the use of a control to block a user. Willens teaches blocking, and it would be obvious to extend blocking to include Stockwell's redirecting function. Requester notes that the Board of Patent Appeals and Interferences (BPAI) explicitly reached essentially the same conclusion with respect to the '118 patent in the previous reexamination. (*See Ex Parte Linksmart Wireless Technology, LLC*, Appeal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011).)

US 6779118	Prior Art Analysis[*]
[1.0] A system comprising:	Willens discloses a "Network access control ***system*** and process." (Willens, Title, emphasis added.)
[1.1] a database with entries	Willens illustrates in Fig. 3 a Remote Authentication Dial In

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit AA

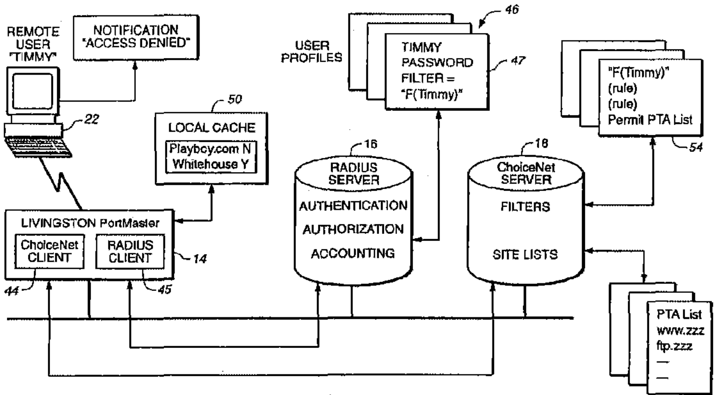
US 6779118	Prior Art Analysis*
correlating each of a plurality of user IDs with an individualized rule set;	User Service (RADIUS) server 16 that stores user profiles 46. As a specific example, Fig. 3 illustrates that the user ID "TIMMY" has a profile 47 with an associated filter "F(Timmy)."  REMOTE USER "TIMMY" NOTIFICATION "ACCESS DENIED" 22 50 LOCAL CACHE Playbcy.com N Whitehouse Y LIVINGSTON PortMaster ChoiceNet CLIENT RADIUS CLIENT 14 44 45 USER PROFILES 46 TIMMY PASSWORD FILTER = "F(Timmy)" 47 16 RADIUS SERVER AUTHENTICATION AUTHORIZATION ACCOUNTING 18 ChoiceNet SERVER FILTERS SITE LISTS "F(Timmy)" (rule) (rule) Permit PTA List 54 PTA List www.zzz ftp.zzz — — 52 *FIG._3* WILLENS FIG. 3 Willens further describes how each user's filter is an "individualized rule set": In addition to the site lists, the network access control server 18 maintains a set of user filters 54 which are used to control Internet access ***for each user***.... The server 14 looks at ***each filter rule*** found in "F(Timmy)" starting from the top. (Willens, 5:58-66, emphasis added.) Since Willens teaches that the user filters control Internet access *for each user*, it is understood that Willens contemplates the plurality of user profiles 46 being correlated to a "plurality of user IDs" as recited in the claim. Thus, the user profiles 46 are a "database with entries correlating each of a plurality of user IDs with an individualize rule set," as recited in the claim.
[1.2] a dial-up network server that receives user IDs from users' computers;	Willens teaches that users connect to a network via dial-up connections or through a local area network (LAN) router: In the network 21 connected by backbone 20, ***users are connected to the network*** by dial-up

Exhibit AA

US 6779118	**Prior Art Analysis***
	connections 22 through the communications server 14 or ***via a local area network (LAN) router*** 24, also through the communications server 14. (Willens, 3:60-64, emphasis added.) Willens further teaches that users must log in, which is understood to require providing a user ID: ***When user 22 logs in*** through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:6-12, emphasis added.) Thus, the local area network (LAN) router 24 teaches a "dial-up network server that receives user IDs from users' computers" as recited in the claim under at least the Patent Owner's asserted interpretation of the claim. For example, the Patent Owner has specifically asserted that a LAN communication link employs a "dial-up network server": The inventors specifically disclosed that the connection between the user's computer and the "dial-up network server" was not limited to a connection via a modem: "The PC 100 first connects to the ***dial-up network server*** 102. The connection is ***typically*** created using a computer modem, ***however a local area network (LAN) or other communications link can be employed.***" ['118 Patent] at 3:57-60 (emphasis added). (Linksmart Claim Construction Brief at 14, emphasis added.) In addition, the Patent Owner asserts that a router is a "dial-up network server." (*See, e.g.*, Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.) Alternatively, Willens also teaches that users may connect via "dial-up connections 22 through the communications server 14." More specifically, Willens teaches that users connect to Remote

Exhibit AA

US 6779118	Prior Art Analysis*
	Authentication ***Dial In*** User Service (RADIUS) client software 45 on communications server 14: RADIUS client software 45 is also resident on the communications server 14. When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:6-12, emphasis added.) It would have been obvious to one of skill in the art that for the RADIUS server 16 to verify a user's password, the user must also specific a user ID so that the RADIUS server 16 can locate the correct user profile to be used to verify the supplied password. Furthermore, the RADIUS standard, as defined in Request for Comments (RFC) 2138, states that a "User-Name" attribute "indicates the name of the user to be authenticated." (RFC 2138 at 5.1.) Thus, the "User-Name" attribute is a "user ID" as recited in the claim. An access request message sent from the RADIUS client 45 to the RADIUS server 16 "MUST contain a User-Name attribute." (RFC 2138 at 4.1.) Thus, it would have been obvious that the RADIUS client software 45 should receive the user's user ID so that the user ID may be sent to the RADIUS server 16, as required by the RADIUS communication standard defined in RFC 2138. Willens also discloses a "Remote user 22" who uses a "PC or Macintosh accessing the Internet." (Willens, 4:59-62.) The user's PC or Macintosh is a user's computer. As noted above in portion, [1.1] Willens teaches that the system supports a plurality of users, and thus, multiple "users' computers" as recited in the claim. In summary, the RADIUS client software 45 resident on the communications server 14 teaches a "dial-up network server that receives user IDs from users' computers" as recited in the claim. Alternatively, the local area network (LAN) router 24 teaches a "dial-up network server that receives user IDs from users' computers" under at least the patent owner's interpretation of the claim.

Exhibit AA

US 6779118	**Prior Art Analysis**[*]
[1.3] a redirection server connected to the dial-up network server and a public network, and	Willens discloses a communications server 14 that "either permits or denies access" to network resources. (Willens, 6:6.) More specifically, the communications server 14 includes client software 44 that receives the user's filter "for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) Willens provides a specific example in which user Timmy requests information from the site www.playboy.com: In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. The ***server 14 looks at each filter rule*** found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the ***server 14 either permits or denies access*** and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site. (Willens, 5:60–6:9.) Willens further discloses that the communications server 14 applies the user's associated filter by allowing (routing) or blocking (dropping) packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets*** to be sent and received by the network served by the communications server 14.

Exhibit AA

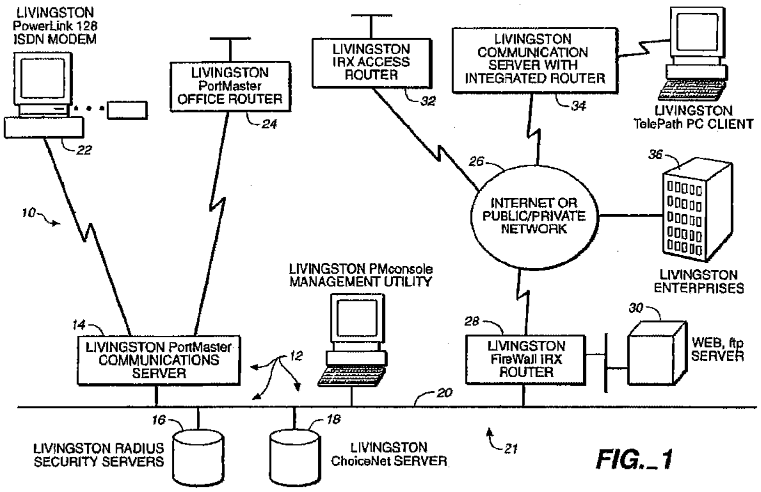
US 6779118	**Prior Art Analysis**
	(Willens, 6:10-15 (emphasis added).) Thus, the client software 44 on the communications server 14 is a "redirection server." Willens illustrates in Fig. 1 that the communications server 14 is connected to the local area network (LAN) router 24 (the "dial-up network server" under the Patent Owner's claim interpretation) and, through a backbone 20, to the Internet 26. The Internet is a "public network."  LIVINGSTON PowerLink 128 ISDN MODEM 22 LIVINGSTON PortMaster OFFICE ROUTER 24 LIVINGSTON IRX ACCESS ROUTER 32 LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER 34 LIVINGSTON TelePath PC CLIENT 36 26 INTERNET OR PUBLIC/PRIVATE NETWORK LIVINGSTON ENTERPRISES 10 LIVINGSTON PMconsole MANAGEMENT UTILITY 14 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 28 LIVINGSTON FireWall IRX ROUTER 30 WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 *FIG._1* WILLENS FIG. 1 Alternatively, Willens illustrates in Fig. 2 that the client software 44 is co-located with, and therefore connected to, the RADIUS client 45 (the "dial-up network server") on communications server 14.
	To the extent that Willens does not expressly disclose that the client software 44 on the communications server 14 provides a "redirecting" function, Stockwell teaches a filtering rule example that "intercepts all incoming connections that go the external side of the local Sidewinder (192.168.1.192) and ***redirects*** them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31, emphasis added.) Stockwell further discloses that a filter rule can "Redirect the IP address to a different machine" or "Redirect the port number to a different port." (Stockwell, 2:46-47.)

Exhibit AA

US 6779118	**Prior Art Analysis**[*]
	It would have been obvious to incorporate the redirection rule of Stockwell into the system of Willens, e.g., to redirect a user from a disallowed website an allowed website, for at least the reasons given above. In summary, Willens and Stockwell render obvious "a redirection server connected to the dial-up network server and a public network" as recited in the claim. As evidence to support this interpretation, the '118 patent describes a redirection server as a server that "controls the user's access to the network" by "checking data packets and blocking or allowing the packets as a function of the rule sets." ('118 Patent, 4:51-52 and 63-65.)
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	Willens discloses "one or more Remote ***Authentication*** Dial In User Service (RADIUS) servers 16." (Willens, 3:57-58 (emphasis added).) Willens discloses that the RADIUS server 16 checks a user's authorization: When user 22 logs in through the communications server 14, the RADIUS client software 45 first ***determines if user 22 is authorized by checking his password through RADIUS server 16***, utilizing user profiles 46. (Willens, 5:9-12.) Willens illustrates in Fig. 3 that the RADIUS server 16 is connected to the user profiles 46 (the "database"), the RADIUS client 45 (the "dial-up network server"), and the communications server 14 with its client software 44 (the "redirection server"). Willens also describes RADIUS server 16 in Fig. 3 as providing "AUTHENTICATION" and "ACCOUNTING" functions.

Exhibit AA

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td></td><td>

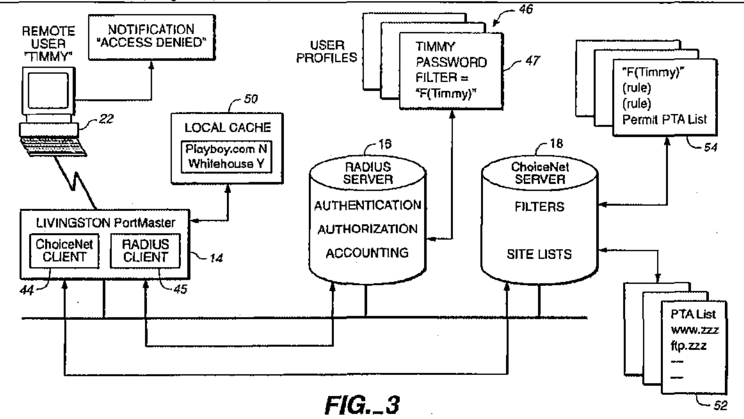


FIG._3
WILLENS FIG. 3

Alternatively, Willens illustrates in Fig. 1 that the RADIUS server 16 is connected to the local area network (LAN) router 24 (the "dial-up network server") and the communications server 14 with its client software 44 (the "redirection server").

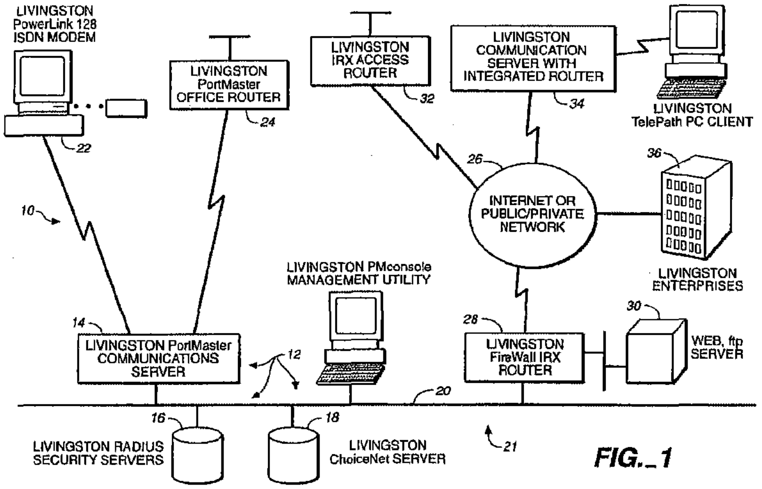

LIVINGSTON PowerLink 128 ISDN MODEM
22
LIVINGSTON PortMaster OFFICE ROUTER
24
LIVINGSTON IRX ACCESS ROUTER
32
LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER
34
LIVINGSTON TelePath PC CLIENT
36
26
INTERNET OR PUBLIC/PRIVATE NETWORK
LIVINGSTON ENTERPRISES
10
LIVINGSTON PMconsole MANAGEMENT UTILITY
28
30
WEB, ftp SERVER
14
LIVINGSTON PortMaster COMMUNICATIONS SERVER
12
LIVINGSTON FireWall IRX ROUTER
20
16
18
21
LIVINGSTON RADIUS SECURITY SERVERS
LIVINGSTON ChoiceNet SERVER

FIG._1
WILLENS FIG. 1

Thus, the RADIUS server 16 teaches "an authentication accounting server connected to the database, the dial-up network server and the redirection server" as recited in the claim.

</td></tr>
<tr><td>[1.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily</td><td>Willens discloses that when a user logs in, the RADIUS client 45 (the "dial-up network server") communicates with the RADIUS server 16 (the "authentication accounting server") to verify the user's authorization:</td></tr>
</table>

Exhibit AA

US 6779118	**Prior Art Analysis***
assigned network address for the first user ID to the authentication accounting server;	When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:9-12.) To the extent that Willens does not teach sending a user's user ID, RFC 2138, which defines the RADIUS standard, states that "An Access-Request MUST contain a User-Name attribute." (RFC 2138 at 13.) To the extent that Willens does not teach sending a temporarily assigned network address, RFC 2138 further states that a Framed-IP-Address "indicates the address to be configured for the user.... It MAY be used in an Access-Request packet as a hint by the NAS [network access server, i.e., the RADIUS client] to the [RADIUS] server that it would prefer that address." (RFC 2138 at 29.) A RADIUS User-Name is a "user ID." A Framed-IP-Address is an "assigned network address for the first user ID." It would be obvious to those of skill in the art that the Framed-IP-Address could be a temporarily assigned address since the address need only be valid for the duration of the dial-up networking session. When the user dials into the system again at a later time, the user may be assigned a different address.
[1.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	Willens teaches that the RADIUS server (the "authentication accounting server") accesses the user profiles 46 (the "database") to authenticate a user's identity by checking the provided password: When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by ***checking his password through RADIUS server 16, utilizing user profiles 46***. (Willens, 5:5-17.) After authenticating the user, the RADIUS server retrieves the user's filter identification and communicates the user's filter

Exhibit AA

US 6779118	Prior Art Analysis*
	("individualized rule set") to client software 44 on the communications server 14 (the "redirection server"): The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's authorization, the ***RADIUS server 16 supplies the filter identification*** through the RADIUS client 45 software along with the verification acknowledgment for the user 22 ***for use by client software 44*** for controlling access by the user 22 to Internet sites. (Willens, 5:5-17.) Willens further teaches that the client software 44 and communications server 14 apply the filter rules using a user's temporarily assigned network address: The ***source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter***, and to identify the site for which the user desires access. An example source address identifying a user might be: 192.168.51.50 An example destination address identifying a site requested by the user might be: 172.16.3.4 The server 14 uses such addresses in packet headers for making decisions on the handing of IP packets, such as for firewall security. (Willens, 6:35-46.) Thus, Willens teaches that the client software 44 on communications server 14 uses the user's network address in applying the user's corresponding filter rules. To enable this functionality to work as described in Willens, it would have been obvious for the RADIUS server 16 to provide the user's temporarily assigned network address to the client software 44

Exhibit AA

US 6779118	Prior Art Analysis
	and communications server 14. And RFC 2138, describing the RADIUS communications protocol employed by the RADIUS server 16, provides a "Framed-IP-Address" that "indicates the address to be configured for the user." (RFC 2138 at 29.) In summary, Willens renders obvious "wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server."
[1.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	Willens discloses that the client software 44 on communications server 14 (the "redirection server") uses the user's filter "for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) Willens provides a specific example in which the communications server 14 processes a request from user Timmy for information from the site www.playboy.com using the user's individualized "F(Timmy)" filter: In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. The ***server 14 looks at each filter rule*** found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the ***server 14 either permits or denies access*** and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.

Exhibit AA

US 6779118	**Prior Art Analysis**
	(Willens, 5:60–6:9.) It is understood that the website "www.playboy.com" is a website on the Internet, a public network. Willens further discloses that the communications server 14 processes communications to and from a user's computer by applying the user's associated filter and blocking or allowing packets to be sent or received: > In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets to be sent and received*** by the network served by the communications server 14. (Willens, 6:10-15 (emphasis added).) In summary, Willens teaches "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set."
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	Willens discloses that the client software 44 communications server 14 provides control over data to and from users' computers: > In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop ***packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of ***server 14 provides bidirectional (input/output) packet filtering*** for source and destination addresses, for protocol (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), IP, Internetwork Packet Exchange ("IPX") and port (Hypertext Transport Protocol

Exhibit AA

US 6779118	Prior Art Analysis*
	("http"), etc.). (Willens, 6:10-22.) The multiple packets sent and received by a user and filtered by the communications server 14 are a "plurality of data to and from the users' computers" as recited in the claim. And as analyzed above in portion [1.7], Willens teaches filtering packets using an individualized rule set, such as the filter "F(Timmy)" associated with the individual user "Timmy". Willens further discloses that the communications server 14 uses a set of user filters that are specific to each user: In addition to the site lists, the network access control server 18 maintains a set of user filters 54 which are used ***to control Internet access for each user***. In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. (Willens, 5:58-64.) The user filters used to control Internet access for each user are an "individualized rule set." In summary, Willens teaches "wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set," as recited in the claim.
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Willens discloses blocking data based on the user's filter: The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name

Exhibit AA

US 6779118	**Prior Art Analysis***
	"PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or ***denies access*** and updates it's local cache 50. In the event of denial of service, ***the server 14 sends a denial message back to user*** 22, informing him that he cannot access that site. (Willens, 5:64-6:9.) Willens further discloses blocking data to and from a user's computer by dropping packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or ***drop packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. (Willens, 6:10-16.) By dropping packets and denying access to the network, the communication server 14 "blocks the data to and from the users' computers." Thus, Willens teaches "wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set" as recited in the claim.
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Willens discloses allowing data based on the user's filter: The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name

Exhibit AA

US 6779118	Prior Art Analysis*
	"PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either ***permits*** or denies ***access*** and updates it's local cache 50. (Willens, 5:64-6:7.) Willens further discloses allowing data to and from a user's computer by routing packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to ***route*** or drop ***packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. (Willens, 6:10-16.) By routing packets and allowing access to the network, the communication server 14 "allows the data to and from the users' computers." Thus, Willens teaches "wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set" as recited in the claim.
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portions [1.3] and [2.0]. As analyzed in portion [2.0], Willens teaches applying an individualized filter to control data to and from a user's computer. And as analyzed in portion [1.3], Stockwell teaches an example filtering rule that "intercepts all incoming connections that go the external side of the local Sidewinder (192.168.1.192) and ***redirects*** them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31, emphasis added.) It would have been obvious to expand Willens' filtering capabilities by incorporating redirection filter rules, like those taught by Stockwell, for at least the reasons provided above.

Exhibit AA

US 6779118	**Prior Art Analysis**
	Thus, Willens and Stockwell render obvious "wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set."
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	Stockwell contemplates that each rule can specify redirection of a packet to an alternate destination IP address, port, or both. (Stockwell, 2:33-46.) Stockwell also contemplates providing multiple rules. (*See, e.g.*, Stockwell 12:49-13:7.) Multiple rules may be used to specify multiple destinations. Thus, Stockwell render obvious that packets may be redirected to multiple destinations.
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	Willens teaches centralizing users' individualized filters and associated filter lists to ease the administrative burden: If not, the client software 44 sends a lookup request to the network access server 18, which ***stores the centralized permitted site list*** and the filters to be used as masks for checking access classifications of requested sites, to download the filter "F(Timmy)", which is maintained in the server 14 memory for the rest of the user 22's session. The client software 44 also keeps the local cache 50 of recently requested sites and recently used user filters for efficiency. This list includes both sites for which access was recently permitted, such as whitehouse.gov as well as sites for which access was recently denied, such as playboy.com. (Willens, 5:21-31, emphasis added.) Willens further provides an example scenario in which a user's filter includes a rule that refers to a specific permitted site list, the "PTA List": The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the ***rule permit "PTA List"***, the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name

Exhibit AA

US 6779118	Prior Art Analysis*
	"PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site. (Willens, 5:64-6:9.) Thus, Willens teaches that the filter "F(Timmy)" refers to the centralized list "PTA List." It would have been obvious that other users' filters could similarly refer to this list. For example, one of ordinary skill in the art would understand that a PTA List in this context refers to a list of websites reviewed by the school's Parent Teacher Association. Thus, it would have been obvious to associate this filter list with the user IDs for all students in the school. The centralized permit site list, such as the example "PTA List," is a common individualized rule set to which the users' filters, and thus their user IDs, are correlated. In summary, Willens renders obvious "wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set."
[8.0] In a system comprising	See analysis of portion [1.0].
[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[8.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the	See analysis of portion [1.3].

Exhibit AA

US 6779118	Prior Art Analysis*
redirection server,	
[8.4] the method comprising the steps of:	Willens discloses "a method of controlling a user's access to a network." (Willens, 10:31-32.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[8.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[9.0] The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]
[10.0] The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0]
[11.0] The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0]

Exhibit AA

US 6779118	Prior Art Analysis
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0]
[13.0] The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[14.0] The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0]. And as analyzed in portion [1.1], Willens teaches a database with entries for plurality of user IDs. In view of Willens' teaching of a database having user ID entries, it would have been obvious to create a plurality of user ID entries in the database.
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portions [1.1] and [1.7]. Willens discloses that "Firewall filters are defined as an explicit set of rules based on either ***permit or deny syntax***." (Willens, 6:15-16.) The permit and deny actions are "a plurality of functions used to control passing between the user and a public network."
[16.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [1.6]. Willens discloses that the communications server 14 (with its client software 44, the "redirection server") communicates with ChoiceNet server 18 to automatically update the list of permitted sites used to control users' access: Installed on one of several supported UNIX platforms, the ChoiceNet server 18 software

Exhibit AA

US 6779118	Prior Art Analysis*
	provides lookups of sites for the server 14 or routers 24, 32 or 34 against a list of permitted sites. The ***server software also automatically maintains the permit list*** by downloading updated versions of the list over the Internet and compiling the list for use by the client software 42. As a result of this self maintenance capability, the server 18 requires minimal administrative attention. (Willens, 5:38-45.) Willens further discloses that the "server based permit list that can be ***easily updated on a daily or hourly basis***." (Willens, 4:42-44.) The permit list of allowed destination sites is "at least a portion of the rule set" for a user. For example, as shown in the analysis of portion [1.7], the example permitted site list "PTA List" is used to control access for user Timmy. By working in conjunction with, and relying upon, ChoiceNet server 18 to automatically maintain the list of permitted sites, the communications server 14 is "configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address."
[16.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	Willens discloses modifying the list of sites a user is permitted to access as a function of time: Finally, instead of trying to maintain an unwieldy list of deny keywords on every desktop, the subsystem 12 provides for a central, server based ***permit list that can be easily updated on a daily or hourly basis***, and that cannot be tampered with by the end users. (Willens, 4:40-45.) Updating the permit list on a daily or hourly basis teaches modifying a rule set as a function of time. Willens also teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login

US 6779118	**Prior Art Analysis**[*]
	information, such as a password: ***When user 22 logs in through the communications server 14***, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's authorization, the RADIUS server 16 ***supplies the filter identification*** through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 ***for controlling access by the user*** 22 to Internet sites. (Willens, 5:8-18, emphasis added.) Thus, Willens teaches that the filtering rules are updated when the user accesses the login location of the communications server 14. The user's password is "data transmitted to or from the user." As support for this interpretation of the claim, note that the Patent Owner asserts that a user's login information is "data transmitted to or from the user." (*See* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 57.) Willens further teaches updating a local cache of filtering rules based on a location the user accesses: This look-up contains the list name "PTA List" and ***the site Timmy is trying to access*** (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and ***updates it's local cache 50***. (Willens, 6:2-7, emphasis added.) The site the user Timmy is trying to access is a "location" as recited in the claim. The update to the communications server 14's local cache of filtering rules teaches "modification of at least a portion of the rule set" as recited in the claim. Thus, Willens renders obvious "modification of at least a portion

Exhibit AA

US 6779118	Prior Art Analysis*
	of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access" as recited in the claim. Furthermore, blocking a website based on some combination of the recited bases—time, data transmitted to or from the user, or location the user accesses—would have been obvious to one of skill in the art. For example, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work. Similarly in a school environment, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to school. Thus, although an initial rule set might be permissive, it would be obvious to modify the rules for a particular user at a later time after it is found that the user's data transmissions or locations accessed are unproductive or inappropriate. Accordingly, Requester has provided an independent explanation of the pertinence and manner of applying the prior art to this claim limitation. The Board adopted similar reasoning in the previous reexamination where it found that this limitation would have been obvious to one of skill in the art. (*See* Board Decision at 10.) Accordingly, it would have been obvious to "allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses." For example, it would have been obvious, in view of Willens, to block or redirect a user after discovering inappropriate communications or an excessive amount of time at a site unrelated to school.
[16.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portion [16.4]. Willens discloses updating a list of permitted sites on a daily or hourly basis. Thus, Willens discloses modifying a portion of the rule set as a function of time.
[17.0] A system comprising:	See analysis of portion [1.0].
[17.1] a redirection server	See analysis of portions [1.3] and [1.6].

Exhibit AA

US 6779118	Prior Art Analysis*
programmed with a user's rule set correlated to a temporarily assigned network address;	
[17.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[17.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[17.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[17.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4]. Willens discloses updating rules used to control access based on a user's profile and filters when a user logs into the communications server 14: When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22

Exhibit AA

US 6779118	**Prior Art Analysis***
	to Internet sites. The client software 44 then checks to see if the filter "F(Timmy)" is stored locally in cache 50. If it is, the client software 44 uses it for controlling access. (Willens, 5:9-21.) It is understood that when a user logs into the communications server 14, data is transmitted from the user. For example, Willens discloses that "If multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests." (Willens, 6:52-55.) The login information is "data transmitted to or from the user." Thus, Willens renders obvious "modification of at least a portion of the rule set as a function of the data transmitted to or from the user" as recited in the claim.
[18.0] A system comprising:	See analysis of portion [1.0].
[18.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[18.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[18.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[18.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a	See analysis of portion [16.4].

Exhibit AA

US 6779118	Prior Art Analysis*
function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[18.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4]. As shown there, Willens teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses.
[19.0] A system comprising:	See analysis of portion [1.0].
[19.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[19.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[19.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[19.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[19.5] wherein the redirection server is	See analysis of portions [16.4] and [16.5].

Exhibit AA

US 6779118	Prior Art Analysis
configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	
[20.0] A system comprising:	See analysis of portion [1.0].
[20.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[20.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[20.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[20.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[20.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].
[21.0] A system comprising:	See analysis of portion [1.0].
[21.1] a redirection server	See analysis of portions [1.3] and [1.6].

Exhibit AA

US 6779118	**Prior Art Analysis***
programmed with a user's rule set correlated to a temporarily assigned network address;	
[21.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[21.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[21.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[21.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[22.0] A system comprising:	See analysis of portion [1.0].
[22.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[22.2] wherein the rule set contains at least one of a	See analysis of portion [16.2].

Exhibit AA

US 6779118	Prior Art Analysis*
plurality of functions used to control passing between the user and a public network;	
[22.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[22.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[22.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[23.0] A system comprising:	See analysis of portion [1.0].
[23.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[23.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td>[23.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;</td><td>See analysis of portion [16.3].</td></tr>
<tr><td>[23.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and</td><td>See analysis of portion [16.4].</td></tr>
<tr><td>[23.5] wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.</td><td>Willens illustrates the recited network architecture in Fig. 1. The communications server 14 (with its client software 44, the "redirection server") has a "user side" that connects to a remote user's computer 22 and a "network side" that connects to the network backbone 20. The remote user's computer 22 connects to the network backbone 20 through the communications server 14.

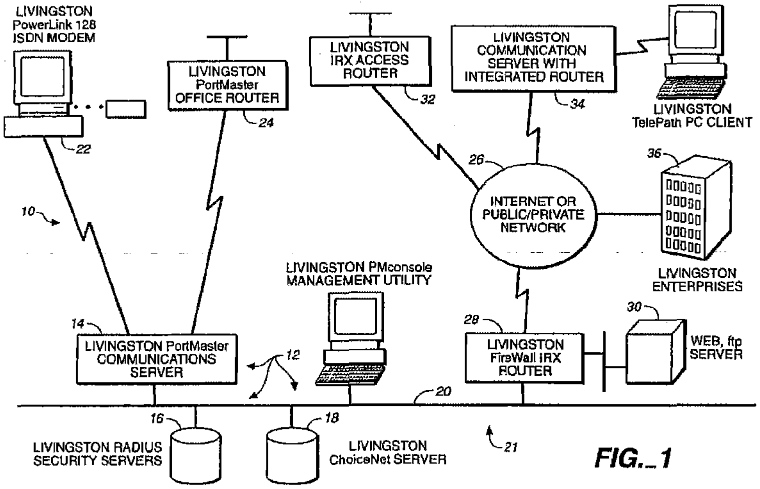

LIVINGSTON PowerLink 128 ISDN MODEM
22
10
LIVINGSTON PortMaster OFFICE ROUTER
24
LIVINGSTON IRX ACCESS ROUTER
32
LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER
34
LIVINGSTON TelePath PC CLIENT
26
INTERNET OR PUBLIC/PRIVATE NETWORK
36
LIVINGSTON ENTERPRISES
LIVINGSTON PMconsole MANAGEMENT UTILITY
14
LIVINGSTON PortMaster COMMUNICATIONS SERVER
12
28
LIVINGSTON FireWall IRX ROUTER
30
WEB, ftp SERVER
20
16
18
LIVINGSTON RADIUS SECURITY SERVERS
LIVINGSTON ChoiceNet SERVER
21

FIG._1

WILLENS FIG. 1

Alternatively, considering the router 24 as the "dial-up network server," Fig. 1 illustrates that the communications server 14 has</td></tr>
</table>

Exhibit AA

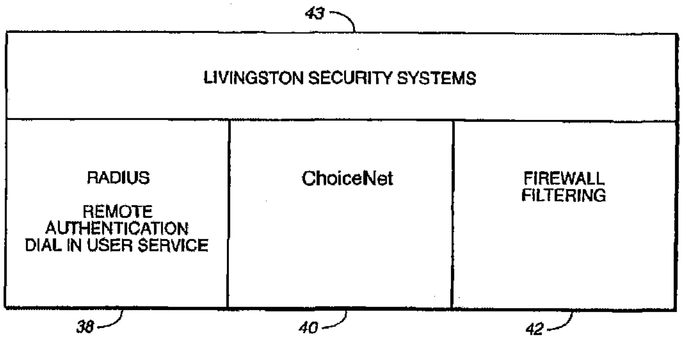
US 6779118	Prior Art Analysis*
	a "user side" (top) that is connected to the router 24 and a "network side" (bottom) that is connected to the network 20 and Internet 26. Willens further illustrates in Fig. 2 that the access control architecture includes a RADIUS client on one side ("user side") and the firewall filtering on the other side ("network side"): As represented in FIG. 2, the access control subsystem 12 incorporates integrated software modules 38, 40 and 42, respectively comprising the RADIUS module, the network access module, and the firewall filtering module in security systems software 43. (Willens, 4:12-16.)  43 LIVINGSTON SECURITY SYSTEMS RADIUS REMOTE AUTHENTICATION DIAL IN USER SERVICE ChoiceNet FIREWALL FILTERING 38 40 42 Willens Fig. 2 Willens also discloses that a user's computer receives a temporarily assigned IP address that is used for communication with the network. See analysis of portion [1.5].
[24.0] The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	As analyzed in portion [16.3], Willens teaches that the communications server 14 (together with its client software 44, the "redirection server") communicates with ChoiceNet server 18 to automatically update the list of permitted sites used to control users' access. As illustrated in Fig. 3, the communications server 14 communicates with the ChoiceNet server 18 via network backbone 20. Thus, Willens teaches that the instructions to modify a user's individualized filter profile are received by the communications server 14 on a network side.

