Regarding the assertion that the invention is somehow new because the redirection server supports automated rule modification, the Requester points out that Coss et al. disclose the firewall 211 supports automated rule modification:

> Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>** A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be removed from the rule set. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. [Coss et al., col. 8, lines 24-36, emphasis added]

Regarding the assertion that the invention is somehow new because the modification is a function of some combination of time, data transmitted to or from the user, or location the user accesses, the Requester points out that Coss et al. disclose that dynamic rule modification is a function of these features:

> Exemplary dynamic rules include **<u>a "one-time"</u>** rule which is only used for a single session, **<u>a time-limited rule</u>** which is used only for a specified time period, and a **<u>threshold rule</u>** which is used only when certain conditions are satisfied. Another type of dynamic rule includes **<u>rules which define a host group</u>**, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set. Other dynamic rules may be used to facilitate rule setup in certain specific types of processing applications. For example, an FTP proxy application could use a **<u>dynamic rule to authorize establishment of an FTP data channel in response to a data request</u>**. The dynamic rule in this example would typically **<u>not be loaded until a data request is made over the FTP control session</u>**, and could be **<u>limited to one use and made active for only a limited time period</u>**. The rule set therefore need not include a separate data channel rule for use with all requests. As a result, the rule specification and rule processing are simplified, and security is improved. [Coss et al., col. 8, lines 37-55, emphasis added]

Regarding the assertion that the invention is somehow new because the instructions to modify the rule set are received from either the user side or the network side of the redirection server, the Requester points out that Coss et al. disclose receiving instructions from a firewall administrator:

> "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties</u>**, e.g., a trusted application, remote proxy or **<u>firewall administrator</u>**, to authorize specific network sessions." [Coss et al., col. 8, lines 26-31, emphasis added]

Coss et al.'s Figure 1 illustrates Administrator processor 115 is on the **<u>network side</u>** of the firewalls 111, 113, 114:

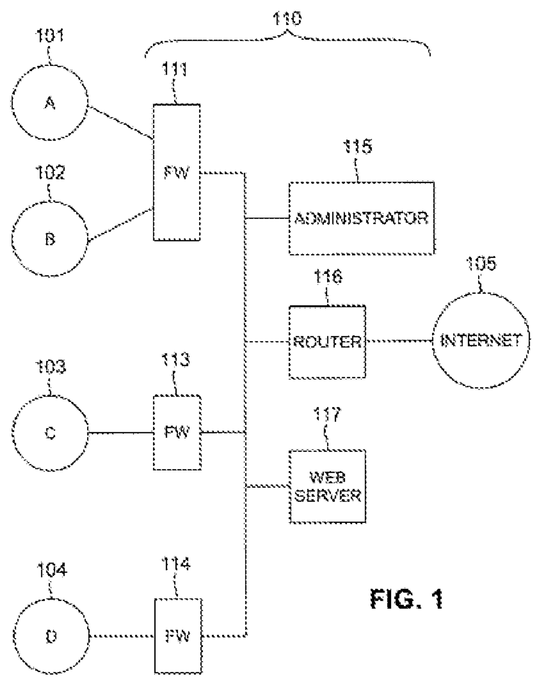


FIG. 1

Coss et al.'s Figure 2 illustrates Administrator processor (ADM) 215 is on the **<u>user side</u>** of firewall 211:

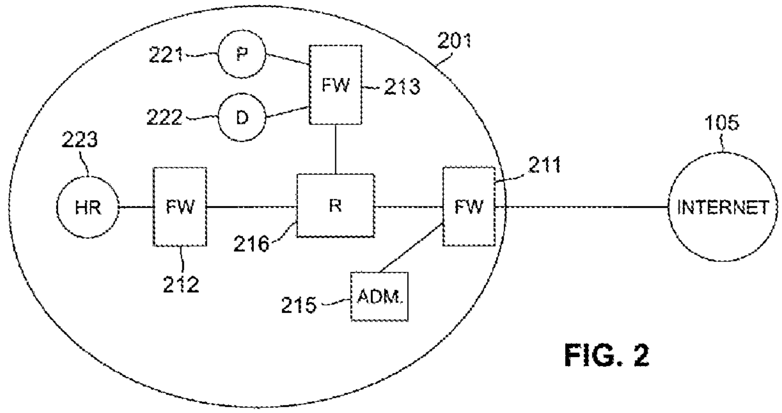


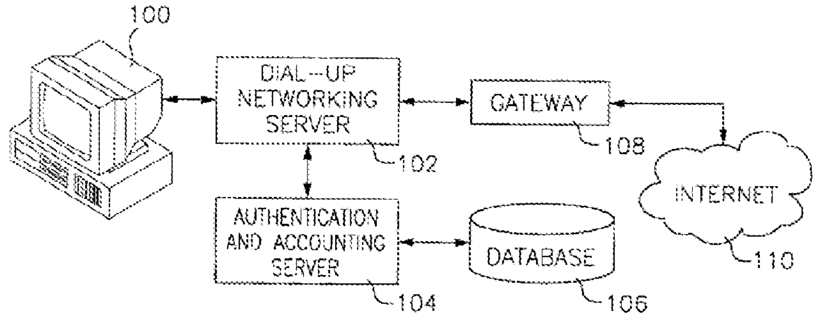
FIG. 2

Regarding the assertion that the invention is somehow new because the rule modification involves removing or reinstating at least a part of the rule set, the Requester points out that Coss et al. disclose removing a rule from a currently programmed rule set:

> Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. **A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be removed from the rule set.** The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. [Coss et al., col. 8, lines 24-36, emphasis added]

Regarding the assertion that the invention is somehow new because the redirection server is located *between* the user computer and the public network, the Requester points out that Coss et al. illustrate in Figure 2 (shown above) that firewall 211 is connected *between* the user site 201 and the Internet 105. Additionally, the APA in Figure 1 of the `118 patent illustrates that it was well-known to locate a gateway 108 *between* a user computer 100 and a public network such as the Internet 110:

FIG. 1



As set forth below in sections III and IV of this request, each of claims 16-24, 26-27, 36-43 and 68-90 is unpatentable as obvious over Coss et al. in view of the APA. The record shows that no application of this combination of prior art references was ever applied to any claims of the `118 patent.

II. REQUIREMENTS FOR *EX PARTE* REEXAMINATION REQUEST

Requester requests *ex parte* reexamination of U.S. Patent No. 6,779,118 ("the `118 patent") under 37 C.F.R. § 1.510. In support of its request for *ex parte* reexamination, Requester provides the following:

1 Fee for requesting reexamination – 37 C.F.R. § 1.510(a)

Authorization for the Office to charge the credit card information provided at the time of submission for the $2,520.00 filing fee for the present *ex parte* reexamination request, as set forth in 37 C.F.R. § 1.20(c)(1) and 37 C.F.R. § 1.510(a). Authorization is hereby given that any additional fees required may be charged to the same credit card.

2 Prior Art Patents and Printed Publications Forming the Basis of this Request – 37 C.F.R. § 1.510(a)

The `118 patent claims priority to U.S. provisional application No. 60/084,014, filed on May 4, 1998. Reexamination of the `118 patent is hereby requested on the basis of the following prior art patents and printed publications:

A. U.S. Patent 6,088,451, hereinafter, He et al.

He et al. lists a filing date of June 28, 1996. Since the filing date is prior to the filing date of the provisional application of the `118 patent, He et al. is at least prior art under 35 U.S.C. 102(e).

B. U.S. Patent 6,233,686, hereinafter Zenchelsky et al.

Zenchelsky et al. lists a filing date of January 17, 1997. Since the filing date is prior to the filing date of the provisional application of the `118 patent, Zenchelsky et al. is at least prior art under 35 U.S.C. 102(e).

C. U.S. Patent 5,848,233, hereinafter, Radia et al.

Radia et al. lists a filing date of December 9, 1996. Since the filing date is prior to the filing date of the provisional application of the `118 patent, Radia et al. is at least prior art under 35 U.S.C. 102(e).

D. U.S. Patent 6,170,012, hereinafter, Coss et al.

Coss et al. lists a filing date of September 12, 1997. Since the filing date is prior to the filing date of the provisional application of the `118 patent, Coss et al. is at least prior art under 35 U.S.C. 102(e).

E. U.S. Patent 6,779,118 B1, FIG. 1 and Col. 1, lines 15-67, hereinafter, the Admitted Prior Art (APA)

MPEP 2258 section (F) entitled, "Admissions; Use of Admissions" states, "37 CFR 1.104(c)(3) provides that admissions by the patent owners as to matters affecting patentability may be utilized in a reexamination proceeding."

Col. 1, lines 15-67 of the `118 patent begin as follows:

"In <u>prior art systems</u> as shown in FIG. 1 …" (emphasis added)

As there is no indication or evidence in the record that the described prior art systems are the work of the inventors of the `118 patent, these statements by the inventors in a printed publication already included in the record (i.e., published U.S. Patent 6,779,118 B1) constitute an admission of known prior art systems and may therefore be relied upon for both anticipation and obviousness determinations, regardless of whether the published U.S. Patent 6,779,118 B1 itself would otherwise qualify as prior art under the statutory categories of 35 U.S.C. 102. *Riverwood Int'l Corp. v. R.A. Jones & Co., 324 F.3d 1346, 1354, 66 USPQ2d 1331, 1337 (Fed. Cir. 2003); Constant v. Advanced Micro-Devices Inc., 848 F.2d 1560, 1570, 7 USPQ2d 1057, 1063 (Fed. Cir. 1988).*

3 Statement pointing out each substantial new question of patentability based on prior patents and printed publications – 37 C.F.R. § 1.510(b)(1)

This section provides a statement pointing out each substantial new question of patentability ("SNQ") raised by this Request. A detailed description setting forth the pertinency of each SNQ with respect to each of claim of the `118 patent is provided below in Section III and claim charts showing the manner of applying the cited prior art to every claim for each SNQ are provided below in Section IV.

A. Claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA

Requester respectfully submits that claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent are unpatentable as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. Although rejections of other claims on the basis of He et al. in view of Zenchelsky et al., and further in view of the APA were affirmed by the Board Of Patent Appeals and Interferences in the Decision on Appeal dated August 23, 2011, the combination of He et al., Zenchelsky et al, and the APA was never applied in any rejections of claims 2-7, 9-14, 16-24, and 26-43. The combination of He et al., Zenchelsky et al, and the APA is not cumulative of any of the art previously applied to these claims. A reasonable examiner would consider He et al., Zenchelsky et al, and the APA pertinent to the patentability of the requested claims. The specific details of the pertinence and manner of applying He et al., Zenchelsky et al, and the APA to each of the above-identified claims in support of this substantial new question of patentability are presented below in Sections III and IV.

B. Claims 2-7, 9-14, 28-35, and 44-67 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over Radia et al. in view of the APA, and further in view of Coss et al.

Requester respectfully submits that claims 2-7, 9-14, 28-35, and 44-67 of the `118 patent are unpatentable as being obvious over Radia et al. in view of the APA, and further in view of Coss et al. Although the Radia et al. reference was disclosed in an applicant submitted information disclosure statement during the prior reexamination proceedings, Radia et al. was not discussed on the record and was never relied upon in any rejection of the claims. Radia et al. is not cumulative of any of the previously applied art. A reasonable examiner would consider Radia et al. pertinent to the patentability of the requested claims. Although admissions found in the `118 patent related to known redirection methods were relied upon to reject claims in the prior reexamination proceedings, the APA was not applied in a rejection of the claims in the manner done in this Request. A reasonable examiner would consider the APA pertinent to the patentability of the requested claims. The Coss et al. reference is not of record in either the original examination or prior reexamination proceedings of the `118 patent. Co-filed patents by Coss et al. (e.g., U.S. Patents 6,098,172 and 6,154,775) were disclosed in an applicant submitted information disclosure statement in the prior reexamination proceedings; however, no patent by Coss was ever discussed on the record or relied upon in any rejection of the claims. Coss et al. is not cumulative of any of the previously applied art. A reasonable examiner would consider Coss et al. pertinent to the patentability of the requested claims. The specific details of the pertinence and manner of applying Radia et al., the APA, and Coss et al. to each of the above-identified claims in support of this substantial new question of patentability are presented below in Sections III and IV.

C. Claims 16-24, 26-27, 36-43 and 68-90 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over Coss et al. in view of the APA

Requester respectfully submits that claims 16-24, 26-27, 36-43 and 68-90 of the `118 patent are unpatentable as being obvious over Coss et al. in view of the APA. The Coss et al. reference is not of record in either the original examination or prior reexamination proceedings of the `118 patent. Co-filed patents by Coss et al. (e.g., U.S. Patents 6,098,172 and 6,154,775) were disclosed in an applicant submitted information disclosure statement in the prior reexamination proceedings; however, no patent by Coss was ever discussed on the record or relied upon in any rejection of the claims. Coss et al. is not cumulative of any of the previously applied art. A reasonable examiner would consider Coss et al. pertinent to the patentability of the requested claims. Although admissions found in the `118 patent related to known redirection methods were relied upon to reject claims in the prior reexamination proceedings, the APA was not applied in a rejection of the claims in the manner done in this Request. A reasonable examiner would consider the APA pertinent to the patentability of the requested claims. The specific details of the pertinence and manner of applying Coss et al. and the APA to each of the above-identified claims in support of this substantial new question of patentability are presented below in Sections III and IV.

4 Identification of every claim for which reexamination is requested, and a detailed explanation of the pertinency and manner of applying the cited prior art to every claim for which reexamination is requested – 37 C.F.R. § 1.510(b)(2)

Reexamination of all non-canceled and enforceable claims of the `118 patent, i.e., claims 2-7, 9-14, 16-24 and 26-90, is hereby requested. A detailed explanation of the pertinency and manner of applying the cited prior art to every claim for which reexamination is requested is found below in Sections III and IV.

5 Copy of every patent or printed publication relied upon – 37 C.F.R. § 1.510(b)(3)

Copies of each patent and printed publication relied upon in this Request are attached to the Request in Appendices 1-5.

6 Copy of the entire patent including the front face, drawings, and specification/claims (in double column format) for which reexamination is requested, and a copy of any disclaimer, certificate of correction, or reexamination certificate issued in the patent – 37 C.F.R. § 1.510(b)(4)

A copy of the `118 patent is attached to this Request in Appendix 5. A copy of the reexamination certificate issued in the `118 patent is attached to this Request in Appendix 6.

7 Certification that a copy of the request has been served in its entirety on the patent owner – 37 C.F.R. § 1.510(b)(5)

A copy of the Certificate of Service is attached to this Request in Appendix 7. Pursuant to 37 C.F.R. § 1.510(b)(5), this Request is being served on the Patent Owner at:

Hershkovitz & Associates, LLC
2845 Duke Street
Alexandria VA 22314

III. DETAILED EXPLANATION OF THE PERTINENCY OF EACH SNQ

1 Claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA

Requester respectfully submits that claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent are unpatentable as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. The holding on page 10 of the Decision on Appeal in the prior reexamination of the `118 affirmed the rejections of previously presented dependent claims 32, 37, 42 and 47 as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. Since claims 32, 37, 42 and 47 depended from independent claims 1, 8, 15, 25, the Board found that it follows that the independent claims must too be obvious over the same references and entered a new ground of rejection for independent claims 1, 8, 15, 25. In response to the Decision on Appeal, the patent owner canceled the independent claims 1, 8, 15, 25. The record is thereby clear that canceled independent claims 1, 8, 15 and 25 are unpatentable as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. In order for any of claims 2-7, 9-14, 16-24, and 26-43 (as they are now numbered and which were dependent upon independent claims 1, 8, 15 and 25 at the time of appeal) to be patentable, the additional limitation(s) introduced in each claim that is/are not found in corresponding unpatentable independent claim 1, 8, 15, 25 must be the distinguishing feature(s) that render(s) these claims patentable. However, as described herein, the limitations introduced in claims 2-7, 9-14, 16-24, and 26-43 are obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. The record shows there was never any application of the combination of He et al., Zenchelsky et al., and the APA as set forth below in any rejection of claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent. The combination of He et al., Zenchelsky et al., and the APA is not cumulative of any of the art previously applied to these claims. A reasonable examiner would consider the below-described application of He et al., Zenchelsky et al., and the APA pertinent to the patentability of these claims for at least the reasons discussed below. A claim chart setting forth the manner of applying He et al., Zenchelsky et al., and the APA to each of the above-identified claims in support of this substantial new question of patentability is provided below in Section IV of this Request.

Claim 2 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the redirection server (He et al; credential server 204) further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set (He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access. Also see He et al at col. 16, lines 61-67 for detail of user credentials).

Claim 3 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the redirection server (He et al; credential server 204) further blocks the data to and from the users' computers as a function of the individualized rule set (He et al; credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Conversely, network elements 104 which cannot be accessed in accordance with the user credentials are inherently blocked from access. Also see He et al at col. 19, lines 24-31 which describe the scenario where the user access ticket is actively voided, corresponding to a blocking action).

Claim 4 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the redirection server further allows the data to and from the users' computers as a function of the individualized rule set (He et al. col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data exchange occurs between accessed network elements 104).

Claim 5 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set (He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data access to network elements 104 corresponds to data moving to and from users' computers).

Claim 6 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set (He et al; FIG 10, plural network elements 104 represent multiple potential destinations for interaction based on particular user credentials).

Claim 7 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set (He et al; col. 16, line 54 through line 68. Each database entry (record) includes a user ID accompanied by user credentials. The user credentials are the individualized rules for a particular user).

Claim 9 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set (He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access. Also see He et al at col 16, lines 61-67 for detail of user credentials).

Claim 10 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of blocking the data to and from the users' computers as a function of the individualized rule set (He et al; credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Conversely, network elements 104 which cannot be accessed in accordance with the user credentials are inherently blocked from access. Also see He et al. at col. 19, lines 24-31 which describe the scenario where the user access ticket is actively voided, corresponding to a blocking action).

Claim 11 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of allowing the data to and from the users' computers as a function of the individualized rule set. (He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data exchange occurs between accessed network elements 104).

Claim 12 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set (He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data access to network elements 104 corresponds to data moving to and from users' computers).

Claim 13 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set (He et al; FIG 10, plural network elements 104 represent multiple potential destinations for interaction based on particular user credentials).

Claim 14 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose 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 (He et al; col. 16, line 54 through line 68. Each database entry (record) includes a user ID accompanied by user credentials. The user credentials are the individualized rules for a particular user).

Claim 16

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time (He et al., col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)"). It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 17

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose 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 (This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can modify the rule set, for example, by deleting it. The system administrator is one of the system users).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 18

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose 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 attempts to access (This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can modify the rule set, for example, by deleting it. The location of the administrator is the location at which modification is permitted).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 19

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al.

further disclose 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 (He et al; col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account. Any actions of administrator inherently occur over some given period time).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 20

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by

Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose 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. (This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The system administrator is one of the system users).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 21

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose 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. (This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al. at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The location of the administrator is the location at which modification is permitted).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 22

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set.

Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose 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. (He et al; col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account. Any actions of administrator inherently occur over some given period time. He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The location of the administrator is the location at which modification is permitted).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 23

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). He et al. further disclose wherein the redirection server (He et al; credential server 204) has a user side (He et al; FIG 10, any one of or both of the dial up server 1002 and dial up access network 1004) that is connected to a computer (He et al; FIG 10, user element 102) using the temporarily assigned network address (Zenchelsky et al; col. 1, lines 29-35) and a network side (He et al; FIG 10, any one of or both of the interconnection network 106 and network elements 104) connected to a computer network (He et al; interconnection network 106) and wherein the computer (He et al; FIG 10, user element 102) using the temporarily assigned network address (Zenchelsky et al; col. 1, lines 29-35) is connected to the computer network through the redirection server (He et al; FIG 10, computer 102 is connected to the interconnection network 106 via the credential server 204).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 24

He et al. disclose 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 et al., col. 17, lines 19-21 refer to a network administrator modifying any portion of a user account. He et al. at FIG 10 illustrates that users presenting input to the network (a network administrator is also a user). Accordingly, instructions transmitted from a network administrator originate at terminal 102 and proceed through the user side elements 1002, 1004 as well as the network side element 106).

Claim 26 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of modifying at least a portion of the user's rule set (He et al., col 17, lines 19-21, the administrator is allowed to create or delete any portion of the user account) as a function of one or more of: time (any actions of administrator inherently occur over some given period time), data transmitted to or from the user (He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete any portion of the user account), and location or locations the user attempts to access (the location of the administrator is the location at which modification is permitted).

Claim 27 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose further including the step of removing or reinstating at least a portion of the user's rule set (He et al., col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account) as a function of one or more of: time (any actions of administrator inherently occur over some given period time), the data transmitted to or from the user (He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account), and a location or locations the user attempts to access (the location of the administrator is the location at which modification is permitted).

Claim 28 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 28 recites wherein the individual rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 29 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the individual 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 (Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a standard rule set).

Claim 30 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 30 recites wherein the individual rule set includes at least one rule allowing access based on a request type and a destination address. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 31 (includes limitations of canceled claim 1 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 31 recites wherein the individual rule set includes at least one rule allowing access based on a request type and a destination address. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 32 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 32 recites wherein the individual rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 33 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose wherein the individual 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 (Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a standard rule set).

Claim 34 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 34 recites wherein the individual rule set includes at least one rule allowing access based on a request type and a destination address. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 35 (includes limitations of canceled claim 8 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 35 recites wherein the individual 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. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 36

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by

Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). Wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 37

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). Wherein the individual 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 (Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a standard rule set).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 38

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary

IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). Wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 39

He et al. disclose a system (He et al; FIG 10) comprising: a redirection server (He et al; FIG 10, credential server 204) programmed with a user's rule set (He et al; col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set) correlated to a temporarily assigned network address (Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al); 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 (He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208); 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 et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts) and wherein the redirection server is configured to allow automated modification of at least a portion of the rule set (He et al; col 17, lines 19-21, any of the user account information can be modified) as a function of some combination of time, data transmitted to or from the user, or location the user attempts to access (He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited). 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. A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim 40 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 40 recites wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 41 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

He et al. disclose 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 (Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a standard rule set).

Claim 42 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 42 recites wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim 43 (includes limitations of canceled claim 25 known to be obvious over He et al. in view of Zenchelsky et al., and further in view of the APA)

Claim 43 recites 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. A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

SNQ raised

Because the above teachings of He et al., Zenchelsky et al., and the APA. were not applied in any rejection of the above-identified claims during the initial prosecution and prior reexamination of the `118 Patent, a substantial new question of patentability is raised.

2 Claims 2-7, 9-14, 28-35, and 44-67 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over Radia et al. in view of the APA, and further in view of Coss et al.

Requester respectfully submits that claims 2-7, 9-14, 28-35, and 44-67 of the `118 patent are unpatentable as being obvious over Radia et al. in view of the APA, and further in view of Coss et al. A reasonable examiner would consider Radia et al., the APA, and Coss et al. pertinent to the patentability of the requested claims for at least the reasons discussed below. A claim chart setting forth the pertinence and manner of applying Radia et al., APA, and Coss et al. to each of the above-identified claims in support of this substantial new question of patentability is provided below in Section IV of this Request.

Claim 2 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the router (Radia et al.; FIG. 1, router 106) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose *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. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set (Coss et al; col. 2, lines 57-60 and FIG. 3 showing individualized rule set for host B having rule No. 10 controlling FTP data to host B, and rule No. 30 controlling Telnet data from host B). Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al.; col. 4, lines 39-43) allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 3 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the router (Radia et al.; FIG. 1, router 106) further blocks the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose *the redirection server* further blocks the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. (Coss et al. show in FIG. 3, rule No. 20 blocking data from host A; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data to host A.) Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al. col. 4, lines 39-43) allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 4 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the router (Radia et al.; FIG. 1, router 106) further allows the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al;

Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose *the redirection server* further allows the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose in FIG. 4 a first session key rule (A, B, TELNET) allowing data to host B, and second session key rule (B, A, TELNET) allowing data from host B. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 5 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the router (Radia et al.; FIG. 1, router 106) further controls data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose *the redirection server* further redirects the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. (Coss et al., col. 9, lines 6-16 describing "two-way reflection") Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect data (i.e., also referred to as 'proxy' data by Coss et al.) to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 6 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the router (Radia et al.; FIG. 1, router 106) further controls data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary

IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose *the redirection server* further redirects the data from the users' computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose in step 1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" (Coss et al; col. 9, lines 39-42). These destination proxy servers include different destinations such as "authentication, mail handling, and virus scanning." (Coss et al., col. 1, lines 45-49) Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a Telnet proxy server. Coss et al. further state, "For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request.” It is inherent that data was also redirected to the FTP proxy application as a function of the individualized rule set. Coss et al. also disclose rule set categories such as “Source host group identifier or IP address”, “Destination host group identifier or IP address”, and “Rule action, e.g., ‘pass’, ‘drop’, or ‘proxy’” (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect (i.e., proxy) data from the users’ computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 7 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach “uses a router to link its internal intranet with an external network, such as the Internet”) , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set (Radia et al; "default login profile" described in col. 3, lines 23-33)

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router

106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim 9 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Further including the step of controlling a plurality of data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of:

1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the step of controlling a plurality of data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set (Coss et al; col. 2, lines 57-60 and FIG. 3 showing individualized rule set for host B having rule No. 10 controlling FTP data to host B, and rule No. 30 controlling Telnet data from host B). Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al.; col. 4, lines 39-43) allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 10 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Further including the step of blocking the data from the users' computers as a function of the individualized rule set. (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the step of blocking the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. (Coss et al. show in FIG. 3, rule No. 20 blocking data from host A; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data to host A.) Coss et al. also disclose rule set categories such as “Source host group identifier or IP address”, “Destination host group identifier or IP address”, and “Rule action, e.g., ‘pass’, ‘drop’, or ‘proxy’” (Coss et al. col. 4, lines 39-43) allowing the firewall 211 to block (i.e., drop) data to and from the users’ computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 11 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach “uses a router to link its internal intranet with an external network, such as the Internet”), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Further including the step of allowing the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, “filter IP packets in accordance with filtering profile” and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the step of allowing the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose in FIG. 4 a first session key rule (A, B, TELNET) allowing data to host B, and second session key rule (B, A, TELNET) allowing data from host B. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 12 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Further including the step of controlling the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the step of redirecting the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. (Coss et al., col. 9, lines 6-16 describing "two-way reflection") Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect data (i.e., also referred to as 'proxy' data by Coss et al.) to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 13 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Further including the step of controlling the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would

have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the step of *redirecting* the data from the users' computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose in step 1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" (Coss et al; col. 9, lines 39-42). These destination proxy servers include different destinations such as "authentication, mail handling, and virus scanning." (Coss et al., col. 1, lines 45-49) Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a Telnet proxy server. Coss et al. further state, "For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request." It is inherent that data was also redirected to the FTP proxy application as a function of the individualized rule set. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect (i.e., proxy) data from the users' computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 14 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). 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 (Radia et al; "default login profile" described in col. 3, lines 23-33).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al;

col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim 28 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) (Radia et al; col. 6, lines 30-36 describing rules based on "protocol type", and col. 8, lines 6-8 describing rules associated with a "domain name service" (DNS).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would

have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose at least one rule as a function of a type of *IP service*. However, Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. (Coss et al; Figure 3, "Service" column in rule table providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL" and col. 4, lines 2-11) It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 29 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. (Radia et al; col. 3, lines 5-22 and col. 3, lines 34-40)

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would

have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) However, Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 30 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address (Radia et al; col. 6, lines 14-18; col. 6, lines 30-36; and col. 6, lines 18-29).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on a request type and a destination address. However, Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 31 (includes limitations of canceled claim 1)

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose that 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. However, Coss et al. disclose that 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 32 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) (Radia et al; col. 6, lines 30-36 describing rules based on "protocol type", and col. 8, lines 6-8 describing rules associated with a "domain name service" (DNS).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose at least one rule as a function of a type of *IP service*. However, Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. (Coss et al; Figure 3, "Service" column in rule table providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL" and col. 4, lines 2-11) It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 33 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. (Radia et al; col. 3, lines 5-22 and col. 3, lines 34-40)

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) However, Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 34 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.;

FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14). Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address (Radia et al; col. 6, lines 14-18; col. 6, lines 30-36; and col. 6, lines 18-29).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on a request type and a destination address. However, Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 35 (includes limitations of canceled claim 8)

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected to the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.;

FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected to the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Radia et al. do not explicitly disclose that 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. However, Coss et al. disclose that 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 44

Radia et al. disclose a system (Radia et al.; FIG. 1, system 100) comprising: a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receive user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet") , and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106); wherein a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID is communicated to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); 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 router (Radia et al.; FIG. 9, steps 908 to 910); and wherein data directed toward the public network from the one of the users' computers are processed by the router according to the individualized rule set (Radia et al.; col. 10 lines 11-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected between the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim 45

Radia et al. disclose the router (Radia et al.; FIG. 1, router 106) further provides control over a plurality of data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose *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. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set (Coss et al; col. 2, lines 57-60 and FIG. 3 showing individualized rule set for host B having rule No. 10 controlling FTP data to host B, and rule No. 30 controlling Telnet data from host B). Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al.; col. 4, lines 39-43) allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 46

Radia et al. disclose the router (Radia et al.; FIG. 1, router 106) further blocks the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose *the redirection server* further blocks the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. (Coss et al. show in FIG. 3, rule No. 20 blocking data from host A; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data to host A.) Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al. col. 4, lines 39-43) allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 47

Radia et al. disclose the router (Radia et al.; FIG. 1, router 106) further allows the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose *the redirection server* further allows the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose in FIG. 4 a first session key rule (A, B, TELNET) allowing data to host B, and second session key rule (B, A, TELNET) allowing data from host B. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 48

Radia et al. disclose the router (Radia et al.; FIG. 1, router 106) further controls data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose *the redirection server* further *redirects* the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. (Coss et al., col. 9, lines 6-16 describing "two-way reflection") Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect data (i.e., also referred to as 'proxy' data by Coss et al.) to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 49

Radia et al. disclose the router (Radia et al.; FIG. 1, router 106) further controls data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose *the redirection server* further *redirects* the data from the users' computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose in step 1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" (Coss et al; col. 9, lines 39-42). These destination proxy servers include different destinations such as "authentication, mail handling, and virus scanning." (Coss et al., col. 1, lines 45-49) Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a Telnet proxy server. Coss et al. further state, "For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request." It is inherent that data was also redirected to the FTP proxy application as a function of the individualized rule set. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect (i.e., proxy) data from the users' computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 50

Radia et al. disclose wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set (Radia et al; "default login profile" described in col. 3, lines 23-33)

Claim 51

Radia et al. disclose wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) (Radia et al; col. 6, lines 30-36 describing rules based on "protocol type", and col. 8, lines 6-8 describing rules associated with a "domain name service" (DNS).

Radia et al. do not explicitly disclose at least one rule as a function of a type of *IP service*. However, Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. (Coss et al; Figure 3, "Service" column in rule table providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL" and col. 4, lines 2-11) It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 52

Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. (Radia et al; col. 3, lines 5-22 and col. 3, lines 34-40)

Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) However, Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 53

Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address (Radia et al; col. 6, lines 14-18; col. 6, lines 30-36; and col. 6, lines 18-29).

Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on a request type and a destination address. However, Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 54

Radia et al. do not explicitly disclose that 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. However, Coss et al. disclose that 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 55

Radia et al. do not disclose that 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*. However, Coss et al. disclose that firewall 211 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. Coss et al; col. 4, lines 1-6 and col. 9, lines 39-44 stating, "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values". It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 56

Radia et al. disclose in a system (Radia et al.; FIG. 1, system 100) comprising a database (Radia et al.; FIG. 3, filtering profile database 316) with entries correlating each of a plurality of user IDs with an individualized rule set (Radia et al.; FIG. 4, sequence of filtering profiles 400); modems (Radia et al.; FIG. 1, modems 104) that receives user IDs from users' computers (Radia et al.; FIG. 1, pc 102); a router (Radia et al.; FIG. 1, router 106) connected between the modems and a public network (Radia et al.; col. 2, lines 5-7 teach "uses a router to link its internal intranet with an external network, such as the Internet"), and an authentication accounting server (Radia et al.; FIG. 1, combination of access network control server ANCS 112 & services management system SMS 114) connected to the database (Radia et al.; FIG. 3, filtering profile database 316), the modems (Radia et al.; FIG. 1, modems 104) and the router (Radia et al.; FIG. 1, router 106), 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 to the authentication accounting server (Radia et al.; FIG. 7, step 706 and col. 9 lines 62-64); communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the router 106 from the authentication accounting server (Radia et al.; FIG. 9, steps 908 to 910); and processing data directed toward the public network from the one of the users' computers according to the individualized rule set (Radia et al.; col. 10 lines 11-14).

Radia et al. do not explicitly disclose a dial-up network server; however, the APA discloses a dial-up networking server (APA; FIG. 1, dial-up networking server 102) that receives user IDs from users' computers (APA; col. 1, lines 20-21) and communicates a first user ID for one of the users' computers and a temporarily assigned network address for the first user ID to an authentication accounting server (APA; col. 1, lines 21-24). It would have been obvious to replace the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to log in through the dial-up networking server as suggested by the APA rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 as suggested by the APA rather than by the DHCP server 110.

Radia et al. do not explicitly disclose *a redirection server* connected between the dial-up network server and a public network; however, Coss et al. disclose a redirection server (Coss et al; FIG. 2, firewall 211) that supports dynamically loaded user-specific access rules (Coss et al; col. 8, lines 24-31) that is connected between a user site 201 and a public network (Coss et al; Internet 105) and that controls the user's access to the network by utilizing redirection functionality (Coss et al; Abstract states "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65). It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby unburden the router 106 from having to utilize application proxies, as suggested by Coss et al. Furthermore, Radia et al. suggest using other types of networking technologies in addition to a router 106 (Radia et al; col. 1, lines 13-16). Therefore, it would have been obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 is another type of networking technology. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the system 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim 57

Radia et al. discloses further including the step of controlling a plurality of data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose the step of controlling a plurality of data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set (Coss et al; col. 2, lines 57-60 and FIG. 3 showing individualized rule set for host B having rule No. 10 controlling FTP data to host B, and rule No. 30 controlling Telnet data from host B). Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al.; col. 4, lines 39-43) allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 58

Radia et al. disclose further including the step of blocking the data from the users' computers as a function of the individualized rule set. (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose the step of blocking the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. (Coss et al. show in FIG. 3, rule No. 20 blocking data from host A; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data to host A.) Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al. col. 4, lines 39-43) allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 59

Radia et al. disclose further including the step of allowing the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose the step of allowing the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose in FIG. 4 a first session key rule (A, B, TELNET) allowing data to host B, and second session key rule (B, A, TELNET) allowing data from host B. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 60

Radia et al. disclose further including the step of controlling the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14).

Radia et al. do not explicitly disclose the step of redirecting the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. (Coss et al., col. 9, lines 6-16 describing "two-way reflection") Coss et al.

also disclose rule set categories such as “Source host group identifier or IP address”, “Destination host group identifier or IP address”, and “Rule action, e.g., ‘pass’, ‘drop’, or ‘proxy’” (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect data (i.e., also referred to as ‘proxy’ data by Coss et al.) to and from the users’ computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 61

Radia et al. disclose further including the step of controlling the data from the users' computers as a function of the individualized rule set (Radia et al.; FIG. 6, step 606, “filter IP packets in accordance with filtering profile” and col. 10, lines 6-14).

Radia et al. do not explicitly disclose the step of *redirecting* the data from the users’ computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users’ computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose in step 1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy” (Coss et al; col. 9, lines 39-42). These destination proxy servers include different destinations such as “authentication, mail handling, and virus scanning.” (Coss et al., col. 1, lines 45-49) Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a Telnet proxy server. Coss et al. further state, “For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request.” It is inherent that data was also redirected to the FTP proxy application as a function of the individualized rule set. Coss et al. also disclose rule set categories such as “Source host group identifier or IP address”, “Destination host group identifier or IP address”, and “Rule action, e.g., ‘pass’, ‘drop’, or ‘proxy’” (Coss et al; col. 4, lines 39-43) allowing the firewall 211 to redirect (i.e., proxy) data from the users’ computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG.

1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 62

Radia et al. disclose 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 (Radia et al; "default login profile" described in col. 3, lines 23-33).

Claim 63

Radia et al. disclose wherein the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) (Radia et al; col. 6, lines 30-36 describing rules based on "protocol type", and col. 8, lines 6-8 describing rules associated with a "domain name service" (DNS).

Radia et al. do not explicitly disclose at least one rule as a function of a type of *IP service*. However, Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. (Coss et al; Figure 3, "Service" column in rule table providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL" and col. 4, lines 2-11) It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 64

Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. (Radia et al; col. 3, lines 5-22 and col. 3, lines 34-40)

Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) However, Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 65

Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address (Radia et al; col. 6, lines 14-18; col. 6, lines 30-36; and col. 6, lines 18-29).

Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on a *request* type and a destination address. However, Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 66

Radia et al. do not explicitly disclose that 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. However, Coss et al. disclose that 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim 67

Radia et al. do not explicitly disclose redirecting 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*. However, Coss et al. disclose that firewall 211 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. Coss et al; col. 4, lines 1-6 and col. 9, lines 39-44 stating, "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values". It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

SNQ raised

Because the above teachings of Radia et al., the APA, and Coss et al. were not applied in any rejection of the claims during the initial prosecution and prior reexamination of the `118 Patent, a substantial new question of patentability is raised.

3 Claims 16-24, 26-27, 36-43 and 68-90 are unpatentable under 35 U.S.C. § 103(a) as being obvious over Coss et al. in view of the APA

Requester respectfully submits that claims 16-24, 26-27, 36-43 and 68-90 are unpatentable under 35 U.S.C. § 103(a) as being obvious over Coss et al. in view of the APA. A reasonable examiner would consider Coss et al. and the APA pertinent to the patentability of the requested claims for at least the reasons discussed below. A claim chart setting forth the pertinence and manner of applying Coss et al. and the APA to each of the above-identified claims in support of this substantial new question of patentability is provided below in Section IV of this Request.