Exhibit AA

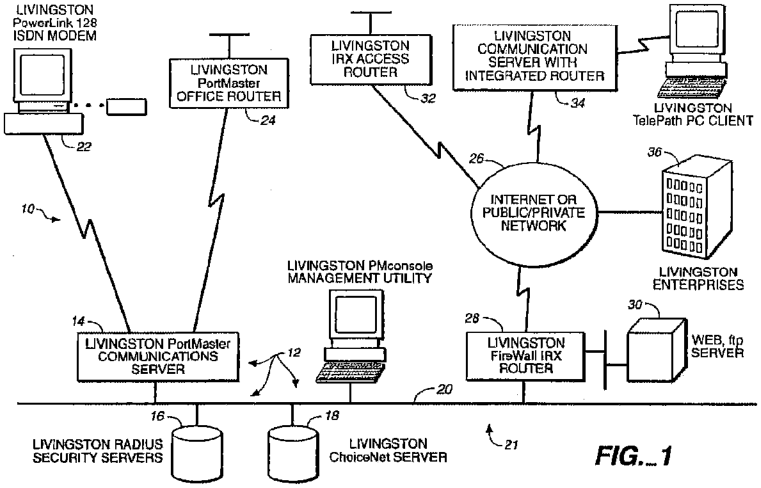
US 6779118	Prior Art Analysis*
	 LIVINGSTON PowerLink 128 ISDN MODEM LIVINGSTON PortMaster OFFICE ROUTER LIVINGSTON IRX ACCESS ROUTER LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER LIVINGSTON TelePath PC CLIENT 22 24 32 34 36 26 10 INTERNET OR PUBLIC/PRIVATE NETWORK LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 14 28 30 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 LIVINGSTON FireWall IRX ROUTER WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 *FIG._1* WILLENS FIG. 1 In summary, Willens renders obvious “wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server” as recited in the claim.
[25.0] In a system comprising	See analysis of portion [1.0].
[25.1] a redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portion [1.3] and [1.5].
[25.2] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.2].
[25.3] the method comprising the step of:	See analysis of portion [8.4].
[25.4] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	Willens teaches that when a user requests access to a network site that is not in the client software 44's local cache 50, the request is initially denied while the data needed to further evaluate the request is obtained: When a request for access is made by the user for which a determination cannot be made using the local cache 50, ***the server 14 drops the packet***

Exhibit AA

US 6779118	Prior Art Analysis*
	making the request to allow time for access and response from the server 18. Since drops are common on the Internet, the packet making the request is retransmitted a number of times before the request times out, typically at 30 seconds or so. The source and destination addresses in the header packet are used to identify the user, ***allowing selection of the appropriate user filter***, and to identify the site for which the user desires access. An example source address identifying a user might be: 192.168.51.50 An example destination address identifying a site requested by the user might be: 172.16.3.4 ***The server 14 uses such addresses in packet headers for making decisions on the handing of IP packets***, such as for firewall security. Little additional overhead at the server is required to use these addresses for the purposes of identifying user filters and sites for determining site access in this system and process. If a particular source address represents a node that is associated with a single user who has no access restriction, then no further checking is required and no user filter need be employed. If multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests. (Willens, 6:29-55, emphasis added.) Thus, Willens discusses using the user's network address to make decisions on the handling of access requests. Willens teaches that the applied user-specific filter is modified by loading further details about the appropriate user filter from the ChoiceNet server 18 while the user's network address remains the same.

Exhibit AA

US 6779118	Prior Art Analysis*
	Thus, Willens renders obvious "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server" as recited in the claim.
[25.5] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.5].
[25.6] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.5].
[25.7] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[26.0] The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[27.0] The method of claim 25, further including the step of removing or	See analysis of portion [16.4]. Willens teaches that a list of allowed network sites can "can be easily updated on a daily or hourly basis." (Willens, 4:43-44.) It would have been obvious

Exhibit AA

US 6779118	**Prior Art Analysis***
reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	that updating the list would involve removing or adding sites, which teaches "removing or reinstating at least a portion of the user's rule set." Thus Willens renders obvious "removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses" as recited in the claim.
[28.0] The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	Willens teaches that the filter rules are defined based in part on a specific protocol and port communicating over Internet Protocol (IP): In practice, the access control system and process is implemented using an extension of the ***Internet Protocol (IP) firewall packet filtering*** employed by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, ***for protocol*** (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), ***IP***, Internetwork Packet Exchange ("IPX") ***and port*** (Hypertext Transport Protocol ("http"), etc.). (Willens at 6:10-22, emphasis added.) Defining filters based on a protocol and a port render obvious a "rule [included] as a function of a type of IP (Internet Protocol) server" as recited in the claim.
[29.0] The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	Willens teaches applying an initial temporary filter that drops a user's packet to allow time for Willens' system to evaluate whether to permit the requested access: When a request for access is made by the user for which a determination cannot be made using the local cache 50, ***the server 14 drops the packet making the request to allow time for access and***

Exhibit AA

US 6779118	Prior Art Analysis
	> ***response from the server 18***. Since drops are common on the Internet, the packet making the request is retransmitted a number of times before the request times out, typically at 30 seconds or so. The source and destination addresses in the header packet are used to identify the user, allowing ***selection of the appropriate user filter***, and to identify the site for which the user desires access. (Willens, 6:29-38, emphasis added.) Dropping the first packet of a new access request—thereby temporarily denying access—is an "initial temporary rule set." The appropriate user filter is a "standard rule set." Thus, Willens renders obvious "wherein the individualized rule set includes an initial temporary rule set and a standard rule set" as recited in the claim.
[29.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	As analyzed in portion [29.0], Willens teaches applying an initial filter to deny an access request until the appropriate user filter can be loaded and used to evaluate the access request. (Willens, 6:29-38.) Thus, Willens teaches using the initial filter until the appropriate user filter is consulted, after which the appropriate user filter is used. Thus, Willens renders obvious "wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set" as recited in the claim.
[30.0] The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	Willens teaches filtering rules that allow access, by routing packets, based on a destination address, protocol, and port: > In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets*** to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of

Exhibit AA

US 6779118	Prior Art Analysis
	server 14 provides bidirectional (input/output) ***packet filtering for source and destination addresses***, ***for protocol*** (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), IP, Internetwork Packet Exchange ("IPX") ***and port*** (Hypertext Transport Protocol ("http"), etc.). (Willens at 6:10-22, emphasis added.) Filtering rules based on a destination address, protocol, and port renders obvious "at least one rule allowing access based on a request type and a destination address" as recited in the claim.
[31.0] The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	As analyzed in portion [30.0], Willens renders obvious controlling access using a rule based on a request type and a destination address. And as analyzed in portion [1.3], Willens and Stockwell render obvious redirecting a user's network traffic. Thus, Willens and Stockwell render obvious "at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address" as recited in the claim.
[32.0] The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[33.0] The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[33.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[34.0] The method of claim	See analysis of portion [30.0].

Exhibit AA

US 6779118	Prior Art Analysis*
8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	
[35.0] The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[36.0] A system comprising:	See analysis of portion [1.0].
[36.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[36.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[36.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[36.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user	See analysis of portion [16.4].

Exhibit AA

US 6779118	Prior Art Analysis*
accesses; and	
[36.5] wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[37.0] A system comprising:	See analysis of portion [1.0].
[37.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[37.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[37.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[37.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[37.5] wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[37.6] wherein the redirection server is configured to utilize the temporary rule set for an	See analysis of portion [29.1].

Exhibit AA

US 6779118	Prior Art Analysis*
initial period of time and to thereafter utilize the standard rule set.	
[38.0] A system comprising:	See analysis of portion [1.0].
[38.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[38.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[38.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[38.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[38.5] wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[39.0] A system comprising:	See analysis of portion [1.0].
[39.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].

Exhibit AA

US 6779118	Prior Art Analysis*
[39.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[39.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[39.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[39.5] wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[40.0] The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[41.0] The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set,	See analysis of portion [29.0].
[42.0] The method of claim 25, wherein the modified	See analysis of portion [30.0].

Exhibit AA

US 6779118	Prior Art Analysis
rule set includes at least one rule allowing access based on a request type and a destination address.	
[43.0] The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[44.0] A system comprising:	See analysis of portion [1.0].
[44.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[44.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[44.3] a redirection server connected between the dial-up network server and a public network, and	As analyzed in portion [1.3], Willens teaches client software 44 on communications server 14, which Willens and Stockwell render obvious as providing a "redirection server." And as analyzed in portion [1.2], Willens teaches that a user may connect via local area network (LAN) router 24. The Patent Owner asserts that a router is a "dial-up network server." (*See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.) And as analyzed in portion [1.2], Willens also teaches that a user may connect via dial-up modem to RADIUS client software 45 on communications server 14, which is a "dial-up network server." Willens illustrates these components in Fig. 1, which shows that the communications server 14 is between the LAN router 24 and the public Internet 26, and between the dial-up connection from computer 22 and the public Internet 26:

Exhibit AA

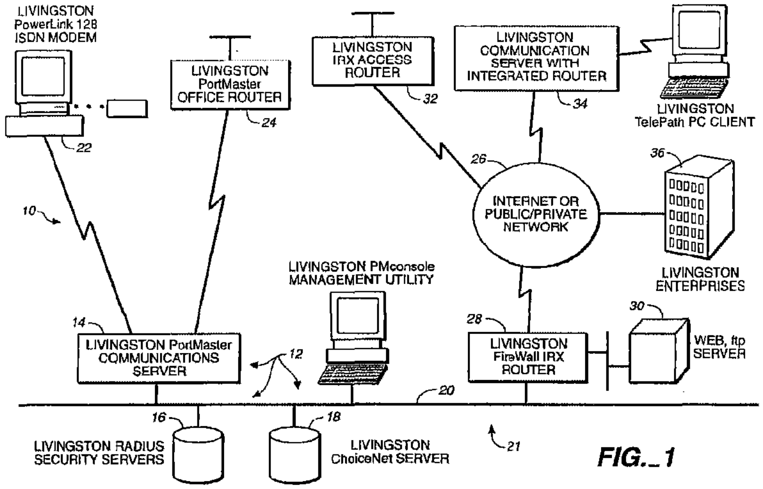
US 6779118	Prior Art Analysis*
	 LIVINGSTON PowerLink 128 ISDN MODEM LIVINGSTON PortMaster OFFICE ROUTER LIVINGSTON IRX ACCESS ROUTER LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER LIVINGSTON TelePath PC CLIENT 22 24 32 34 36 26 10 INTERNET OR PUBLIC/PRIVATE NETWORK LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 14 28 30 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 LIVINGSTON FireWall IRX ROUTER WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 FIG._1 WILLENS FIG. 1 And while Willens teaches a communications server 14 that includes both client software 44 (providing access control) and RADIUS client software 45 (providing dial-up communication services), it would have been obvious that if these functions were separated into two distinct servers, the client software 44 should be located between the RADIUS client software 45 and the public Internet network. Willens specifically teaches that "client software 44 [is] for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) To perform this function, the client software 45 must be on the data path between the user and the Internet. Thus, Willens and Stockwell render obvious "a redirection server connected between the dial-up network server and a public network" as recited in the claim.
[44.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	See analysis of portion [1.4].
[44.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the	See analysis of portion [1.5].

Exhibit AA

US 6779118	Prior Art Analysis*
authentication accounting server;	
[44.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	See analysis of portion [1.6].
[44.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	See analysis of portion [1.7].
[45.0] The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0].
[46.0] The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[47.0] The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[48.0] The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0].
[49.0] The system of claim	See analysis of portion [6.0].

Exhibit AA

US 6779118	Prior Art Analysis*
44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	
[50.0] The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	See analysis of portion [7.0].
[51.0] The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[52.0] The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[52.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[53.0] The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[54.0] The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on	See analysis of portion [31.1].

Exhibit AA

US 6779118	Prior Art Analysis*
a request type and an attempted destination address.	
[55.0] The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	See analysis of portion [1.3]. Stockwell teaches that a filter rule can "Redirect the IP address to a different machine." (Stockwell, 2:46.) Stockwell further provides a filtering rule example that "intercepts all incoming connections that go the external side of the local Sidewinder (192.168.1.192) and ***redirects*** them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31, emphasis added.) It is understood that the addresses "192.168.1.192" and "172.17.192.48" are destination IP addresses. Thus, Willens and Stockwell render obvious "wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set" as recited in the claim.
[56.0] In a system comprising	See analysis of portion [1.0].
[56.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[56.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[56.3] a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portions [1.3] and [44.3].
[56.4] the method comprising the steps of:	See analysis of portion [8.4].
[56.5] communicating a first user ID for one of the users' computers and a temporarily	See analysis of portion [1.5].

Exhibit AA

US 6779118	Prior Art Analysis*
assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	
[56.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[56.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[57.0] The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0].
[58.0] The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[59.0] The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[60.0] The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0].

Exhibit AA

US 6779118	Prior Art Analysis
[61.0] The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[62.0] The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDS, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[63.0] The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[64.0] The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[64.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[65.0] The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[66.0] The method of claim 56, wherein the	See analysis of portion [31.0].

Exhibit AA

US 6779118	Prior Art Analysis*
individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[67.0] The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	See analysis of portion [55.0].
[68.0] A system comprising:	See analysis of portion [1.0].
[68.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[68.2] the redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[68.3] wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [16.2].
[68.4] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and	See analysis of portion [16.3].
[68.5] wherein the redirection server is	See analysis of portion [16.4].

Exhibit AA

US 6779118	Prior Art Analysis*
configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.	
[69.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[70.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].
[71.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[72.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[73.0] The system of claim 68, wherein the redirection sewer is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].

Exhibit AA

US 6779118	Prior Art Analysis*
[74.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[75.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.4], [18.5] and [22.5].
[76.0] The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	See analysis of portion [23.5].
[77.0] The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[78.0] The system of claim 68, wherein the modified	See analysis of portion [28.0].

Exhibit AA

US 6779118	**Prior Art Analysis***
rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	
[79.0] The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[79.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set	See analysis of portion [29.1].
[80.0] The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[81.0] The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[82.0] The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.	See analysis of portion [55.0].
[83.0] In a system comprising	See analysis of portion [1.0].
[83.1] a redirection server	See analysis of portions [1.3] and [44.3].

Exhibit AA

US 6779118	**Prior Art Analysis**[*]
connected between a user computer and a public network,	
[83.2] the redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portions [1.3] and [1.6].
[83.3] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.1].
[83.4] the method comprising the step of:	See analysis of portion [8.4].
[83.5] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	See analysis of portion [25.4].
[83.6] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.0].
[83.7] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.0].
[83.8] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the	See analysis of portion [24.0].

Exhibit AA

US 6779118	Prior Art Analysis*
user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	
[84.0] The method of claim 83, further including; the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[85.0] The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[86.0] The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service,	See analysis of portion [28.0].
[87.0] The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[87.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[88.0] The method of claim 83, wherein the modified	See analysis of portion [30.0].

Exhibit AA

US 6779118	Prior Art Analysis*
rule set includes at least one rule allowing access based on a request type and a destination address.	
[89.0] The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[90.0] The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.	See analysis of portion [55.0].

Exhibit AA

Proposed Rejection #2. **Claims 2–7, 9-14, 16-24, and 26-90 are obvious over Willens in view of RFC 2138 and Admitted Prior Art under 35 U.S.C. § 103(a).**

Reasons to Combine Willens, RFC 2138, and Admitted Prior Art

Willens describes a system for controlling users' access to a public network using Remote Authentication Dial In User Service (RADIUS). A RADIUS client communicates with a RADIUS server. RFC 2138 defines the standard protocol for these RADIUS communications. Thus, Willens and RFC 2138 include overlapping and complementary material regarding the same subject matter. Indeed, Steven Willens, the sole named inventor of the Willens patent, is a co-author of RFC 2138. A person of ordinary skill in the art would have viewed the relationship between Willens and RFC 2138 as an explicit suggestion to combine the teachings of the two references. For example, it would have been obvious to one of ordinary skill in the art in reviewing Willens, to refer to RFC 2138 for further details regarding the communications between Willens' RADIUS client and RADIUS server.

Regarding the Admitted Prior Art, the '118 Patent provides that redirection was a known technique. For example, the Patent Owner states:

> The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page-hence the redirection of the user begins.

('118 Patent, 1:53-57.)

The Patent Owner's admission shows that persons of skill in the art were familiar with redirection as a technique and how to do it in at least the context of web servers and browsers. Thus, the Admitted Prior Art includes the technique of redirection and renders obvious the replacement of a destination address by another destination address as a function of an individualized rule set. For example, an address blocked for a particular user would be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. It would have been obvious to extend the filtering capabilities of Willens to include such redirection capabilities and features.

Furthermore, it would also be obvious to perform redirection by replacing a first destination address in an IP packet header by a second destination because it requires only applying a known technique (replacement of one destination address for another) to a known device (the packet filters of Willens) to yield predictable results (redirection from one website to another). (*See* MPEP § 2143, *citing KSR.*)

Requester has provided an independent explanation of the reasons to combine these prior art references. Requester notes that in an earlier reexamination, the Board of Patent Appeals and Interferences found, with respect to the '118 Patent, that redirection is an obvious extension of thc usc of a control to block a uscr. Scc *Ex Parte Linksmart Wireless Technology, LLC*, Appcal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011) (hereinafter, the "BPAI Decision".)

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis[*]</th></tr>
<tr><td>[1.0] A system comprising:</td><td>Willens discloses a "Network access control <b><i>system</i></b> and process." (Willens, Title, emphasis added.)</td></tr>
<tr><td>[1.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;</td><td>Willens illustrates in Fig. 3 a Remote Authentication Dial In User Service (RADIUS) server 16 that stores user profiles 46. As a specific example, Fig. 3 illustrates that the user ID "TIMMY" has a profile 47 with an associated filter "F(Timmy)."

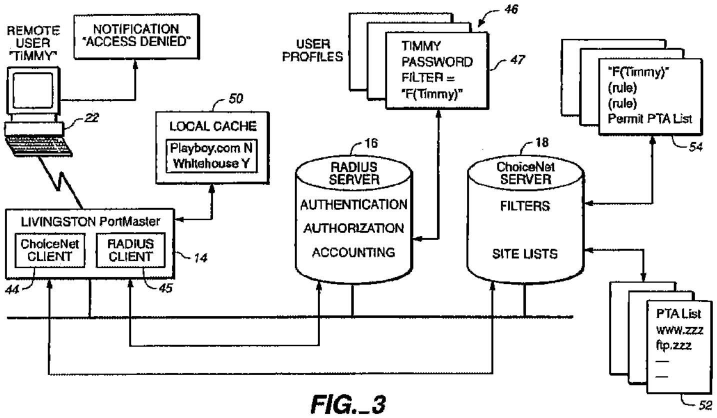


FIG._3
WILLENS FIG. 3

Willens further describes how each user's filter is an "individualized rule set":

> In addition to the site lists, the network access control server 18 maintains a set of user filters 54 which are used to control Internet access <b><i>for each user</i></b>.... The server 14 looks at <b><i>each filter rule</i></b> found in "F(Timmy)" starting from the top.

(Willens, 5:58-66, emphasis added.)</td></tr>
</table>

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit AA

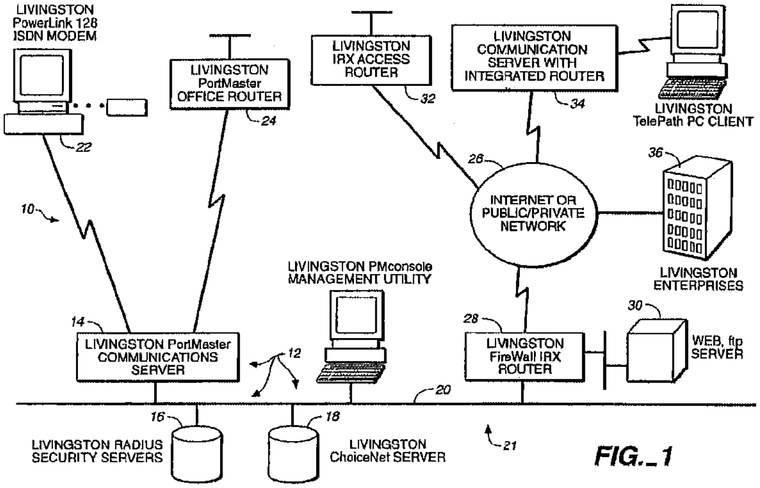
US 6779118	Prior Art Analysis*
	Since Willens teaches that the user filters control Internet access *for each user*, it is understood that Willens contemplates the plurality of user profiles 46 being correlated to a "plurality of user IDs" as recited in the claim. Thus, the user profiles 46 are a "database with entries correlating each of a plurality of user IDs with an individualize rule set," as recited in the claim.
[1.2] a dial-up network server that receives user IDs from users' computers;	Willens teaches that users connect to a network via dial-up connections or through a local area network (LAN) router: In the network 21 connected by backbone 20, ***users are connected to the network*** by dial-up connections 22 through the communications server 14 or ***via a local area network (LAN) router*** 24, also through the communications server 14. (Willens, 3:60-64, emphasis added.) Willens further teaches that users must log in, which is understood to require providing a user ID: ***When user 22 logs in*** through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:6-12, emphasis added.) Thus, the local area network (LAN) router 24 teaches a "dial-up network server that receives user IDs from users' computers" as recited in the claim under at least the Patent Owner's asserted interpretation of the claim. For example, the Patent Owner has specifically asserted that a LAN communication link employs a "dial-up network server": The inventors specifically disclosed that the connection between the user's computer and the "dial-up network server" was not limited to a connection via a modem: "The PC 100 first

US 6779118	Prior Art Analysis*
	connects to the ***dial-up network server*** 102. The connection is ***typically*** created using a computer modem, ***however a local area network (LAN) or other communications link can be employed***." ['118 Patent] at 3:57-60 (emphasis added). (Linksmart Claim Construction Brief at 14, emphasis added.) In addition, the Patent Owner asserts that a router is a "dial-up network server." (*See, e.g.*, Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.) Alternatively, Willens also teaches that users may connect via "dial-up connections 22 through the communications server 14." More specifically, Willens teaches that users connect to Remote Authentication ***Dial In*** User Service (RADIUS) client software 45 on communications server 14: RADIUS client software 45 is also resident on the communications server 14. When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:6-12, emphasis added.) It would have been obvious to one of skill in the art that for the RADIUS server 16 to verify a user's password, the user must also specific a user ID so that the RADIUS server 16 can locate the correct user profile to be used to verify the supplied password. Furthermore, the RADIUS standard, as defined in Request for Comments (RFC) 2138, states that a "User-Name" attribute "indicates the name of the user to be authenticated." (RFC 2138 at 5.1.) Thus, the "User-Name" attribute is a "user ID" as recited in the claim. An access request message sent from the RADIUS client 45 to the RADIUS server 16 "MUST contain a User-Name attribute." (RFC 2138 at 4.1.) Thus, it would have been obvious that the RADIUS client software 45 should receive the user's user ID so that the user ID may be sent to the RADIUS server 16, as required by the RADIUS communication standard defined in RFC 2138.

Exhibit AA

US 6779118	**Prior Art Analysis***
	Willens also discloses a "Remote user 22" who uses a "PC or Macintosh accessing the Internet." (Willens, 4:59-62.) The user's PC or Macintosh is a user's computer. As noted above in portion, [1.1] Willens teaches that the system supports a plurality of users, and thus, multiple "users' computers" as recited in the claim. In summary, the RADIUS client software 45 resident on the communications server 14 teaches a "dial-up network server that receives user IDs from users' computers" as recited in the claim. Alternatively, the local area network (LAN) router 24 teaches a "dial-up network server that receives user IDs from users' computers" under at least the patent owner's interpretation of the claim.
[1.3] a redirection server connected to the dial-up network server and a public network, and	Willens discloses a communications server 14 that "either permits or denies access" to network resources. (Willens, 6:6.) More specifically, the communications server 14 includes client software 44 that receives the user's filter "for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) Willens provides a specific example in which user Timmy requests information from the site www.playboy.com: In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. The ***server 14 looks at each filter rule*** found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the ***server 14 either permits or denies access*** and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot

Exhibit AA

US 6779118	Prior Art Analysis*
	access that site. (Willens, 5:60–6:9.) Willens further discloses that the communications server 14 applies the user's associated filter by allowing (routing) or blocking (dropping) packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets*** to be sent and received by the network served by the communications server 14. (Willens, 6:10-15 (emphasis added).) Thus, the client software 44 on the communications server 14 is a "redirection server." Willens illustrates in Fig. 1 that the communications server 14 is connected to the local area network (LAN) router 24 (the "dial-up network server" under the Patent Owner's claim interpretation) and, through a backbone 20, to the Internet 26. The Internet is a "public network."  LIVINGSTON PowerLink 128 ISDN MODEM LIVINGSTON PortMaster OFFICE ROUTER LIVINGSTON IRX ACCESS ROUTER LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER LIVINGSTON TelePath PC CLIENT 22 24 32 34 26 36 10 INTERNET OR PUBLIC/PRIVATE NETWORK LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 30 28 14 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 LIVINGSTON FireWall IRX ROUTER WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 FIG._1 WILLENS FIG. 1 Alternatively, Willens illustrates in Fig. 2 that the client software

US 6779118	Prior Art Analysis*
	44 is co-located with, and therefore connected to, the RADIUS client 45 (the "dial-up network server") on communications server 14. The Admitted Prior Art teaches controlling access to resources by redirecting traffic, for example, World Wide Web traffic: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that in directing the user away from the website, the user's access to the website is blocked. Thus, redirection is an obvious extension of blocking and could be used, for example, to replace an address with another address,

Exhibit AA

US 6779118	Prior Art Analysis[*]
	perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Requester notes that the Board made similar findings in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.) It would have been obvious to add the redirection feature known in the prior art to the packet filtering capabilities of Willens at least for the reasons given above. In summary, Willens and the Admitted Prior Art render obvious "a redirection server connected to the dial-up network server and a public network" as recited in the claim. As evidence to support this interpretation, the '118 patent describes a redirection server as a server that "controls the user's access to the network" by "checking data packets and blocking or allowing the packets as a function of the rule sets." ('118 Patent, 4:51-52 and 63-65.)
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	Willens discloses "one or more Remote ***Authentication*** Dial In User Service (RADIUS) servers 16." (Willens, 3:57-58 (emphasis added).) Willens discloses that the RADIUS server 16 checks a user's authorization: When user 22 logs in through the communications server 14, the RADIUS client software 45 first ***determines if user 22 is authorized by checking his password through RADIUS server 16***, utilizing user profiles 46. (Willens, 5:9-12.) Willens illustrates in Fig. 3 that the RADIUS server 16 is connected to the user profiles 46 (the "database"), the RADIUS client 45 (the "dial-up network server"), and the communications server 14 with its client software 44 (the "redirection server"). Willens also describes RADIUS server 16 in Fig. 3 as providing "AUTHENTICATION" and "ACCOUNTING" functions.

Exhibit AA

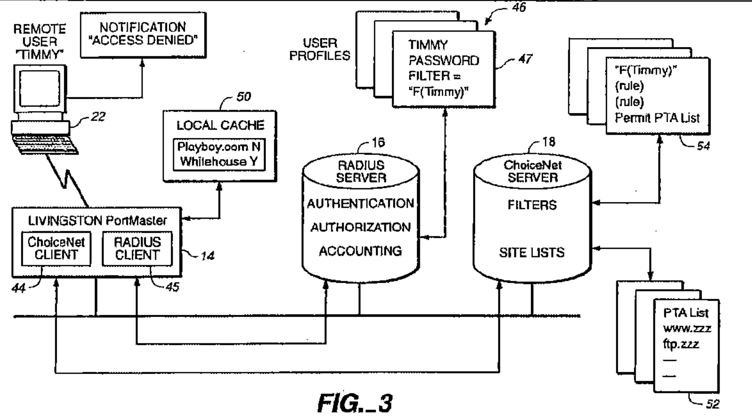
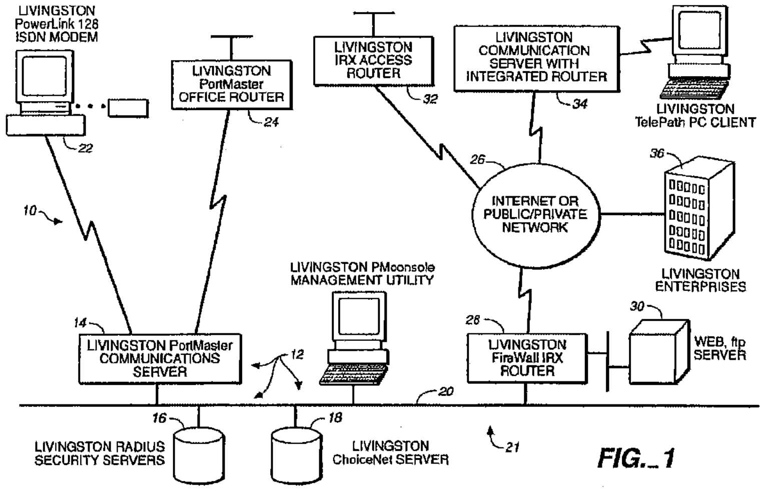
US 6779118	Prior Art Analysis*
	 REMOTE USER "TIMMY" NOTIFICATION "ACCESS DENIED" 22 50 LOCAL CACHE Playboy.com N Whitehouse Y LIVINGSTON PortMaster ChoiceNet CLIENT RADIUS CLIENT 14 44 45 USER PROFILES 46 TIMMY PASSWORD FILTER = "F(Timmy)" 47 16 RADIUS SERVER AUTHENTICATION AUTHORIZATION ACCOUNTING 18 ChoiceNet SERVER FILTERS SITE LISTS "F(Timmy)" (rule) (rule) Permit PTA List 54 PTA List www.zzz ftp.zzz 52 *FIG._3* WILLENS FIG. 3 Alternatively, Willens illustrates in Fig. 1 that the RADIUS server 16 is connected to the local area network (LAN) router 24 (the "dial-up network server") and the communications server 14 with its client software 44 (the "redirection server").  LIVINGSTON PowerLink 128 ISDN MODEM 22 LIVINGSTON PortMaster OFFICE ROUTER 24 LIVINGSTON IRX ACCESS ROUTER 32 LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER 34 LIVINGSTON TelePath PC CLIENT 10 26 INTERNET OR PUBLIC/PRIVATE NETWORK 36 LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 14 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 28 LIVINGSTON FireWall IRX ROUTER 30 WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 *FIG._1* WILLENS FIG. 1 Thus, the RADIUS server 16 teaches "an authentication accounting server connected to the database, the dial-up network server and the redirection server" as recited in the claim.
[1.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily	Willens discloses that when a user logs in, the RADIUS client 45 (the "dial-up network server") communicates with the RADIUS server 16 (the "authentication accounting server") to verify the user's authorization:

Exhibit AA

US 6779118	Prior Art Analysis*
assigned network address for the first user ID to the authentication accounting server;	When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. (Willens, 5:9-12.) To the extent that Willens does not teach sending a user's user ID, RFC 2138, which defines the RADIUS standard, states that "An Access-Request MUST contain a User-Name attribute." (RFC 2138 at 13.) To the extent that Willens does not teach sending a temporarily assigned network address, RFC 2138 further states that a Framed-IP-Address "indicates the address to be configured for the user.... It MAY be used in an Access-Request packet as a hint by the NAS [network access server, i.e., the RADIUS client] to the [RADIUS] server that it would prefer that address." (RFC 2138 at 29.) A RADIUS User-Name is a "user ID." A Framed-IP-Address is an "assigned network address for the first user ID." It would be obvious to those of skill in the art that the Framed-IP-Address could be a temporarily assigned address since the address need only be valid for the duration of the dial-up networking session. When the user dials into the system again at a later time, the user may be assigned a different address.
[1.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	Willens teaches that the RADIUS server (the "authentication accounting server") accesses the user profiles 46 (the "database") to authenticate a user's identity by checking the provided password: When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by ***checking his password through RADIUS server 16, utilizing user profiles 46***. (Willens, 5:5-17.) After authenticating the user, the RADIUS server retrieves the user's filter identification and communicates the user's filter

Exhibit AA

US 6779118	Prior Art Analysis*
	("individualized rule set") to client software 44 on the communications server 14 (the "redirection server"): The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's authorization, the ***RADIUS server 16 supplies the filter identification*** through the RADIUS client 45 software along with the verification acknowledgment for the user 22 ***for use by client software 44*** for controlling access by the user 22 to Internet sites. (Willens, 5:5-17.) Willens further teaches that the client software 44 and communications server 14 apply the filter rules using a user's temporarily assigned network address: The ***source and destination addresses in the header packet are used to identify the user, allowing selection of the appropriate user filter***, and to identify the site for which the user desires access. An example source address identifying a user might be: 192.168.51.50 An example destination address identifying a site requested by the user might be: 172.16.3.4 The server 14 uses such addresses in packet headers for making decisions on the handing of IP packets, such as for firewall security. (Willens, 6:35-46.) Thus, Willens teaches that the client software 44 on communications server 14 uses the user's network address in applying the user's corresponding filter rules. To enable this functionality to work as described in Willens, it would have been obvious for the RADIUS server 16 to provide the user's temporarily assigned network address to the client software 44

Exhibit AA

US 6779118	**Prior Art Analysis***
	and communications server 14. And RFC 2138, describing the RADIUS communications protocol employed by the RADIUS server 16, provides a "Framed-IP-Address" that "indicates the address to be configured for the user." (RFC 2138 at 29.) In summary, Willens renders obvious "wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server."
[1.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	Willens discloses that the client software 44 on communications server 14 (the "redirection server") uses the user's filter "for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) Willens provides a specific example in which the communications server 14 processes a request from user Timmy for information from the site www.playboy.com using the user's individualized "F(Timmy)" filter: In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. The ***server 14 looks at each filter rule*** found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the ***server 14 either permits or denies access*** and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.