Claim 16 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow modification of at least a portion of the rule set as a function of time. (Coss et al; "time-limited rule which is used only for a specified time period", col. 2, lines 35-36 and "the dynamic rule … made active for only a limited time period", col. 8, lines 48-52).

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 17 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "dynamic rule… not be loaded until a data request is made over the FTP control session", col. 8, lines 48-52)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 18 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "Destination host group identifier or IP address", col. 4 line 40; and "Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set" in col. 8, lines 37-52.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 19 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines

48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time. (Coss et al; "Rule Timeout – Number of second of inactivity before rule is removed from rule list", col. 4, lines 48-49; "time-limited rule", col. 2, lines 25-36; "dynamic rule…made active for only a limited time period", col. 8, lines 48-52; and "Once a dynamic rule has served its function, it can be removed from the rule set", col. 8, lines 32-34.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 20 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; “one-time rule”, time-limited rule”, “threshold rule” col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al. “dynamic rule…not be loaded until a data request is made over the FTP control session”, col. 8, lines 48-52; and “Once a dynamic rule has served its function, it can be removed from the rule set”, col. 8, lines 32-34.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 21 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states “the firewall can be enabled to redirect a network session to a separate server for processing” also see col. 8, lines 56-65 describing “Proxy Reflection in according with the present invention involves redirecting a network session to another, ‘remote’ proxy server for processing, and then later passing it back via the firewall to the intended destination.”), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; “IP address”, col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; “Dynamic rules” Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al. "Destination host group identifier or IP address", col. 4 line 40; "Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set", col. 8, lines 37-52; and "Once a dynamic rule has served its function, it can be removed from the rule set", col. 8, lines 32-34.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 22 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet

105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "Once a dynamic rule has served its function, it can be removed from the rule set." col. 8, lines 32-34)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 23 (includes limitations of canceled claim 15)

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2 side of firewall 211 connected to user site 201) that is connected to a computer (at user site 201) using the assigned network address and a network side (Coss et al; FIG. 2 side of firewall 211 connected to Internet 105) connected to a computer network (Internet 105). Wherein the computer (at user site 201) using the assigned network address (IP address) is connected to the computer network through the redirection server (Coss et al; FIG. 2, firewall 211). (Coss et al; "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." col. 3, lines 53-54)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 24

Coss et al. disclose wherein instructions to the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "dynamic rules…can be loaded at any time by trusted parties, e.g., … firewall administrator"; Figure 1 illustrates Administrator processor 115 is on the network side of the firewalls 111, 113, 114. Figure 2 illustrates Administrator processor (ADM) 215 is on the user side of firewall 211.)

Claim 26 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). 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. (Coss et al; "dynamic rules", "one-time rule", "time-limited rule", "threshold rule", col. 2, lines 29-41; "dynamic rules…loaded at any time" col. 8, lines 26, 31; and "dynamic rule…not be loaded until a data request is made over the FTP control session", col. 8, lines 48-52.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Claim 27 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). 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, data transmitted to or from the user, and a location or locations the user access. (Coss et al; "dynamic rules", "one-time rule", "time-limited rule", "threshold rule", col. 2, lines 29-41; "dynamic rules…loaded at any time" col. 8, lines 26, 31; "dynamic rule…not be loaded until a data request is made over the FTP control session", col. 8, lines 48-52; and "Once a dynamic rule has served its function, it can be removed from the rule set.", col. 8, lines 32-34.)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary

IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Claim 36

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the rule set includes at least one rule as a function of a type of IP service.

(Coss et al; Figure 3, "Service" column in rule table providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL" and col. 4, lines 2-11)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule as a function of a type of IP service. However, it would have been obvious that the modified rule set includes at least one rule as a function of a type of IP service. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with at least one rule as a function of a type of IP service) yields predictable results that the modified rule set may also include at least one rule as a function of a type of IP service.

Claim 37

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired.

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set) yields predictable results that the modified rule set may also cause the firewall 211 to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

Claim 38

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11.

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule allowing access based on a request type and a destination address. However, it would have been obvious that the modified rule set includes at least one rule allowing access based on a request type and a destination address. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule allowing access based on a request type and a destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule allowing access based on a request type and a destination address.

Claim 39

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination."), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52); and wherein the 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and an attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet."

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 40 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; "dynamic rules…can be loaded at any time by trusted parties, e.g., …firewall administrator", col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). Wherein the rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. (Coss et al; "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL", also see col. 4, lines 2-11)

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule as a function of a type of IP service. However, it would have been obvious that the modified rule set includes at least one rule as a function of a type of IP service. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with at least one rule as a function of a type of IP service) yields predictable results that the modified rule set may also include at least one rule as a function of a type of IP service.

Claim 41 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; "dynamic rules…can be loaded at any time by trusted parties, e.g., …firewall administrator", col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). Wherein the rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe "a time-limited rule" which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired.

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary

IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Coss et al. do not explicitly disclose that 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set) yields predictable results that the modified rule set may also cause the firewall 211 to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

Claim 42 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; “IP address”, col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; “dynamic rules…can be loaded at any time by trusted parties, e.g., …firewall administrator”, col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). Wherein the rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = “PASS”) based on a request type of “MAIL” and a destination host of “D”. Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11.

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary

IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule allowing access based on a request type and a destination address. However, it would have been obvious that the modified rule set includes at least one rule allowing access based on a request type and a destination address. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule allowing access based on a request type and a destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule allowing access based on a request type and a destination address.

Claim 43 (includes limitations of canceled claim 25)

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); the method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; “dynamic rules…can be loaded at any time by trusted parties, e.g., …firewall administrator”, col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211). Wherein the 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = “PROXY”) based on a request type of “TELNET” and an attempted destination host of “C”. Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, “In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet.”

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary

IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Coss et al. do not explicitly disclose 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 68

Coss et al. disclose a system (Coss et al; FIG. 2) comprising: a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") connected between a user computer (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105), the redirection server (Coss et al; FIG. 2, firewall 211) programed with a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, functions of PASS, DROP, PROXY) used to control data passing between the user (Coss et al. FIG. 2, at user site 201) and a public network (Coss et al. FIG. 2, Internet 105); wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow automated modification of at least a portion of the rule set correlated to the network address (Coss et al; "Dynamic rules" Col. 8, lines 24-31); 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 (Coss et al; "one-time rule", time-limited rule", "threshold rule" col. 2, lines 29-41; and see col. 8, lines 48-52).

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (disclosed temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers at user site 201, as suggested by the APA systems.

Claim 69

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow modification of at least a portion of the rule set as a function of time. (Coss et al; "time-limited rule which is used only for a specified time period", col. 2, lines 35-36 and "the dynamic rule … made active for only a limited time period", col. 8, lines 48-52).

Claim 70

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "dynamic rule… not be loaded until a data request is made over the FTP control session", col. 8, lines 48-52)

Claim 71

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "Destination host group identifier or IP address", col. 4 line 40; and "Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set" in col. 8, lines 37-52.)

Claim 72

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to allow the removal or reinstatement of at least a portion of the rule set as a function of time. (Coss et al; "Rule Timeout – Number of second of inactivity before rule is removed from rule list", col. 4, lines 48-49; "time-limited rule", col. 2, lines 25-36; "dynamic rule…made active for only a limited time period", col. 8, lines 48-52; and "Once a dynamic rule has served its function, it can be removed from the rule set", col. 8, lines 32-34.)

Claim 73

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al. "dynamic rule…not be loaded until a data request is made over the FTP control session", col. 8, lines 48-52; and "Once a dynamic rule has served its function, it can be removed from the rule set", col. 8, lines 32-34.)

Claim 74

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al. "Destination host group identifier or IP address", col. 4 line 40; "Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set", col. 8, lines 37-52; and "Once a dynamic rule has served its function, it can be removed from the rule set", col. 8, lines 32-34.)

Claim 75

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "Once a dynamic rule has served its function, it can be removed from the rule set." col. 8, lines 32-34)

Claim 76

Coss et al. disclose wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2 side of firewall 211 connected to user site 201) that is connected to a computer (at user site 201) using the assigned network address and a network side (Coss et al; FIG. 2 side of firewall 211 connected to Internet 105) connected to a computer network (Internet 105). Wherein the computer (at user site 201) using the assigned network address (IP address) is connected to the computer network through the redirection server (Coss et al; FIG. 2, firewall 211). (Coss et al; "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." col. 3, lines 53-54)

Claim 77

Coss et al. disclose wherein instructions to the redirection server (Coss et al; FIG. 2, firewall 211) 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. (Coss et al; "dynamic rules…can be loaded at any time by trusted parties, e.g., … firewall administrator"; Figure 1 illustrates Administrator processor 115 is on the network side of the firewalls 111, 113, 114. Figure 2 illustrates Administrator processor (ADM) 215 is on the user side of firewall 211.)

Claim 78

Coss et al. disclose wherein the rule set includes at least one rule as a function of a type of IP (Internet Protocol) service. (Coss et al; "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as “FTP”, “TELNET”, and “MAIL”, also see col. 4, lines 2-11)

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule as a function of a type of IP service. However, it would have been obvious that the modified rule set includes at least one rule as a function of a type of IP service. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with at least one rule as a function of a type of IP service) yields predictable results that the modified rule set may also include at least one rule as a function of a type of IP service.

Claim 79

Coss et al. disclose wherein the rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe “a time-limited rule” which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired.

Coss et al. do not explicitly disclose that 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set) yields predictable results that the modified rule set may also cause the firewall 211 to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

Claim 80

Coss et al. disclose wherein the rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule allowing access based on a request type and a destination address. However, it would have been obvious that the modified rule set includes at least one rule allowing access based on a request type and a destination address. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule allowing access based on a request type and a destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule allowing access based on a request type and a destination address.

Claim 81

Coss et al. disclose wherein the 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and an attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet."

Coss et al. do not explicitly disclose 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 82

Coss et al. disclose that the redirection server (Coss et al; FIG. 2, Firewall 211) 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. Coss et al; col. 4, lines 1-6 and col. 9, lines 39-44 stating, "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values".

Claim 83

Coss et al. disclose, in a system (FIG. 2) comprising a redirection server (Coss et al; FIG. 2, firewall 211, abstract states "the firewall can be enabled to redirect a network session to a separate server for processing" also see col. 8, lines 56-65 describing "Proxy Reflection in according with the present invention involves redirecting a network session to another, 'remote' proxy server for processing, and then later passing it back via the firewall to the intended destination.") connected between a user computer (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105), the redirection server (Coss et al; FIG. 2, firewall 211) containing a user's rule set (Coss et al; col. 3, lines 31-33, FIG. 3) correlated to a network address (Coss et al; "IP address", col. 4, line 39); wherein the user's rule set contains at least one of a plurality of functions (Coss et al; FIG. 3, function of PASS, DROP, PROXY) used to control data passing between the user (Coss et al; FIG. 2, at user site 201) and a public network (Coss et al; FIG. 2, Internet 105); a method (Coss et al; FIGs. 5A, 5B, 7, 9, 10A, 10B) 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 network address in the redirection server (Coss et al; col. 8, lines 26-31); and wherein the redirection server (Coss et al; FIG. 2, firewall 211) has a user side (Coss et al; FIG. 2, side of Firewall 211 connected to user site 201) that is connected to a computer (inherent that user site 201 includes a computer) using the network address (IP address) and a network side (Coss et al; FIG. 2, side of Firewall 211 connected to Internet 105) connected to a computer network (Coss et al; FIG. 2, Internet 105) and wherein the computer (Coss et al; FIG. 2, at user site 201) using the network address (IP address) is connected to the computer network (Coss et al; FIG. 2, Internet 105) through the redirection server (Coss et al; col. 3, lines 53-54) and the method further includes the step of receiving instructions by the redirection server (Coss et al; FIG. 2, firewall 211) 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 (Coss et al; col. 8, lines 26-31, FIG. 1 shows Administrator processor 115 is on the network side of firewalls 111,113,114; and FIG. 2 shows Administrator processor 215 is on the user side of firewall 211).

Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a temporarily assigned network address. However, the APA discloses that dial-up users are often provided with a temporarily assigned IP address (APA; col. 1, lines 15-37). Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned such as in the APA. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results of assigning a user a temporary IP address. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Coss et al. do not explicitly disclose that the firewall 211 has a user side that is connected to a computer using the temporarily assigned network address. However, it is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to even include a firewall 211 with the rule set correlated to the assigned IP address between user site 201 and the Internet 105. Furthermore, as firewall 211 is disclosed programmed with a user's rule set correlated to an IP address, it would have been obvious that the computer's IP address may be temporarily assigned is done in the APA systems. See the above paragraph for further explanation of why temporarily assigned IP addresses are obvious given the APA.

Claim 84

Coss et al. disclose 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. (Coss et al; “dynamic rules”, “one-time rule”, “time-limited rule”, “threshold rule”, col. 2, lines 29-41; “dynamic rules…loaded at any time” col. 8, lines 26, 31; and “dynamic rule…not be loaded until a data request is made over the FTP control session”, col. 8, lines 48-52.)