Exhibit AA

US 6779118	**Prior Art Analysis***
	(Willens, 5:60–6:9.) It is understood that the website "www.playboy.com" is a website on the Internet, a public network. Willens further discloses that the communications server 14 processes communications to and from a user's computer by applying the user's associated filter and blocking or allowing packets to be sent or received: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets to be sent and received*** by the network served by the communications server 14. (Willens, 6:10-15 (emphasis added).) In summary, Willens teaches "wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set."
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	Willens discloses that the client software 44 communications server 14 provides control over data to and from users' computers: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or drop ***packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of ***server 14 provides bidirectional (input/output) packet filtering*** for source and destination addresses, for protocol (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), IP, Internetwork Packet Exchange ("IPX") and port (Hypertext Transport Protocol

Exhibit AA

US 6779118	Prior Art Analysis*
	("http"), etc.). (Willens, 6:10-22.) The multiple packets sent and received by a user and filtered by the communications server 14 are a "plurality of data to and from the users' computers" as recited in the claim. And as analyzed above in portion [1.7], Willens teaches filtering packets using an individualized rule set, such as the filter "F(Timmy)" associated with the individual user "Timmy". Willens further discloses that the communications server 14 uses a set of user filters that are specific to each user: In addition to the site lists, the network access control server 18 maintains a set of user filters 54 which are used ***to control Internet access for each user***. In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. (Willens, 5:58-64.) The user filters used to control Internet access for each user are an "individualized rule set." In summary, Willens teaches "wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set," as recited in the claim.
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Willens discloses blocking data based on the user's filter: The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name

Exhibit AA

US 6779118	**Prior Art Analysis***
	"PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or ***denies access*** and updates it's local cache 50. In the event of denial of service, ***the server 14 sends a denial message back to user*** 22, informing him that he cannot access that site. (Willens, 5:64-6:9.) Willens further discloses blocking data to and from a user's computer by dropping packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to route or ***drop packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. (Willens, 6:10-16.) By dropping packets and denying access to the network, the communication server 14 "blocks the data to and from the users' computers." Thus, Willens teaches "wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set" as recited in the claim.
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Willens discloses allowing data based on the user's filter: The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name

Exhibit AA

US 6779118	Prior Art Analysis*
	> "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either ***permits*** or denies ***access*** and updates it's local cache 50. (Willens, 5:64-6:7.) Willens further discloses allowing data to and from a user's computer by routing packets: > In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking whether to ***route*** or drop ***packets to be sent and received*** by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. (Willens, 6:10-16.) By routing packets and allowing access to the network, the communication server 14 "allows the data to and from the users' computers." Thus, Willens teaches "wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set" as recited in the claim.
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	Willens discloses a communications server 14 that "either permits or denies access" to network resources. (Willens, 6:6.) More specifically, the communications server 14 includes client software 44 that receives the user's filter "for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) Willens provides a specific example in which user Timmy requests information from the site www.playboy.com: > In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the

Exhibit AA

US 6779118	Prior Art Analysis*
	local cache to determine if the request will be granted. The ***server 14 looks at each filter rule*** found in "F(Timmy)" starting from the top. When it reaches the rule permit "PTA List", the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the ***server 14 either permits or denies access*** and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site. (Willens, 5:60–6:9.) Willens further discloses that the communications server 14 applies the user's associated filter by allowing (routing) or blocking (dropping) packets: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets*** to be sent and received by the network served by the communications server 14. (Willens, 6:10-15 (emphasis added).) As analyzed above in portion [1.3], the client software 44 on the communications server 14 controls a user's access to network resources and is a "redirection server." The Admitted Prior Art teaches controlling access to resources by redirecting traffic, for example, World Wide Web traffic: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However,

Exhibit AA

US 6779118	**Prior Art Analysis***
	redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that in directing the user away from the website, the user's access to the website is blocked. Thus, redirection is an obvious extension of blocking and could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Requester notes that the Board made similar findings in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.) It would have been obvious to add the redirection feature known in the prior art to the packet filtering capabilities of Willens at least for the reasons given above. And as analyzed above in portion [1.7], Willens teaches filtering packets using an individualized rule set, such as the filter

Exhibit AA

US 6779118	Prior Art Analysis*
	"F(Timmy)" associated with the individual user "Timmy". Willens further discloses that the communications server 14 uses a set of user filters that are specific to each user: In addition to the site lists, the network access control server 18 maintains a set of user filters 54 which are used ***to control Internet access for each user***. In response to the user 22 request for access, assuming the appropriate entries are found in local cache 50, the server 14 applies the filter "F(Timmy)" 54 as a mask to the site list in the local cache to determine if the request will be granted. (Willens, 5:58-64.) The user filters used to control Internet access for each user are an "individualized rule set." See also the analysis of portions [1.3] and [2.0]. As analyzed in portion [2.0], Willens teaches applying an individualized filter to control data to and from a user's computer. And as analyzed in portion [1.3], the Admitted Prior Art teaches redirection. It would have been obvious to incorporate the redirection technique of the Admitted Prior Art into the system of Willens at least for the reasons given above, in portion [1.3], and in the Reasons to Combine. As shown in the analysis of portion [2.0], it would be obvious to perform the function on data both to and from the user's computer. Thus, Willens and the Admitted Prior Art render obvious "wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set."
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	The system of Willens is intended to be used for controlling users' access to the Internet, including the World Wide Web. (Willens, 1:51-54.) Those of skill in the art would have recognized that the Internet and World Wide Web include numerous potential destinations. Willens further teaches that each user may have multiple rules used to specify access restrictions. (Willens, 5:58-60.)

Exhibit AA

US 6779118	**Prior Art Analysis**[*]
	Thus, it would have been obvious that packets may be redirected to multiple destinations.
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	Willens teaches centralizing users' individualized filters and associated filter lists to ease the administrative burden: If not, the client software 44 sends a lookup request to the network access server 18, which ***stores the centralized permitted site list*** and the filters to be used as masks for checking access classifications of requested sites, to download the filter "F(Timmy)", which is maintained in the server 14 memory for the rest of the user 22's session. The client software 44 also keeps the local cache 50 of recently requested sites and recently used user filters for efficiency. This list includes both sites for which access was recently permitted, such as whitehouse.gov as well as sites for which access was recently denied, such as playboy.com. (Willens, 5:21-31, emphasis added.) Willens further provides an example scenario in which a user's filter includes a rule that refers to a specific permitted site list, the "PTA List": The server 14 looks at each filter rule found in "F(Timmy)" starting from the top. When it reaches the ***rule permit "PTA List"***, the server 14 looks into its local cache 50 to see if www.playboy.com is on the PTA List. If not, the server 14 sends a filter look-up request to the server 18. This look-up contains the list name "PTA List" and the site Timmy is trying to access (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and updates it's local cache 50. In the event of denial of service, the server 14 sends a denial message back to user 22, informing him that he cannot access that site.

Exhibit AA

US 6779118	**Prior Art Analysis***
	(Willens, 5:64-6:9.) Thus, Willens teaches that the filter "F(Timmy)" refers to the centralized list "PTA List." It would have been obvious that other users' filters could similarly refer to this list. For example, one of ordinary skill in the art would understand that a PTA List in this context refers to a list of websites reviewed by the school's Parent Teacher Association. Thus, it would have been obvious to associate this filter list with the user IDs for all students in the school. The centralized permit site list, such as the example "PTA List," is a common individualized rule set to which the users' filters, and thus their user IDs, are correlated. In summary, Willens renders obvious "wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set."
[8.0] In a system comprising	See analysis of portion [1.0].
[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[8.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portion [1.3].
[8.4] the method comprising the steps of:	Willens discloses "a method of controlling a user's access to a network." (Willens, 10:31-32.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the	See analysis of portion [1.5].

Exhibit AA

US 6779118	Prior Art Analysis*
dial-up network server to the authentication accounting server;	
[8.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[9.0] The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]
[10.0] The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0]
[11.0] The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0]
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0]
[13.0] The method of claim 8, further including the step of redirecting the data from	See analysis of portion [6.0].

Exhibit AA

US 6779118	Prior Art Analysis*
the users' computers to multiple destinations a function of the individualized rule set.	
[14.0] The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0]. And as analyzed in portion [1.1], Willens teaches a database with entries for plurality of user IDs. In view of Willens' teaching of a database having user ID entries, it would have been obvious to create a plurality of user ID entries in the database.
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portions [1.1] and [1.7]. Willens discloses that "Firewall filters are defined as an explicit set of rules based on either ***permit or deny syntax***." (Willens, 6:15-16.) The permit and deny actions are "a plurality of functions used to control passing between the user and a public network."
[16.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [1.6]. Willens discloses that the communications server 14 (with its client software 44, the "redirection server") communicates with ChoiceNet server 18 to automatically update the list of permitted sites used to control users' access: Installed on one of several supported UNIX platforms, the ChoiceNet server 18 software provides lookups of sites for the server 14 or routers 24, 32 or 34 against a list of permitted sites. The ***server software also automatically maintains the permit list*** by downloading updated versions of the list over the Internet and compiling the list for use by the client software 42. As a result of this self maintenance capability, the server 18 requires minimal administrative attention.

Exhibit AA

US 6779118	Prior Art Analysis*
	(Willens, 5:38-45.) Willens further discloses that the "server based permit list that can be ***easily updated on a daily or hourly basis***." (Willens, 4:42-44.) The permit list of allowed destination sites is "at least a portion of the rule set" for a user. For example, as shown in the analysis of portion [1.7], the example permitted site list "PTA List" is used to control access for user Timmy. By working in conjunction with, and relying upon, ChoiceNet server 18 to automatically maintain the list of permitted sites, the communications server 14 is "configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address."
[16.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	Willens discloses modifying the list of sites a user is permitted to access as a function of time: Finally, instead of trying to maintain an unwieldy list of deny keywords on every desktop, the subsystem 12 provides for a central, server based ***permit list that can be easily updated on a daily or hourly basis***, and that cannot be tampered with by the end users. (Willens, 4:40-45.) Updating the permit list on a daily or hourly basis teaches modifying a rule set as a function of time. Willens also teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password: ***When user 22 logs in through the communications server 14***, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's

Exhibit AA

US 6779118	Prior Art Analysis
	authorization, the RADIUS server 16 ***supplies the filter identification*** through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 ***for controlling access by the user*** 22 to Internet sites. (Willens, 5:8-18, emphasis added.) Thus, Willens teaches that the filtering rules are updated when the user accesses the login location of the communications server 14. The user's password is "data transmitted to or from the user." As support for this interpretation of the claim, note that the Patent Owner asserts that a user's login information is "data transmitted to or from the user." (*See* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 57.) Willens further teaches updating a local cache of filtering rules based on a location the user accesses: This look-up contains the list name "PTA List" and ***the site Timmy is trying to access*** (www.playboy.com). The server 18 searches list 52 and sends back the result. Based on the result, the server 14 either permits or denies access and ***updates it's local cache 50***. (Willens, 6:2-7, emphasis added.) The site the user Timmy is trying to access is a "location" as recited in the claim. The update to the communications server 14's local cache of filtering rules teaches "modification of at least a portion of the rule set" as recited in the claim. Furthermore, blocking a website based on some combination of the recited bases—time, data transmitted to or from the user, or location the user accesses—would have been obvious to one of skill in the art. For example, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work. Similarly in a school environment, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between

Exhibit AA

US 6779118	Prior Art Analysis*
	the user and the website or after discovering the user spends excessive time at the site unrelated to school. Thus, although an initial rule set might be permissive, it would be obvious to modify the rules for a particular user at a later time after it is found that the user's data transmissions or locations accessed are unproductive or inappropriate. Thus, Willens renders obvious "modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access" as recited in the claim. Accordingly, Requester has provided an independent explanation of the pertinence and manner of applying the prior art to this claim limitation. Requester notes that the Board similarly found that this limitation would have been obvious to one of skill in the art. (*See* Board Decision at 10.)
[16.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portion [16.4]. Willens discloses updating a list of permitted sites on a daily or hourly basis. Thus, Willens discloses modifying a portion of the rule set as a function of time.
[17.0] A system comprising:	See analysis of portion [1.0].
[17.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[17.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[17.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].

Exhibit AA

US 6779118	Prior Art Analysis*
[17.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[17.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4]. Willens discloses updating rules used to control access based on a user's profile and filters when a user logs into the communications server 14: When user 22 logs in through the communications server 14, the RADIUS client software 45 first determines if user 22 is authorized by checking his password through RADIUS server 16, utilizing user profiles 46. The user profiles 46 also identify a filter "F(Timmy)" in his user profile 46. After checking user 22's authorization, the RADIUS server 16 supplies the filter identification through the RADIUS client 45 software along with the verification acknowledgment for the user 22 for use by client software 44 for controlling access by the user 22 to Internet sites. The client software 44 then checks to see if the filter "F(Timmy)" is stored locally in cache 50. If it is, the client software 44 uses it for controlling access. (Willens, 5:9-21.) It is understood that when a user logs into the communications server 14, data is transmitted from the user. For example, Willens discloses that "If multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests." (Willens, 6:52-55.) The login information is "data transmitted to or from the user." Thus, Willens renders obvious "modification of at least a portion of the rule set as a function of the data transmitted to or from the user" as recited in the claim.

Exhibit AA

US 6779118	Prior Art Analysis*
[18.0] A system comprising:	See analysis of portion [1.0].
[18.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[18.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[18.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[18.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[18.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4]. As shown there, Willens teaches modifying a user's filtering rules based on a user's accessing of a login location and providing login information, such as a password. Willens further teaches updating a local cache of filtering rules based on a location the user accesses.
[19.0] A system comprising:	See analysis of portion [1.0].
[19.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].

Exhibit AA

US 6779118	Prior Art Analysis*
[19.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[19.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[19.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[19.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[20.0] A system comprising:	See analysis of portion [1.0].
[20.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[20.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[20.3] wherein the redirection server is	See analysis of portion [16.3].

Exhibit AA

US 6779118	Prior Art Analysis
configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	
[20.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[20.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].
[21.0] A system comprising:	See analysis of portion [1.0].
[21.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[21.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[21.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].

Exhibit AA

US 6779118	Prior Art Analysis*
[21.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[21.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[22.0] A system comprising:	See analysis of portion [1.0].
[22.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[22.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[22.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[22.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some	See analysis of portion [16.4].

Exhibit AA

US 6779118	Prior Art Analysis*
combination of time, data transmitted to or from the user, or location the user accesses; and	
[22.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[23.0] A system comprising:	See analysis of portion [1.0].
[23.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[23.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[23.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[23.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].

Exhibit AA

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td>[23.5] wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.</td><td>

Willens illustrates the recited network architecture in Fig. 1. The communications server 14 (with its client software 44, the "redirection server") has a "user side" that connects to a remote user's computer 22 and a "network side" that connects to the network backbone 20. The remote user's computer 22 connects to the network backbone 20 through the communications server 14.

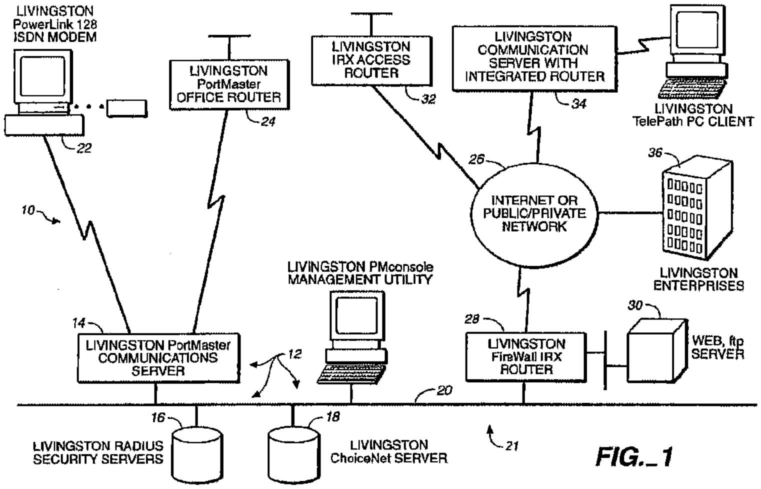

LIVINGSTON PowerLink 128 ISDN MODEM
LIVINGSTON PortMaster OFFICE ROUTER
LIVINGSTON IRX ACCESS ROUTER
LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER
LIVINGSTON TelePath PC CLIENT
22
24
32
34
26
36
10
INTERNET OR PUBLIC/PRIVATE NETWORK
LIVINGSTON ENTERPRISES
LIVINGSTON PMconsole MANAGEMENT UTILITY
14
28
30
LIVINGSTON PortMaster COMMUNICATIONS SERVER
12
LIVINGSTON FireWall IRX ROUTER
WEB, ftp SERVER
20
16
18
LIVINGSTON RADIUS SECURITY SERVERS
LIVINGSTON ChoiceNet SERVER
21

FIG._1

WILLENS FIG. 1

Alternatively, considering the router 24 as the "dial-up network server," Fig. 1 illustrates that the communications server 14 has a "user side" (top) that is connected to the router 24 and a "network side" (bottom) that is connected to the network 20 and Internet 26.

Willens further illustrates in Fig. 2 that the access control architecture includes a RADIUS client on one side ("user side") and the firewall filtering on the other side ("network side"):

> As represented in FIG. 2, the access control subsystem 12 incorporates integrated software modules 38, 40 and 42, respectively comprising the RADIUS module, the network access module, and the firewall filtering module in security systems software 43.

(Willens, 4:12-16.)

</td></tr>
</table>

Exhibit AA

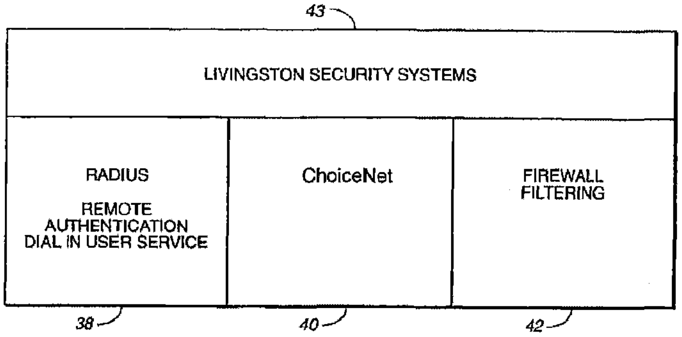
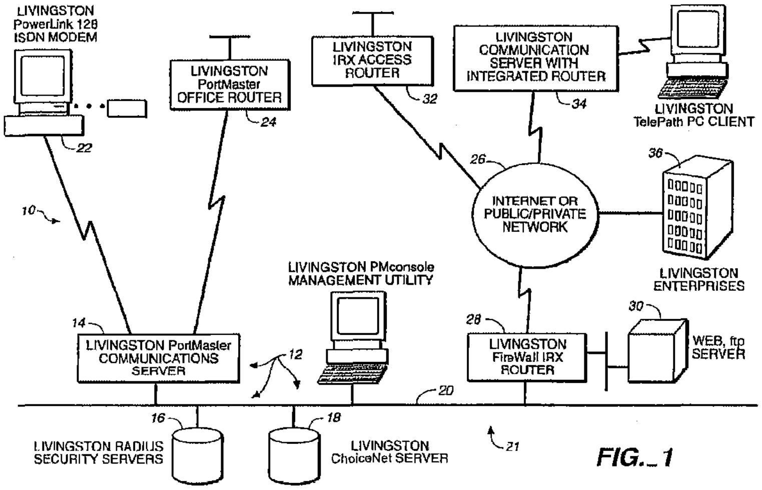
US 6779118	Prior Art Analysis*
	 43 LIVINGSTON SECURITY SYSTEMS RADIUS REMOTE AUTHENTICATION DIAL IN USER SERVICE ChoiceNet FIREWALL FILTERING 38 40 42 WILLENS FIG. 2 Willens also discloses that a user's computer receives a temporarily assigned IP address that is used for communication with the network. See analysis of portion [1.5].
[24.0] The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	As analyzed in portion [16.3], Willens teaches that the communications server 14 (together with its client software 44, the "redirection server") communicates with ChoiceNet server 18 to automatically update the list of permitted sites used to control users' access. As illustrated in Fig. 3, the communications server 14 communicates with the ChoiceNet server 18 via network backbone 20. Thus, Willens teaches that the instructions to modify a user's individualized filter profile are received by the communications server 14 on a network side.  LIVINGSTON PowerLink 128 ISDN MODEM 22 10 LIVINGSTON PortMaster OFFICE ROUTER 24 LIVINGSTON IRX ACCESS ROUTER 32 LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER 34 LIVINGSTON TelePath PC CLIENT 26 INTERNET OR PUBLIC/PRIVATE NETWORK 36 LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 14 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 28 LIVINGSTON FireWall IRX ROUTER 30 WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 FIG._1 WILLENS FIG. 1

Exhibit AA

US 6779118	Prior Art Analysis*
	In summary, Willens renders obvious "wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server" as recited in the claim.
[25.0] In a system comprising	See analysis of portion [1.0].
[25.1] a redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portion [1.3] and [1.5].
[25.2] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.2].
[25.3] the method comprising the step of:	See analysis of portion [8.4].
[25.4] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	Willens teaches that when a user requests access to a network site that is not in the client software 44's local cache 50, the request is initially denied while the data needed to further evaluate the request is obtained: When a request for access is made by the user for which a determination cannot be made using the local cache 50, ***the server 14 drops the packet making the request to allow time for access and response from the server 18***. Since drops are common on the Internet, the packet making the request is retransmitted a number of times before the request times out, typically at 30 seconds or so. The source and destination addresses in the header packet are used to identify the user, ***allowing selection of the appropriate user filter***, and to identify the site for which the user desires access. An example source address identifying a user might be: 192.168.51.50 An example destination address identifying a site requested by the user might be:

Exhibit AA

US 6779118	**Prior Art Analysis***
	172.16.3.4 ***The server 14 uses such addresses in packet headers for making decisions on the handing of IP packets***, such as for firewall security. Little additional overhead at the server is required to use these addresses for the purposes of identifying user filters and sites for determining site access in this system and process. If a particular source address represents a node that is associated with a single user who has no access restriction, then no further checking is required and no user filter need be employed. If multiple users are associated with a particular address node, then login information is used to determine which user filter should be applied for access requests. (Willens, 6:29-55, emphasis added.) Thus, Willens discusses using the user's network address to make decisions on the handling of access requests. Willens teaches that the applied user-specific filter is modified by loading further details about the appropriate user filter from the ChoiceNet server 18 while the user's network address remains the same. Thus, Willens renders obvious "modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server" as recited in the claim.
[25.5] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.5].
[25.6] wherein the computer	See analysis of portion [23.5].

Exhibit AA

US 6779118	Prior Art Analysis*
using the temporarily assigned network address is connected to the computer network through the redirection server and	
[25.7] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[26.0] The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[27.0] The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4]. Willens teaches that a list of allowed network sites can "can be easily updated on a daily or hourly basis." (Willens, 4:43-44.) It would have been obvious that updating the list would involve removing or adding sites, which teaches "removing or reinstating at least a portion of the user's rule set." Thus Willens renders obvious "removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses" as recited in the claim.
[28.0] The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	Willens teaches that the filter rules are defined based in part on a specific protocol and port communicating over Internet Protocol (IP): In practice, the access control system and process is implemented using an extension of the ***Internet Protocol (IP) firewall packet filtering*** employed

Exhibit AA

US 6779118	Prior Art Analysis*
	by the communications server 14 for checking whether to route or drop packets to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) packet filtering for source and destination addresses, ***for protocol*** (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), ***IP***, Internetwork Packet Exchange ("IPX") ***and port*** (Hypertext Transport Protocol ("http"), etc.). (Willens at 6:10-22, emphasis added.) Defining filters based on a protocol and a port render obvious a "rule [included] as a function of a type of IP (Internet Protocol) server" as recited in the claim.
[29.0] The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	Willens teaches applying an initial temporary filter that drops a user's packet to allow time for Willens' system to evaluate whether to permit the requested access: When a request for access is made by the user for which a determination cannot be made using the local cache 50, ***the server 14 drops the packet making the request to allow time for access and response from the server 18***. Since drops are common on the Internet, the packet making the request is retransmitted a number of times before the request times out, typically at 30 seconds or so. The source and destination addresses in the header packet are used to identify the user, allowing ***selection of the appropriate user filter***, and to identify the site for which the user desires access. (Willens, 6:29-38, emphasis added.) Dropping the first packet of a new access request—thereby temporarily denying access—is an "initial temporary rule set." The appropriate user filter is a "standard rule set."

Exhibit AA

US 6779118	Prior Art Analysis*
	Thus, Willens renders obvious "wherein the individualized rule set includes an initial temporary rule set and a standard rule set" as recited in the claim.
[29.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	As analyzed in portion [29.0], Willens teaches applying an initial filter to deny an access request until the appropriate user filter can be loaded and used to evaluate the access request. (Willens, 6:29-38.) Thus, Willens teaches using the initial filter until the appropriate user filter is consulted, after which the appropriate user filter is used. Thus, Willens renders obvious "wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set" as recited in the claim.
[30.0] The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	Willens teaches filtering rules that allow access, by routing packets, based on a destination address, protocol, and port: In practice, the access control system and process is implemented using an extension of the Internet Protocol (IP) firewall packet filtering employed by the communications server 14 for checking ***whether to route or drop packets*** to be sent and received by the network served by the communications server 14. Firewall filters are defined as an explicit set of rules based on either permit or deny syntax. The firewall filtering of server 14 provides bidirectional (input/output) ***packet filtering for source and destination addresses***, ***for protocol*** (Transport Layer Protocol("TCP"), User Datagram Protocol ("UDP"), IP, Internetwork Packet Exchange ("IPX") ***and port*** (Hypertext Transport Protocol ("http"), etc.). (Willens at 6:10-22, emphasis added.) Filtering rules based on a destination address, protocol, and port renders obvious "at least one rule allowing access based on a request type and a destination address" as recited in the claim.
[31.0] The system of claim 1, wherein the	As analyzed in portion [30.0], Willens renders obvious controlling access using a rule based on a request type and a

Exhibit AA

US 6779118	Prior Art Analysis*
individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	destination address. And as analyzed in portion [1.3], Willens and the Admitted Prior Art render obvious redirecting a user's network traffic. Thus, Willens and the Admitted Prior Art render obvious "at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address" as recited in the claim.
[32.0] The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[33.0] The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[33.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[34.0] The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[35.0] The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[36.0] A system comprising:	See analysis of portion [1.0].

Exhibit AA

US 6779118	**Prior Art Analysis***
[36.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[36.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[36.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[36.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[36.5] wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[37.0] A system comprising:	See analysis of portion [1.0].
[37.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[37.2] wherein the rule set contains at least one of a plurality of functions used to control passing between	See analysis of portion [16.2].

Exhibit AA

US 6779118	Prior Art Analysis*
the user and a public network;	
[37.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[37.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[37.5] wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[37.6] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[38.0] A system comprising:	See analysis of portion [1.0].
[38.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[38.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[38.3] wherein the	See analysis of portion [16.3].

Exhibit AA

US 6779118	Prior Art Analysis*
redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	
[38.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[38.5] wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[39.0] A system comprising:	See analysis of portion [1.0].
[39.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[39.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[39.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[39.4] wherein the redirection server is	See analysis of portion [16.4].

Exhibit AA

US 6779118	Prior Art Analysis*
configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[39.5] wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[40.0] The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[41.0] The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set,	See analysis of portion [29.0].
[42.0] The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[43.0] The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[44.0] A system comprising:	See analysis of portion [1.0].
[44.1] a database with entries correlating each of a plurality of user IDs with an	See analysis of portion [1.1].

Exhibit AA

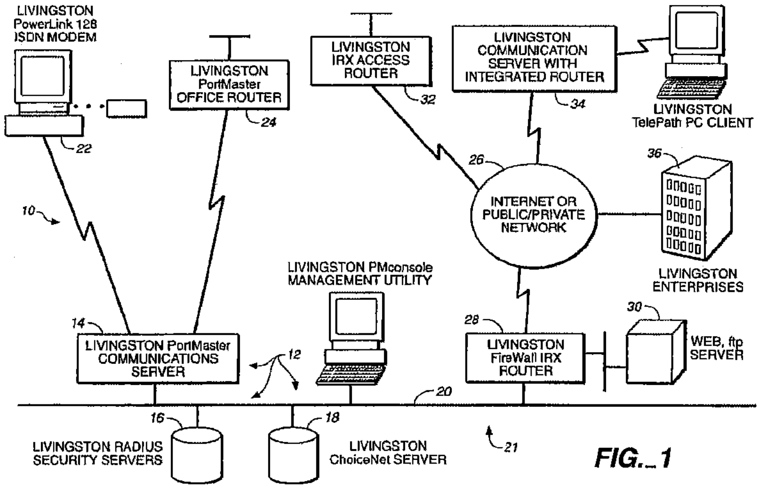
US 6779118	**Prior Art Analysis***
individualized rule set;	
[44.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[44.3] a redirection server connected between the dial-up network server and a public network, and	As analyzed in portion [1.3], Willens teaches client software 44 on communications server 14. The Admitted Prior Art teaches redirection as one technique for blocking a user's access to a network destination. Thus, Willens and the Admitted Prior Art render obvious providing a "redirection server." And as analyzed in portion [1.2], Willens teaches that a user may connect via local area network (LAN) router 24. The Patent Owner asserts that a router is a "dial-up network server." (*See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9.) And as analyzed in portion [1.2], Willens also teaches that a user may connect via dial-up modem to RADIUS client software 45 on communications server 14, which is a "dial-up network server." Willens illustrates these components in Fig. 1, which shows that the communications server 14 is between the LAN router 24 and the public Internet 26, and between the dial-up connection from computer 22 and the public Internet 26:  LIVINGSTON PowerLink 128 ISDN MODEM LIVINGSTON PortMaster OFFICE ROUTER LIVINGSTON IRX ACCESS ROUTER LIVINGSTON COMMUNICATION SERVER WITH INTEGRATED ROUTER LIVINGSTON TelePath PC CLIENT 22 24 32 34 26 36 10 INTERNET OR PUBLIC/PRIVATE NETWORK LIVINGSTON ENTERPRISES LIVINGSTON PMconsole MANAGEMENT UTILITY 14 LIVINGSTON PortMaster COMMUNICATIONS SERVER 12 28 LIVINGSTON FireWall IRX ROUTER 30 WEB, ftp SERVER 20 16 18 LIVINGSTON RADIUS SECURITY SERVERS LIVINGSTON ChoiceNet SERVER 21 FIG._1 WILLENS FIG. 1 And while Willens teaches a communications server 14 that includes both client software 44 (providing access control) and

Exhibit AA

US 6779118	Prior Art Analysis*
	RADIUS client software 45 (providing dial-up communication services), it would have been obvious that if these functions were separated into two distinct servers, the client software 44 should be located between the RADIUS client software 45 and the public Internet network. Willens specifically teaches that "client software 44 [is] for controlling access by the user 22 to Internet sites." (Willens, 5:17-18.) To perform this function, the client software 45 must be on the data path between the user and the Internet. Thus, Willens and the Admitted Prior Art render obvious "a redirection server connected between the dial-up network server and a public network" as recited in the claim.
[44.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	See analysis of portion [1.4].
[44.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	See analysis of portion [1.5].
[44.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	See analysis of portion [1.6].
[44.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	See analysis of portion [1.7].

Exhibit AA

US 6779118	Prior Art Analysis*
[45.0] The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0].
[46.0] The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[47.0] The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[48.0] The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0].
[49.0] The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	See analysis of portion [6.0].
[50.0] The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	See analysis of portion [7.0].
[51.0] The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].

Exhibit AA

US 6779118	Prior Art Analysis*
[52.0] The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[52.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[53.0] The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[54.0] The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.1].
[55.0] The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above with respect to claim 44 (and citing to claim 1) that the prior art teaches blocking and redirection as a function of an individualized rule set. The Admitted Prior Art teaches controlling access to resources by redirecting World Wide Web traffic but notes that the same technique can be applied to any IP (Internet protocol) service: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, ***redirection is not limited to WWW traffic, and the concept is valid for all IP services***. To illustrate how redirection is accomplished,

Exhibit AA

US 6779118	Prior Art Analysis*
	consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60 (emphasis added).) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that redirection could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Thus, it would have been obvious to redirect a user's request by "replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set" as recited in the claim. Requester notes that the Board found a similar claim limitation to be obvious in view of the Admitted Prior Art in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.)
[56.0] In a system comprising	See analysis of portion [1.0].
[56.1] a database with entries correlating each of a	See analysis of portion [1.1].

Exhibit AA

US 6779118	Prior Art Analysis*
plurality of user IDs with an individualized rule set;	
[56.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[56.3] a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portions [1.3] and [44.3].
[56.4] the method comprising the steps of:	See analysis of portion [8.4].
[56.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[56.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[56.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[57.0] The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the	See analysis of portion [2.0].

Exhibit AA

US 6779118	Prior Art Analysis*
individualized rule set.	
[58.0] The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[59.0] The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[60.0] The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0].
[61.0] The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[62.0] The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDS, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[63.0] The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[64.0] The method of claim 56, wherein the individualized rule set	See analysis of portion [29.0].

Exhibit AA

US 6779118	Prior Art Analysis
includes an initial temporary rule set and a standard rule set, and	
[64.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[65.0] The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[66.0] The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[67.0] The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	See analysis of portion [55.0].
[68.0] A system comprising:	See analysis of portion [1.0].
[68.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[68.2] the redirection server programmed with a user's	See analysis of portions [1.3] and [1.6].

Exhibit AA

US 6779118	Prior Art Analysis*
rule set correlated to a temporarily assigned network address;	
[68.3] wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [16.2].
[68.4] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and	See analysis of portion [16.3].
[68.5] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.	See analysis of portion [16.4].
[69.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[70.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].
[71.0] The system of claim 68, wherein the redirection server is configured to allow	See analysis of portions [16.4] and [18.5].

Exhibit AA

US 6779118	Prior Art Analysis*
modification of at least a portion of the rule set as a function of the location or locations the user accesses.	
[72.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[73.0] The system of claim 68, wherein the redirection sewer is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [17.5].
[74.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[75.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.4], [18.5] and [22.5].
[76.0] The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side	See analysis of portion [23.5].

Exhibit AA

US 6779118	Prior Art Analysis*
connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	
[77.0] The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[78.0] The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[79.0] The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[79.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set	See analysis of portion [29.1].
[80.0] The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[81.0] The system of claim 68, wherein the modified rule set includes at least one	See analysis of portion [31.0].

Exhibit AA

US 6779118	Prior Art Analysis*
rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[82.0] The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.	See analysis of portion [55.0].
[83.0] In a system comprising	See analysis of portion [1.0].
[83.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[83.2] the redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portions [1.3] and [1.6].
[83.3] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.1].
[83.4] the method comprising the step of:	See analysis of portion [8.4].
[83.5] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	See analysis of portion [25.4].
[83.6] and wherein the redirection server has a user	See analysis of portion [23.0].

Exhibit AA

US 6779118	Prior Art Analysis*
side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	
[83.7] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.0].
[83.8] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[84.0] The method of claim 83, further including; the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[85.0] The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[86.0] The method of claim	See analysis of portion [28.0].

Exhibit AA

US 6779118	Prior Art Analysis*
83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service,	
[87.0] The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[87.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[88.0] The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[89.0] The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[90.0] The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.	See analysis of portion [55.0].

Exhibit BB

Claim Charts with respect to Radia for Obviousness

Exhibit BB

Contents

References
Radia (Exhibit E, U.S. 5848233)
Wong '727 (Exhibit F, U.S. 5835727)
Stockwell (Exhibit G, U.S. 5950195)
Wong '178 (Exhibit H, U.S. 6073178)
Admitted Prior Art

Requester provides canceled claims 1, 8, and 25 in the claim chart below because other claims depend from those canceled claims or include the same features as those canceled claims. Requester does not propose new rejections for canceled claims 1, 8, and 25.

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Exhibit BB

Proposed Rejection #3. Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Stockwell under 35 U.S.C. § 103(a).

Reasons to combine Radia, Wong '727, and Stockwell

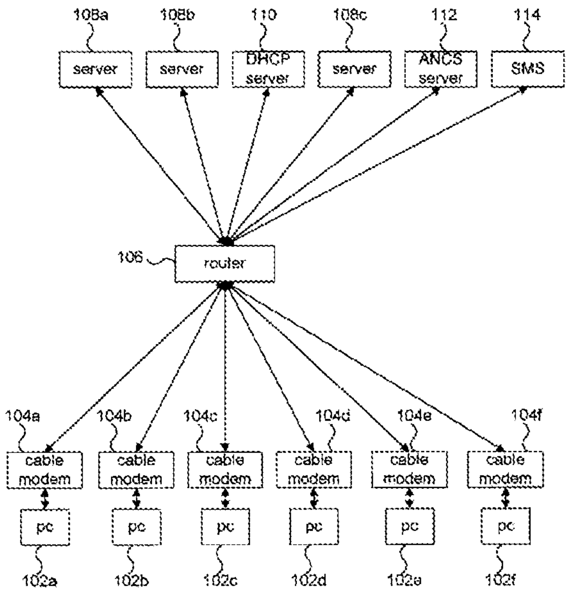
A description of Radia is provided in the accompanying Request for Reexamination and will not be repeated here. Radia and Wong '727 share overlapping inventors, mutually incorporate one another by reference, and describe the same or similar system. Thus, these references include an express teaching that their disclosures should be combined. It would have been obvious to one of skill in the art to do so.

Radia discloses applying individualized filtering rules to multiple users. Wong '727 illustrates in Fig. 7 that a filtering profile database includes a plurality of user IDs, and each user ID is correlated with a set of profile IDs that define filtering rules. In addition to the express reasons to combine given above, it would also be obvious to include a filtering database organized in the manner described by Wong '727 in the system of Radia in order to provide a way to store and access the filtering profiles for the multiple users. Also, modifying Radia according to the teaching of Wong '727 to provide the organized filtering database is a "use of known technique to improve similar devices (methods, or products) in the same way." (*See* MPEP § 2143, *citing KSR International Co. v. Teleflex Inc.*, 550 U.S. ____, ____, 82 USPQ2d 1385, 1396 (2007).)

Radia and Stockwell are both directed to providing a configurable network device that provides IP packet filtering. Stockwell includes a teaching that a network device, such as a firewall, can redirect a communication to an alternate destination. It would have been obvious to incorporate this redirection feature into the packet filters of Radia. The redirection feature would improve a similar device (the filtering capabilities of Radia) in the same way. (*See* MPEP § 2143, *citing KSR.*) The combination is also obvious because it requires only applying a known technique (redirection) to a known device (the packet filters of Radia) to yield predictable results (a packet filter with the ability to redirect packets). (*See* MPEP § 2143, *citing KSR.*) Radia teaches blocking, and it would be obvious to extend blocking to include Stockwell's redirecting feature.

Furthermore, redirection is an obvious extension of the use of a control to block a user. Radia and Wong'727 teach blocking, and it would be obvious to extend blocking to include Stockwell's redirecting function. Requester notes that the Board of Patent Appeals and Interferences (BPAI) explicitly reached essentially the same conclusion with respect to the '118 patent in the previous reexamination. (*See Ex Parte Linksmart Wireless Technology, LLC*, Appeal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011).)

Exhibit BB

US 6779118	Prior Art Analysis[*]
[1.0] A system comprising:	Radia illustrates a computer network in Fig. 1. The computer network is a system.  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1
[1.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia discloses a "filtering profile database" that includes a profile ID and filtering rules: The ***filtering profile database*** 316 of SMS 114 ***includes a set of filtering profiles*** of the type shown in FIG. 4 and generally designated 400. Filtering profile 400 ***includes a profile id*** 402 ***and a series of filtering rules***, of which filtering rules 404a through 404c are representative. The profile id 402 is used by SMS 114 and ANCS 112 as an internal identifier for the filtering profile 400. (Radia, 6:5-11.) And Radia incorporates by reference U.S. App. 08/762,393, now

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit BB

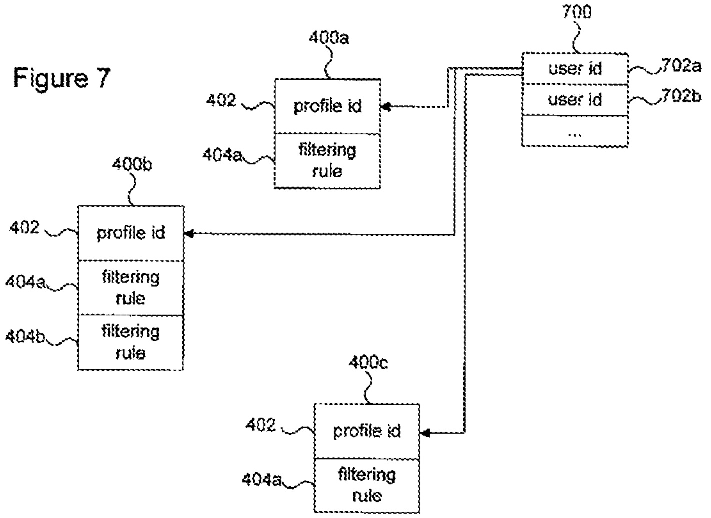
US 6779118	Prior Art Analysis*
	U.S. 5,835,727 to Wong. (Radia, 1:12-16.) Wong '727 illustrates in Fig. 7 that the filtering profile database includes a plurality of user IDs, and each user ID is correlated with a set of profile IDs that define filtering rules:  Figure 7 700 user id 702a user id 702b ... 400a 402 profile id 404a filtering rule 400b 402 profile id 404a filtering rule 404b filtering rule 400c 402 profile id 404a filtering rule WONG '727 FIG. 7 Wong '727 further discloses that "an index 700 is shown for filtering profile database. Index 700 has one entry 702 for each network user." (Wong '727, 6:50-51.) The filter profile database is a "database." The user ID entries 702 are "entries correlating each of a plurality of user IDs," and the group of filtering rules associated with each user ID is an "individualized rule set."
[1.2] a dial-up network server that receives user IDs from users' computers;	Radia discloses a cable modem 104 and cable router 106, illustrated in Fig. 1, that connect a client system (computer) 102 to a network.

Exhibit BB

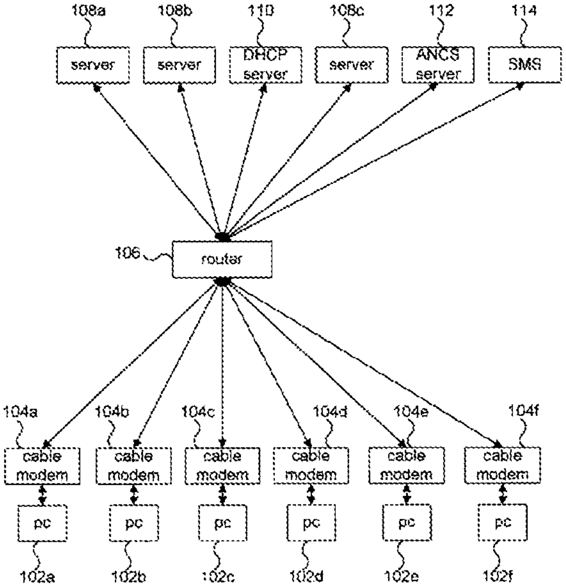
US 6779118	Prior Art Analysis*
	 108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 The cable modem of Radia is a "dial-up network server." As evidence that the above analysis comports with the broadest reasonable interpretation of the claims, it is noted that the '118 patent states that "The dial-up network server 102 is used to establish a communications link with the user's PC using a standard communications protocol." ('118 Patent, 3:60-63.) The '118 Patent further describes a dial-up network server as providing a network connection for a computer through a "modem, … local area network (LAN), or other communications link." ('118 Patent, 3:57-60.) Also, with respect to the '118 patent, a federal court understood a dial-up network server to be any "server that is used to establish a communications link with the user's PC." (Claim Construction order at 13.) Thus, the cable modem of Radia discloses a dial-up network server. Alternatively, the router 106 may be the claimed "dial-up network server." The Patent Owner has asserted that a router is a "dial-up network server." *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9. Furthermore, it is suggested that both the cable modem 104 and the router 106 receive the user IDs from user computers. For instance, Wong '727 states: Network users login to the network using one of the

Exhibit BB

US 6779118	Prior Art Analysis*
	client systems as a host. As part of the login process, the SMS authenticates the user using a password or other authentication method. Subsequently, the SMS locates the user's filtering profile sequence. (Wong '727 at 2:50-54.) According to Wong '727, the user logs in at the user computer and provides a password or other authentication method. A user ID is a type of authentication method. The user's ID is received by the SMS 114 (see Fig. 1 above) via the cable modem and router.
[1.3] a redirection server connected to the dial-up network server and a public network, and	The '118 patent describes a redirection server as a server that "controls the user's access to the network" by "checking data packets and blocking or allowing the packets as a function of the rule sets." ('118 Patent, 4:51-52 and 63-65.) Radia discloses an "access network control server (ANCS)" that configures a router to enforce the packet filter (Radia, 5: 42-43): In step 604, the ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 ***to establish a packet filter*** for IP packets originating from the client system 102b. For example, in some cases the packet filter may be established by reconfiguring the modem 104b connected to client system 102. Alternatively, ***the packet filter may be established by reconfiguring router*** 106. (Radia, 6:66 –7:2.) Radia further discloses that "the packet filter uses the rules of the login filtering profile sequence to selectively ***forward or discard IP packets*** originating from the client system." (Radia, 3:18-20.) By implementing the packet filter, the router controls a user's access to the network. Thus, the router and the ANCS together form a "redirection server." Regarding the interpretation of the router as teaching both the "dial-up network server" and "redirection server" limitations, the Patent Owner has stated that the claimed dial-up network server and the redirection server may be the same device. *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9 ("For

Exhibit BB

US 6779118	Prior Art Analysis*
	example, the network server can be the router running the SSG or ISG software.") and at 18 ("In these configurations, the SSG is the redirection server."). Under one interpretation of the claim language, the redirection server must be capable of redirection. (*See* BPAI Decision at 5.) Stockwell discloses filtering rules for redirecting IP communications: > This rule intercepts all incoming connections that go [sic] the external side of the local Sidewinder (192.168.1.192) and ***redirects them to shade.sctc.com*** (172.17.192.48). (Stockwell, 2:29-31.) It would have been obvious to add the redirection feature of Stockwell to the packet filtering capabilities of Radia at least for the reasons given above in the Reasons to Combine.
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	Radia discloses a "services management system (SMS)." (Radia, 5:43-44.) The SMS acts as a "login server." (Radia, 8:51-53.) > Method 900 begins with step 906 where ***SMS 114 waits for a user login***. More specifically, as discussed with regard to method 700, for a preferred embodiment of network 100, users login to network 100 using a login applet that communicates with a ***login server, such as SMS*** 114. (Radia, 9:37-42.) Wong '727 states that "As part of the login process, the ***SMS authenticates the user*** using a password or other authentication method." (Wong '727, 2:51-53.) The services management system (SMS) is an "authentication accounting server." Radia illustrates an example SMS in Fig. 3. The filtering profile database is incorporated into the SMS, and thus the SMS is "connected to the database" as recited in the claim: > SMS 114 is shown in more detail in FIG. 3 to include

Exhibit BB

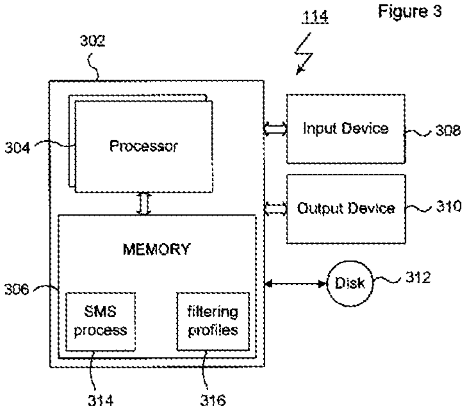
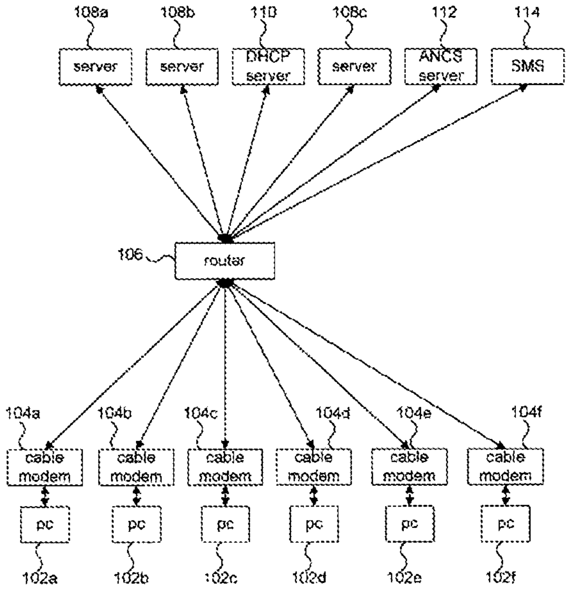
US 6779118	Prior Art Analysis*
	a computer system 302 that, in turn, includes a processor, or processors 304, and a memory 306.... An SMS process 314 and a ***filtering profile database 316 are shown to be resident in memory 306*** of computer system 302. (Radia, 5:56-65.)  114 Figure 3 302 304 Processor MEMORY 306 SMS process filtering profiles 314 316 Input Device 308 Output Device 310 Disk 312 RADIA FIG. 3 Radia further illustrates in Fig. 1 that the SMS is connected to the router ("redirection server") and (through the router) to the cable modems ("dial-up network server"):  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1

Exhibit BB

US 6779118	Prior Art Analysis*
[1.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	Radia discloses that "user logins are handled by downloading small, specifically tailored applications, known as 'login applets,' to client systems 102." (Radia, 8:30-32.) The login applet communicates with the SMS (the "authentication accounting server") via IP packets. (Radia, 8:53-62.) The login communications include at least a user ID (see analysis at [1.2]), and the IP packets sent by the login applet include the client system's IP address as the source IP address. Radia discloses that the client system receives an IP address from a DHCP server: A DHCP server system 110 is also included in computer network 100 and connected to cable router 106. DHCP server system 110 is a computer or other system that implements Dynamic Host Configuration Protocol (DHCP) defined in Internet RFC 1541. Functionally, DHCP server system 110 provides for allocation of IP addresses within network 100. When client systems 102 initially connect to cable router 106, ***each client system 102 requests and receives an IP address from DHCP server*** system 110. (Radia, 5:28-36.) And as is typical for DHCP address assignments, Radia states that the IP address assignment is temporary: More specifically, in systems that use the DHCP protocol for allocation of IP addresses, ***each IP address is allocated for a finite period of time.*** Systems that do not renew their IP address leases may lose their allocated IP addresses. (Radia, 7:51-55.) The IP packets sent by the login applet transit through the cable modem (the "dial-up network server"). (Radia Fig. 1.) Thus, the cable modem communicates the user's login information and temporarily assigned IP address to the SMS (previously identified as the "authentication accounting server.")
[1.6] wherein the authentication	Radia discloses that the SMS (the "authentication accounting server") accesses the filtering profile database and retrieves a user's

Exhibit BB

US 6779118	Prior Art Analysis*
accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	filtering profile: In step 908, which follows, a sequence of filtering profiles 400 associated with the user are retrieved, by SMS 114, from filtering profile database 316. (Radia, 9:46-47.) Radia also discloses that the SMS communicates the filtering profile and temporary IP address to the ANCS, which subsequently reconfigures the router (as analyzed in portion [1.3] the ANCS and router collectively are a "redirection server"): Step 908 is followed by step 910 where the sequence of user ***filtering profiles 400 is downloaded by SMS 114 to ANCS 112***. At the same time, the IP address of the client system 102 acting as a host for the user is passed by the SMS 114 to the ANCS 112. In the following step, the ANCS 112 uses each of the filtering rules 404 included in the sequence of user filtering profiles 400 to establish a packet filter for IP packets originating from the client system 102 acting as a host for the user.... Alternatively, ***the packet filter may be established by reconfiguring router*** 106. (Radia, 9:60–10:7 (emphasis added).)
[1.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	As explained at [1.1], the filtering rules associated with the user IDs are individualized rule sets. Radia discloses that the ANCS and the cable modem use the filtering profile to process IP packets from the user's PC: In the following step, the ANCS 112 uses each of the filtering rules 404 included in the sequence of user filtering profiles 400 to ***establish a packet filter for IP packets originating from the client system*** 102 acting as a host for the user.... Subsequently, ***the packet filter established by the ANCS 112 is used to filter IP packets that originate from the client system*** 102 acting as a host for the user, allowing the packets that are associated with the network privileges of the user.

Exhibit BB

US 6779118	Prior Art Analysis*
	(Radia, 9:64–10:14 (emphasis added).) Radia discloses processing IP packets according to the established filter: In step 606, the packet filter established by the ANCS 112 in step 604 is used to filter packets that originate from the client system 102b. More specifically, ***each packet that originates from client system 102b is examined***. Packets that do not include a destination address that corresponds to server system 108c are discarded. Likewise packets that do not have a protocol type of UDP or a port number of 63 are discarded. (Radia, 7:9-16.) Additionally, Radia suggests using packet filters in a context in which a "company uses a router to link its internal intranet with an external network, such as the Internet." (Radia, 2:6-7.) In such a scenario, servers 108 would be connected to router 106 over the Internet. The Internet is a public network.
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	Stockwell contemplates that each rule can specify redirection of a packet to an alternate destination IP address, port, or both. (Stockwell, 2:33-46.) Stockwell also contemplates providing multiple rules. (*See, e.g.*, Stockwell 12:49-13:7.) Multiple rules may be used to specify multiple destinations. Thus, Stockwell discloses that packets may be redirected to multiple destinations.
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	Wong '727 discloses that a network may provide various services, and "each service has a filtering profile." (Radia, 5:37-38.) The filtering profile for each service is a "common individualized rule set." And Wong '727 discloses that each user ID is associated with one or more service filtering profiles, for example, based on the user's subscriptions: Within SMS 114, each network user has a filtering profile sequence. ... The filtering profiles 400 that are included in a user's filtering profile sequence correspond to the services to which the user

Exhibit BB

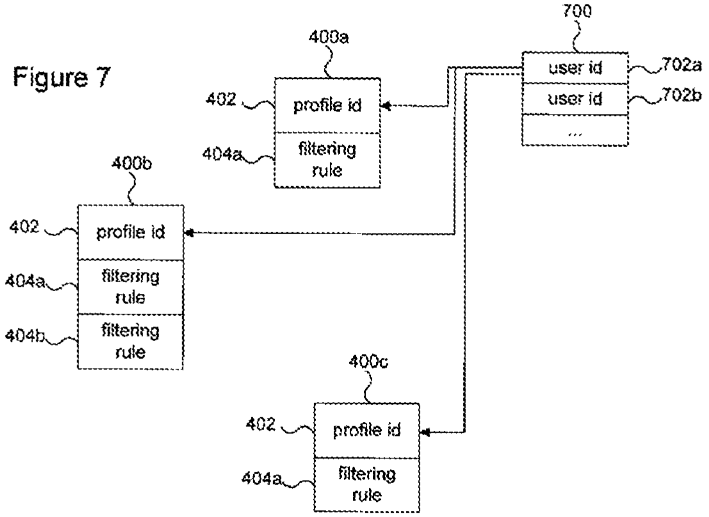
US 6779118	Prior Art Analysis*
	subscribes. Thus, if a user were to subscribe to the sports news services, his filtering profile sequence would include the filtering profile 400 shown in FIG. 6. The user's filtering profile sequence would also include filtering profiles for any other services to which the user subscribes. (Radia, 6:36-47.) It would have been obvious that a second user of the same sports news service would also have a filtering profile corresponding to the same service. Wong '727 describes the relationship between a user ID and a service filtering profile with reference to Fig. 7, below. In FIG. 7 an index 700 is shown for filtering profile database. Index 700 has one entry 702 for each network user. Each entry 702 references the filtering profiles 400 that correspond to the services to which the network user subscribes. Thus entry 702a references filtering profiles 400a and 400b. This allows the sequence of filtering profiles associated with network users to be retrieved. (Radia, 6:49-56.)  Figure 7 700 400a user id 702a user id 702b ... 402 profile id 404a filtering rule 400b 402 profile id 404a filtering rule 404b filtering rule 400c 402 profile id 404a filtering rule WONG '727 FIG. 7 According to the example above with two users of the same sports new service, the database would include an entry for each user correlated with the rule set for the sports news service. Thus, Wong '727, incorporated by reference into Radia, discloses that the user id

Exhibit BB

US 6779118	Prior Art Analysis*
	entries in the database are correlated with common filtering profiles.
[8.0] In a system comprising	See analysis of portion [1.0].
[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[8.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portion [1.3].
[8.4] the method comprising the steps of:	Radia discloses a method: The present invention relates generally to security in computer networks. More specifically, the ***present invention is a method*** and apparatus that allows IP packets within a network to be selectively filtered based on events within the network. (Radia, 1:48-52.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[8.6] communicating the individualized rule set that correlates with the	See analysis of portion [1.6].

Exhibit BB

US 6779118	Prior Art Analysis*
first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[13.0] The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[14.0] The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user	See analysis of portion [1.1]. Radia discloses that the packet filter controls the passing of data between a user and the network: In step 606, the packet filter established by the ANCS 112 in step 604 is used to filter packets that originate

Exhibit BB

US 6779118	Prior Art Analysis*
and a public network;	from the client system 102b. More specifically, ***each packet that originates from client system 102b is examined***. Packets that do not include a destination address that corresponds to server system 108c are discarded. Likewise packets that do not have a protocol type of UDP or a port number of 63 are discarded. (Radia, 7:9-16.) The packet filter of Radia performs at least one of a plurality of functions by examining, passing, and discarding packets. See analysis at [1.7] regarding the Internet as a public network.
[16.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [1.6]. Furthermore, Radia discloses that the ANCS automatically configures the modem or router to implement the packet filter: In step 604, the ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 to establish a packet filter for IP packets originating from the client system 102b. The packet filter is established by reconfiguring one or more of the components of the network 100 that forward packets originating at the client system 102b. For example, in some cases the ***packet filter may be established by reconfiguring the modem*** 104b connected to client system 102. **Alternatively, the packet filter may be established by *reconfiguring router* 106.** (Radia, 6:66–7:8.) Radia also discloses that a profile applied to a user computer may change and that the ANCS reconfigures components of the network to replace a first packet filter with another packet filter according to the changed profile. (Radia, 3:3:33-50.) Thus, the ANCS (which, in part, corresponds to the claimed redirection server) allows automated modification of a portion of the rule set.
[16.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as	Radia discloses the redirection server allows modification of a portion of the rule set 1) as a function of data transmitted to or from the user and 2) as a combination of time and a location the user accesses.

Exhibit BB

US 6779118	Prior Art Analysis*
a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	First, it is noted that Radia discloses returning the redirection server to a default configuration when a user logs out: Although not shown, it may be appreciated that the network 100 may be reconfigured to reestablish a default state after the user logs out from the client system 102. (Radia, 10:15-17.) A message that the user has logged out of the client system is "data transmitted to or from the user." Thus, Radia discloses modifying the active rule set as a function of data transmitted to or from the user. Additionally, Radia discloses that a profile applied to a user computer may change and that the ANCS reconfigures components of the network to replace a first packet filter with another packet filter according to the changed profile. (Radia, 3:3:33-50.) For instance, Radia describes with respect to Fig. 7 that a user computer is associated with a login profile during the login process. (Radia, Fig. 7 at step 708.). The ANCS establishes packet filters according to the login profile. (Radia, Fig. 7 at step 710-712.) After the user is logged in, the ANCS accesses other profiles for the user and implements the new packet filters corresponding to the profiles. (Radia, Fig. 9.) Thus, the ANCS (which, in part, corresponds to the claimed redirection server) allows modification of a portion of the rule set. In the scenario described above, the login profile (included in the rule set) is used only so long as the user is in the login process. Once the user completes the login process, the ANCS implements new packet filters based on a different portion of the user's rule set. Therefore, the ANCS is a redirection server that allows modification of a portion of the rule set as a function of time (the time for the user to login). In the example above, the ANCS allows modification of the rule set as the user transitions from the login process. The login filtering profile (which is used during the login process) is established to allow the user computer to access the DHCP server, a DNH server, and a login server. (Radia, 7:50-51; 8:6-8; and 8:51-53.) Once the login process is over, and the user does not need to access those

Exhibit BB

US 6779118	Prior Art Analysis*
	resources, the ANCS implements other packet filters based on other filter profiles. (Radia, Fig. 9). Accordingly, the ANCS (which, in part, corresponds to the claimed redirection server) allows modification of at least a portion of the rule set as a function of a location the user accesses (the accessed location includes, e.g., the DHCP server, the DNH server, and the login server). Thus, in the scenarios above that include the login process, the ANCS allows modification of the rule set as a combination of time and location the user accesses. Furthermore, blocking a website based on some combination of the recited bases—time, data transmitted to or from the user, or location the user accesses—would have been obvious to one of skill in the art. For example, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work. Similarly in a school environment, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to school. Thus, although an initial rule set might be permissive, it would be obvious to modify the rules for a particular user at a later time after it is found that the user's data transmissions or locations accessed are unproductive or inappropriate. Requester has provided an independent explanation of the pertinence and manner of applying the prior art to this claim limitation. The Board adopted similar reasoning in the previous reexamination where it found that this limitation would have been obvious to one of skill in the art. (*See* Board Decision at 10.) Accordingly, it would have been obvious to "allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses." For example, it would have been obvious, in view of Radia and Stockwell, to block or redirect a user after discovering inappropriate communications or an excessive amount of time at a site unrelated to work.
[16.5] wherein the redirection server is configured to allow modification of at least a	See analysis at portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
portion of the rule set as a function of time.	
[17.0] A system comprising:	See analysis of portion [1.0].
[17.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[17.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[17.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[17.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[17.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4].
[18.0] A system	See analysis of portion [1.0].

Exhibit BB

US 6779118	Prior Art Analysis*
comprising:	
[18.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[18.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[18.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[18.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[18.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4].
[19.0] A system comprising:	See analysis of portion [1.0].
[19.1] a redirection server programmed with	See analysis of portions [1.3] and [1.6].

Exhibit BB

US 6779118	Prior Art Analysis*
a user's rule set correlated to a temporarily assigned network address;	
[19.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[19.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[19.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[19.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portion [16.4], where the modification includes removal of the portion of the rule set that corresponds to the login filtering profile.
[20.0] A system comprising:	See analysis of portion [1.0].
[20.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].

Exhibit BB

US 6779118	Prior Art Analysis*
[20.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[20.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[20.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[20.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[21.0] A system comprising:	See analysis of portion [1.0].
[21.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[21.2] wherein the rule set contains at least one of a plurality of	See analysis of portion [16.2].

Exhibit BB

US 6779118	Prior Art Analysis*
functions used to control passing between the user and a public network;	
[21.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[21.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[21.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4], where the modification includes removal of the portion of the rule set that corresponds to the login filtering profile.
[22.0] A system comprising:	See analysis of portion [1.0].
[22.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[22.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user	See analysis of portion [16.2].

Exhibit BB

US 6779118	Prior Art Analysis*
and a public network;	
[22.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[22.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[22.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[23.0] A system comprising:	See analysis of portion [1.0].
[23.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[23.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user	See analysis of portion [16.2].

Exhibit BB

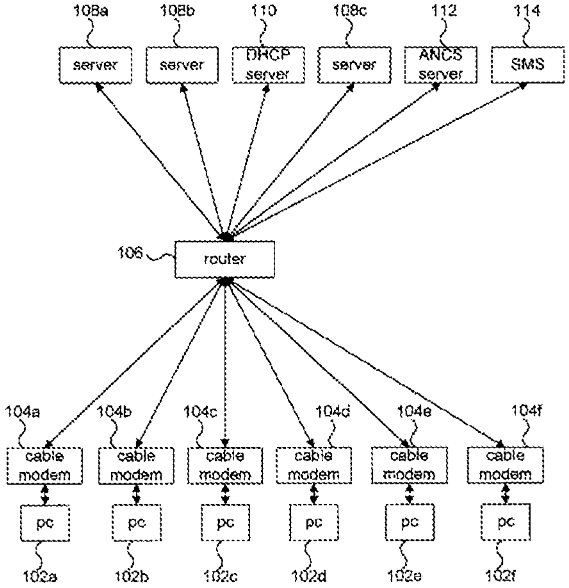
US 6779118	Prior Art Analysis*
and a public network;	
[23.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[23.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[23.5] wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	Radia illustrates the recited network architecture in Fig. 1. The router 106 ("redirection server") has a "user side" that connects to a user's PC through a cable modem and a "network side" that connects to various servers.  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1

Exhibit BB

US 6779118	Prior Art Analysis*
	Radia also discloses that a user's computer receives a temporarily assigned IP address from a DHCP server. See analysis of portion [1.5].
[24.0] The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	Radia discloses that the router 106 receives instructions to modify its filtering rules from the ANCS server 112, illustrated in Fig. 1 above as located on the "network side" of the router: In step 604, the ***ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 to establish a packet filter*** for IP packets originating from the client system 102b. The packet filter is established by reconfiguring one or more of the components of the network 100 that forward packets originating at the client system 102b. For example, in some cases the packet filter may be established by reconfiguring the modem 104b connected to client system 102. Alternatively, the packet filter may be established by ***reconfiguring router 106***. (Radia, 6:66–7:8 (emphasis added).)
[25.0] In a system comprising	See analysis of portion [1.0].
[25.1] a redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portion [1.3] and [1.5].
[25.2] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.2].
[25.3] the method comprising the step of:	See analysis of portion [8.4].
[25.4] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the	Radia discloses that when a client system (PC) initially connects to the router 106, the router 106 is reconfigured with a "login filtering" profile. (See Radia, 7:38-49.) Subsequently, after a user logs into the system, "a sequence of filtering profiles 400 associated with the user are retrieved" and used to reconfigure the router 106. (See

Exhibit BB

US 6779118	Prior Art Analysis*
temporarily assigned network address in the redirection server; and	Radia, 9:46–10:14.) Radia discloses that the temporarily-assigned IP address remains the same through the procedure, as the IP address is allocated to the computer during a first step of four steps in the login process (Radia, 7:50-60).
[25.5] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.5].
[25.6] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.5].
[25.7] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[26.0] The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
accesses.	
[27.0] The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[28.0] The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	Radia discloses that the filtering rules 404 can include a protocol type: Filtering rule 404 also includes a protocol type 506. **Protocol type 506 corresponds to the protocol type of an IP packet. Thus, the protocol type 506 of each filtering rule 404 has a value that corresponds to an IP packet type, such as TCP, UDP, ICMP, etc.** To match a particular filtering rule 404, an IP packet must have a protocol type that matches the protocol type 506 included in the filtering rule 404. (Radia, 6:29-36 (emphasis added).) Therefore, Radia discloses that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.
[29.0] The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	Radia discloses that when a client system (PC) initially connects to the router 106, the router 106 is reconfigured with a "login filtering" profile. (See Radia, 7:38-49.) Subsequently, after a user logs into the system, "a sequence of filtering profiles 400 associated with the user are retrieved" and used to reconfigure the router 106. (See Radia, 9:46–10:14.) Therefore, Radia discloses an initial temporary rule set and a standard rule set. Wong '727 shows creating a default filtering profile from a standard template. (Wong '727, 7:9-11). Therefore, Wong also teaches a standard rule set.
[29.1] wherein the	As mentioned at [29.0], Radia teaches an initial, temporary rule set

Exhibit BB

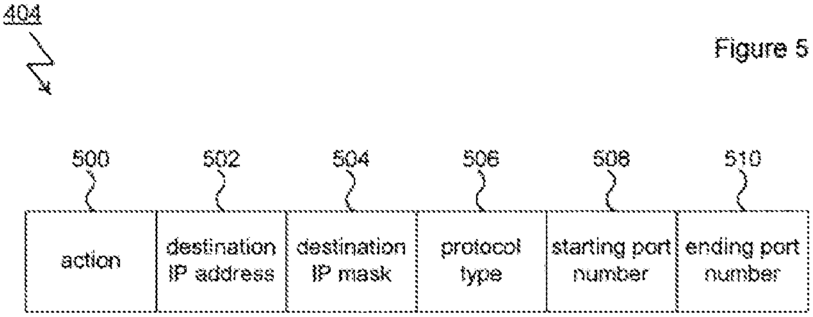
US 6779118	Prior Art Analysis*
redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	that is used during login. Subsequent to login, the user is assigned to another rule set, which in this scenario can include the standard rule set taught by Wong '727.
[30.0] The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	Radia discloses an example rule 404 that can specify an action 500 based on a number of criteria, including destination IP address, destination mask (both are types of destination), and protocol type (a request type—for example, a TCP-type request or an ICMP-type request). (Radia, Fig. 5 and 6:5-45).  404 Figure 5 500 502 504 506 508 510 action destination IP address destination IP mask protocol type starting port number ending port number RADIA FIG. 5
[31.0] The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	As shown above at [1.3], it would have been obvious to add the redirection feature of Stockwell to the filtering of Radia, where Stockwell discloses redirecting data to a new destination address. Furthermore, the rules of Radia may take an action based on an attempted destination address and a request type. See analysis at [30.0], citing Radia at Fig. 5 and 6:5-45. Thus, the combination of prior art discloses redirecting the data to a new address based on a request type and an attempted destination address.
[32.0] The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[33.0] The method of claim 8, wherein the individualized rule set	See analysis of portion [29.0].

Exhibit BB

US 6779118	Prior Art Analysis*
includes an initial temporary rule set and a standard rule set, and	
[33.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[34.0] The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[35.0] The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[36.0] A system comprising:	See analysis of portion [1.0].
[36.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[36.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[36.3] wherein the redirection server is configured to allow automated modification	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
of at least a portion of the rule set correlated to the temporarily assigned network address;	
[36.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[36.5] wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[37.0] A system comprising:	See analysis of portion [1.0].
[37.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[37.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[37.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[37.4] wherein the	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[37.5] wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[37.6] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[38.0] A system comprising:	See analysis of portion [1.0].
[38.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[38.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[38.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
[38.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[38.5] wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[39.0] A system comprising:	See analysis of portion [1.0].
[39.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[39.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[39.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[39.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[39.5] wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[40.0] The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[41.0] The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set,	See analysis of portion [29.0].
[41.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[42.0] The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[43.0] The method of claim 25, wherein the modified rule set	See analysis of portion [31.0].

Exhibit BB

US 6779118	Prior Art Analysis*
includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[44.0] A system comprising:	See analysis of portion [1.0].
[44.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[44.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[44.3] a redirection server connected between the dial-up network server and a public network, and	See analysis of portion [1.3]. Radia teaches a redirection server that includes the router 106 and the ANCS 112. As shown in the annotated figure below, Radia's redirection server is placed between the dial-up network servers (cable modems 104) and servers 108 on the public network.

Exhibit BB

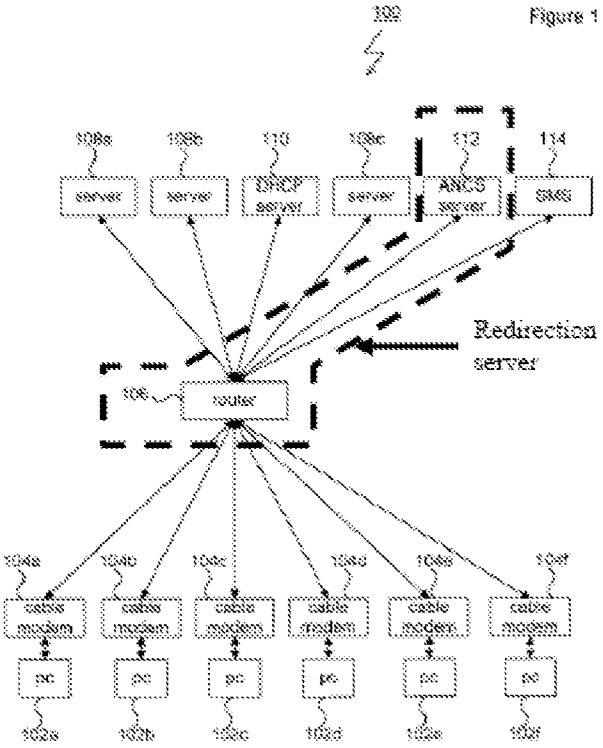
US 6779118	Prior Art Analysis*
	 100 Figure 1 108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS Redirection server 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 (ANNOTATED)
[44.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	See analysis of portion [1.4].
[44.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	See analysis of portion [1.5].
[44.6] wherein the authentication accounting server	See analysis of portion [1.6].