Claim 85

Coss et al. disclose 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, data transmitted to or from the user, and a location or locations the user access. (Coss et al; “dynamic rules”, “one-time rule”, “time-limited rule”, “threshold rule”, col. 2, lines 29-41; “dynamic rules…loaded at any time” col. 8, lines 26, 31; “dynamic rule…not be loaded until a data request is made over the FTP control session”, col. 8, lines 48-52; and “Once a dynamic rule has served its function, it can be removed from the rule set.”, col. 8, lines 32-34.)

Claim 86

Coss et al. disclose wherein the rule set includes at least one rule as a function of a type of IP service. (Coss et al; Figure 3, “Service” column in rule table providing rules as a function of types of IP services such as “FTP”, “TELNET”, and “MAIL” and col. 4, lines 2-11)

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule as a function of a type of IP service. However, it would have been obvious that the modified rule set includes at least one rule as a function of a type of IP service. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with at least one rule as a function of a type of IP service) yields predictable results that the modified rule set may also include at least one rule as a function of a type of IP service.

Claim 87

Coss et al. disclose wherein the rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection server (Coss et al; FIG. 2, firewall 211) is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. (Coss et al; col. 8, lines 37-40 describe “a time-limited rule” which is used only for a specified time period). Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired.

Coss et al. do not explicitly disclose that 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set) yields predictable results that the modified rule set may also cause the firewall 211 to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.

Claim 88

Coss et al. disclose wherein the rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose in Figure 3 Rule No. 40 allowing access (i.e., action = “PASS”) based on a request type of “MAIL” and a destination host of “D”. Also see the categories "Source Host," "Destination Host" and "Service" descried by Coss et al. at col. 4, lines 2-11.

Coss et al. do not explicitly disclose that the *modified* rule set includes at least one rule allowing access based on a request type and a destination address. However, it would have been obvious that the modified rule set includes at least one rule allowing access based on a request type and a destination address. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule allowing access based on a request type and a destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule allowing access based on a request type and a destination address.

Claim 89

Coss et al. disclose wherein the 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. For instance, Coss et al. disclose Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and an attempted destination host of "C". Proxy actions are equivalent to redirection in the disclosure of Coss et al. Also see Coss et al; col. 4, lines 2-11 stating, "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet."

Coss et al. do not explicitly disclose 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. However, it would have been obvious that 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. For example, applying a known technique (dynamic rule modification) to a known device (firewall 211 programmed with rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address) yields predictable results that the firewall is programmed with a modified rule set including at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.

Claim 90

Coss et al. disclose that the redirection server (Coss et al; FIG. 2, Firewall 211) 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. Coss et al; col. 4, lines 1-6 and col. 9, lines 39-44 stating, "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values".

SNQ raised

Because the above teachings of Coss et al. and the APA were not applied in any rejection of the claims during the initial prosecution and prior reexamination of the `118 Patent, a substantial new question of patentability is raised.

IV. CLAIM CHARTS SHOWING MANNER OF APPLYING THE CITED PRIOR ART TO EVERY CLAIM FOR EACH SNQ

The following is a quotation of 35 U.S.C. § 103(a) which forms the basis for applying the above-identified prior art to the claims of `118 patent:

(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.

1 Claim chart showing how each of claims 2-7, 9-14, 16-24, and 26-43 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA

The record shows that canceled claims 1, 8, 15 and 25 are unpatentable as obvious over He et al. in view of Zenchelsky et al., and further in view of the APA. In the Decision on Appeal, the Board entered a new ground of rejection of independent claims 1, 8, 15 and 25 as being obvious over He et al. in view of Zenchelsky et al., and further in view of the APA The Patent Owner did not request a rehearing and instead cancelled claims 1, 8, 15 and 25 in response to the Board's Decision. This action by the Patent Owner constitutes an admission that the new ground of rejection is sound; the limitations of canceled claims 1, 8, 15, and 25 are therefore not addressed in the following claim table.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
2.	The system of claim 1, wherein the redirection server further	He et al. disclose wherein the redirection server (He et al; credential server 204) further provides control

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	provides control over a plurality of data to and from the users' computers as a function of the individualized rule set.	over a plurality of data to and from the users' computers as a function of the individualized rule set. For example, see He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access. Also see He et al at col. 16, lines 61-67 for detail of user credentials.
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.	He et al. disclose wherein the redirection server (He et al; credential server 204) further blocks the data to and from the users' computers as a function of the individualized rule set For example, see He et al; credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Conversely, network elements 104 which cannot be accessed in accordance with the user credentials are inherently blocked from access. Also see He et al at col. 19, lines 24-31 which describe the scenario where the user access ticket is actively voided, corresponding to a blocking action.
4.	The system of claim 1, wherein the redirection server further	He et al. disclose wherein the redirection server further allows the data to and from the users'

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	allows the data to and from the users' computers as a function of the individualized rule set.	computers as a function of the individualized rule set. For example, see He et al. col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data exchange occurs between accessed network elements 104.
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.	He et al. disclose wherein the redirection server further redirects the data to and from the users' computers as a function of the individualized rule set. For example, see He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data access to network elements 104 corresponds to data moving to and from users' computers.
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.	He et al. disclose wherein the redirection server further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set. For example, see He et al; FIG 10, plural network elements 104 represent multiple potential destinations for interaction based on particular user

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		credentials.
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.	He et al. disclose wherein the database entries for a plurality of the plurality of users' IDs are correlated with a common individualized rule set. For example, see He et al; col. 16, line 54 through line 68. Each database entry (record) includes a user ID accompanied by user credentials. The user credentials are the individualized rules for a particular user.
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.	He et al. disclose further including the step of controlling a plurality of data to and from the users' computers as a function of the individualized rule set. For example, see He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access. Also see He et al at col 16, lines 61-67 for detail of user credentials.
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.	He et al. disclose further including the step of blocking the data to and from the users' computers as a function of the individualized rule set. For example, see He et al; credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Conversely, network

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		elements 104 which cannot be accessed in accordance with the user credentials are inherently blocked from access. Also see He et al. at col. 19, lines 24-31 which describe the scenario where the user access ticket is actively voided, corresponding to a blocking action.
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.	He et al. disclose further including the step of allowing the data to and from the users' computers as a function of the individualized rule set. For example, see He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data exchange occurs between accessed network elements 104.
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.	He et al. disclose further including the step of redirecting the data to and from the users' computers as a function of the individualized rule set. For example, He et al; col. 19, lines 2-11, credential server 204 retrieves user credentials which correspond to an individualized rule set that controls access to network elements 104. Data access to network elements 104 corresponds to data moving to and from users' computers.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
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.	He et al. disclose further including the step of redirecting the data from the users' computers to multiple destinations a function of the individualized rule set. For example, see He et al; FIG 10, plural network elements 104 represent multiple potential destinations for interaction based on particular user credentials.
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.	He et al. disclose 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. For example, see He et al; col. 16, line 54 through line 68. Each database entry (record) includes a user ID accompanied by user credentials. The user credentials are the individualized rules for a particular user.
16.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	wherein the redirection server is configured to allow automated modification of at least a	He et al. disclose wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	portion of the rule set correlated to the temporarily assigned network address;	temporarily assigned network address. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		be a combination that invokes only one of the elements recited.
	wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	He et al. disclose wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time. For example: He et al., col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified.
17.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	wherein the redirection server is configured to allow automated	He et al. disclose wherein the redirection server is configured to allow automated modification of at

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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	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: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. disclose 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. This feature is optionally recited earlier in the claim. Such optional recitations do not carry

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can modify the rule set, for example, by deleting it. The system administrator is one of the system users.
18.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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,

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		however, contains html code instructing the browser to request some other WWW page – hence the redirection of the user begins." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	user accesses; and	For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. disclose 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 attempts to access. This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		which can modify the rule set, for example, by deleting it. The location of the administrator is the location at which modification is permitted.
19.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. disclose 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. For example: He et al; col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account. Any actions of administrator inherently occur over some given period time.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
20.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a	He discloses 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.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	public network;	For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		"lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. further disclose 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. This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The system administrator is one of the system users.
21.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	set correlated to a temporarily assigned network address;	set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. further disclose 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. This feature is optionally recited earlier in the claim. Such optional recitations do not carry patentable weight (MPEP 2106, Section C). Nonetheless, He et al. at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The location of the administrator is the location at which modification is permitted.
22.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	He et al. further disclose 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. For example: He et al; col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account. Any actions of administrator inherently occur over some given period time. He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account. The location of the administrator is the location at which modification

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		is permitted).
23.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	wherein the rule set contains at least one of a plurality of functions used to control data	He discloses wherein the rule set contains at least one of a plurality of functions used to control data

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	passing between the user and a public network;	passing between the user and a public network. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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	He et al. further disclose 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. For example: He et al; FIG 10, credential server 204 has a user side being any one of or both of the dial up server 1002 and dial up access network 1004 that is connected to a computer (He et al; FIG 10, user element 102) using the temporarily assigned network address (Zenchelsky et al; col. 1, lines 29-35) and a network side being any one of or both of the interconnection network 106 and network

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		elements 104 connected to a computer network (He et al; interconnection network 106)
	wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	He et al. disclose wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server. For example: He et al; FIG 10, computer 102 is connected to the interconnection network 106 via the credential server 204.
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.	He et al. disclose 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. For example: He et al., col. 17, lines 19-21 refer to a network administrator modifying any portion of a user account. He et al. at FIG 10 illustrates that users presenting input to the network (a network administrator is also a user). Accordingly, instructions transmitted from a network administrator originate at terminal 102 and proceed through the user side elements 1002, 1004 as well as the network side element 106.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
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 accesses.	He et al. disclose 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. For example: He et al., col 17, lines 19-21, the administrator is allowed to create or delete any portion of the user account as a function of one or more of: time (any actions of administrator inherently occur over some given period time) He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete any portion of the user account In He et al, the location of the administrator is the location at which modification is permitted.
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 a location or locations the user accesses.	He et al. disclose 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. For example: He et al., col 17, lines 19-21, the administrator is allowed to create or delete (i.e. remove or reinstate) any portion of the user account as a function of one

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		or more of: time (any actions of administrator inherently occur over some given period time) He et al at col 17, lines 19-21 define data input being supplied by a system administrator which can create or delete (i.e. remove or reinstate) any portion of the user account In He et al. the location of the administrator is the location at which modification is permitted.
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.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	He et al. disclose wherein the individual 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. Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		set and then utilizing a 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.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
33.	The method of claim 8, wherein the individualized rule set includes an initial temporary rule set and a standard rule set,	He et al. disclose wherein the individual 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

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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.	initial period of time and to thereafter utilize the standard rule set. Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a 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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
36.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	assigned network address;	address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
37.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	wherein the modified rule set includes an initial temporary rule set and a standard rule set, and wherein the redirection	He et al. discloses wherein the individual 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

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	server is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set.	initial period of time and to thereafter utilize the standard rule set. Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a standard rule set.
38.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 states "The browser next sends a request to the server requesting the page. In

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	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;	He discloses 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. For example: <u>He et al</u>; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	of time, data transmitted to or from the user, or location the user accesses; and	user, or location the user accesses. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the "lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	wherein the modified rule set includes at least one rule allowing access based on a request type and a destination address.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
39.	A system comprising:	He et al; FIG 10 is a system.
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	He et al; FIG 10, credential server 204 is similar to a redirection server programmed with a user's rule set correlated to a temporarily assigned network address For example, col. 19, line 3, credential server retrieves user credentials, which correspond to a rule set. When the credential server 204 retrieves the user credentials, it is programmed with that particular rule set. Alternatively, providing access by the credential server to the database containing the rule set can constitute being programmed with the rule set. He et al. do not explicitly disclose the credential server 204 controls the user's access to the network using redirection functionality. However, the APA col. 1, lines 53-57 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." Also see APA col. 1, lines 38-40 stating, "The redirection of Internet traffic is most often done with World Wide Web (WWW) traffic (more specifically, traffic using the HTTP (hypertext transfer protocol)") It

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		would have been obvious to incorporate redirection functionality into the system of He et al. because redirection is an obvious extension of blocking already performed by He et al. For example, an address blocked for a particular user could be replaced with another address, perhaps a safer website or a website explaining organizational policy regarding the blocked website. He et al. do not explicitly disclose a temporary network address. However, Zenchelsky et al; col. 1, lines 30-35 establish well known nature of assigning temporary IP address to user at session login; col. 1, lines 60-64 establish well known nature of having source and destination address encoded into communication packets as necessary to facilitate communication between source and destination. It would have been obvious to one of ordinary skill in the art to modify He et al; so to provide temporary IP address to a user node and additionally encode data communication packets with source and destination address as necessarily to facilitate communication through a switched packet network as taught by Zenchelsky et al.
	wherein the rule set contains at least one of a plurality of functions used to control data passing between the user and a	He discloses 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.