Exhibit BB

US 6779118	Prior Art Analysis*
accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	
[44.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	See analysis of portion [1.7].
[49.0] The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	See analysis of portion [6.0].
[50.0] The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	See analysis of portion [7.0].
[51.0] The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[52.0] The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a	See analysis of portion [29.0].

Exhibit BB

US 6779118	Prior Art Analysis*
standard rule set, and	
[52.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[53.0] The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[54.0] The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.1].
[55.0] The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above with respect to claim 44 (and citing to claim 1) that the prior art teaches blocking and redirection as a function of an individualized rule set. Stockwell teaches that a filter rule can "Redirect the IP address to a different machine." (Stockwell, 2:46.) Stockwell further provides a filtering rule example that "intercepts all incoming connections that go the external side of the local Sidewinder (192.168.1.192) and ***redirects*** them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31, emphasis added.) It is understood that the addresses "192.168.1.192" and "172.17.192.48" are destination IP addresses. One of skill in the art would understand that IP addresses are used in IP packet headers to indicate the source and destination of the packet. Stockwell further teaches that redirection filtering rules can cause a change in a packet's destination IP address: The rules determine whether the connection is

Exhibit BB

US 6779118	Prior Art Analysis*
	allowed or denied. A rule can also have one or more side effects. A side effect causes the proxy to change its behavior in some fashion. For example, a common side effect is ***to redirect the destination IP address to an alternate machine***. (Stockwell, 5:24-30, emphasis added.) In view of Stockwell's teaching of redirecting a connection's destination to an alternate IP address, it would have been obvious to redirect data by replacing the destination address in an IP packet header with the alternate IP address. Thus, Radia and Stockwell render obvious "replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set" as recited in the claim.
[56.0] In a system comprising	See analysis of portion [1.0].
[56.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[56.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[56.3] a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portions [1.3] and [44.3].
[56.4] the method comprising the steps of:	See analysis of portion [8.4].
[56.5] communicating a first user ID for one of	See analysis of portion [1.5].

Exhibit BB

US 6779118	Prior Art Analysis*
the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	
[56.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[56.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[61.0] The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[62.0] The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDS, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[63.0] The method of claim 56, wherein the individualized rule set	See analysis of portion [28.0].

Exhibit BB

US 6779118	Prior Art Analysis*
includes at least one rule as a function of a type of IP (Internet Protocol) service.	
[64.0] The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[64.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[65.0] The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[66.0] The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[67.0] The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination	It was shown above that claim 56 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [55.0].

Exhibit BB

US 6779118	Prior Art Analysis*
address as a function of the individualized rule set.	
[68.0] A system comprising:	See analysis of portion [1.0].
[68.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[68.2] the redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[68.3] wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [16.2].
[68.4] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and	See analysis of portion [16.3].
[68.5] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.	See analysis of portion [16.4].
[69.0] The system of claim 68, wherein the redirection server is	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
configured to allow modification of at least a portion of the rule set as a function of time.	
[70.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4].
[71.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4].
[72.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[73.0] The system of claim 68, wherein the redirection sewer is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[74.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.

Exhibit BB

US 6779118	Prior Art Analysis*
of at least a portion of the rule set as a function of the location or locations the user accesses.	
[75.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[76.0] The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	See analysis of portion [23.5].
[77.0] The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].

Exhibit BB

US 6779118	Prior Art Analysis*
[78.0] The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[79.0] The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[79.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set	See analysis of portion [29.1].
[80.0] The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[81.0] The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[82.0] The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP	It was shown above that claim 68 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [55.0].

Exhibit BB

US 6779118	Prior Art Analysis*
(Internet protocol) packet header by a second destination address as a function of the modified rule set.	
[83.0] In a system comprising	See analysis of portion [1.0].
[83.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[83.2] the redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portions [1.3] and [1.6].
[83.3] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.1].
[83.4] the method comprising the step of:	See analysis of portion [8.4].
[83.5] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	See analysis of portion [25.4].
[83.6] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a	See analysis of portion [23.0].

Exhibit BB

US 6779118	Prior Art Analysis*
computer network and	
[83.7] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.0].
[83.8] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[84.0] The method of claim 83, further including; the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[85.0] The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.

Exhibit BB

US 6779118	Prior Art Analysis*
[86.0] The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service,	See analysis of portion [28.0].
[87.0] The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[87.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[88.0] The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[89.0] The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[90.0] The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP	It was shown above that claim 83 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [55.0].

Exhibit BB

US 6779118	Prior Art Analysis*
(Internet Protocol) packet header by a second destination address as a function of the individualized rule set.	

Exhibit BB

Proposed Rejection #4. Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Stockwell and further in view of Wong '178 under 35 U.S.C. § 103(a).

Reasons to combine Radia, Wong '727, and Stockwell with Wong '178

A description of the proposed combination of Radia, Wong '727, and Stockwell is provided is provided above. Radia, Wong '727, and Wong '178 share overlapping inventors, mutually incorporate one another by reference, and describe the same or similar system. Thus, these references include an express teaching that their disclosures should be combined. It would have been obvious to one of skill in the art to do so.

Wong '178 discloses a technique that includes filtering both upstream and downstream packets. In addition to the express reasons to combine given above, it would also be obvious to include upstream and downstream packet filtering in the system of Radia in order to provide increased security to the Radia system. Also, modifying Radia according to the teaching of Wong '178 to provide upstream and downstream filtering is a "use of known technique to improve similar devices (methods, or products) in the same way." (*See* MPEP § 2143, *citing KSR.*)

Exhibit BB

US 6779118	Prior Art Analysis[*]
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 1 (now canceled) is obvious over Radia, Wong '727, and Stockwell. As shown above at [1.7] Radia discloses filtering packets according to a function of individualized rule sets. Furthermore, Radia incorporates by reference (at 1:27-30) U.S. App. 08/762,709, now U.S. 6,073,178 to Wong. Wong '178 discloses "a method using [sic] for selectively forwarding, by router 106, of packets based on learned assignments of IP addresses." (Wong '178, 8:40-42.) Wong '178 discloses categorizing packets into "upstream" (from the client system) and "downstream" (to the client system) packets: Generally, routers categorize packets into "upstream" and "downstream" packets. In the case of the network topology shown for network 100, upstream packets are packets that originate at one of the client systems 102. Downstream packets are packets that are directed at one of the client systems 102. (Wong '178, 8:47-52.) Wong '178 further discloses filtering both upstream and downstream packets based in part on their source and destination IP addresses: If a downstream packet is detected in step 804, execution of method 800 continues at step 806 where the router 106 extracts the packet's destination address. ***Using this destination address, the router 106, in step 808 "looks up" the trusted identifier of the client system*** 102 that is associated with the destination address of the received packet (this association is formed by the router 106 during

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit BB

US 6779118	Prior Art Analysis*
	execution of method 600). In step 810, a test is performed to ascertain whether a trusted identifier was actually located in step 808. If a trusted identifier was located in step 808, execution of method 800 continues at step 812 where the router 106 forwards the received packet to client system associated with the trusted identifier. In the alternative, if no trusted identifier is associated with the destination address of the packet, ***the router 106 discards the packet*** in step 814. ... In step 822, ***the router 106 compares the source address of the received packet with the authorized IP addresses*** that were looked up in step 820. If the source address of the packet matches one of the authorized IP addresses, the router 106 forwards the packet in step 824. Alternatively, if the source address of the received packet does not match one of the authorized IP addresses, the router 106 discards the packet in step 826. (Wong '178, 8:53 – 9:20, emphasis added). Thus Radia, which incorporates Wong '178 by reference, discloses providing control over data both *sent to* and *received from* the client systems. This may be performed as a function of individualized rule sets, as disclosed by Radia.
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Radia further discloses discarding packets that do not meet the filtering criteria established for a user: Subsequently, the new packet filter ***uses the rules of the user filtering profile*** sequence to selectively forward or ***discard IP packets*** originating from the client system. (Radia, 3:47-50.) Discarding the IP packet results in blocking data from the user's computer. As shown above at [2.0], it would be obvious to perform the function on data both <u>to and from</u> the user's computer.

Exhibit BB

US 6779118	Prior Art Analysis*
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Radia further discloses forwarding packets that meet the filtering criteria established for a user: Subsequently, the new packet filter ***uses the rules of the user filtering profile*** sequence to ***selectively forward*** or discard IP packets originating from the client system. (Radia, 3:47-50.) Forwarding the IP packets results in allowing data from the user's computer. As shown above at [2.0], it would be obvious to perform the function on data both to and from the user's computer.
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Stockwell further discloses a filtering rule example that "intercepts all incoming connections that go [sic] the external side of the local Sidewinder (192.168.1.192) and ***redirects*** them to shade.sctc.com (172.17.192.48)." (Stockwell, 2:29-31, emphasis added.) Stockwell further discloses that a filter rule can "Redirect the IP address to a different machine" or "Redirect the port number to a different port." (Stockwell, 2:46-47.) It would have been obvious to incorporate the redirection rule of Stockwell into the system of Radia at least for the reasons given above. As shown above at [2.0], it would be obvious to perform the function on data both to and from the user's computer.
[9.0] The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [2.0].
[10.0] The method of claim 8, further including the step of	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Stockwell.

Exhibit BB

US 6779118	Prior Art Analysis*
blocking the data to and from the users' computers as a function of the individualized rule set.	Additionally, see analysis of portion [3.0].
[11.0] The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [4.0].
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [5.0].
[45.0] The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [2.0].
[46.0] The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [3.0].
[47.0] The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function	It was shown above that claim 44 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [4.0].

Exhibit BB

US 6779118	Prior Art Analysis*
of the individualized rule set.	
[48.0] The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [5.0].
[57.0] The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [2.0].
[58.0] The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [3.0].
[59.0] The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [4.0].
[60.0] The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Stockwell. Additionally, see analysis of portion [5.0].

Exhibit BB

Proposed Rejection #5. Claims 6, 7, 13, 14, 16-24, 26-44, 49-56, and 61-90 are obvious over Radia in view of Wong '727 and further in view of Admitted Prior Art under 35 U.S.C. § 103(a).

Reasons to combine Radia, Wong '727, and Admitted Prior Art

A description of Radia is provided in the accompanying Request for Reexamination and will not be repeated here. Radia and Wong '727 share overlapping inventors, mutually incorporate one another by reference, and describe the same or similar system. Thus, these references include an express teaching that their disclosures should be combined. It would have been obvious to one of skill in the art to do so.

Radia discloses applying individualized filtering rules to multiple users. Wong '727 illustrates in Fig. 7 that a filtering profile database includes a plurality of user IDs, and each user ID is correlated with a set of profile IDs that define filtering rules. In addition to the express reasons to combine given above, it would also be obvious to include a filtering database organized in the manner described by Wong '727 in the system of Radia in order to provide a way to store and access the filtering profiles for the multiple users. Also, modifying Radia according to the teaching of Wong '727 to provide the organized filtering database is a "use of known technique to improve similar devices (methods, or products) in the same way." (*See* MPEP § 2143, *citing KSR International Co. v. Teleflex Inc.*, 550 U.S. ___, ___, 82 USPQ2d 1385, 1396 (2007).)

Furthermore, it would also be obvious to perform redirection by replacing a first destination address in an IP packet header by a second destination because it requires only applying a known technique (replacement of one destination address for another) to a known device (the packet filters of Radia) to yield predictable results (redirection from one website to another). (*See* MPEP § 2143, *citing KSR*.)

Requester has provided an independent explanation of the reasons to combine these prior art references. Requester notes that in an earlier reexamination, the Board of Patent Appeals and Interferences found, with respect to the '118 Patent, that redirection is an obvious extension of the use of a control to block a user. See *Ex Parte Linksmart Wireless Technology, LLC*, Appeal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011) (hereinafter, the "BPAI Decision".)

US 6779118	Prior Art Analysis[*]
[1.0] A system comprising:	Radia illustrates a computer network in Fig. 1. The computer network is a system.

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit BB

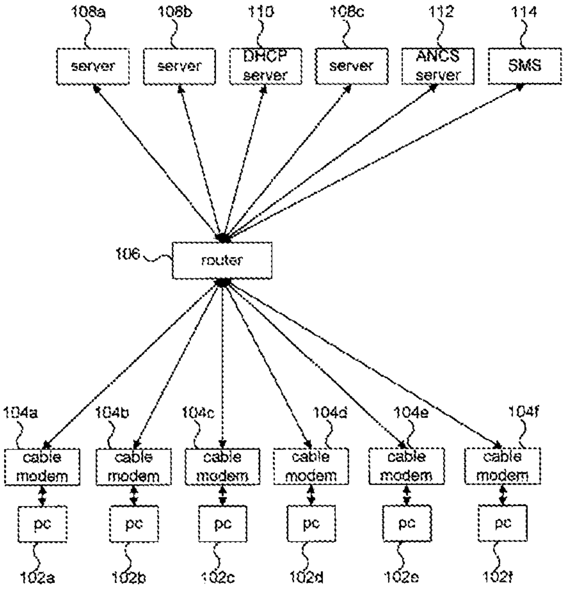
US 6779118	Prior Art Analysis*
	 108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1
[1.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia discloses a "filtering profile database" that includes a profile ID and filtering rules: The ***filtering profile database*** 316 of SMS 114 ***includes a set of filtering profiles*** of the type shown in FIG. 4 and generally designated 400. Filtering profile 400 ***includes a profile id*** 402 ***and a series of filtering rules***, of which filtering rules 404a through 404c are representative. The profile id 402 is used by SMS 114 and ANCS 112 as an internal identifier for the filtering profile 400. (Radia, 6:5-11.) And Radia incorporates by reference U.S. App. 08/762,393, now U.S. 5,835,727 to Wong. (Radia, 1:12-16.) Wong '727 illustrates in Fig. 7 that the filtering profile database includes a plurality of user IDs, and each user ID is correlated with a set of profile IDs that define filtering rules:

Exhibit BB

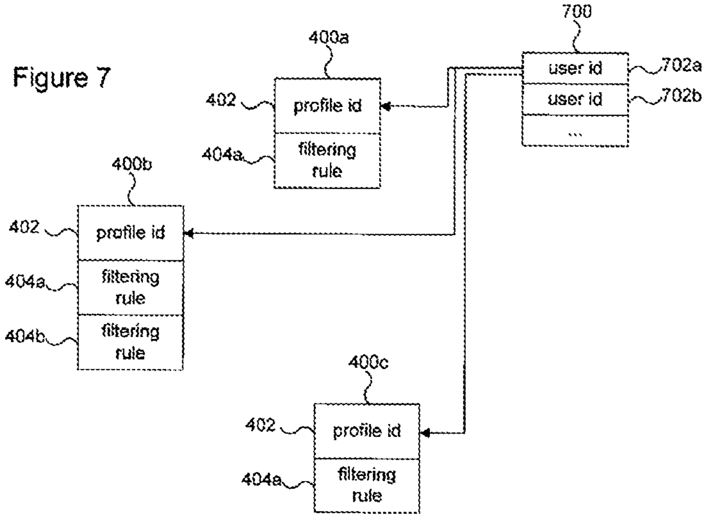
US 6779118	Prior Art Analysis*
	 Figure 7 700 400a user id 702a user id 702b ... 402 profile id 404a filtering rule 400b 402 profile id 404a filtering rule 404b filtering rule 400c 402 profile id 404a filtering rule WONG '727 FIG. 7 Wong '727 further discloses that "an index 700 is shown for filtering profile database. Index 700 has one entry 702 for each network user." (Wong '727, 6:50-51.) The filter profile database is a "database." The user ID entries 702 are "entries correlating each of a plurality of user IDs," and the group of filtering rules associated with each user ID is an "individualized rule set."
[1.2] a dial-up network server that receives user IDs from users' computers;	Radia discloses a cable modem 104 and cable router 106, illustrated in Fig. 1, that connect a client system (computer) 102 to a network.

Exhibit BB

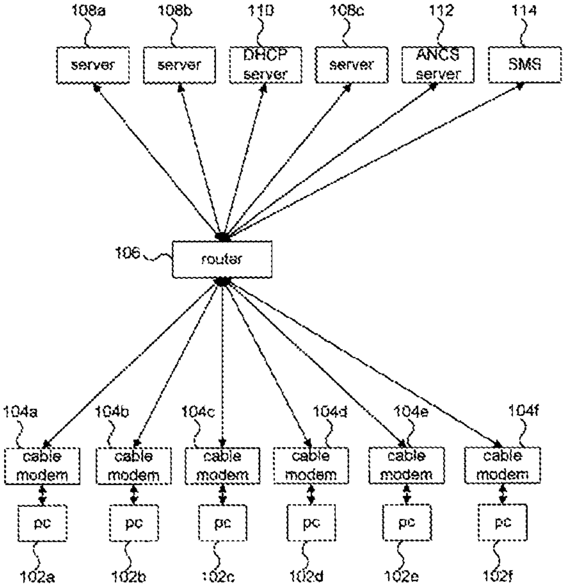
US 6779118	Prior Art Analysis*
	 108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 The cable modem of Radia is a "dial-up network server." As evidence that the above analysis comports with the broadest reasonable interpretation of the claims, it is noted that the '118 patent states that "The dial-up network server 102 is used to establish a communications link with the user's PC using a standard communications protocol." ('118 Patent, 3:60-63.) The '118 Patent further describes a dial-up network server as providing a network connection for a computer through a "modem, … local area network (LAN), or other communications link." ('118 Patent, 3:57-60.) Also, with respect to the '118 patent, a federal court understood a dial-up network server to be any "server that is used to establish a communications link with the user's PC." (Claim Construction order at 13.) Thus, the cable modem of Radia discloses a dial-up network server. Alternatively, the router 106 may be the claimed "dial-up network server." The Patent Owner has asserted that a router is a "dial-up network server." *See, e.g.,* Exhibit D-2, Linksmart Infringement Contentions Against Cisco IOS at 9. Furthermore, it is suggested that both the cable modem 104 and the router 106 receive the user IDs from user computers. For instance, Wong '727 states: Network users login to the network using one of the

Exhibit BB

US 6779118	Prior Art Analysis*
	client systems as a host. As part of the login process, the SMS authenticates the user using a password or other authentication method. Subsequently, the SMS locates the user's filtering profile sequence. (Wong '727 at 2:50-54.) According to Wong '727, the user logs in at the user computer and provides a password or other authentication method. A user ID is a type of authentication method. The user's ID is received by the SMS 114 (see Fig. 1 above) via the cable modem and router.
[1.3] a redirection server connected to the dial-up network server and a public network, and	Radia discloses an "access network control server (ANCS)" that configures a router to enforce the packet filter (Radia, 5: 42-43): In step 604, the ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 ***to establish a packet filter*** for IP packets originating from the client system 102b. For example, in some cases the packet filter may be established by reconfiguring the modem 104b connected to client system 102. Alternatively, ***the packet filter may be established by reconfiguring router*** 106. (Radia, 6:66 –7:2.) Radia further discloses that "the packet filter uses the rules of the login filtering profile sequence to selectively ***forward or discard IP packets*** originating from the client system." (Radia, 3:18-20.) By implementing the packet filter, the router controls a user's access to the network. Thus, the router and the ANCS together form a "redirection server." As evidence of this interpretation, the '118 patent describes a redirection server as a server that "controls the user's access to the network" by "checking data packets and blocking or allowing the packets as a function of the rule sets." ('118 Patent, 4:51-52 and 63-65.) Regarding the interpretation of Radia's router as teaching both the "dial-up network server" and "redirection server" limitations, the Patent Owner has stated that the claimed dial-up network server and the redirection server may be the same device. *See, e.g.*, Exhibit D-

Exhibit BB

US 6779118	Prior Art Analysis*
	2, Linksmart Infringement Contentions Against Cisco IOS at 9 ("For example, the network server can be the router running the SSG or ISG software.") and at 18 ("In these configurations, the SSG is the redirection server."). The Admitted Prior Art teaches controlling access to resources by redirecting traffic, for example, World Wide Web traffic: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that in directing the user away from the website, the user's access to the website is blocked. Thus, redirection is an obvious extension of blocking and could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked

Exhibit BB

US 6779118	Prior Art Analysis*
	websites. Requester notes that the Board made similar findings in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.) It would have been obvious to add the redirection feature known in the prior art to the packet filtering capabilities of Radia at least for the reasons given above. In summary, Radia and the Admitted Prior Art render obvious "a redirection server connected to the dial-up network server and a public network" as recited in the claim. As evidence to support this interpretation, the '118 patent describes a redirection server as a server that "controls the user's access to the network" by "checking data packets and blocking or allowing the packets as a function of the rule sets." ('118 Patent, 4:51-52 and 63-65.)
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	Radia discloses a "services management system (SMS)." (Radia, 5:43-44.) The SMS acts as a "login server." (Radia, 8:51-53.) Method 900 begins with step 906 where ***SMS 114 waits for a user login***. More specifically, as discussed with regard to method 700, for a preferred embodiment of network 100, users login to network 100 using a login applet that communicates with a ***login server, such as SMS*** 114. (Radia, 9:37-42.) Wong '727 states that "As part of the login process, the ***SMS authenticates the user*** using a password or other authentication method." (Wong '727, 2:51-53.) The services management system (SMS) is an "authentication accounting server." Radia illustrates an example SMS in Fig. 3. The filtering profile database is incorporated into the SMS, and thus the SMS is "connected to the database" as recited in the claim: SMS 114 is shown in more detail in FIG. 3 to include a computer system 302 that, in turn, includes a processor, or processors 304, and a memory 306....

Exhibit BB

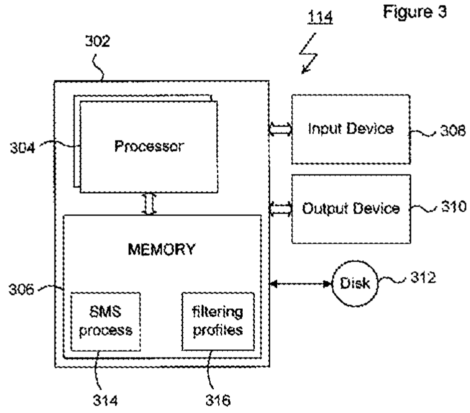
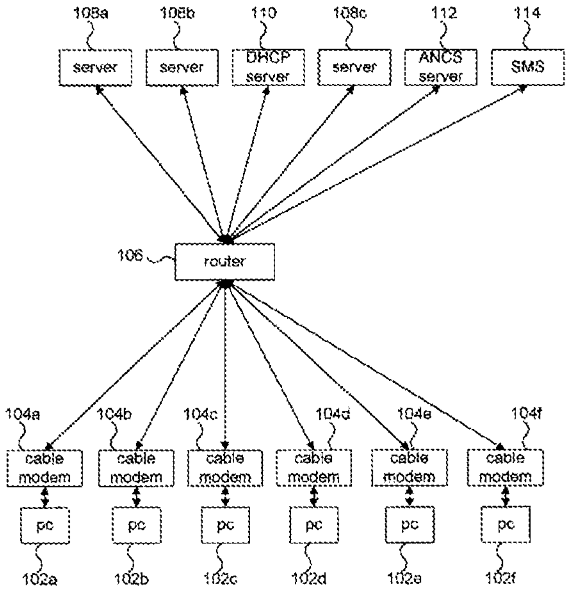
US 6779118	Prior Art Analysis*
	An SMS process 314 and a ***filtering profile database 316 are shown to be resident in memory 306*** of computer system 302. (Radia, 5:56-65.)  114 Figure 3 302 304 Processor Input Device 308 Output Device 310 MEMORY 306 Disk 312 SMS process filtering profiles 314 316 RADIA FIG. 3 Radia further illustrates in Fig. 1 that the SMS is connected to the router ("redirection server") and (through the router) to the cable modems ("dial-up network server"):  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1
[1.5] wherein the dial-up network server	Radia discloses that "user logins are handled by downloading small, specifically tailored applications, known as 'login applets,' to client

Exhibit BB

US 6779118	Prior Art Analysis*
communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	systems 102." (Radia, 8:30-32.) The login applet communicates with the SMS (the "authentication accounting server") via IP packets. (Radia, 8:53-62.) The login communications include at least a user ID (see analysis at [1.2]), and the IP packets sent by the login applet include the client system's IP address as the source IP address. Radia discloses that the client system receives an IP address from a DHCP server: A DHCP server system 110 is also included in computer network 100 and connected to cable router 106. DHCP server system 110 is a computer or other system that implements Dynamic Host Configuration Protocol (DHCP) defined in Internet RFC 1541. Functionally, DHCP server system 110 provides for allocation of IP addresses within network 100. When client systems 102 initially connect to cable router 106, ***each client system 102 requests and receives an IP address from DHCP server*** system 110. (Radia, 5:28-36.) And as is typical for DHCP address assignments, Radia states that the IP address assignment is temporary: More specifically, in systems that use the DHCP protocol for allocation of IP addresses, ***each IP address is allocated for a finite period of time***. Systems that do not renew their IP address leases may lose their allocated IP addresses. (Radia, 7:51-55.) The IP packets sent by the login applet transit through the cable modem (the "dial-up network server"). (Radia Fig. 1.) Thus, the cable modem communicates the user's login information and temporarily assigned IP address to the SMS (previously identified as the "authentication accounting server.")
[1.6] wherein the authentication accounting server accesses the database	Radia discloses that the SMS (the "authentication accounting server") accesses the filtering profile database and retrieves a user's filtering profile:

Exhibit BB

US 6779118	Prior Art Analysis*
and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	In step 908, which follows, a sequence of filtering profiles 400 associated with the user are retrieved, by SMS 114, from filtering profile database 316. (Radia, 9:46-47.) Radia also discloses that the SMS communicates the filtering profile and temporary IP address to the ANCS, which subsequently reconfigures the router (as analyzed in portion [1.3] the ANCS and router collectively are a "redirection server"): Step 908 is followed by step 910 where the sequence of user ***filtering profiles 400 is downloaded by SMS 114 to ANCS 112***. At the same time, the IP address of the client system 102 acting as a host for the user is passed by the SMS 114 to the ANCS 112. In the following step, the ANCS 112 uses each of the filtering rules 404 included in the sequence of user filtering profiles 400 to establish a packet filter for IP packets originating from the client system 102 acting as a host for the user.... Alternatively, ***the packet filter may be established by reconfiguring router*** 106. (Radia, 9:60–10:7 (emphasis added).)
[1.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	As explained at [1.1], the filtering rules associated with the user IDs are individualized rule sets. Radia discloses that the ANCS and the cable modem use the filtering profile to process IP packets from the user's PC: In the following step, the ANCS 112 uses each of the filtering rules 404 included in the sequence of user filtering profiles 400 to ***establish a packet filter for IP packets originating from the client system*** 102 acting as a host for the user.... Subsequently, ***the packet filter established by the ANCS 112 is used to filter IP packets that originate from the client system*** 102 acting as a host for the user, allowing the packets that are associated with the network privileges of the user. (Radia, 9:64–10:14 (emphasis added).)

Exhibit BB

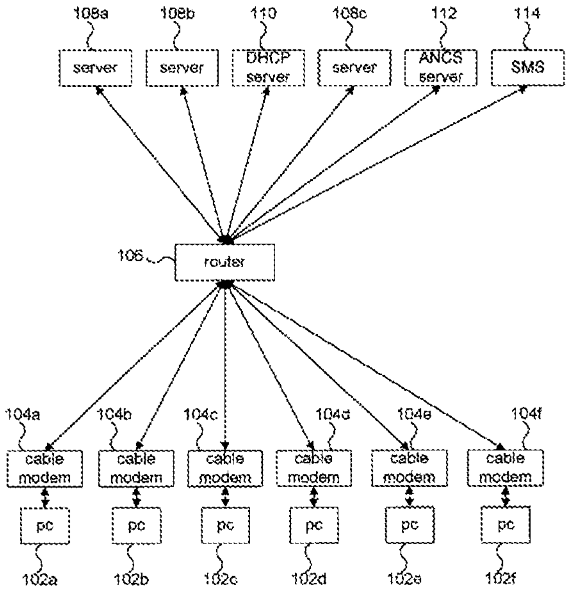
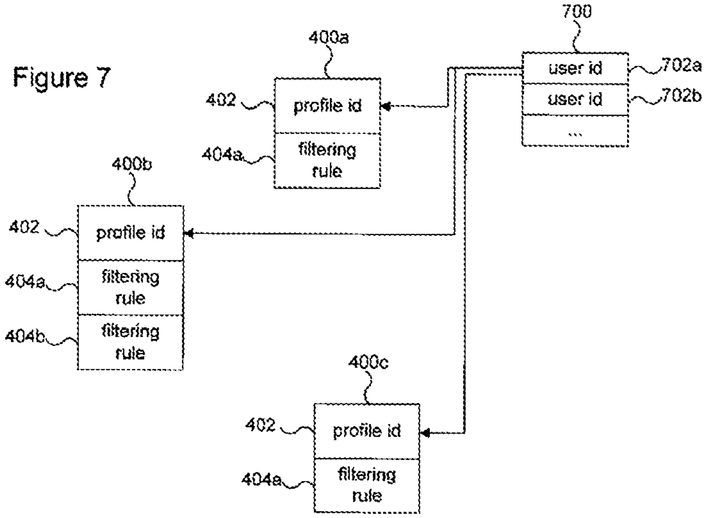
US 6779118	Prior Art Analysis*
	Radia discloses processing IP packets according to the established filter: In step 606, the packet filter established by the ANCS 112 in step 604 is used to filter packets that originate from the client system 102b. More specifically, ***each packet that originates from client system 102b is examined***. Packets that do not include a destination address that corresponds to server system 108c are discarded. Likewise packets that do not have a protocol type of UDP or a port number of 63 are discarded. (Radia, 7:9-16.) Additionally, Radia suggests using packet filters in a context in which a "company uses a router to link its internal intranet with an external network, such as the Internet." (Radia, 2:6-7.) In such a scenario, servers 108 would be connected to router 106 over the Internet. The Internet is a public network.
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	Radia illustrates in Fig. 1 that there are multiple potential destinations (servers 108) for a user's network requests:  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 The servers 108 "are intended to represent the broad range of server

Exhibit BB

US 6779118	Prior Art Analysis*
	systems that may be found within computer networks." (Radia, 5:23-28.) It would have been obvious for a filtering rule to redirect a user to any one or more of the servers 108.
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	Wong '727 discloses that a network may provide various services, and "each service has a filtering profile." (Radia, 5:37-38.) The filtering profile for each service is a "common individualized rule set." And Wong '727 discloses that each user ID is associated with one or more service filtering profiles, for example, based on the user's subscriptions: Within SMS 114, each network user has a filtering profile sequence. … The filtering profiles 400 that are included in a user's filtering profile sequence correspond to the services to which the user subscribes. Thus, if a user were to subscribe to the sports news services, his filtering profile sequence would include the filtering profile 400 shown in FIG. 6. The user's filtering profile sequence would also include filtering profiles for any other services to which the user subscribes. (Radia, 6:36-47.) It would have been obvious that a second user of the same sports news service would also have a filtering profile corresponding to the same service. Wong '727 describes the relationship between a user ID and a service filtering profile with reference to Fig. 7, below. In FIG. 7 an index 700 is shown for filtering profile database. Index 700 has one entry 702 for each network user. Each entry 702 references the filtering profiles 400 that correspond to the services to which the network user subscribes. Thus entry 702a references filtering profiles 400a and 400b. This allows the sequence of filtering profiles associated with network users to be retrieved. (Radia, 6:49-56.)

Exhibit BB

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td></td><td>


WONG '727 FIG. 7

According to the example above with two users of the same sports new service, the database would include an entry for each user correlated with the rule set for the sports news service. Thus, Wong '727, incorporated by reference into Radia, discloses that the user id entries in the database are correlated with common filtering profiles.
</td></tr>
<tr><td>[8.0] In a system comprising</td><td>See analysis of portion [1.0].</td></tr>
<tr><td>[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;</td><td>See analysis of portion [1.1].</td></tr>
<tr><td>[8.2] a dial-up network server that receives user IDs from users' computers;</td><td>See analysis of portion [1.2].</td></tr>
<tr><td>[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,</td><td>See analysis of portion [1.3].</td></tr>
</table>

Exhibit BB

US 6779118	Prior Art Analysis*
[8.4] the method comprising the steps of:	Radia discloses a method: The present invention relates generally to security in computer networks. More specifically, the ***present invention is a method*** and apparatus that allows IP packets within a network to be selectively filtered based on events within the network. (Radia, 1:48-52.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[8.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[13.0] The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[14.0] The method of claim 8, further	See analysis of portion [7.0].