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	public network;	For example: He et al; col. 16, lines 61-67, credentials define plural functions. Also, note the additional functions at col. 17, lines 6-27 attributed to the overall server system 208
	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 et al. disclose 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. For example: He et al; col. 17, lines 19-21, database tool associated with server system 208 can create or delete user accounts
	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	He et al. disclose 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. For example: He et al; col 17, lines 19-21, any of the user account information can be modified. He et al; col 17, line 13 attributes a "lifetime" to the authentication. Since any portion of the user account can be modified, the length of the

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
		"lifetime" can be modified as well. Alternatively, since the modification can be made at any time, the modification can occur "as a function of time". The "data transmitted" and "location" are optional recitations, and thus do not carry patentable weight in the current claim (MPEP 2106, Section C). It is also noted that the phrase "some combination" does not necessarily require two or more of the elements to be present. For example, a subcombination could be a combination that invokes only one of the elements recited.
	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.	A "rule" does not change the structure of a physical system, and also does not change the functionality of the system unless the rule is executed. Since this rule imparts neither structure nor new functionality (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
41.	The method of claim 25, wherein the modified rule set	<u>He et al.</u> disclose wherein the modified rule set includes an initial temporary rule set and a standard

Claim No.	Claim language	Corresponding features disclosed by He et al. in view of Zenchelsky et al., and further in view of the APA
	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.	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. Each "user credential" of He et al corresponds to a rule. Since multiple user credentials exist in the system of He et al, invoking a first user's credentials and subsequently invoking a second user's credentials corresponds to utilizing a temporary rule set and then utilizing a 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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).
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.	A "rule" does not change the structure of a physical system, and additionally does not affect method steps performed unless the rule is invoked. Since this rule imparts neither structure nor any additional method steps (it is not executed or invoked) it imparts no additional patentable weight (*In re Ngai* 367 F.3d 1336, USPQ2d 1862 (Fed. Cir. 2004)).

2 Claim chart showing how each of claims 2-7, 9-14, 28-35, and 44-67 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over Radia et al. in view of the APA, and further in view of Coss et al.

As shown in the attached reexamination certificate of the `118 patent, independent claims 1 and 8 are cancelled but original dependent claims 2-7 and 9-14 remain enforceable. As dependent claims 2-7 and 9-14 include all limitations of their respective original base claims 1 and 8, the limitations of original claims 1 and 8 are also addressed in the below table.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
1.	A system comprising:	Radia et al. Figure 1: computer network 100 is a system
	a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia et al. Figure 3: filtering profiles 316 are a database with entries correlating each of a plurality of user IDs with an individualized rule set For instance, Radia et al. disclose: "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**. In general, it may be appreciated that various users of network 100 will have varying types of allowed access. As a result, **different network users will require different filtering profiles 400. Generally, these filtering profiles 400 are defined separately for each user** using either automatic or manual generation techniques. For the present invention, **these filtering profiles 400 are preferably maintained in filtering profile database 316 and retrieved using the identity of**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>the particular user</u>." [9:46-56, emphasis added]
	a dial-up network server that receives user IDs from users' computers;	Radia et al. disclose in Figure 1 that modems 104 (which may be telephone - i.e., dial-up) and DHCP server 110 establish a communications link with the user's PC. A login applet on the user's computer (one of PCs 102) communicates with a login server and allows users to login to the network 100. For instance, Radia et al. disclose: "A **<u>cable modem 104</u>** is connected to each client system 102." [1:11-12, emphasis added] "For example, an internet service provider (ISP) may have users who connect, login, logoff and disconnect to its network over time **<u>using telephone or able modems</u>**." [2:45-48, emphasis added] "The client systems, which are typically personal computers using cable modems, connect to the router. **<u>As part of the connection process, each client system receives a dynamically allocated IP address from the DHCP server.</u>**" [2:67-3:4, emphasis added] "For a preferred embodiment of network 100, user logins are handled by downloading small, specifically tailored applications, known as "login applets," to client systems 102. The login applets

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		are downloaded from a server system, such as server system 108, or in some cases, from SMS 114." [8:30-34, emphasis added] "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**." [9:39-42, emphasis added] However, Radia et al. do not explicitly disclose *a dial-up network server* that receives user IDs from users' computers. Admitted prior art (APA) systems in Figure 1 of the `118 patent include a dial-up networking server 102 that receives user IDs from users' computers 100. The APA systems are described as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** and then logs the connection and assigned IP address." [`118 patent, col. 1, lines 15-37, emphasis added] It would have been obvious to substitute the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to login through the dial-up networking server rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 rather than by the DHCP server 110.
	a redirection server connected to the dial-up network server and a public network, and	Radia et al. Figure 1: router 106 is connected to the dial-up network server (substituted for DHCP server 110 and login applet) and server systems 108 of the network 100. Router 106 is similar to a redirection server because router 106 is connected

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		between the user's computer (PC 102) and the network's server systems 108, and controls the user's access to the network's server systems 108. Radia et al. further disclose that the network is a public network such as the Internet: "For example, assume that a company uses a router to link its internal intranet with an external network, **<u>such as the Internet</u>**." [2:5-7, emphasis added] However, Radia et al. do not explicitly disclose that the router 106 controls the user's access to the public network *by utilizing redirection functionality*. Coss et al. disclose a firewall that is connected between a user's computer and a public network that controls the user's access to the network by utilizing redirection functionality: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "This invention relates to the **<u>prevention of unauthorized access in computer networks</u>** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis] "Dynamic rules are rules which are included with the access rules as a need arises, for processing

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby prevent the router 106 from having to utilize application proxies, as suggested by Coss et al. Radia et al. further disclose that other networking technologies may be used instead of router 106, stating: "The use of cable router 106 and cable modems 104 is also intended to be exemplary and it should be appreciated **<u>that other networking technologies and topologies are equally practical.</u>**" [1:13-16, emphasis added] Therefore, it would have been further obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 disclosed by Coss et al. is another type of networking technology and Radia et al. suggest other types of network technology is equally practical. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the network 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	an authentication accounting server connected to the database, the dial-up network server and the redirection server;	In Radia et al. Figure 1, access network control server ANCS 112 and services management system SMS 114 together are an authentication accounting server because ANCS 112 and SMS 114 are connected to the database (filtering profiles 316 within SMS 114 – see Figure 3), the dial-up network server (substituted for DHCP server 110 and login applet), and the redirection server (Coss's firewall 211 in the position of router 106 in Radia's FIG. 1). Radia et al. further disclose that the ANCS 112 and SMS 114 determine whether a user ID is authorized to access the network. For instance, Radia et al. disclose: "FIG. 9 is a flowchart showing the steps associated with a preferred embodiment of a method for **<u>allocation of privileges to a user in a computer network</u>**." [4:59-61, emphasis added] "Method 900 includes step **<u>performed by SMS 114 and ANCS 112</u>**." [9:35-36, emphasis added] "In step 908, which follows, a sequence of filtering profiles 400 **<u>associated with the user</u>** are retrieved, by SMS 114, from filtering profile database 316. In general, it may be appreciated that **<u>various users of network 100 will have varying types of allowed</u>**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>access</u>." [9:46-50, emphasis added] "In FIG. 1, ANCS 112 and SMS 114 are shown as separate entities. It should be appreciated, however, that the present invention specifically anticipates that **<u>ANCS 112 and SMS 114 may be implemented using a single computer system</u>** that includes ANCS process 214, SMS process 314 and filtering profile database 316." [5:65-6:4, emphasis added]
	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 et al. disclose a login applet on a PC 102 and the DHCP server 110 respectively communicate a first user ID (entered using the login applet) for one of the users' computers (one of PCs 102) and a temporarily assigned network address (dynamically assigned IP address) for the first user ID to the authentication accounting server (SMS 114). For instance, Radia et al. disclose the login applet communicates from PC 102 to SMS 114: "Method 900 begins with step 906 where SMS 114 **<u>waits for a user login</u>**. More specifically, as discussed with regard to method 700, for a preferred embodiment of network 100, **<u>users login to network 100 using a login applet that communicates with a login server, such as SMS 114</u>**." [9:37-42, emphasis added] Radia et al. also disclose the DHCP server 110

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		passes the temporarily assigned network address for the first user ID to the SMS 114: "Method 700 begins with step 706 where **SMS 114 waits for the allocation of an IP address to a client system 102.** More specifically, for a preferred embodiment of network 100, power-on or reset of a client system 102 is followed by connection of the client system 102 to router 106. As part of this connection, the connecting client system 102 requests and receives a dynamically allocated IP address from DHCP server 110. This allocation requires that a number of messages pass between DHCP server 110 and the client system 102 requesting a new IP address. The last of these messages is a DHCPACK message sent by the DHCP server 110 to the client system 102. **To monitor the allocation of IP addresses, SMS 114 monitors DHCP messages within network 100.** Step 706 corresponds, in a general sense, to the methods and procedures that are executed by SMS 114 to wait for and detect DHCPACK messages within network 100." [7:21-34, emphasis added] With reference to FIG. 9, it is inherent that the SMS 114 also receives the IP address of the client system 102 because Radia et al. disclose "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**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>the ANCS 112</u>." [9:62-64, emphasis added] Radia et al. further disclose that the IP address of the client system (one of PCs 102) is temporarily assigned: "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." [7:51-55, emphasis added] However, Radia et al. do not explicitly disclose that *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. In the admitted prior art (APA) system of FIG. 1, the dial-up network server 102 communicates a first user ID for one of the users' computers 100 and a temporarily assigned network address for the first user ID to the authentication accounting server 104. For instance, the APA systems are described as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		authentication and accounting server 104." [`118 patent, Col. 1, lines 15-37, emphasis added] It would have been obvious to not remove these useful features of the APA systems when substituting the APA dial-up networking server 102 for the DHCP server 110 and login applet in FIG. 1 of Radia et al. This would have been obvious because simple substitution of the known dial-up networking server 102 for the DHCP server 110 and login applet obtains predictable results that the dial-up networking server 102 notifies the authentication accounting server of user details. It would further have been obvious that the dial-up network server should continue to behave in this way because, rather than the SMS 114 receiving the user ID and IP address respectively from the login applet and DHCP server 110, the SMS 114 would receive this information from the dial-up networking server, as suggested by the APA.
	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	Radia et al. disclose the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set (sequence of filtering profiles 400) that correlates with the first user ID (identity of the user) and the temporarily assigned network address (dynamic IP address) to the router 106.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	redirection server; and	For instance, Radia et al. disclose: FIG. 9: step 906 "wait for user login", step 908 "retrieve user filter profile from database", step 910 "download user profile to ancs", and step 920 "reconfigure network components" "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". [9:46-48, emphasis added] "For the present invention, these filtering profiles 400 are preferably maintained in filtering profile database 316 and **retrieved using the identity of the particular user**." [9:53 -56, emphasis added] "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." [9:60-64, emphasis added] "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**." [9:64-10:1, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"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 102 acting as a host for the user. For example, in some cases, the packet filter may be established by reconfiguring the modem 104 connected to the client system 102. Alternatively, the packet filter may be established by reconfiguring router 106." [10:1-7, emphasis added] It is inherent that the "packet filter for IP packets originating from the client system 102" communicated to the router 106 includes the temporarily assigned (i.e., dynamic) IP address of the client system 102 in order to identify the IP packets originating from the client system 102. However, Radia et al. do not explicitly disclose the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address *to the redirection server*. It would have been obvious to have the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the firewall 211 of Coss et al. A first reason is Radia et al. teach reconfiguring one or more network components that

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		forward packets originating at the client system 102, and the firewall 211 of Coss et al. is a network component that forwards packets originating at a client system. As such, Radia et al. suggest reconfiguring the firewall 211. It would have further been obvious to use a known technique (i.e., communicating an individualized rule set to thereby reconfiguring a router 106) to improve a similar device (firewall 211) in the same way. Additionally, Coss et al. disclose dynamic rules can be loaded into the firewall 211 at any time by trusted applications to thereby authorize specific network sessions. For instance, Coss et al. teach: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31, emphasis added] It therefore would have further been obvious to have the ANCS 112 communicate the individualized rule set to the firewall 211 of Coss et al. because the ANCS 112 is a trusted application that authorizes specific network sessions, as