Exhibit BB

US 6779118	Prior Art Analysis*
including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [1.1]. Radia discloses that the packet filter controls the passing of data between a user and the network: In step 606, the packet filter established by the ANCS 112 in step 604 is used to filter packets that originate from the client system 102b. More specifically, ***each packet that originates from client system 102b is examined***. Packets that do not include a destination address that corresponds to server system 108c are discarded. Likewise packets that do not have a protocol type of UDP or a port number of 63 are discarded. (Radia, 7:9-16.) The packet filter of Radia performs at least one of a plurality of functions by examining, passing, and discarding packets. See analysis at [1.7] regarding the Internet as a public network.
[16.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [1.6]. Furthermore, Radia discloses that the ANCS automatically configures the modem or router to implement the packet filter: In step 604, the ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 to establish a packet filter for IP packets originating from the client system 102b. The packet filter is established by reconfiguring one or more of the

US 6779118	Prior Art Analysis*
	components of the network 100 that forward packets originating at the client system 102b. For example, in some cases the ***packet filter may be established by reconfiguring the modem*** 104b connected to client system 102. **Alternatively, the packet filter may be established by *reconfiguring router* 106.** (Radia, 6:66–7:8.) Radia also discloses that a profile applied to a user computer may change and that the ANCS reconfigures components of the network to replace a first packet filter with another packet filter according to the changed profile. (Radia, 3:3:33-50.) Thus, the ANCS (which, in part, corresponds to the claimed redirection server) allows automated modification of a portion of the rule set.
[16.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	Radia discloses the redirection server allows modification of a portion of the rule set 1) as a function of data transmitted to or from the user and 2) as a combination of time and a location the user accesses. First, it is noted that Radia discloses returning the redirection server to a default configuration when a user logs out: Although not shown, it may be appreciated that the network 100 may be reconfigured to reestablish a default state after the user logs out from the client system 102. (Radia, 10:15-17.) A message that the user has logged out of the client system is "data transmitted to or from the user." Thus, Radia discloses modifying the active rule set as a function of data transmitted to or from the user. Additionally, Radia discloses that a profile applied to a user computer may change and that the ANCS reconfigures components of the network to replace a first packet filter with another packet filter according to the changed profile. (Radia, 3:3:33-50.) For instance, Radia describes with respect to Fig. 7 that a user computer is associated with a login profile during the login process. (Radia, Fig. 7 at step 708.). The ANCS establishes packet filters according

Exhibit BB

US 6779118	Prior Art Analysis*
	to the login profile. (Radia, Fig. 7 at step 710-712.) After the user is logged in, the ANCS accesses other profiles for the user and implements the new packet filters corresponding to the profiles. (Radia, Fig. 9.) Thus, the ANCS (which, in part, corresponds to the claimed redirection server) allows modification of a portion of the rule set. In the scenario described above, the login profile (included in the rule set) is used only so long as the user is in the login process. Once the user completes the login process, the ANCS implements new packet filters based on a different portion of the user's rule set. Therefore, the ANCS is a redirection server that allows modification of a portion of the rule set as a function of time (the time for the user to login). In the example above, the ANCS allows modification of the rule set as the user transitions from the login process. The login filtering profile (which is used during the login process) is established to allow the user computer to access the DHCP server, a DNH server, and a login server. (Radia, 7:50-51; 8:6-8; and 8:51-53.) Once the login process is over, and the user does not need to access those resources, the ANCS implements other packet filters based on other filter profiles. (Radia, Fig. 9). Accordingly, the ANCS (which, in part, corresponds to the claimed redirection server) allows modification of at least a portion of the rule set as a function of a location the user accesses (the accessed location includes, e.g., the DHCP server, the DNH server, and the login server). Thus, in the scenarios above that include the login process, the ANCS allows modification of the rule set as a combination of time and location the user accesses. Furthermore, blocking a website based on some combination of the recited bases—time, data transmitted to or from the user, or location the user accesses—would have been obvious to one of skill in the art. For example, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work. Similarly in a school environment, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to school. Thus, although an initial rule set might be permissive, it would be obvious to modify the rules for a particular

Exhibit BB

US 6779118	Prior Art Analysis*
	user at a later time after it is found that the user's data transmissions or locations accessed are unproductive or inappropriate. Thus, it would have been obvious to "allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses" as recited in the claim. For example, it would have been obvious, in view of Radia and the Admitted Prior Art, to block or redirect a user after discovering inappropriate communications or an excessive amount of time at a site unrelated to work. Requester has provided an independent explanation of the pertinence and manner of applying the prior art to this claim limitation. Requester notes that the Board similarly found that this limitation would have been obvious to one of skill in the art. (*See* Board Decision at 10.)
[16.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis at portion [16.4].
[17.0] A system comprising:	See analysis of portion [1.0].
[17.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[17.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[17.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
the temporarily assigned network address;	
[17.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[17.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4].
[18.0] A system comprising:	See analysis of portion [1.0].
[18.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[18.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[18.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[18.4] wherein the	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[18.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4].
[19.0] A system comprising:	See analysis of portion [1.0].
[19.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[19.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[19.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[19.4] wherein the redirection server is configured to allow modification of at least a	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[19.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portion [16.4], where the modification includes removal of the portion of the rule set that corresponds to the login filtering profile.
[20.0] A system comprising:	See analysis of portion [1.0].
[20.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[20.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[20.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[20.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
from the user, or location the user accesses; and	
[20.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[21.0] A system comprising:	See analysis of portion [1.0].
[21.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[21.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[21.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[21.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
[21.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4], where the modification includes removal of the portion of the rule set that corresponds to the login filtering profile.
[22.0] A system comprising:	See analysis of portion [1.0].
[22.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[22.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[22.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[22.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[22.5] wherein the redirection server is	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.

Exhibit BB

US 6779118	Prior Art Analysis*
configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	
[23.0] A system comprising:	See analysis of portion [1.0].
[23.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[23.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[23.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[23.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[23.5] wherein the redirection server has a	Radia illustrates the recited network architecture in Fig. 1. The router 106 ("redirection server") has a "user side" that connects to a

Exhibit BB

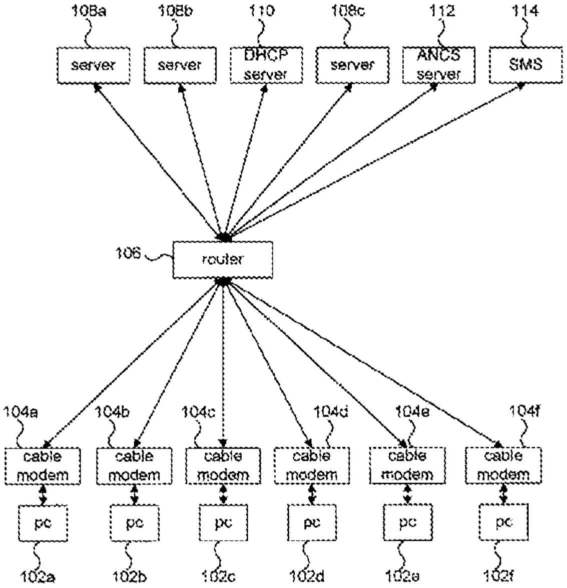
US 6779118	Prior Art Analysis*
user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	user's PC through a cable modem and a "network side" that connects to various servers.  108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 Radia also discloses that a user's computer receives a temporarily assigned IP address from a DHCP server. See analysis of portion [1.5].
[24.0] The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	Radia discloses that the router 106 receives instructions to modify its filtering rules from the ANCS server 112, illustrated in Fig. 1 above as located on the "network side" of the router: In step 604, the ***ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 to establish a packet filter*** for IP packets originating from the client system 102b. The packet filter is established by reconfiguring one or more of the components of the network 100 that forward packets originating at the client system 102b. For example, in some cases the packet filter may be established by reconfiguring the modem 104b connected to client system 102. Alternatively, the packet filter may be established by ***reconfiguring router 106***. (Radia, 6:66–7:8 (emphasis added).)

Exhibit BB

US 6779118	Prior Art Analysis*
[25.0] In a system comprising	See analysis of portion [1.0].
[25.1] a redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portion [1.3] and [1.5].
[25.2] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.2].
[25.3] the method comprising the step of:	See analysis of portion [8.4].
[25.4] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	Radia discloses that when a client system (PC) initially connects to the router 106, the router 106 is reconfigured with a "login filtering" profile. (See Radia, 7:38-49.) Subsequently, after a user logs into the system, "a sequence of filtering profiles 400 associated with the user are retrieved" and used to reconfigure the router 106. (See Radia, 9:46–10:14.) Radia discloses that the temporarily-assigned IP address remains the same through the procedure, as the IP address is allocated to the computer during a first step of four steps in the login process (Radia, 7:50-60).
[25.5] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.5].
[25.6] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection	See analysis of portion [23.5].

Exhibit BB

US 6779118	Prior Art Analysis*
server and	
[25.7] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[26.0] The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[27.0] The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[28.0] The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	Radia discloses that the filtering rules 404 can include a protocol type: Filtering rule 404 also includes a protocol type 506. **Protocol type 506 corresponds to the protocol type of an IP packet. Thus, the protocol type 506 of each filtering rule 404 has a value that corresponds to an IP packet type, such as TCP, UDP, ICMP, etc.** To match a particular filtering rule

Exhibit BB

US 6779118	Prior Art Analysis*
	404, an IP packet must have a protocol type that matches the protocol type 506 included in the filtering rule 404. (Radia, 6:29-36 (emphasis added).) Therefore, Radia discloses that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.
[29.0] The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	Radia discloses that when a client system (PC) initially connects to the router 106, the router 106 is reconfigured with a "login filtering" profile. (See Radia, 7:38-49.) Subsequently, after a user logs into the system, "a sequence of filtering profiles 400 associated with the user are retrieved" and used to reconfigure the router 106. (See Radia, 9:46–10:14.) Therefore, Radia discloses an initial temporary rule set and a standard rule set. Wong '727 shows creating a default filtering profile from a standard template. (Wong '727, 7:9-11). Therefore, Wong also teaches a standard rule set.
[29.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	As mentioned at [29.0], Radia teaches an initial, temporary rule set that is used during login. Subsequent to login, the user is assigned to another rule set, which in this scenario can include the standard rule set taught by Wong '727.
[30.0] The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	Radia discloses an example rule 404 that can specify an action 500 based on a number of criteria, including destination IP address, destination mask (both are types of destination), and protocol type (a request type—for example, a TCP-type request or an ICMP-type request). (Radia, Fig. 5 and 6:5-45).

Exhibit BB

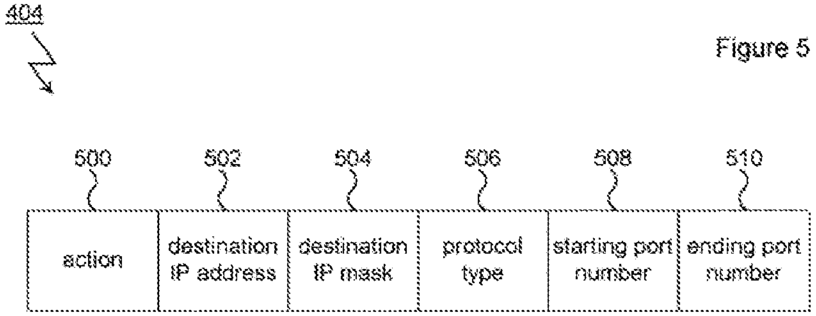
US 6779118	**Prior Art Analysis***
	 404 Figure 5 500 502 504 506 508 510 action destination IP address destination IP mask protocol type starting port number ending port number RADIA FIG. 5
[31.0] The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	As shown above at [1.3], it would have been obvious to add the redirection feature of the Admitted Prior Art to the filtering of Radia, where Admitted Prior Art discloses redirecting data to a new destination address: In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. ***The browser then requests the redirected WWW page*** according to the URL contained in the first page's html code. ('118 Patent, 1:54-58, emphasis added.) Furthermore, the rules of Radia may take an action based on an attempted destination address and a request type. See analysis at [30.0], citing Radia at Fig. 5 and 6:5-45. Thus, the combination of prior art discloses redirecting the data to a new address based on a request type and an attempted destination address.
[32.0] The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[33.0] The method of claim 8, wherein the individualized rule set	See analysis of portion [29.0].

Exhibit BB

US 6779118	Prior Art Analysis*
includes an initial temporary rule set and a standard rule set, and	
[33.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[34.0] The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[35.0] The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[36.0] A system comprising:	See analysis of portion [1.0].
[36.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[36.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[36.3] wherein the redirection server is configured to allow automated modification	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
of at least a portion of the rule set correlated to the temporarily assigned network address;	
[36.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[36.5] wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[37.0] A system comprising:	See analysis of portion [1.0].
[37.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[37.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[37.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[37.4] wherein the	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[37.5] wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[37.6] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[38.0] A system comprising:	See analysis of portion [1.0].
[38.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[38.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[38.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
[38.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[38.5] wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[39.0] A system comprising:	See analysis of portion [1.0].
[39.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[39.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[39.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[39.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	
[39.5] wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[40.0] The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[41.0] The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set,	See analysis of portion [29.0].
[41.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[42.0] The method of claim 25, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[43.0] The method of claim 25, wherein the modified rule set	See analysis of portion [31.0].

Exhibit BB

US 6779118	Prior Art Analysis*
includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[44.0] A system comprising:	See analysis of portion [1.0].
[44.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[44.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[44.3] a redirection server connected between the dial-up network server and a public network, and	See analysis of portion [1.3]. Radia teaches a redirection server that includes the router 106 and the ANCS 112. As shown in the annotated figure below, Radia's redirection server is placed between the dial-up network servers (cable modems 104) and servers 108 on the public network.

Exhibit BB

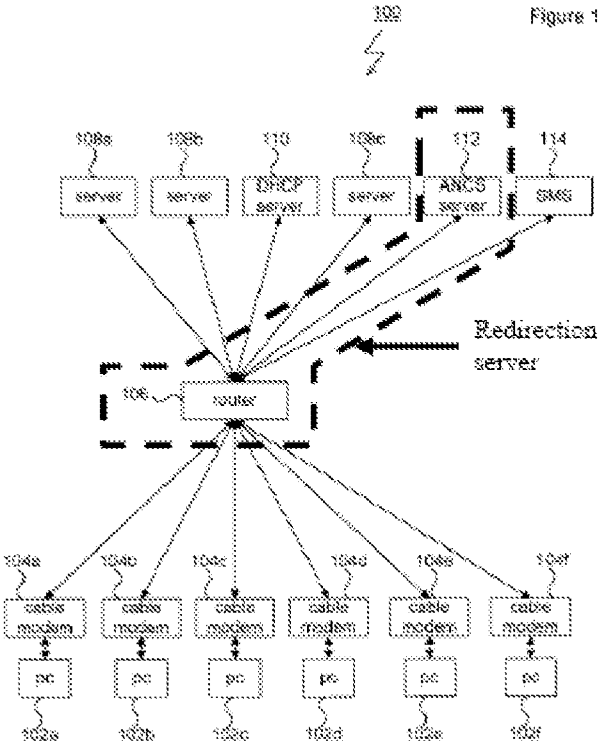
US 6779118	Prior Art Analysis*
	 100 Figure 1 108a 108b 110 108c 112 114 server server DHCP server server ANCS server SMS Redirection server 106 router 104a 104b 104c 104d 104e 104f cable modem cable modem cable modem cable modem cable modem cable modem pc pc pc pc pc pc 102a 102b 102c 102d 102e 102f RADIA FIG. 1 (ANNOTATED)
[44.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	See analysis of portion [1.4].
[44.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	See analysis of portion [1.5].
[44.6] wherein the authentication accounting server	See analysis of portion [1.6].

Exhibit BB

US 6779118	Prior Art Analysis*
accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	
[44.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	See analysis of portion [1.7].
[49.0] The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	See analysis of portion [6.0].
[50.0] The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	See analysis of portion [7.0].
[51.0] The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[52.0] The system of claim 44, wherein the individualized rule set includes an initial temporary rule set and a	See analysis of portion [29.0].

Exhibit BB

US 6779118	Prior Art Analysis*
standard rule set, and	
[52.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[53.0] The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[54.0] The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.1].
[55.0] The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above with respect to claim 44 (and citing to claim 1) that the prior art teaches blocking and redirection as a function of an individualized rule set. The Admitted Prior Art teaches controlling access to resources by redirecting World Wide Web traffic but notes that the same technique can be applied to any IP (Internet protocol) service: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, ***redirection is not limited to WWW traffic, and the concept is valid for all IP services***. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing

Exhibit BB

US 6779118	Prior Art Analysis*
	in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60 (emphasis added).) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that redirection could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Thus, it would have been obvious to redirect a user's request by "replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set" as recited in the claim. Requester notes that the Board found a similar claim limitation to be obvious in view of the Admitted Prior Art in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.)
[56.0] In a system comprising	See analysis of portion [1.0].
[56.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[56.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].

Exhibit BB

US 6779118	Prior Art Analysis*
[56.3] a redirection server connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portions [1.3] and [44.3].
[56.4] the method comprising the steps of:	See analysis of portion [8.4].
[56.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[56.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[56.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[61.0] The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a	See analysis of portion [6.0].

Exhibit BB

US 6779118	Prior Art Analysis*
function of the individualized rule set.	
[62.0] The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDS, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[63.0] The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[64.0] The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[64.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[65.0] The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[66.0] The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a	See analysis of portion [31.0].

Exhibit BB

US 6779118	Prior Art Analysis*
new destination address based on a request type and an attempted destination address.	
[67.0] The method of claim 56, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and the Admitted Prior Art. Additionally, see analysis of portion [55.0].
[68.0] A system comprising:	See analysis of portion [1.0].
[68.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[68.2] the redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[68.3] wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [16.2].
[68.4] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned	See analysis of portion [16.3].

Exhibit BB

US 6779118	Prior Art Analysis*
network address; and	
[68.5] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.	See analysis of portion [16.4].
[69.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portion [16.4].
[70.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4].
[71.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4].
[72.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.

Exhibit BB

US 6779118	Prior Art Analysis*
of time.	
[73.0] The system of claim 68, wherein the redirection sewer is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[74.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[75.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[76.0] The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily	See analysis of portion [23.5].

Exhibit BB

US 6779118	Prior Art Analysis*
assigned network address is connected to the computer network through the redirection server.	
[77.0] The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[78.0] The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[79.0] The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[79.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set	See analysis of portion [29.1].
[80.0] The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[81.0] The system of claim 68, wherein the	See analysis of portion [31.0].

Exhibit BB

US 6779118	Prior Art Analysis*
modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[82.0] The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the modified rule set.	It was shown above that claim 68 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [55.0].
[83.0] In a system comprising	See analysis of portion [1.0].
[83.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[83.2] the redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portions [1.3] and [1.6].
[83.3] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.1].
[83.4] the method comprising the step of:	See analysis of portion [8.4].
[83.5] modifying at least a portion of the user's rule set while the user's	See analysis of portion [25.4].

Exhibit BB

US 6779118	Prior Art Analysis*
rule set remains correlated to the temporarily assigned network address in the redirection server; and	
[83.6] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.0].
[83.7] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.0].
[83.8] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[84.0] The method of claim 83, further including; the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from	See analysis of portion [16.4].

Exhibit BB

US 6779118	Prior Art Analysis*
the user, and location or locations the user accesses.	
[85.0] The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[86.0] The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service,	See analysis of portion [28.0].
[87.0] The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[87.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[88.0] The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[89.0] The method of claim 83, wherein the	See analysis of portion [31.0].

Exhibit BB

US 6779118	Prior Art Analysis*
modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	
[90.0] The method of claim 83, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above that claim 83 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [55.0].

Exhibit BB

Proposed Rejection #6. Claims 2-5, 9-12, 45-48, and 57-60 are obvious over Radia in view of Wong '727 and Admitted Prior Art and further in view of Wong '178 under 35 U.S.C. § 103(a).

Reasons to combine Radia, Wong '727, and Admitted Prior Art with Wong '178

A description of the proposed combination of Radia, Wong '727, and Admitted Prior Art is provided is provided above. Radia, Wong '727, and Wong '178 share overlapping inventors, mutually incorporate one another by reference, and describe the same or similar system. Thus, these references include an express teaching that their disclosures should be combined. It would have been obvious to one of skill in the art to do so.

Wong '178 discloses a technique that includes filtering both upstream and downstream packets. In addition to the express reasons to combine given above, it would also be obvious to include upstream and downstream packet filtering in the system of Radia in order to provide increased security to the Radia system. Also, modifying Radia according to the teaching of Wong '178 to provide upstream and downstream filtering is a "use of known technique to improve similar devices (methods, or products) in the same way." (*See* MPEP § 2143, *citing KSR.*)

Exhibit BB

US 6779118	Prior Art Analysis[*]
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 1 (now canceled) is obvious over Radia, Wong '727, and Admitted Prior Art. As shown above at [1.7] Radia discloses filtering packets according to a function of individualized rule sets. Furthermore, Radia incorporates by reference (at 1:27-30) U.S. App. 08/762,709, now U.S. 6,073,178 to Wong. Wong '178 discloses "a method using [sic] for selectively forwarding, by router 106, of packets based on learned assignments of IP addresses." (Wong '178, 8:40-42.) Wong '178 discloses categorizing packets into "upstream" (from the client system) and "downstream" (to the client system) packets: > Generally, routers categorize packets into "upstream" and "downstream" packets. In the case of the network topology shown for network 100, upstream packets are packets that originate at one of the client systems 102. Downstream packets are packets that are directed at one of the client systems 102. (Wong '178, 8:47-52.) Wong '178 further discloses filtering both upstream and downstream packets based in part on their source and destination IP addresses: > If a downstream packet is detected in step 804, execution of method 800 continues at step 806 where the router 106 extracts the packet's destination address. ***Using this destination address, the router 106, in step 808 "looks up" the trusted identifier of the client system*** 102 that is associated with the destination address of the received packet (this association is formed by the router 106 during

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit BB

US 6779118	Prior Art Analysis*
	execution of method 600). In step 810, a test is performed to ascertain whether a trusted identifier was actually located in step 808. If a trusted identifier was located in step 808, execution of method 800 continues at step 812 where the router 106 forwards the received packet to client system associated with the trusted identifier. In the alternative, if no trusted identifier is associated with the destination address of the packet, ***the router 106 discards the packet*** in step 814. . . . In step 822, ***the router 106 compares the source address of the received packet with the authorized IP addresses*** that were looked up in step 820. If the source address of the packet matches one of the authorized IP addresses, the router 106 forwards the packet in step 824. Alternatively, if the source address of the received packet does not match one of the authorized IP addresses, the router 106 discards the packet in step 826. (Wong '178, 8:53 – 9:20, emphasis added). Thus Radia, which incorporates Wong '178 by reference, discloses providing control over data both *sent to* and *received from* the client systems. This may be performed as a function of individualized rule sets, as disclosed by Radia.
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Radia further discloses discarding packets that do not meet the filtering criteria established for a user: Subsequently, the new packet filter ***uses the rules of the user filtering profile*** sequence to selectively forward or ***discard IP packets*** originating from the client system. (Radia, 3:47-50.) Discarding the IP packet results in blocking data from the user's computer. As shown above at [2.0], it would be obvious to perform the function on data both to and from the user's computer.

Exhibit BB

US 6779118	Prior Art Analysis*
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. Radia further discloses forwarding packets that meet the filtering criteria established for a user: Subsequently, the new packet filter ***uses the rules of the user filtering profile*** sequence to ***selectively forward*** or discard IP packets originating from the client system. (Radia, 3:47-50.) Forwarding the IP packets results in allowing data from the user's computer. As shown above at [2.0], it would be obvious to perform the function on data both to and from the user's computer.
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	Radia discloses an "access network control server (ANCS)" that configures a router to enforce the packet filter (Radia, 5: 42-43): In step 604, the ANCS 112 uses the single filtering rule 404 included in the filtering profile 400 ***to establish a packet filter*** for IP packets originating from the client system 102b. For example, in some cases the packet filter may be established by reconfiguring the modem 104b connected to client system 102. Alternatively, ***the packet filter may be established by reconfiguring router*** 106. (Radia, 6:66 –7:2.) Radia further discloses that "the packet filter uses the rules of the login filtering profile sequence to selectively ***forward or discard IP packets*** originating from the client system." (Radia, 3:18-20.) By implementing the packet filter, the router controls a user's access to the network. As analyzed above in portion [1.3], the router and the ANCS together form a "redirection server." Radia also discloses a "filtering profile database" that includes a profile ID and filtering rules: The ***filtering profile database*** 316 of SMS 114 ***includes a set of filtering profiles*** of the type shown

Exhibit BB

US 6779118	Prior Art Analysis*
	in FIG. 4 and generally designated 400. Filtering profile 400 ***includes a profile id*** 402 ***and a series of filtering rules***, of which filtering rules 404a through 404c are representative. The profile id 402 is used by SMS 114 and ANCS 112 as an internal identifier for the filtering profile 400. (Radia, 6:5-11.) As analyzed above in portion [1.1], the group filtering rules associated with each user ID is an "individualized rule set." The Admitted Prior Art teaches controlling access to resources by redirecting traffic, for example, World Wide Web traffic: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.)

Exhibit BB

US 6779118	Prior Art Analysis*
	Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that in directing the user away from the website, the user's access to the website is blocked. Thus, redirection is an obvious extension of blocking and could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Requester notes that the Board made similar findings in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.) It would have been obvious to incorporate the redirection technique of the Admitted Prior Art into the system of Radia at least for the reasons given above and in the Reasons to Combine. As shown above at [2.0], it would be obvious to perform the function on data both to and from the user's computer. See also the analysis of portions [1.3] and [2.0]. Thus, Radia and the Admitted Prior Art render obvious "wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set."
[9.0] The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [2.0].
[10.0] The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [3.0].
[11.0] The method of claim 8, further including the step of allowing the data to and from the users'	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [4.0].

Exhibit BB

US 6779118	Prior Art Analysis*
computers as a function of the individualized rule set.	
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 8 (now canceled) is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [5.0].
[45.0] The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [2.0].
[46.0] The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [3.0].
[47.0] The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [4.0].
[48.0] The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 44 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [5.0].

Exhibit BB

US 6779118	Prior Art Analysis*
[57.0] The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [2.0].
[58.0] The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [3.0].
[59.0] The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [4.0].
[60.0] The method of claim 56, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	It was shown above that claim 56 is obvious over Radia, Wong '727, and Admitted Prior Art. Additionally, see analysis of portion [5.0].

Exhibit CC

Claim Charts with respect to He, Zenchelsky, and the Admitted Prior Art for Obviousness

Customer No.: 000027683

Haynes and Boone, LLP
IP Section
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone [214] 651.5000
Fax [214] 200.0853

Exhibit CC

Contents

References
He (Exhibit L, U.S. 6088451)
Zenchelsky (Exhibit K, U.S. 6233686)
Admitted Prior Art (APA)

Requester provides canceled claims 1, 8, and 25 in the claim chart below because other claims depend from those canceled claims or include the same features as those canceled claims. Requester does not propose new rejections for canceled claims 1, 8, and 25.

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

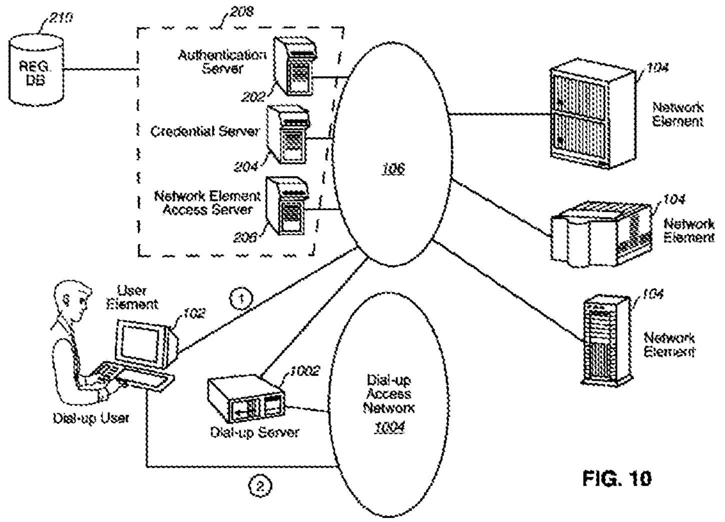
Exhibit CC

Proposed Rejection #7. Claims 2–7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky and the Admitted Prior Art under 35 U.S.C. § 103(a).

Reasons to Combine He, Zenchelsky, and the Admitted Prior Art

He teaches a system for controlling users' access to network resources. Zenchelsky is similarly directed to controlling users' access to a network, such as the Internet. The Admitted Prior Art discusses controlling users' access to web sites on the Internet by redirecting users' to an alternate destination. Thus, all of the references are generally directed to complementary technologies. Their combination is merely the application of known techniques (as taught by Zenchelsky and the Admitted Prior Art) to a known system (He) to yield predictable results. It would have been obvious to combine their teachings.

Requester notes that in a previous reexamination, the Board found—and the Patent Owner did not contest—that it would have been obvious to combine their teachings. *See Ex Parte Linksmart Wireless Technology, LLC*, Appeal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011) [*hereinafter* Board Decision or BPAI Decision].

US 6779118	Prior Art Analysis[*]
[1.0] A system comprising:	He discloses a system in Fig. 10:  210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 Dial-up User 1002 Dial-up Server Dial-up Access Network 1004 2 FIG. 10

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit CC

US 6779118	Prior Art Analysis*
[1.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	He discloses a database 210 (illustrated in Fig. 10). He further teaches a user ID associated with user credentials. The user credentials correspond to an individualized rule set: The authentication server 202 can maintain a ***database of records for the user accounts*** in the registration database 210. Each record of a user account generally comprises the following information: (1) The user identifier. This identifier is required and must be unique throughout the entire network within the same realm or administrative domain. It is the legal representation of the user in the network. (2) An alias user identifier. This alias identifier is optional whose purpose is to allow the same user to be identified through multiple means. (3) ***The list of user credentials***. This list shall reflect the most recent changes to the privilege set for the user. The privilege set can be built on previous achievements or credit history. For internal network users, however, it shall primarily be used to reflect the user's job responsibilities or affiliation with specific organizations that is the usual way of defining job responsibilities. (He, 16:50–67 (emphasis added).)
[1.2] a dial-up network server that receives user IDs from users' computers;	He teaches a dial-up server 1002 to "interface dial-up users with the network" (He, 30:42), illustrated in Fig 10:

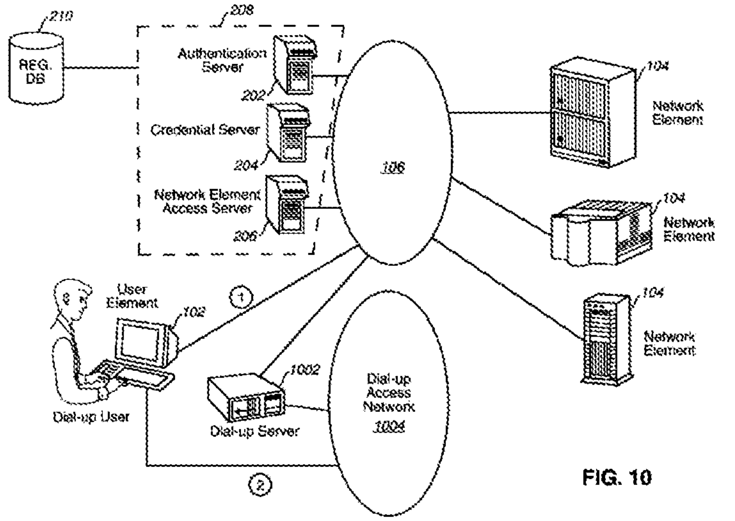
US 6779118	Prior Art Analysis*
	 210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 1002 Dial-up Access Network 1004 Dial-up User Dial-up Server 2 FIG. 10 He further teaches that the user transmits a user identifier to the authentication server: The user uses a user element 102 and initiates the authentication process by requesting to send a request message to the authentication server 202. The request message contains the user identifier presented to the authentication server 202 for user network authentication. (He, 17:55-60.) For users connected via the dial-up access network, it is understood that transmission of a user identifier to the authentication server 202 would first transit the dial-up server.
[1.3] a redirection server connected to the dial-up network server and a public network, and	He teaches a credential server 204: The credential server 204 responsible for controlling network user credentials or privileges, which is essential for effective network access control. (12:66–13:1.) As illustrated in Fig. 10, the credential server 204 is connected to the dial-up server 1002 via public network

Exhibit CC

US 6779118	Prior Art Analysis*
	106. The Admitted Prior Art teaches controlling access to resources by redirecting traffic on a public network, for example, World Wide Web traffic: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.) It would have been obvious to one of skill in the art to supplement the access control functions of the credential server to further include redirection capabilities that were already known in the art. For example, an address blocked

US 6779118	Prior Art Analysis*
	for a particular user would be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Thus, redirection is an obvious extension of the use of a control to block the user. Requester notes that the Board reached a similar conclusion in a previous reexamination of the '118 patent. (*See* Board Decision at 9.)
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	He teaches an authentication server 202. As illustrated in Fig. 10, the authentication server 202 is connected to the database 210. The authentication server 202 is also connected, through the network 106, to the dial-up server 1002 and credential (redirection) server 204.
[1.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	He teaches that a user logs onto the network via dial-up server 1002, which transmits the user's user ID to the authentication server: In the normal situation, a dial-up user access request is handled in the following steps: (1) The user dials into the dial-up server. The server authenticates the user based on any one of the available mechanisms in the module. (2) The dial-up server invokes the Kerberos client process and ***uses the user identifier and password to authenticate the user to the network***. (3) If Kerberos authentication is successful, user access to network elements will proceed with the security services offered by the Kerberos network security servers. (He, 31:1-9.) Zenchelsky teaches assigning a temporary IP address to a user at logon: A "user" is a computer that does not have a

Exhibit CC

US 6779118	Prior Art Analysis*
	fixed, assigned network address. To obtain connectivity to the Internet, for example, a user must commonly obtain a temporary IP address from a host with a pool of such addresses. Such a temporary IP address is retained by the user only for the duration of a single session of connectivity with the Internet. (Zenchelsky, 1:30-35.) Zenchelsky further teaches that each packet transmitted or received by the user includes the user's temporary IP address encoded as the source or destination: Information flows in certain networks in packets. A "packet" is a quantum of information that that has a header ***containing a source and a destination address***. . . . Another example of a packet identifier is a packet 5-tuple, which is the packet's source and destination address, source and destination port, and protocol. Packets with 5-tuples flow in connectionless packet switched networks. (Zenchelsky, 1:36-38 & 1:60-64.) The Admitted Prior Art further describes a dial-up network server sending a user's user ID and temporary IP address to an authentication and accounting server: The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104. ('118 Patent, 1:21-24.) It would have been obvious to one of ordinary skill in the art to modify He so as to provide a temporary IP address to

Exhibit CC

US 6779118	Prior Art Analysis*
	a user node and additionally to encode communications packets with that temporary IP address as the source or destination so as facilitate communication through a switched packet network as taught by Zenchelsky and the Admitted Prior Art.
[1.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	He teaches that the authentication server looks up a user in the database and obtains the user's credentials, which are an individualized rule set: (2) Upon receiving the user request message, the authentication server 202 uses the user identifier in the message to look up the user registration database 210 and retrieves a record corresponding to that user (user record). A response message is prepared by the authentication server 202 and sent back to the user. (He, 17:61-66.) He further teaches that the user's credentials are then presented to the credential ("redirection") server: The response message contains a general ticket for the user to communicate with the credential server 204 for authentification. ... (1) The user sends a message to the credential server 204 to request for a list of the user credentials. The message contains the ticket obtained by the user from the authentication server 202. The credential server 204 will not accept and process the request without being presented with the correct ticket from the user. The request message is encrypted with the temporary user-credential server secret key so that only the credential server 204 is able to retrieve the content of the message. (He, 17:67-18:1 & 18:57-65.)
[1.7] wherein data directed toward	He discloses that users direct data toward the public

Exhibit CC

US 6779118	Prior Art Analysis*
the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	network: By presenting the correct secret key to the local access control system, the user authenticates his/her identity to the network. The correctness of the user-supplied secret key is verified through the process of decrypting the response message. It is the ability to retrieve the ticket in the message that allows the user to proceed with the network access control process to access network resources and information. (He, 18:24-31.) For example, the user sends a request message to the credential server: The user sends a message to the credential server 204 to request for a list of the user credentials. The message contains the ticket obtained by the user from the authentication server 202. (He, 18:57-60.) He further teaches that the credential (redirection) server processes the user's request message using the user's credentials, which are an individualized rule set: Upon receiving the request message, the credential server 204 retrieves the information in the ticket and verifies that the request is indeed sent from the correct user. Based on the user identifier, the credential server 204 will retrieve the list of user credentials from the registration database 210 and enclose the list in a credential ticket. The credential ticket is sent back in a response message and will be used for the user to communicate with the network element access server 206. (He, 19:2-8.)