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		suggested by Coss et al.
	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.	Radia et al. disclose that data directed toward the public network from the one of the users' computers (one of PCs 102) are processed by the router 106 according to the individualized rule set. For instance, Radia et al. disclose: "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." [10:11-14, emphasis added] However, Radia et al. do not explicitly disclose that data directed toward the public network from the one of the user's computers is processed *by the redirection server* according to the individualized rule set. Coss et al. disclose data directed toward the public network from the one of the users' computers are processed by firewall 211 according to the individualized rule set. For instance, Coss et al. disclose: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		access rules for processing packets." [2:29-32, emphasis added] "With a capability for supporting multiple security domains, **<u>a single firewall can support multiple users, each with a separate security policy</u>**." [3:31-34, emphasis added] "The particular rule set that is applied for any packet can be determined based on information such as the **<u>incoming and outgoing network interfaces</u>** as well as the **<u>network source and destination addresses</u>**." [1:67-2:4, emphasis added] It would have been obvious that when substituting router 106 in the network of Radia et al. with the firewall 211 of Coss et al., subsequent to the firewall 211 of Coss et al. being reconfigured by the ANCS 112, data directed toward the public network from the one of the user's computers would be processed by the firewall 211 according to the individualized rule set. A first reason is the ANCS 112 is disclosed to reconfigure the router 106 to process data in this way, and the firewall 211 is simply another type of networking component. In other words, simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		is reconfigured to process data directed toward the public network in the same way. Another reason is it would have been obvious to use a known technique (reconfiguring a router 106 to process outgoing data according to the individualized rule set) to improve a similar device (firewall 211) in the same way.
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.	Radia et al disclose that router 106 in FIG. 1 further provides control over a plurality of data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *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. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "The latter embodiment can allow the firewall techniques of the invention to provide, for example, parental control of Internet and video access in the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		home." [2:57-60] See FIG. 3, rule No. 10 controlling FTP data **to host B**, and rule No. 30 controlling Telnet data **from host B**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" [4:39-43] allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 further blocks data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *the redirection server* further blocks the data *to and*

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		from the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 3, rule No. 20 blocking data **from host A**; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data **to host A**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', '**drop'**, or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 further allows the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *the redirection server* further allows the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 4, first session key rule (A, B, TELNET) allowing data **<u>to host B</u>**, and second session key rule (B, A, TELNET) allowing data **<u>from host B</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., '**<u>pass</u>**', 'drop', or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose *the redirection server further redirects the data to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "For some users and proxy applications, the connection should appear at the destination to be coming from the original source rather than the remote system. This applies, e.g., to services which check the source IP address to ensure that it matches the user who signed up for the requested service. **<u>This capability is provided by "dual reflection" (or "two-way reflection"), with the source address of the outgoing connection changed back from the remote proxy to the</u>**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		original user's source address. This change is effected at the firewall, as each packet is received from the proxy and sent to the destination." [9:6-16, emphasis added] Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**proxy**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose *the redirection server* further redirects the data from the users' computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users' computers

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" [9:39-42] "Proxy processes have also been developed for other special-purpose applications, e.g., to perform services such as **<u>authentication, mail handling, and virus scanning</u>**." [1:45-49, emphasis added] Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data **<u>to a Telnet proxy server</u>**. Coss et al. further state, "For example, an **<u>FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request." It is inherent that data was also redirected to the FTP proxy application as a function of the individualized rule set. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**<u>proxy</u>**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data from the users'

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the database entries for a plurality of the plurality of the users' IDs are correlated with a common individualized rule set. For instance, "In the above description, we have set a default profile called the default login profile. The default login profile is a static profile that **<u>applies to ALL newly connected client systems</u>**. This way the SMS does not need to be aware as new client systems are connected. "**<u>One may also consider setting the default profile to a null profile and for each client system as the client system connects</u>**; for example, since a client system that connects may do a DHCP operation, this event can trigger the SMS to **<u>set the</u>**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>login profile for the newly connected computer</u>." [3:23-33, emphasis added]
8.	In a system comprising	Radia et al. Figure 1: computer network 100 is a system
	a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia et al. Figure 3: filtering profiles 316 are a database with entries correlating each of a plurality of user IDs with an individualized rule set. For instance, Radia et al. disclose: "In step 908, which follows, **<u>a sequence of filtering profiles 400 associated with the user</u>** are retrieved, by SMS 114, from **<u>filtering profile database 316</u>**. In general, it may be appreciated that various users of network 100 will have varying types of allowed access. As a result, **<u>different network users will require different filtering profiles 400. Generally, these filtering profiles 400 are defined separately for each user</u>** using either automatic or manual generation techniques. For the present invention, **<u>these filtering profiles 400 are preferably maintained in filtering profile database 316 and retrieved using the identity of the particular user</u>**." [9:46-56, emphasis added]
	a dial-up network server that receives user IDs from users' computers;	Radia et al. disclose in Figure 1 that modems 104 (which may be telephone - i.e., dial-up) and DHCP server 110 establish a communications link with the user's PC. A login applet on the user's computer

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		(one of PCs 102) allows users to login to the network 100. For instance, Radia et al. disclose: "A **<u>cable modem 104</u>** is connected to each client system 102." [1:11-12, emphasis added] "For example, an internet service provider (ISP) may have users who connect, login, logoff and disconnect to its network over time **<u>using telephone or able modems</u>**." [2:45-48, emphasis added] "The client systems, which are typically personal computers using cable modems, connect to the router. **<u>As part of the connection process, each client system receives a dynamically allocated IP address from the DHCP server.</u>**" [2:67-3:4, emphasis added] "For a preferred embodiment of network 100, user logins are handled by downloading small, specifically tailored applications, known as "login applets," to client systems 102. The login applets are downloaded from a server system, such as server system 108, or in some cases, from SMS 114." [8:30-34, emphasis added] "More specifically, as discussed with regard to method 700, for a preferred embodiment of network

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		100, **<u>users login to network 100 using a login applet that communicates with a login server, such as SMS 114</u>**." [9:39-42, emphasis added] However, Radia et al. do not explicitly disclose *a dial-up network server* that receives user IDs from users' computers. Admitted prior art (APA) systems in Figure 1 of the `118 patent include a dial-up networking server 102 that receives user IDs from users' computers 100. The APA systems are described as follows: "In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), **<u>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.</u>** 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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		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." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] It would have been obvious to substitute the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to login through the dial-up networking server rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 rather than by the DHCP server 110.
	a redirection server connected to the dial-up network server and a public network, and	Radia et al. Figure 1: router 106 is connected to the dial-up network server (substituted for DHCP server 110 and login applet) and server systems 108 of the network 100. Router 106 is similar to a redirection server because router 106 is connected between the user's computer (PC 102) and the network's server systems 108, and controls the user's access to the network's server systems 108.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		Radia et al. further disclose that the network is a public network such as the Internet: "For example, assume that a company uses a router to link its internal intranet with an external network, **<u>such as the Internet</u>**." [2:5-7, emphasis added] However, Radia et al. do not explicitly disclose that the router 106 controls the user's access to the public network *by utilizing redirection functionality*. Coss et al. disclose a firewall that is connected between a user's computer and a public network that controls the user's access to the network by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "This invention relates to the **<u>prevention of unauthorized access in computer networks</u>** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] It would be obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		traffic at the firewall 211 to thereby prevent the router 106 from having to utilize application proxies, as suggested by Coss et al. Radia et al. further disclose that other networking technologies may be used instead of router 106, stating: "The use of cable router 106 and cable modems 104 is also intended to be exemplary and it should be appreciated **that other networking technologies and topologies are equally practical.**" [1:13-16, emphasis added] Therefore, it would have been further obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 disclosed by Coss et al. is another type of networking technology and Radia et al. suggest other types of network technology is equally practical. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the network 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.
	an authentication accounting server connected to the database, the dial-up network	Radia et al. Figure 1 disclose access network control server ANCS 112 and services management system SMS 114 together are an authentication

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	server and the redirection server,	accounting server because ANCS 112 and SMS 114 are connected to the database (filtering profiles 316 within SMS 114 – see Figure 3), the dial-up network server (substituted for DHCP server 110 and login applet), and the redirection server (Coss's firewall 211 in the position of router 106 in Radia's FIG. 1). Radia et al. further disclose that the ANCS 112 and SMS 114 determine whether a user ID is authorized to access the network. For instance, Radia et al. disclose: "FIG. 9 is a flowchart showing the steps associated with a preferred embodiment of a method for <u>**allocation of privileges to a user in a computer network**</u>." [4:59-61, emphasis added] "Method 900 includes step <u>**performed by SMS 114 and ANCS 112**</u>." [9:35-36, emphasis added] "In step 908, which follows, a sequence of filtering profiles 400<u>**associated with the user**</u> are retrieved, by SMS 114, from filtering profile database 316. In general, it may be appreciated that <u>**various users of network 100 will have varying types of allowed access**</u>." [9:46-50, emphasis added] "In FIG. 1, ANCS 112 and SMS 114 are shown as separate entities. It should be appreciated, however,

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		that the present invention specifically anticipates that **ANCS 112 and SMS 114 may be implemented using a single computer system** that includes ANCS process 214, SMS process 314 and filtering profile database 316." [5:65-6:4, emphasis added]
	the method comprising the steps of:	Method disclosed by Radia et al. in Figure 9
	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;	Radia et al. disclose a login applet on a PC 102 and the DHCP server 110 respectively communicate a first user ID (entered using the login applet) for one of the users' computers (one of PCs 102) and a temporarily assigned network address (dynamically assigned IP address) for the first user ID to the authentication accounting server (SMS 114). For instance, Radia et al. disclose the login applet communicates from PC 102 to SMS 114: "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**." [9:37-42, emphasis added] Radia et al. also disclose the DHCP server 110 passes the temporarily assigned network address for

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		the first user ID to the SMS 114: "Method 700 begins with step 706 where **<u>SMS 114 waits for the allocation of an IP address to a client system 102.</u>** More specifically, for a preferred embodiment of network 100, power-on or reset of a client system 102 is followed by connection of the client system 102 to router 106. As part of this connection, the connecting client system 102 requests and receives a dynamically allocated IP address from DHCP server 110. This allocation requires that a number of messages pass between DHCP server 110 and the client system 102 requesting a new IP address. The last of these messages is a DHCPACK message sent by the DHCP server 110 to the client system 102. **<u>To monitor the allocation of IP addresses, SMS 114 monitors DHCP messages within network 100.</u>** Step 706 corresponds, in a general sense, to the methods and procedures that are executed by SMS 114 to wait for and detect DHCPACK messages within network 100." [7:21-34, emphasis added] With reference to FIG. 9, it is inherent that the SMS 114 also receives the IP address of the client system 102 from the dial-up network server because Radia et al. disclose "At the same time, **<u>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</u>**."

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		[9:62-64, emphasis added] Radia et al. further disclose that the IP address of the client system (one of PCs 102) is temporarily assigned: "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." [7:51-55, emphasis added] However, Radia et al. do not explicitly disclose 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. In the admitted prior art (APA) system of FIG. 1, the dial-up network server 102 communicates a first user ID for one of the users' computers 100 and a temporarily assigned network address for the first user ID to the authentication accounting server 104. For instance, the APA systems are described as follows: "The dial-up networking server then passes the user ID and password, along with a temporary Internet

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		Protocol (IP) address for use by the user to the ISP's authentication and accounting server 104." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] It would have been obvious to not remove these useful features of the APA systems when substituting the APA dial-up networking server 102 for the DHCP server 110 and login applet in FIG. 1 of Radia et al. This would have been obvious because simple substitution of the known dial-up networking server 102 for the DHCP server 110 and login applet obtains predictable results that the dial-up networking server 102 continues to include the above disclosed features. It would further have been obvious that the dial-up network server should continue to behave in this way because, rather than the SMS 114 receiving the user ID and IP address respectively from the login applet and DHCP server 110, the SMS 114 would receive this information from the dial-up networking server, as suggested by the APA.
	communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the redirection server from the	Radia et al. disclose the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set (sequence of filtering profiles 400) that correlates with the first user ID (identity of the user) and the temporarily assigned network address (dynamic IP address) to the router

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	authentication accounting server;	106. For instance, Radia et al. disclose: FIG. 9: step 906 “wait for user login”, step 908 “retrieve user filter profile from database”, step 910 “download user profile to ancs”, and step 920 “reconfigure network components” “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”. [9:46-48, emphasis added] “For the present invention, these filtering profiles 400 are preferably maintained in filtering profile database 316 and **retrieved using the identity of the particular user**.” [9:53 -56, emphasis added] “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.” [9:60-64, emphasis added] “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**.” [9:64-

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		10:1, emphasis added] "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 102 acting as a host for the user. For example, in some cases, the packet filter may be established by reconfiguring the modem 104 connected to the client system 102. Alternatively, the packet filter may be established by reconfiguring router 106." [10:1-7, emphasis added] It is inherent that the "packet filter for IP packets originating from the client system 102" communicated to the router 106 includes the temporarily assigned (i.e., dynamic) IP address of the client system 102 in order to identify the IP packets originating from the client system 102. However, Radia et al. do not explicitly disclose communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address *to the redirection server* from the ANCS 112 and SMS 114. It would have been obvious to have the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the firewall 211 of