Exhibit CC

US 6779118	Prior Art Analysis*
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	He teaches that the user credentials correspond to an individualized rule set that control access to network resources: > The credential ticket is sent back in a response message and will be used for the user to communicate with the network element access server 206. The response message also contains a temporary secret key generated randomly by the credential server 204 ***to facilitate secure communications between the user and the network element access server*** 206. . . . > By presenting the correct ticket to the credential server 204, the user is able ***to obtain the list of user credentials necessary for requesting access to network resources*** and information. (He, 19:5-11 & 19:32-35 (emphasis added).) Thus, He teaches that the credential server (redirection server) controls the data a user may access as a function of the user's credentials. As previously noted, the credentials are an individualized rule set. Zenchelsky teaches controlling a user's access to data on a network using individualizd rules: > A rule base 53 is loaded into a filter to regulate the flow of information between users 51 and 53 and the hosts P, U, V and W on the Internet. The rule base shown in FIGS. 5a and 5b show only the source and destination addresses for each rule, and omit source and destination ports and protocol for simplicity. (Zenchelsky, 3:46-51.)

Exhibit CC

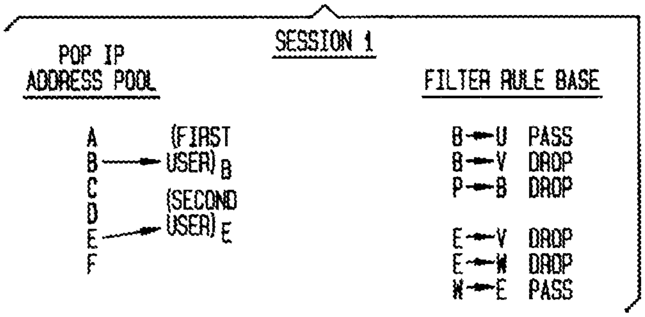
US 6779118	Prior Art Analysis*
	FIG. 5A (PRIOR ART)  SESSION 1 POP IP ADDRESS POOL A B C D E F (FIRST USER) B (SECOND USER) E FILTER RULE BASE B←U PASS B←V DROP P←B DROP E←V DROP E←W DROP W←E PASS As Zenchelsky illustrates in Fig. 5A, a first user "B" is permitted to communicate (pass data) with host U, but not host V. Similarly, second user "E" is permitted to receive data from host W, but may not send data to hosts V or W. Thus, Zenchelsky teaches using individualized rules to control data passing to and from a user's computer. The Admitted Prior Art further describes applying a packet filter to control a user's access to a public network, such as the Internet and the world wide web: Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, ***they can filter outgoing packets sent from users to a specific destination*** as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. Packet filter devices are often used with proxy server systems, which ***provide access control to the Internet and are most often used to control access to the world wide web***.... Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded.

Exhibit CC

US 6779118	Prior Art Analysis*
	('118 Patent, 2:1-38.)
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. It would have been obvious to one of skill in the art that a user's access request should be blocked if the user's credentials do not allow for access to the requested resource. He also describes blocking a user's access request if the user has tampered with the ticket received from the credential server: Any attempts by the user to try to make any changes to the ticket, intentional or unintentional, will be detected by the network element access server when it is used for communications with the server 106 and, therefore, would void the ticket and make it useless. This is to prevent the user from modifying the list of certified user credentials as well as other information in the ticket to gain unauthorized network access rights. (He, 19:24-31.)
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. The credential server "facilitate[s] secure communications,"—that is, allows data to and from the user—using the user's credentials. (He, 19:10.)
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portions [1.3] and [2.0]. The Admitted Prior Art teaches redirection. ('118 Patent, 1:38-60.) It would have been obvious to add the known techniques of data redirection to the credential server of He. For example, it would have been obvious for the credential server to redirect a user who had not yet authenticated his identity to the authentication server for that purpose. As another example, it would have been obvious for the credential server to redirect a user to a particular network

Exhibit CC

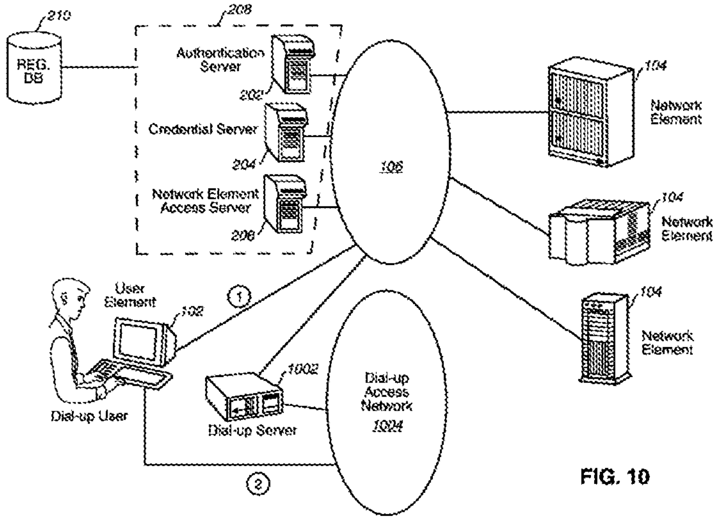
US 6779118	Prior Art Analysis*
	element 104 to provide a requested resource.
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	He illustrates in Fig. 10 that there are multiple potential destinations, such as network elements 104, for further interaction based on a user's credentials:  210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 Dial-up User 1002 Dial-up Server Dial-up Access Network 1004 2 FIG. 10 It would have been obvious for the credential server to redirect users' requests to these multiple destinations.
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	He describes assigning user credentials based on a user's obligations or roles: The user credentials for a user may be determined in a variety of ways. They may be established based on criteria that are related to the past history of the user regarding the behaviors of access to network resources and information. They may also be established ***based on the current obligations or roles the user plays*** in the network. For example, the organization that consists of a department number and a location code can reflect the current responsibility the users have in their job and, therefore, can be used as the user credentials to determine the access rights for the users to access network elements. Other user credentials can be similarly identified and used for the access control purposes that help enforce the

Exhibit CC

US 6779118	Prior Art Analysis*
	principle of "need-to-know." (He, 13:30-42, emphasis added.) It would have been obvious that multiple users with common obligations or roles could be correlated to a common credential, such as an administrator role credential. He further describes additional rules stored in the database, such as the minimum password length and number of failed log-in attempts: Each record of a user account generally comprises the following information: ... (5) Other administrative information to enhance the effectiveness of the network security mechanisms. The information includes, but not limited to, the minimum length of the password, the required variation of password characters, the expiration date or the lifetime of the password since creation, the maximum lifetime of each authentication, and the maximum number of failed authentication attempts that is allowed before the account is brought to the attention to the system security administrator for examination or is simply disabled temporarily pending such an examination. (He, 16:52-53 & 17:6-18.) It would have been obvious to establish common policies for these rules that would apply to multiple (or all) users.

Exhibit CC

US 6779118	Prior Art Analysis*
[8.0] In a system comprising	See analysis of portion [1.0].
[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[8.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	See analysis of portion [1.3].
[8.4] the method comprising the steps of:	He discloses a method: A high-level description of a method according to the present invention will now be described in connection with a flow diagram 400 in FIG. 4. (He, 25:21-23.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[8.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[9.0] The method of claim 8,	See analysis of portion [2.0]

Exhibit CC

US 6779118	Prior Art Analysis*
further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	
[10.0] The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0]
[11.0] The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0]
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0]
[13.0] The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[14.0] The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portions [1.1] and [1.7]. The user's credentials are a "plurality of functions used to control passing."
[16.3] wherein the redirection	He teaches a database tool associated with the server

Exhibit CC

US 6779118	Prior Art Analysis*
server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	system for creating, modifying, and deleting user accounts: It is desirable that a database tool be provided for the system security administrator to create, delete, disable and modify a user account. Such a tool should provide a user-friendly interface to aid the system security administrator to effectively and conveniently manage user accounts, as would be apparent to a person skilled in the art. This requirement should not be under-looked as correct user account administration and management is the basis for all other effective network access control mechanisms. (He, 17:19-27.) He's database tool is "automated" as required by the claim. Requester notes that in a previous reexamination of the '118 patent, the Patent Office interpreted "automated" as requiring the "use of automation, not the absence of any human intervention." (Board Decision at 7.)
[16.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	He teaches that passwords and authentications should have a defined lifetime, and that a limited number of log-in attempts should be permitted: Each record of a user account generally comprises the following information: ... (5) Other administrative information to enhance the effectiveness of the network security mechanisms. The information includes, but not limited to, the minimum length of the password, the required variation of password characters, the ***expiration date or the lifetime of the password*** since creation,

Exhibit CC

US 6779118	Prior Art Analysis*
	the maximum ***lifetime of each authentication***, and the ***maximum number of failed authentication attempts*** that is allowed before the account is brought to the attention to the system security administrator for examination or is simply disabled temporarily pending such an examination. (He, 16:52-53 & 17:6-18 (emphasis added).) Thus, at the end of an authentication's lifetime, it would have been obvious for the credential server to modify its behavior to cease allowing access to network resources until the user re-authenticates. Similarly, it would have been obvious to refuse access to a user using an expired password. Thus, He teaches modifying a user's credentials as a function of time. A failed authentication attempt is "data transmitted to or from the user." Thus, He teaches modifying a user's credentials (for example, by flagging for administrative review or by disabling the account) as a function of "data transmitted to or from the user." Furthermore, blocking a website based on some combination of the recited bases—time, data transmitted to or from the user, or location the user accesses—would have been obvious to one of skill in the art. For example, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to work. Similarly in a school environment, it would have been obvious in a workplace setting to block a website for a user after discovering inappropriate communications between the user and the website or after discovering the user spends excessive time at the site unrelated to school. Thus, although an initial rule set might be permissive, it would be obvious to modify the rules for a particular user at a later time after it is found that the user's data transmissions or locations accessed are unproductive

Exhibit CC

US 6779118	Prior Art Analysis*
	or inappropriate. Thus, He, Zenchelsky and the Admitted Prior Art render obvious "modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user access" as recited in the claim. Accordingly, Requester has provided an independent explanation of the pertinence and manner of applying the prior art to this claim limitation. Requester notes that the Board similarly found that this limitation would have been obvious to one of skill in the art. (*See* Board Decision at 10.)
[16.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	As shown above in the analysis of portion [16.4], He teaches modifying a user's credentials as a function of time. Additionally, as explained in portion [16.4], modifying a rule set as a function of time would have been obvious.
[17.0] A system comprising:	See analysis of portion [1.0].
[17.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[17.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[17.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[17.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[17.5] wherein the redirection	As shown in the analysis of portion [16.4], He teaches

Exhibit CC

US 6779118	Prior Art Analysis*
server is configured to allow modification of at least a portion of the rule set as a function of the data transmitted to or from the user.	modifying a user's credentials as a function of data transmitted to or from the user. Additionally, as explained in portion [16.4], modifying a rule set as a function of data transmitted to or from the user would have been obvious.
[18.0] A system comprising:	See analysis of portion [1.0].
[18.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[18.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[18.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[18.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[18.5] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [16.4]. It would have been obvious to modify a user's credentials as a function of the location or locations the user accesses.
[19.0] A system comprising:	See analysis of portion [1.0].
[19.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[19.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].

Exhibit CC

US 6779118	Prior Art Analysis*
[19.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[19.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[19.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portions [16.3], [16.4] and [16.5]. He's teaching that an administrator may create or delete any portion of a user account corresponds to the "removal or reinstatement of at least a portion of the rule set."
[20.0] A system comprising:	See analysis of portion [1.0].
[20.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[20.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[20.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[20.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[20.5] wherein the redirection server is configured to allow the removal or reinstatement of at	See analysis of portions [16.3], [16.4] and [17.5]. He teaches removing a portion of a user's rule set, for example, by disabling a user's account after a given number of

Exhibit CC

US 6779118	Prior Art Analysis*
least a portion of the rule set as a function of the data transmitted to or from the user.	authentication failures.
[21.0] A system comprising:	See analysis of portion [1.0].
[21.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[21.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[21.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[21.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[21.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5]. Based on He's teaching of removing a portion of a user's rule set, for example, by disabling a user's account after a given number of authentication failures, it would have been obvious to remove or reinstate at least a portion of the rule set as a function of the location the user accesses. For example, it would have been obvious to disable a user's account if the user made repeated attempts to access an unauthorized resource.
[22.0] A system comprising:	See analysis of portion [1.0].
[22.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[22.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a	See analysis of portion [16.2].

Exhibit CC

US 6779118	Prior Art Analysis*
public network;	
[22.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[22.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[22.5] wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.3], [16.4] and [18.5].
[23.0] A system comprising:	See analysis of portion [1.0].
[23.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[23.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[23.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[23.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or	See analysis of portion [16.4].

Exhibit CC

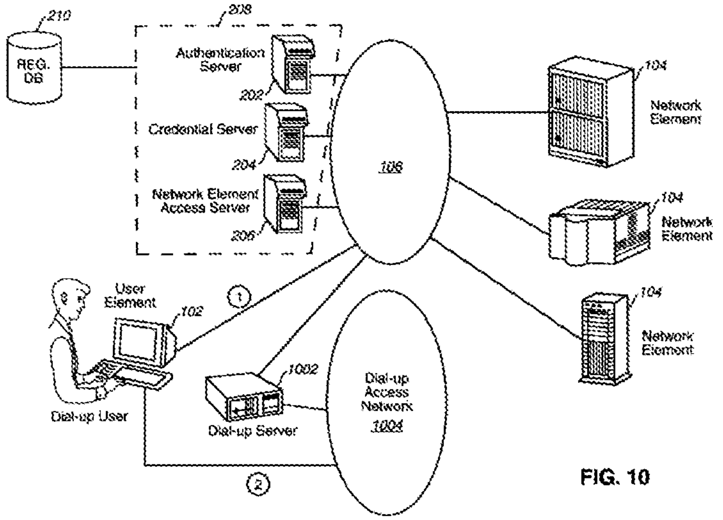
US 6779118	**Prior Art Analysis**[*]
location the user accesses; and	
[23.5] wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	He illustrates in Fig. 10 that the credential server 204 has a "user side," such as the connection to the dial up server 1002 or the dial up access network 1004. The user side is further connected to a user computer 102. As discussed above in portion [1.5], it would have been obvious to assign the user computer 102 a temporary network address as taught by Zenchelsky.  210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 Dial-up User 1002 Dial-up Server Dial-up Access Network 1004 2 FIG. 10 Fig. 10 further illustrates that the credential server has a "network side," such as the connect to network 106 and network elements 104. The user computer 102 is connected to network elements 104 through the credential server 204. For example, as analyzed above in portion [1.3], the credential server 204 controls access to network elements 104. Furthermore, the logical and physical topologies in a network can be very different. The '118 Patent describes the claimed redirection server as being "logically located between the user's computer 100 and the network." ('118 Patent at 4:50-51.) He's credential server 204 is logically located between the user computer 102 and the network elements 104, and thus He teaches the network structure recited in the claim. Requester notes that the Board reached a similar conclusion in a previous reexamination of the '118 patent. (*See* Board Decision at 6.)

Exhibit CC

US 6779118	Prior Art Analysis*
[24.0] The system of claim 23 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	He illustrates in Fig. 10 a user accessing the credential server 204. As analyzed above in portion [16.3], He teaches a network administrator modifying a user's credentials. A network administrator is also a user. Accordingly, a network administrator's instructions originating at user computer 102 proceed through the user side elements 1002 and 1004 as well as the network side element 106.
[25.0] In a system comprising	See analysis of portion [1.0].
[25.1] a redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portion [1.3] and [1.5].
[25.2] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.2].
[25.3] the method comprising the step of:	See analysis of portion [8.4].
[25.4] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	See analysis of portion [16.3].
[25.5] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.5].
[25.6] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.5].
[25.7] the method further includes	See analysis of portion [24.0].

Exhibit CC

US 6779118	Prior Art Analysis*
the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection server.	
[26.0] The method of claim 25, further including the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[27.0] The method of claim 25, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4].
[28.0] The system of claim 1, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	The Admitted Prior Art teaches filtering rules based on the type of IP service: ***Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years***. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, they can filter outgoing packets sent from users to a specific destination as well. ***Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet.*** For example, the packet filter can determine if the packet contains FTP (file transfer protocol) data, WWW data, or Telnet session data. ('118 Patent, 2:1-11 (emphasis added).)

Exhibit CC

US 6779118	Prior Art Analysis*
[29.0] The system of claim 1, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	Zenchelsky teaches both global filtering rules that apply to all users and local filtering rules that are specific to each user: The global pre-rule se 701 usually comprises general rules that apply to all hosts behind the firewall, and are most efficiently applied before any local rules. An example of a global pre-rule is that no telnet (remote login) requests are allowed past the firewall. The local rule base 702 comprises the set of peer rule bases loaded into the filter for authenticated peers. These rule pertain to specific hosts. An example of a local rule is that host A may not receive e-mail from beyond of the firewall. (Zenchelsky, 5:66–6:8.) The global rules are a "temporary rule set," and the local rules are a "standard rule set." In addition, He teaches that there exist multiple users, each with individualized credentials. Thus, a first user's credentials correspond to an "initial temporary rule set" and a second user's credentials correspond to a "standard rule set." Furthermore, it would have been obvious to apply a temporary set of rules before a user is authenticated. For example, He's credential server allows—and even *requires*—an unauthenticated user to communicate with the authentication server for the purpose of becoming authenticated: User credential/privilege control requires that the credential server 204 be relied upon to provide and certify the user credential information to be presented to a network element 104 for the local access control system to make further access decisions on network resources and information. It also

Exhibit CC

US 6779118	Prior Art Analysis*
	requires that the user first establish network authentication with the authentication server 202 in order to obtain a ticket to communicate with the credential server 204. (He, 18:34-41, emphasis added.) It is understood that the credential server does not permit an unauthenticated user to communicate with other servers, such as network elements 104. Thus, He teaches an initial temporary rule set that permits unauthenticated users to communicate with the authentication server. After the user is authenticated, the credential server provides the user's standard rule set.
[29.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	Zenchelsky teaches that the global filtering rules (a "temporary rule set") are always applied even before a user authenticates. After authentication, the user's "standard" rules are applied until the user disconnects: The global pre-rule se 701 usually comprises general rules that apply to all hosts behind the firewall, and are most efficiently applied before any local rules. (Zenchelsky, 5:66–6:1.) In accordance with the present invention, each individual peer is authenticated upon requesting network access. The peer's local rule base is then loaded into the filter of the present invention, either from the peer itself, or from another user, host or peer. When the peer is no longer authenticated to the POP (e.g., the peer loses connectivity or logs off from the POP), the peer's local rule base is ejected (deleted)from the filter. (Zenchelsky, 5:17-24.) The local rule base 702 is the set of all per user rule bases that are dynamically loaded upon authentication and ejected upon loss of

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td></td><td><blockquote>authentication in accordance with the present invention.
...
This rule base architecture advantageously retains the functionality of known filters. For example, if there are rules in the global pre- or post-rule base only, the filter behaves the same as known filters. If there are only rules in the local rule base, the filter has all of the new and innovative features of the present invention without having global rules.</blockquote><p>(Zenchelsky, 6:36-39 & 6:54–59.)</p></td></tr>
<tr><td>[30.0] The system of claim 1, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.</td><td><p>Zenchelsky teaches filtering rules allowing access based on a request type, such as a port number or protocol version, and a destination address:</p>
<table>
<tr><th>SOURCE</th><th>DESTINATION</th><th></th><th></th></tr>
<tr><th>Address, Port</th><th>Address, Port</th><th>VERSION</th><th>ACTION</th></tr>
<tr><td>A,21</td><td>G,32</td><td>4</td><td>PASS</td></tr>
<tr><td>A,22</td><td>H,19</td><td>3</td><td>DROP</td></tr>
<tr><td>G,11</td><td>A,64</td><td>4</td><td>DROP</td></tr>
<tr><td>C,9</td><td>I,23</td><td>4</td><td>PASS</td></tr>
</table>
<p>(Zenchelsky, 3:6–13.)</p>
<p>In addition, the Admitted Prior Art teaches filtering rules allowing access based on a request type and a destination address:</p>
<blockquote>Packet filtering devices allow network administrators to filter packets based on the source and/or destination information, as well as on the type of service being transmitted within each IP packet.</blockquote>
<p>('118 Patent, 2:14-18.)</p></td></tr>
<tr><td>[31.0] The system of claim 1, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a</td><td><p>As analyzed above in portion [1.3], it would have been obvious to combine the system of He and Zenchelsky with the known technique of redirection.</p><p>The Admitted Prior Art further teaches an example of</p></td></tr>
</table>

Exhibit CC

US 6779118	Prior Art Analysis*
request type and an attempted destination address.	redirecting a user's request based on an a request type (for example, communications protocol or specific web page identification) and destination address (for example, the Internet domain name or IP address): First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the ***communications protocol***, the location of the server (typically ***an Internet domain name or IP address***), and the ***location of the page on the remote server***. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. ('118 Patent, 1:46-58 (emphasis added).)
[32.0] The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[33.0] The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[33.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[34.0] The method of claim 8, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].

Exhibit CC

US 6779118	Prior Art Analysis*
[35.0] The method of claim 8, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[36.0] A system comprising:	See analysis of portion [1.0].
[36.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[36.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[36.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[36.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[36.5] wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[37.0] A system comprising:	See analysis of portion [1.0].
[37.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[37.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].

Exhibit CC

US 6779118	Prior Art Analysis*
[37.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[37.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[37.5] wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[37.6] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[38.0] A system comprising:	See analysis of portion [1.0].
[38.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[38.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[38.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[38.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or	See analysis of portion [16.4].

Exhibit CC

US 6779118	Prior Art Analysis*
location the user accesses; and	
[38.5] wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[39.0] A system comprising:	See analysis of portion [1.0].
[39.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[39.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portion [16.2].
[39.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	See analysis of portion [16.3].
[39.4] wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses; and	See analysis of portion [16.4].
[39.5] wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[40.0] The method of claim 25, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[41.0] The method of claim 25, wherein the modified rule set includes an initial temporary rule set and a standard rule set,	See analysis of portion [29.0].
[42.0] The method of claim 25,	See analysis of portion [30.0].

Exhibit CC

US 6779118	Prior Art Analysis*
wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	
[43.0] The method of claim 25, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[44.0] A system comprising:	See analysis of portion [1.0].
[44.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[44.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[44.3] a redirection server connected between the dial-up network server and a public network, and	See analysis of portion [1.3]. During the previous reexamination, the examiner stated that the "between" limitation of portion [44.3] distinguished the claim over the He network. (*See* Notice of Intent to Issue Reexamination Certificate at 4.) However, the examiner failed to consider that this "between" limitation is taught by Zenchelsky and the Admitted Prior Art. For example, Zenchelsky illustrates in Fig. 4 positioning a filter for controlling access (for example, a redirection server) between a user and the Internet: The architecture illustrated in FIG. 4 shows another known solution to providing information systems security on a POP. The known filter 46 implements a security policy for packets flowing between the Internet 45 and hosts 41 and 42. (Zenchelsky, 4:23-27.)

Exhibit CC

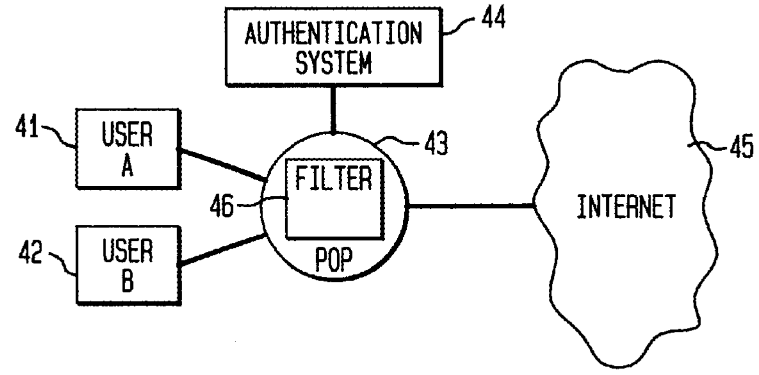
US 6779118	Prior Art Analysis*
	 AUTHENTICATION SYSTEM 44 41 USER A 43 45 FILTER 46 INTERNET 42 USER B POP Zenchelsky further describes a typical scenario of filtering a user's traffic directed toward the public network: FIG. 5a shows a first session where a first user 51 has requested Internet access and been authenticated by a POP and been assigned IP address B from the POP IP address pool 52. Likewise, a second user 53 has been authenticated and been assigned IP address E from the pool 52. A rule base 53 is loaded into a filter to regulate the flow of information between users 51 and 53 and the hosts P, U, V and W on the Internet. The rule base shown in FIGS. 5a and 5b show only the source and destination addresses for each rule, and omit source and destination ports and protocol for simplicity. (Zenchelsky, 3:41-51.) In addition, the Admitted Prior Art teaches that it was known to control access to network resources using a filtering device located between a user's local network and a public network: In a typical configuration, a firewall or other packet filtering device filters all WWW requests to the Internet from a local network, except for packets from the proxy server. That is to say that a packet filter or firewall blocks all traffic originating from within the local network which is destined for

Exhibit CC

US 6779118	Prior Art Analysis*
	connection to a remote server on port 80 (the standard WWW port number). However, the packet filter or firewall permits such traffic to and from the proxy server. Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. When the proxy server receives a packet, the destination is checked against a database for approval. If the destination is allowed, the proxy server simply forwards packets between the local user and the remote server outside the firewall. ('118 Patent, 2:27-42.) Thus, in view of the teachings of Zenchelsky and the Admitted Prior Art, it would have been obvious to position the redirection server between the dial-up network server and a public network.
[44.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	See analysis of portion [1.4].
[44.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	See analysis of portion [1.5].
[44.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	See analysis of portion [1.6].
[44.7] wherein data directed toward the public network from the one of the users' computers are	See analysis of portion [1.7].

Exhibit CC

US 6779118	Prior Art Analysis*
processed by the redirection server according to the individualized rule set.	
[45.0] The system of claim 44, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0].
[46.0] The system of claim 44, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[47.0] The system of claim 44, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[48.0] The system of claim 44, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0].
[49.0] The system of claim 44, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	See analysis of portion [6.0].
[50.0] The system of claim 44, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	See analysis of portion [7.0].
[51.0] The system of claim 44, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[52.0] The system of claim 44, wherein the individualized rule set includes an initial temporary rule	See analysis of portion [29.0].

Exhibit CC

US 6779118	Prior Art Analysis*
set and a standard rule set, and	
[52.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[53.0] The system of claim 44, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[54.0] The system of claim 44, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.1].
[55.0] The system of claim 44, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	It was shown above with respect to claim 44 (and citing to claim 1) that the prior art teaches blocking and redirection as a function of an individualized rule set. The Admitted Prior Art teaches controlling access to resources by redirecting World Wide Web traffic but notes that the same technique can be applied to any IP (Internet protocol) service: The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, ***redirection is not limited to WWW traffic, and the concept is valid for all IP services***. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides

Exhibit CC

US 6779118	Prior Art Analysis*
	information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60 (emphasis added).) Thus, the Admitted Prior Art teaches that redirection may be used, for example, to direct a user away from a website. It would have been obvious that redirection could be used, for example, to replace an address with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Thus, it would have been obvious to redirect a user's request by "replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set" as recited in the claim. Requester notes that the Board found a similar claim limitation to be obvious in view of the Admitted Prior Art in a previous reexamination of the '118 patent. (*See* BPAI Decision at 9.)
[56.0] In a system comprising	See analysis of portion [1.0].
[56.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[56.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[56.3] a redirection server	See analysis of portions [1.3] and [44.3].

Exhibit CC

US 6779118	Prior Art Analysis*
connected between the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the redirection server,	
[56.4] the method comprising the steps of:	See analysis of portion [8.4].
[56.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[56.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[56.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[57.0] The method of claim 56, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0].
[58.0] The method of claim 56, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0].
[59.0] The method of claim 56, further including the step of allowing the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [4.0].
[60.0] The method of claim 56,	See analysis of portion [5.0].

Exhibit CC

US 6779118	Prior Art Analysis*
further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	
[61.0] The method of claim 56, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[62.0] The method of claim 56, further including the step of creating database entries for a plurality of the plurality of users' IDS, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[63.0] The method of claim 56, wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[64.0] The method of claim 56, wherein the individualized rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[64.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[65.0] The method of claim 56, wherein the individualized rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[66.0] The method of claim 56, wherein the individualized rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[67.0] The method of claim 56,	See analysis of portion [55.0].

Exhibit CC

US 6779118	Prior Art Analysis*
wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header by a second destination address as a function of the individualized rule set.	
[68.0] A system comprising:	See analysis of portion [1.0].
[68.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[68.2] the redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[68.3] wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [16.2].
[68.4] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address; and	See analysis of portion [16.3].
[68.5] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses.	See analysis of portion [16.4].
[69.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	See analysis of portions [16.4] and [16.5].
[70.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set	See analysis of portion [17.5].

Exhibit CC

US 6779118	Prior Art Analysis*
as a function of the data transmitted to or from the user.	
[71.0] The system of claim 68, wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portions [16.4] and [18.5].
[72.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time.	See analysis of portion [19.5].
[73.0] The system of claim 68, wherein the redirection sewer is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the data transmitted to or from the user.	See analysis of portion [20.5].
[74.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of the location or locations the user accesses.	See analysis of portion [21.5].
[75.0] The system of claim 68, wherein the redirection server is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of some combination of time, data transmitted to or from the user, or location or locations the user accesses.	See analysis of portions [16.4], [18.5] and [22.5].
[76.0] The system of claim 68, wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network side connected to a computer network and wherein	See analysis of portion [23.5].

Exhibit CC

US 6779118	Prior Art Analysis*
the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	
[77.0] The system of claim 68 wherein instructions to the redirection server to modify the rule set are received by one or more of the user side of the redirection server and the network side of the redirection server.	See analysis of portion [24.0].
[78.0] The system of claim 68, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	See analysis of portion [28.0].
[79.0] The system of claim 68, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[79.1] and wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set	See analysis of portion [29.1].
[80.0] The system of claim 68, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[81.0] The system of claim 68, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[82.0] The system of claim 68, wherein the redirection server is configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet protocol) packet header	See analysis of portion [55.0].

Exhibit CC

US 6779118	Prior Art Analysis*
by a second destination address as a function of the modified rule set.	
[83.0] In a system comprising	See analysis of portion [1.0].
[83.1] a redirection server connected between a user computer and a public network,	See analysis of portions [1.3] and [44.3].
[83.2] the redirection server containing a user's rule set correlated to a temporarily assigned network address	See analysis of portions [1.3] and [1.6].
[83.3] wherein the user's rule set contains at least one of a plurality of functions used to control data passing between the user and a public network;	See analysis of portion [1.1].
[83.4] the method comprising the step of:	See analysis of portion [8.4].
[83.5] modifying at least a portion of the user's rule set while the user's rule set remains correlated to the temporarily assigned network address in the redirection server; and	See analysis of portion [25.4].
[83.6] and wherein the redirection server has a user side that is connected to a computer using the temporarily assigned network address and a network address and a network side connected to a computer network and	See analysis of portion [23.0].
[83.7] wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	See analysis of portion [23.0].
[83.8] the method further includes the step of receiving instructions by the redirection server to modify at least a portion of the user's rule set through one or more of the user side of the redirection server and the network side of the redirection	See analysis of portion [24.0].

Exhibit CC

US 6779118	Prior Art Analysis*
server.	
[84.0] The method of claim 83, further including; the step of modifying at least a portion of the user's rule set as a function of one or more of: time, data transmitted to or from the user, and location or locations the user accesses.	See analysis of portion [16.4].
[85.0] The method of claim 83, further including the step of removing or reinstating at least a portion of the user's rule set as a function of one or more of: time, the data transmitted to or from the user and a location or locations the user accesses.	See analysis of portion [16.4], where the modification includes at least removal of a portion of the rule set.
[86.0] The method of claim 83, wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service,	See analysis of portion [28.0].
[87.0] The method of claim 83, wherein the modified rule set includes an initial temporary rule set and a standard rule set, and	See analysis of portion [29.0].
[87.1] wherein the redirection server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	See analysis of portion [29.1].
[88.0] The method of claim 83, wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	See analysis of portion [30.0].
[89.0] The method of claim 83, wherein the modified rule set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	See analysis of portion [31.0].
[90.0] The method of claim 83, wherein the redirection server is	See analysis of portion [55.0].

Exhibit CC

US 6779118	Prior Art Analysis*
configured to redirect data from the users' computers by replacing a first destination address in an IP (Internet Protocol) packet header by a second destination address as a function of the individualized rule set.	

Exhibit DD

Claim Charts with respect to He, Zenchelsky, Fortinsky and the Admitted Prior Art for Obviousness

Exhibit DD

Contents

References
He (Exhibit L, U.S. 6088451)
Zenchelsky (Exhibit K, U.S. 6233686)
Fortinsky (Exhibit M, U.S. 5815574)
Admitted Prior Art (APA)

Requester provides canceled claims 1, 8, and 25 in the claim chart below because other claims depend from those canceled claims or include the same features as those canceled claims. Requester does not propose new rejections for canceled claims 1, 8, and 25.

The following is a quotation of 35 U.S.C. § 103(a) that forms the basis of all obviousness rejections:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Exhibit DD

Proposed Rejection #8. Claims 2–7, 9-14, 16-24, and 26-90 are obvious over He in view of Zenchelsky, Fortinsky, and the Admitted Prior Art under 35 U.S.C. § 103(a).

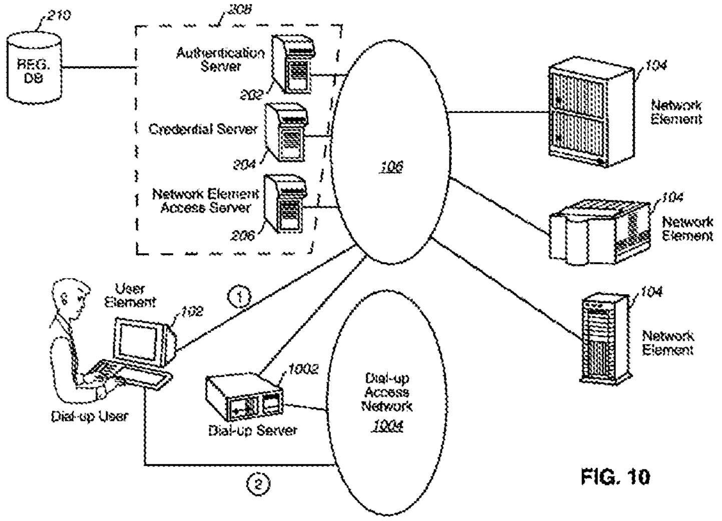
Reasons to Further Combine He, Zenchelsky, the Admitted Prior Art, and Fortinsky

He teaches a system for controlling users' access to network resources. Zenchelsky is similarly directed to controlling users' access to a network, such as the Internet. The Admitted Prior Art discusses controlling users' access to web sites on the Internet by redirecting users' to an alternate destination. Thus, all of the references are generally directed to complementary technologies. Their combination is merely the application of known techniques (as taught by Zenchelsky and the Admitted Prior Art) to a known system (He) to yield predictable results. It would have been obvious to combine their teachings. Their combination is merely the application of known techniques (as taught by Zenchelsky and the admitted prior art) to a known system (He) to yield predictable results. Requester notes that the Board of Patent Appeals and Interferences (BPAI) explicitly reached essentially the same conclusion with respect to the '118 patent in the previous reexamination. (*See Ex Parte Linksmart Wireless Technology, LLC*, Appeal No. 2011-009566, slip opinion at 9 (BPAI, August 23, 2011) [*hereinafter* Board Decision or BPAI Decision].)

He discloses a ticket-based network security architecture using the Kerberos authentication scheme developed at MIT. (*See, e.g.*, He, 29:27–30:7.) With a single authentication, a user can obtain a ticket that provides access to services provided by various network elements. Fortinsky discloses a similar ticket-based security architecture in which a security server provides tickets for accessing application servers on the network. The Fortinsky architecture uses the same Kerberos technology. (Fortinsky, 1:23-30.) Thus, both He and Fortinsky are directed to using MIT's Kerberos authentication and security technology to control users' access to network resources.

Fortinsky further describes a gateway server that, using the Kerberos security technology, allows a user to present a valid ticket to obtain access to an external network. It would have been obvious to incorporate Fortinsky's gateway server into He's network, as this is merely the substitution of a known element (one of He's network elements) for another known in the field (Fortinsky's gateway server.) The combination is also merely the use of a known technique (employing a Kerberos-based gateway server to an external network) to improve a similar system (He's Kerberos-based network) in the same way.

More generally, the claimed arrangement having a redirection server connected *between* the dial-up network server and a public network would have been obvious to try. It is noted that there exist only a limited number of predictable solutions, as these three components can only be connected in a small number of ways. One of ordinary skill in the art would have had a reasonable expectation of success in controlling a user's access to the public network by locating the redirection server, which performs the access control function, *between* the user's dial-up network server and the public network.

US 6779118	Prior Art Analysis[*]
[1.0] A system comprising:	He discloses a system in Fig. 10:  210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 Dial-up User 1002 Dial-up Server Dial-up Access Network 1004 2 FIG. 10
[1.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	He discloses a database 210 (illustrated in Fig. 10). He further teaches a user ID associated with user credentials. The user credentials correspond to an individualized rule set: The authentication server 202 can maintain a ***database of records for the user accounts*** in the registration database 210. Each record of a user account generally comprises the following information: (1) The user identifier. This identifier is required and must be unique throughout the entire network within the same realm or administrative domain. It is the legal representation of the user in the network. (2) An alias user identifier. This alias identifier is optional whose purpose is to

[*] In the context of the present request, the standard provided in MPEP § 2111 for claim interpretation during patent examination may be applied whereas a different standard may be used by a court in litigation. The PTO is not required to interpret claims in the same manner as a court would interpret claims in an infringement suit. The requester and real party in interest reserve the right to argue for a narrower or different construction of any term or claim in any pending or future litigation concerning this patent or any related patents.

Exhibit DD

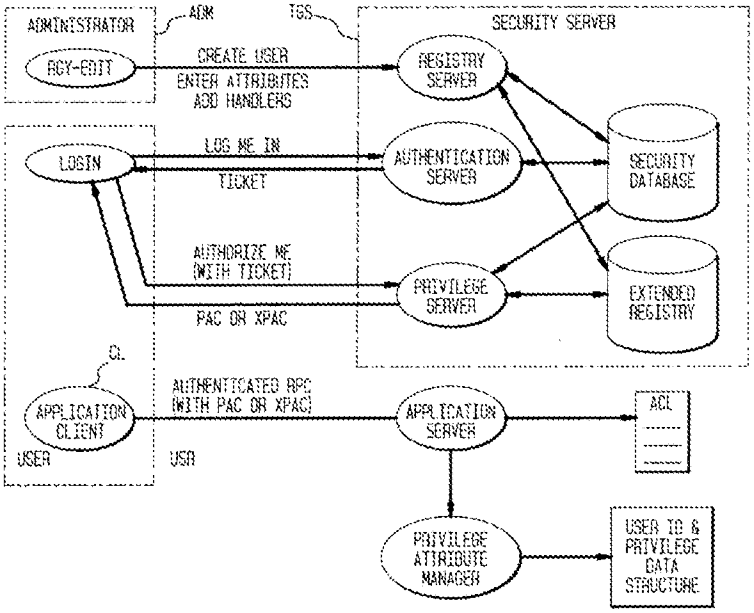
US 6779118	Prior Art Analysis*
	allow the same user to be identified through multiple means. (3) ***The list of user credentials***. This list shall reflect the most recent changes to the privilege set for the user. The privilege set can be built on previous achievements or credit history. For internal network users, however, it shall primarily be used to reflect the user's job responsibilities or affiliation with specific organizations that is the usual way of defining job responsibilities. (He, 16:50–67 (emphasis added).) Also, Fortinsky teaches a database, as illustrated in FIG. 1 below: *FIG. 1*  ADMINISTRATOR ADM TGS SECURITY SERVER RGY-EDIT CREATE USER ENTER ATTRIBUTES ADD HANDLERS REGISTRY SERVER LOGIN LOG ME IN TICKET AUTHENTICATION SERVER SECURITY DATABASE AUTHORIZE ME (WITH TICKET) PRIVILEGE SERVER EXTENDED REGISTRY PAC OR XPAC CL AUTHENTICATED RPC (WITH PAC OR XPAC) APPLICATION CLIENT APPLICATION SERVER ACL USER USR PRIVILEGE ATTRIBUTE MANAGER USER ID & PRIVILEGE DATA STRUCTURE Fortinsky further teaches that the database contains entries that correlate user IDs with a privilege attribute certificate PAC, which are individualized rule sets: A mechanism to ***add extended privilege attributes to the security registry database DB*** is necessary. An example of a suitable

Exhibit DD

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td></td><td>

> mechanism is the Extended Registry Attibute (ERA) mechanism proposed in DCE RFC 6.0 available from the Open Software Foundation. In the rest of this disclosure, this required mechanism is referred to as the ERA. The ERA mechanism will be invoked by the DCE administrator to add extended server and client attributes ERA to the server and client registry entries DB (FIG. 1).

(Fortinsky, 9:35–43(emphasis added).)

> A PAC is a data structure that contains DCE identity and privilege attributes that apply to a DCE client.

(Fortinsky, 5:26–28 (emphasis added).)

</td></tr>
<tr><td>[1.2] a dial-up network server that receives user IDs from users' computers;</td><td>

He teaches a dial-up server 1002 to "interface dial-up users with the network" (He, 30:42), illustrated in Fig 10:

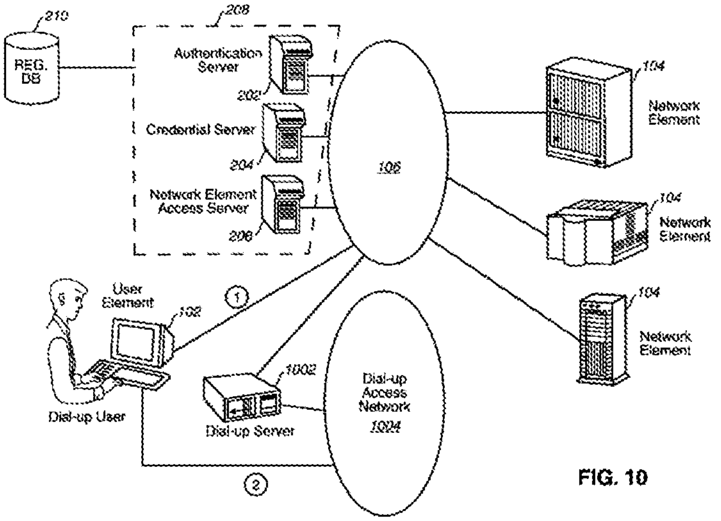


FIG. 10

He further teaches that the user transmits a user identifier to the authentication server:

> The user uses a user element 102 and initiates the authentication process by requesting to send a request message to the authentication server 202. The request

</td></tr>
</table>

Exhibit DD

US 6779118	Prior Art Analysis*
	message contains the user identifier presented to the authentication server 202 for user network authentication. (He, 17:55-60.) For users connected via the dial-up access network, it is understood that transmission of a user identifier to the authentication server 202 would first transit the dial-up server.
[1.3] a redirection server connected to the dial-up network server and a public network, and	Fortinsky discloses a gateway server that provides controlled access to an external resource or network: The extensions provided by the present invention are described further below, in the context of a network N1 as shown diagrammatically in FIG. 2, in which a DCE network also includes a ***gateway server GS through which is accessible a non-DEC server RS, possibly by a secondary non-DEC network N2*** as shown or possibly located in the same machine. (Fortinsky, 5:14-20.)

Exhibit DD

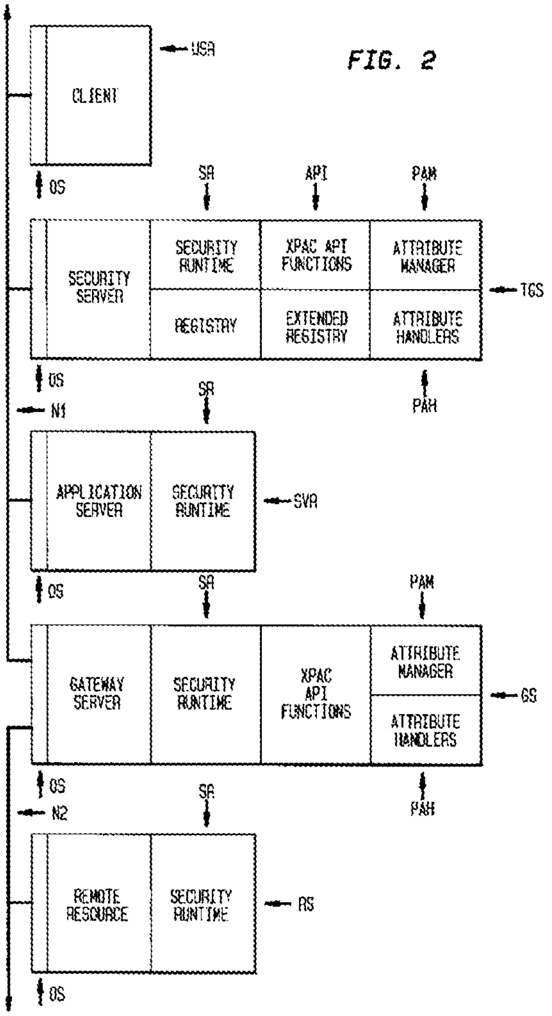
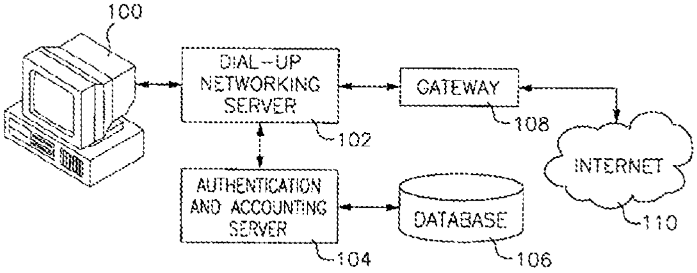
US 6779118	Prior Art Analysis*
	 USA CLIENT OS SA API PAM SECURITY SERVER SECURITY RUNTIME XPAC API FUNCTIONS ATTRIBUTE MANAGER TGS REGISTRY EXTENDED REGISTRY ATTRIBUTE HANDLERS OS N1 SA PAH APPLICATION SERVER SECURITY RUNTIME SVA OS SA PAM GATEWAY SERVER SECURITY RUNTIME XPAC API FUNCTIONS ATTRIBUTE MANAGER GS ATTRIBUTE HANDLERS OS N2 SA PAH REMOTE RESOURCE SECURITY RUNTIME RS OS FIG. 2 FORTINSKY, FIG. 2 Fortinsky further describes how the gateway server controls access to the external resource by requiring a requesting user to present the proper credentials: Server 2 is a server providing gateway access to external resources. To access these resources, a client must present a complex attribute that contains a whole user profile (including userid's, group list, and other security data). (Fortinsky, 8:55-58.)

Exhibit DD

<table>
<tr><th>US 6779118</th><th>Prior Art Analysis*</th></tr>
<tr><td></td><td>

It would have been obvious to one of skill in the art that Fortinsky's external network N2 could be a public network, such as the Internet. For example, the Admitted Prior Art teaches connecting a user to the public Internet via a gateway server 108:

FIG. 1


100
DIAL-UP NETWORKING SERVER
102
GATEWAY
108
INTERNET
110
AUTHENTICATION AND ACCOUNTING SERVER
104
DATABASE
106

'118 Patent, Fig. 1

The Admitted Prior Art teaches controlling access to resources by redirecting traffic on a public network, for example, World Wide Web traffic:

> The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)). However, redirection is not limited to WWW traffic, and the concept is valid for all IP services. To illustrate how redirection is accomplished, consider the following example, which redirects a user's request for a WWW page (typically an html (hypertext markup language) file) to some other WWW page. First, the user instructs the WWW browser (typically software running on the user's PC) to access a page on a remote WWW server by typing in the URL (universal resource locator) or clicking on a URL link. Note that a URL provides information about the communications protocol, the location of the server (typically an Internet domain name or IP address), and the location of the page on the remote server. The browser next sends a request to the

</td></tr>
</table>

Exhibit DD

US 6779118	Prior Art Analysis*
	server requesting the page. In response to the user's request, the web server sends the requested page to the browser. The page, however, contains html code instructing the browser to request some other WWW page--hence the redirection of the user begins. The browser then requests the redirected WWW page according to the URL contained in the first page's html code. ('118 Patent, 1:38-60.) It would have been obvious to one of skill in the art to supplement the access control functions of Fortinsky's gateway server to further include redirection capabilities that were already known in the art. For example, an address blocked for a particular user would be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked websites. Thus, redirection is an obvious extension of the use of a control to block the user. Requester notes that the Board reached a similar conclusion in a previous reexamination of the '118 patent. (*See* Board Decision at 9.)
[1.4] an authentication accounting server connected to the database, the dial-up network server and the redirection server;	He teaches an authentication server 202. As illustrated in Fig. 10, the authentication server 202 is connected to the database 210. The authentication server 202 is also connected, through the network 106, to the dial-up server 1002 and credential (redirection) server 204. Analogously, Fortinsky teaches a security server that includes an authentication server connected to the database, as illustrated in FIG. 1 below:

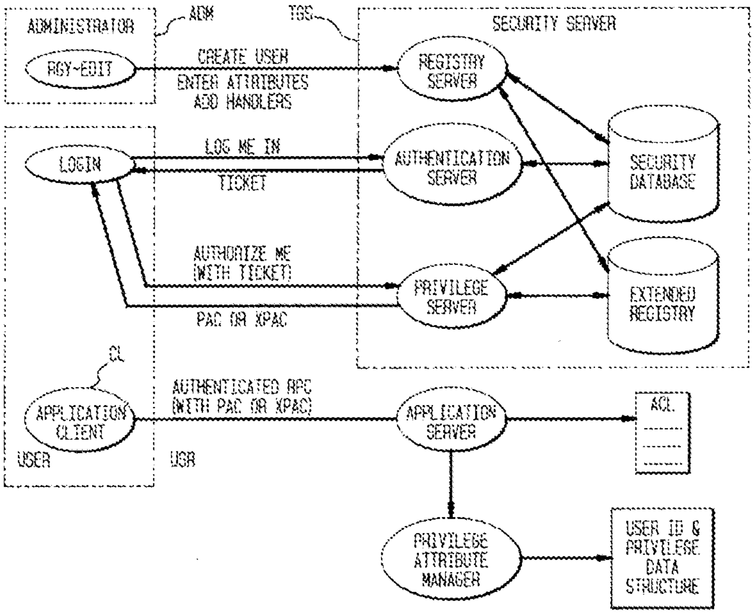
US 6779118	Prior Art Analysis*
	FIG. 1  ADMINISTRATOR ADM TGS SECURITY SERVER RGY-EDIT CREATE USER ENTER ATTRIBUTES ADD HANDLERS REGISTRY SERVER LOGIN LOG ME IN TICKET AUTHENTICATION SERVER SECURITY DATABASE AUTHORIZE ME (WITH TICKET) PRIVILEGE SERVER EXTENDED REGISTRY PAC OR XPAC CL AUTHENTICATED RPC (WITH PAC OR XPAC) APPLICATION CLIENT APPLICATION SERVER ACL USER USR PRIVILEGE ATTRIBUTE MANAGER USER ID & PRIVILEGE DATA STRUCTURE Fortinsky further teaches that the security server (which includes the authentication server) is connected to the gateway (redirection) server, as illustrated in FIG. 2 above in [1.3].
[1.5] wherein the dial-up network server communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to the authentication accounting server;	He teaches that a user logs onto the network via dial-up server 1002, which transmits the user's user ID to the authentication server: In the normal situation, a dial-up user access request is handled in the following steps: (1) The user dials into the dial-up server. The server authenticates the user based on any one of the available mechanisms in the module. (2) The dial-up server invokes the Kerberos client process and ***uses the user identifier and password to authenticate the user to the network***. (3) If Kerberos authentication is successful, user access to network elements will proceed with the security services offered by the Kerberos network security servers.

Exhibit DD

US 6779118	Prior Art Analysis*
	(He, 31:1-9.) Zenchelsky teaches assigning a temporary IP address to a user at logon: A "user" is a computer that does not have a fixed, assigned network address. To obtain connectivity to the Internet, for example, a user must commonly obtain a temporary IP address from a host with a pool of such addresses. Such a temporary IP address is retained by the user only for the duration of a single session of connectivity with the Internet. (Zenchelsky, 1:30-35.) Zenchelsky further teaches that each packet transmitted or received by the user includes the user's temporary IP address encoded as the source or destination: Information flows in certain networks in packets. A "packet" is a quantum of information that that has a header ***containing a source and a destination address***. . . . Another example of a packet identifier is a packet 5-tuple, which is the packet's source and destination address, source and destination port, and protocol. Packets with 5-tuples flow in connectionless packet switched networks. (Zenchelsky, 1:36-38 & 1:60-64.) The Admitted Prior Art further describes a dial-up network server sending a user's user ID and temporary IP address to an authentication and accounting server: The dial-up networking server then passes the user ID and password, along with a temporary Internet Protocol (IP) address for

Exhibit DD

US 6779118	Prior Art Analysis*
	use by the user to the ISP's authentication and accounting server 104. ('118 Patent, 1:21-24.) It would have been obvious to one of ordinary skill in the art to modify He so as to provide a temporary IP address to a user node and additionally to encode communications packets with that temporary IP address as the source or destination so as facilitate communication through a switched packet network as taught by Zenchelsky and the Admitted Prior Art.
[1.6] wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server; and	He teaches that the authentication server looks up a user in the database and obtains the user's credentials, which are an individualized rule set: (2) Upon receiving the user request message, the authentication server 202 uses the user identifier in the message to look up the user registration database 210 and retrieves a record corresponding to that user (user record). A response message is prepared by the authentication server 202 and sent back to the user. (He, 17:61-66.) He further teaches that the user's credentials are then presented to other servers, such as a credential server, which use the data to verify a user's request: The response message contains a general ticket for the user to communicate with the credential server 204 for authentification. ... (1) The user sends a message to the credential server 204 to request for a list of the user credentials. The message contains the ticket obtained by the user from the authentication server 202. The credential server 204 will not accept and process the request without being presented with the correct ticket from the user. The request

Exhibit DD

US 6779118	Prior Art Analysis*
	message is encrypted with the temporary user-credential server secret key so that only the credential server 204 is able to retrieve the content of the message. (He, 17:67-18:1 & 18:57-65.) Similarly, Fortinsky teaches that the authentication server accesses the database to obtain a privilege attribute certificate (PAC), which is an individualized rule set providing the user's privileges. The PAC is then provided to servers when the client requests a service: When the user USR logs in, the log-in process sends a log-in request to an authentication server in the security server TGS which issues a ticket PTGT to the user enabling it to request access to DCE resources. If the user's application client needs to access the resources of a server SVR, it requests a ticket for the purpose from the security server TGS which provides (assuming that the user has appropriate privileges) a server ticket including a PAC for provision by the client to the server SVR. (Fortinsky, 5:4–12 (emphasis added).) Fortinsky further describes an extended PAC (XPAC) that includes the client's privileges and credentials for accessing external network resources: A central feature of the embodiment of the invention being described is the extended PAC or XPAC. A PAC is a data structure that contains DCE identity and privilege attributes that apply to a DCE client. . . . Privileges and identities are entities that every security mechanism defines differently. The identity of a DCE client is expressed in a different form from that of a client in other computing environments such as a local area network. However, regardless

Exhibit DD

US 6779118	Prior Art Analysis*
	of the way the identity and privileges are expressed, the present invention enables a DCF client to present all its various identities and privilege attributes in an XPAC. (Fortinsky, 5:25-26 & 5:56-63 (emphasis added).) Fortinsky describes how the user must subsequently provide the XPAC credentials to the gateway server: The ticket the client receives contains an XPAC rather than a regular DCE PAC. This is transparent to the client. When the client eventually calls the target server, it passes the server ticket containing the XPAC. (Fortinsky, 8:21-24.) Server 2 is a server providing gateway access to external resources. To access these resources, a client must present a complex attribute that contains a whole user profile (including userid's, group list, and other security data). (Fortinsky, 8:55-58.) Fortinsky clarifies that the complex attribute required by the gateway server is encoded in the XPAC: The basic unit of privilege in the XPAC design is the privilege attribute object. This object contains three pieces of information, an attribute type, an attribute encoding, and an attribute value. The attribute encoding specifies how the attribute will be converted to a pickle. There are two general types of attributes: simple and complex. (Fortinsky, 6:2-7.) In summary, Fortinsky teaches that the authentication server provides an XPAC (an "individualized rule set") for

Exhibit DD

US 6779118	Prior Art Analysis*
	transmission to the gateway server ("redirection server"). Thus, the prior art renders obvious "wherein the authentication accounting server accesses the database and communicates the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server" as recited in the claim.
[1.7] wherein data directed toward the public network from the one of the users' computers are processed by the redirection server according to the individualized rule set.	He discloses that users direct data toward the public network: By presenting the correct secret key to the local access control system, the user authenticates his/her identity to the network. The correctness of the user-supplied secret key is verified through the process of decrypting the response message. It is the ability to retrieve the ticket in the message that allows the user to proceed with the network access control process to access network resources and information. (He, 18:24-31.) Fortinsky teaches that the gateway server (the "redirection server") uses the complex attributes included in the XPAC (the "individualized rule set") to control access to the external network and resources: Server 2 is a server providing gateway access to external resources. To access these resources, a client must present a complex attribute that contains a whole user profile (including userid's, group list, and other security data). (Fortinsky, 8:55-58.) It would have been obvious that the "external resources" accessible via Fortinsky's gateway server could include a public network. For example, the Admitted Prior Art illustrates using a gateway 108 to connect to the public Internet:

Exhibit DD

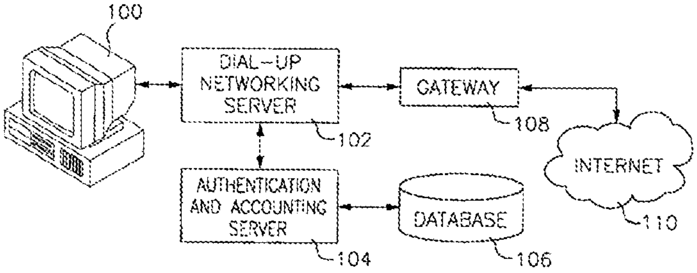
US 6779118	Prior Art Analysis*
	FIG. 1  100 DIAL-UP NETWORKING SERVER 102 GATEWAY 108 INTERNET 110 AUTHENTICATION AND ACCOUNTING SERVER 104 DATABASE 106 '118 Patent, Fig. 1
[2.0] The system of claim 1, wherein the redirection server further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	He teaches that the user credentials correspond to an individualized rule set that control access to network resources: The credential ticket is sent back in a response message and will be used for the user to communicate with the network element access server 206. The response message also contains a temporary secret key generated randomly by the credential server 204 ***to facilitate secure communications between the user and the network element access server*** 206. ... By presenting the correct ticket to the credential server 204, the user is able ***to obtain the list of user credentials necessary for requesting access to network resources*** and information. (He, 19:5-11 & 19:32-35 (emphasis added).) Thus, He teaches that servers, such as Fortinsky's gateway server, controls the data a user may access as a function of the user's credentials. As previously noted, the credentials are an individualized rule set. Fortinsky similarly teaches that the gateway server requires individualized credentials that are used to control access to an external resource: Server 2 is a server providing gateway

Exhibit DD

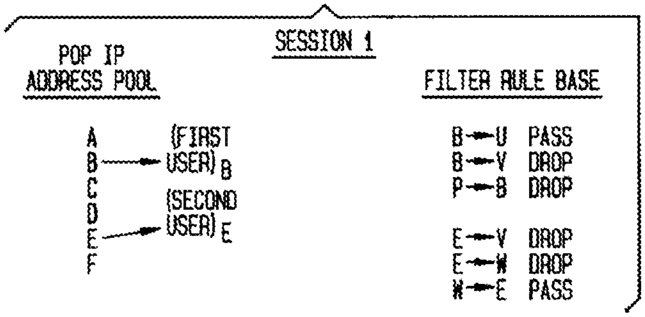
US 6779118	Prior Art Analysis*
	access to external resources. To access these resources, a client ***must present a complex attribute that contains a whole user profile*** (including userid's, group list, and other security data). (Fortinsky, 8:55-58.) Zenchelsky further teaches controlling a user's access to data on a network using individualized rules: A rule base 53 is loaded into a filter to regulate the flow of information between users 51 and 53 and the hosts P, U, V and W on the Internet. The rule base shown in FIGS. 5a and 5b show only the source and destination addresses for each rule, and omit source and destination ports and protocol for simplicity. (Zenchelsky, 3:46-51.) FIG. 5A  (PRIOR ART) SESSION 1 POP IP ADDRESS POOL A B C D E F (FIRST USER) B (SECOND USER) E FILTER RULE BASE B ← U PASS B ← V DROP P ← B DROP E ← V DROP E ← W DROP W ← E PASS As Zenchelsky illustrates in Fig. 5A, a first user "B" is permitted to communicate (pass data) with host U, but not host V. Similarly, second user "E" is permitted to receive data from host W, but may not send data to hosts V or W. Thus, Zenchelsky teaches using individualized rules to control data passing to and from a user's computer. The Admitted Prior Art further describes applying a packet filter to control a user's access to a public network, such as the Internet and the world wide web:

Exhibit DD

US 6779118	Prior Art Analysis*
	Filtering packets at the Internet Protocol (IP) layer has been possible using a firewall device or other packet filtering device for several years. Although packet filtering is most often used to filter packets coming into a private network for security purposes, once properly programed, ***they can filter outgoing packets sent from users to a specific destination*** as well. Packet filtering can distinguish, and filter based on, the type of IP service contained within an IP packet. Packet filter devices are often used with proxy server systems, which ***provide access control to the Internet and are most often used to control access to the world wide web***.... Typically, the proxy server is programed with a set of destinations that are to be blocked, and packets destined for blocked addresses are not forwarded. ('118 Patent, 2:1-38.) Thus, the prior art renders obvious that a redirection server, such as Fortinsky's gateway server "provides control over a plurality of data to and from the users' computers as a function of the individualized rule set" as recited in the claim.
[3.0] The system of claim 1, wherein the redirection server further blocks the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]. It would have been obvious to one of skill in the art that a user's access request should be blocked if the user's credentials do not allow for access to the requested resource. He also describes blocking a user's access request if the user has tampered with the ticket received from the credential server: Any attempts by the user to try to make any changes to the ticket, intentional or unintentional, will be detected by the network element access server when it is used for communications with the server 106

Exhibit DD

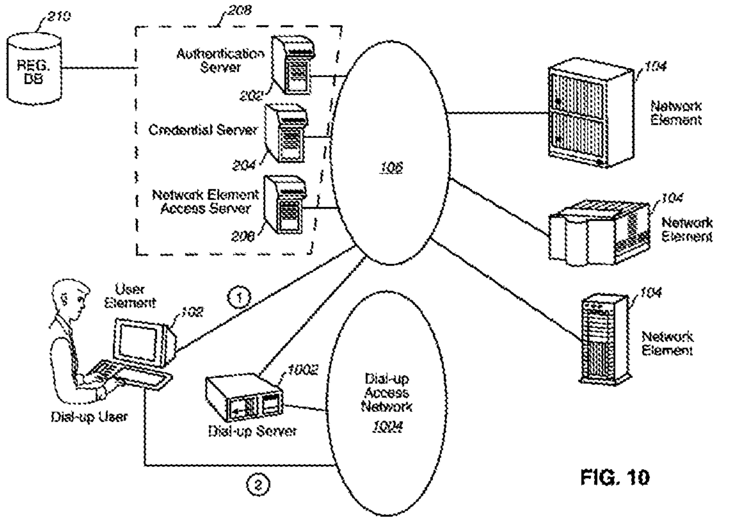
US 6779118	Prior Art Analysis*
	and, therefore, would void the ticket and make it useless. This is to prevent the user from modifying the list of certified user credentials as well as other information in the ticket to gain unauthorized network access rights. (He, 19:24-31.)
[4.0] The system of claim 1, wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set.	See analysis of portions [2.0]. It would have been obvious to one of skill in the art that a user's access request should be allowed if the user's credentials permit access to the requested resource.
[5.0] The system of claim 1, wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set.	See analysis of portions [1.3] and [2.0]. The Admitted Prior Art teaches redirection. ('118 Patent, 1:38-60.) It would have been obvious to add the known technique of data redirection to Fortinsky's gateway server. For example, it would have been obvious to redirect a user's request to the authentication server when the user's request fails to include all of the required security information in an XPAC.
[6.0] The system of claim 1, wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set.	He illustrates in Fig. 10 that there are multiple potential destinations, such as network elements 104, for further interaction based on a user's credentials:  210 REG. DB 208 Authentication Server 202 Credential Server 204 Network Element Access Server 206 106 104 Network Element 104 Network Element 104 Network Element User Element 102 1 Dial-up User 1002 Dial-up Server Dial-up Access Network 1004 2 FIG. 10

Exhibit DD

US 6779118	Prior Art Analysis*
	It would have been obvious for the gateway server to redirect users' requests to multiple destinations. For example, where a user requests to access an external resource for which the user lacks authorization (for example, an Internet web site), it would have been obvious for the gateway server to redirect the user to an internal resource for providing a similar function (for example, a internal web site).
[7.0] The system of claim 1, wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set.	He describes assigning user credentials based on a user's obligations or roles: The user credentials for a user may be determined in a variety of ways. They may be established based on criteria that are related to the past history of the user regarding the behaviors of access to network resources and information. They may also be established ***based on the current obligations or roles the user plays*** in the network. For example, the organization that consists of a department number and a location code can reflect the current responsibility the users have in their job and, therefore, can be used as the user credentials to determine the access rights for the users to access network elements. Other user credentials can be similarly identified and used for the access control purposes that help enforce the principle of "need-to-know." (He, 13:30-42, emphasis added.) It would have been obvious that multiple users with common obligations or roles could be correlated to a common credential, such as an administrator role credential. He further describes additional rules stored in the database, such as the minimum password length and number of failed log-in attempts: Each record of a user account generally

Exhibit DD

US 6779118	Prior Art Analysis*
	comprises the following information: … (5) Other administrative information to enhance the effectiveness of the network security mechanisms. The information includes, but not limited to, the minimum length of the password, the required variation of password characters, the expiration date or the lifetime of the password since creation, the maximum lifetime of each authentication, and the maximum number of failed authentication attempts that is allowed before the account is brought to the attention to the system security administrator for examination or is simply disabled temporarily pending such an examination. (He, 16:52-53 & 17:6-18.) It would have been obvious to establish common policies for these rules that would apply to multiple (or all) users.
[8.0] In a system comprising	See analysis of portion [1.0].
[8.1] a database with entries correlating each of a plurality of user IDs with an individualized rule set;	See analysis of portion [1.1].
[8.2] a dial-up network server that receives user IDs from users' computers;	See analysis of portion [1.2].
[8.3] a redirection server connected to the dial-up network server and a public network, and an authentication accounting server connected to the database, the dial-up network server and the	See analysis of portion [1.3].

Exhibit DD

US 6779118	Prior Art Analysis*
redirection server,	
[8.4] the method comprising the steps of:	He discloses a method: A high-level description of a method according to the present invention will now be described in connection with a flow diagram 400 in FIG. 4. (He, 25:21-23.)
[8.5] communicating a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID from the dial-up network server to the authentication accounting server;	See analysis of portion [1.5].
[8.6] communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server; and	See analysis of portion [1.6].
[8.7] processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	See analysis of portion [1.7].
[9.0] The method of claim 8, further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [2.0]
[10.0] The method of claim 8, further including the step of blocking the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [3.0]
[11.0] The method of claim 8, further including the step of allowing the data to and from the users' computers as a function of	See analysis of portion [4.0]

Exhibit DD

US 6779118	Prior Art Analysis*
the individualized rule set.	
[12.0] The method of claim 8, further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set.	See analysis of portion [5.0]
[13.0] The method of claim 8, further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set.	See analysis of portion [6.0].
[14.0] The method of claim 8, further including the step of creating database entries for a plurality of the plurality of users' IDs, the plurality of users' ID further being correlated with a common individualized rule set.	See analysis of portion [7.0].
[16.0] A system comprising:	See analysis of portion [1.0].
[16.1] a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	See analysis of portions [1.3] and [1.6].
[16.2] wherein the rule set contains at least one of a plurality of functions used to control passing between the user and a public network;	See analysis of portions [1.1] and [1.7]. The user's credentials are a "plurality of functions used to control passing."
[16.3] wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned network address;	He teaches a database tool associated with the server system for creating, modifying, and deleting user accounts: It is desirable that a database tool be provided for the system security administrator to create, delete, disable and modify a user account. Such a tool should provide a user-friendly interface to aid the system security administrator to effectively and conveniently manage user accounts, as would be apparent to a person skilled in the art. This requirement should not be under-looked as correct user account administration and management is the basis for all other effective network access control