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		Coss et al. A first reason is Radia et al. teach reconfiguring one or more network components that forward packets originating at the client system 102, and the firewall 211 of Coss et al. is a network component that forwards packets originating at a client system. As such, Radia et al. suggest reconfiguring the firewall 211. It would have further been obvious to use a known technique (i.e., communicating an individualized rule set to thereby reconfiguring a router 106) to improve a similar device (firewall 211) in the same way. Additionally, Coss et al. disclose dynamic rules can be loaded into the firewall 211 at any time by trusted applications to thereby authorize specific network sessions. For instance, Coss et al. teach: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31, emphasis added] It therefore would have further been obvious to have the ANCS 112 communicate the individualized rule set to the firewall 211 of Coss et

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		al. because the ANCS 112 is a trusted application that authorizes specific network sessions, as suggested by Coss et al.
	and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	Radia et al. disclose processing data directed toward the public network from the one of the users' computers (one of PCs 102) according to the individualized rule set. For instance, Radia et al. disclose: "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." [10:11-14, emphasis added]
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.	Radia et al disclose that router 106 in FIG. 1 further provides control over a plurality of data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose the step of controlling a plurality of data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		provides control over a plurality of data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "The latter embodiment can allow the firewall techniques of the invention to provide, for example, parental control of Internet and video access in the home." [2:57-60] See FIG. 3, rule No. 10 controlling FTP data **to host B**, and rule No. 30 controlling Telnet data **from host B**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" [4:39-43] allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 blocks the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose blocking the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 3, rule No. 20 blocking data **from host A**; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data **to host A**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', '**drop'**, or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 allows the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose allowing the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 4, first session key rule (A, B, TELNET) allowing data **<u>to host B</u>**, and second session key rule (B, A, TELNET) allowing data **<u>from host B</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address",

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		and "Rule action, e.g., '**pass**', 'drop', or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose *redirecting the data to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "For some users and proxy applications, the connection should appear at the destination to be coming from the original source rather than the remote system. This applies, e.g., to services which check the source IP address to ensure that it matches the user who signed up for the requested

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		service. **<u>This capability is provided by "dual reflection" (or "two-way reflection"), with the source address of the outgoing connection changed back from the remote proxy to the original user's source address. This change is effected at the firewall, as each packet is received from the proxy and sent to the destination.</u>**” [9:6-16, emphasis added] Coss et al. also disclose rule set categories such as “Source host group identifier or IP address”, “Destination host group identifier or IP address”, and “Rule action, e.g., ‘pass’, ‘drop’, or ‘**<u>proxy</u>**’” [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data to and from the users’ computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
13.	The method of claim 8, further including the step of redirecting the data from the users'	Radia et al. do not explicitly disclose *redirecting the data from the users' computers to multiple destinations* a function of the individualized rule

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	computers to multiple destinations a function of the individualized rule set.	set. However, Coss et al. disclose firewall 211 redirects the data from the user's computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" [9:39-42] "Proxy processes have also been developed for other special-purpose applications, e.g., to perform services such as <u>**authentication, mail handling, and virus scanning**</u>." [1:45-49, emphasis added] Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a <u>**Telnet proxy server**</u>. Coss et al. further state, "For example, an <u>**FTP proxy application**</u> could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request." Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '<u>**proxy**</u>'"

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		[4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data from the users' computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose 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. For instance, "In the above description, we have set a default profile called the default login profile. The default login profile is a static profile that **<u>applies to ALL newly connected client systems</u>**. This way the SMS does not need to be aware as new client systems are connected. "**<u>One may also consider setting the default profile to a null profile and for each client</u>**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>system as the client system connects</u>; for example, since a client system that connects may do a DHCP operation, this event can trigger the SMS to **<u>set the login profile for the newly connected computer</u>**." [3:23-33, emphasis added]
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.	Radia et al. disclose that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) packet. For instance, Radia et al. disclose: "Filtering rule 404 also includes **<u>a protocol type 506</u>**. **<u>Protocol type 506 corresponds to the protocol type of an IP packet</u>**. 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" [6:30-36, emphasis added] Radia et al. also disclose that at least one rule forwards packets associated with a DNS (domain name service): "The second of the login filtering profiles 400 forwards packets **<u>associated with DNS (domain name service)</u>** address resolution." [8:6-8, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		However, Radia et al. do not explicitly disclose at least one rule as a function of a type of IP *service*. Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. For instance, Coss et al. disclose: "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL". "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, **a designation of a special service which can be called for in a packet**, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" **and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet**." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. For example: "The SMS maintains a series of filtering profiles, each of which includes one or more of filtering rules. **The SMS sets a default filter sequence for the newly connected client system** by downloading the sequence by the SMS to the ANCS. … Subsequently, the packet filter uses the rules of the login filtering profile sequence to selectively forward or discard IP packets originating from the client system. **This filtering sequence will allow newly connected client systems to perform login, but nothing else**." [3:5-22, emphasis added] "A preferred embodiment of the present invention also generates or selects filtering profiles for users. With the login filtering profile sequence in place, a user can use the newly connected client system to

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		login to the network. The user login is monitored by the SMS. **<u>If the user login is successful, the SMS selects or generates a user filtering profile sequence.</u>** The user filtering profile sequence is then downloaded by the SMS to the ANCS…. **<u>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.</u>**" [3:34-50, emphasis added] However, Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. For instance, Coss et al. disclose: "Exemplary dynamic rules include a 'one-time' rule which is only used for a single session, **<u>a time-limited rule which is used only for a specified time period</u>**, and a threshold rule which is used

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		only when certain conditions are satisfied." [8:37-40, emphasis added] Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address. For instance, Radia et al. disclose: "In FIG. 5, it may be seen that each filtering rule 404 includes an action 500. Action 500 specifies the disposition of IP packets that match by a particular filtering rule 404. In particular, <u>**action 500 may indicate that a matched IP packet will be forwarded**</u>, or that a matched IP packet will be

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		discarded." [6:14-18] "Filtering rule 404 also includes **<u>a protocol type 506</u>**. **<u>Protocol type 506 corresponds to the protocol type of an IP packet</u>**. 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" [6:30-36, emphasis added] "Filtering rule 404 also includes a destination IP address 502 and a destination IP mask 504. Destination IP address 502 corresponds to the destination address included in the header of an IP packet. Destination IP mask 504 is similar to destination IP address 502 but corresponds to a range of destination addresses. To match a particular filtering rule 404, an IP packet must either have a destination address that matches the destination address 502 included in the filtering rule 404 or have a destination address that is covered by the destination address mask 504 of the filtering rule 404." [6:18-29, emphasis added] However, Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on *a request type* and a

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		destination address. Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose: Rule No. 40 in Figure 3 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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	Radia et al. do not explicitly disclose that 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.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	request type and an attempted destination address.	However, Coss et al. disclose that 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. For instance, Coss et al. disclose: Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
32.	The method of claim 8, wherein the individualized rule set includes at least one rule as a function of a type of IP	Radia et al. disclose that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) packet. For instance, Radia et al. disclose:

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	(Internet Protocol) service.	"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" [6:30-36, emphasis added] Radia et al. also disclose that at least one rule forwards packets associated with a DNS (domain name service): "The second of the login filtering profiles 400 forwards packets **associated with DNS (domain name service)** address resolution." [8:6-8, emphasis added] However, Radia et al. do not explicitly disclose at least one rule as a function of *a type of IP service*. Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. For instance, Coss et al. disclose: "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL".

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, **a designation of a special service which can be called for in a packet**, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" **and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet**." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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	Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	thereafter utilize the standard rule set.	another sequence. For example: "The SMS maintains a series of filtering profiles, each of which includes one or more of filtering rules. **<u>The SMS sets a default filter sequence for the newly connected client system</u>** by downloading the sequence by the SMS to the ANCS. … Subsequently, the packet filter uses the rules of the login filtering profile sequence to selectively forward or discard IP packets originating from the client system. **<u>This filtering sequence will allow newly connected client systems to perform login, but nothing else</u>**." [3:5-22, emphasis added] "A preferred embodiment of the present invention also generates or selects filtering profiles for users. With the login filtering profile sequence in place, a user can use the newly connected client system to login to the network. The user login is monitored by the SMS. **<u>If the user login is successful, the SMS selects or generates a user filtering profile sequence.</u>** The user filtering profile sequence is then downloaded by the SMS to the ANCS…. **<u>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.</u>**" [3:34-50, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		However, Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. For instance, Coss et al. disclose: "Exemplary dynamic rules include a 'one-time' rule which is only used for a single session, **<u>a time-limited rule which is used only for a specified time period</u>**, and a threshold rule which is used only when certain conditions are satisfied." [8:37-40, emphasis added] Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address. For instance, Radia et al. disclose: "In FIG. 5, it may be seen that each filtering rule 404 includes an action 500. Action 500 specifies the disposition of IP packets that match by a particular filtering rule 404. In particular, **action 500 may indicate that a matched IP packet will be forwarded**, or that a matched IP packet will be discarded." [6:14-18, emphasis added] "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" [6:30-36, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"Filtering rule 404 also includes a destination IP address 502 and a destination IP mask 504. Destination IP address 502 corresponds to the destination address included in the header of an IP packet. Destination IP mask 504 is similar to destination IP address 502 but corresponds to a range of destination addresses. To match a particular filtering rule 404, an IP packet must either have a destination address that matches the destination address 502 included in the filtering rule 404 or have a destination address that is covered by the destination address mask 504 of the filtering rule 404." [6:18-29, emphasis added] However, Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on *a request type* and a destination address. Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose: Rule No. 40 in Figure 3 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose that 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. However, Coss et al. disclose that 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. For instance, Coss et al. disclose: Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". "In FIG. 3, the categories "Source Host,"

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
44.	A system comprising:	Radia et al. Figure 1: computer network 100 is a system
	a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia et al. Figure 3: filtering profiles 316 are a database with entries correlating each of a plurality of user IDs with an individualized rule set For instance, Radia et al. disclose: "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**. In general, it may be appreciated that various users of network 100 will have varying types of allowed access. As a result, **different network users will require different filtering profiles 400. Generally, these filtering profiles 400 are defined separately for each user** using

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		either automatic or manual generation techniques. For the present invention, **these filtering profiles 400 are preferably maintained in filtering profile database 316 and retrieved using the identity of the particular user**." [9:46-56, emphasis added]
	a dial-up network server that receives user IDs from users' computers;	Radia et al. disclose in Figure 1 that modems 104 (which may be telephone - i.e., dial-up) and DHCP server 110 establish a communications link with the user's PC. A login applet on the user's computer (one of PCs 102) communicates with a login server and allows users to login to the network 100. For instance, Radia et al. disclose: "A **cable modem 104** is connected to each client system 102." [1:11-12, emphasis added] "For example, an internet service provider (ISP) may have users who connect, login, logoff and disconnect to its network over time **using telephone or able modems**." [2:45-48, emphasis added] "The client systems, which are typically personal computers using cable modems, connect to the router. **As part of the connection process, each client system receives a dynamically allocated IP address from the DHCP server.**" [2:67-3:4, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"For a preferred embodiment of network 100, user logins are handled by downloading small, specifically tailored applications, known as "login applets," to client systems 102. The login applets are downloaded from a server system, such as server system 108, or in some cases, from SMS 114." [8:30-34, emphasis added] "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**." [9:39-42, emphasis added] However, Radia et al. do not explicitly disclose *a dial-up network server* that receives user IDs from users' computers. Admitted prior art (APA) systems in Figure 1 of the `118 patent include a dial-up networking server 102 that receives user IDs from users' computers 100. The APA systems are described as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		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." [`118 patent, col. 1, lines 15-37, emphasis added] It would have been obvious to substitute the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to login through the dial-up networking server rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 rather than by the DHCP server 110.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	a redirection server connected between the dial-up network server and a public network, and	Radia et al. Figure 1: router 106 is connected between the dial-up network server (substituted for DHCP server 110 and login applet) and server systems 108 of the network 100. Router 106 is similar to a redirection server because router 106 is connected between the user's computer (PC 102) and the network's server systems 108, and controls the user's access to the network's server systems 108. Radia et al. further disclose that the network is a public network such as the Internet: "For example, assume that a company uses a router to link its internal intranet with an external network, **such as the Internet**." [2:5-7, emphasis added] However, Radia et al. do not explicitly disclose that the router 106 controls the user's access to the public network *by utilizing redirection functionality*. Coss et al. disclose a firewall that is connected between a user's computer and a public network that controls the user's access to the network by utilizing redirection functionality: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the firewall replaces the destination address in the packet with the host address of the proxy**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		application and, if necessary, it can also change the service port." [Coss et al., col. 8, lines 56-65, emphasis added] It would have been obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby prevent the router 106 from having to utilize application proxies, as suggested by Coss et al. Radia et al. further disclose that other networking technologies may be used instead of router 106, stating: "The use of cable router 106 and cable modems 104 is also intended to be exemplary and it should be appreciated **that other networking technologies and topologies are equally practical.**" [1:13-16, emphasis added] Therefore, it would have been further obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 disclosed by Coss et al. is another type of networking technology and Radia et al. suggest other types of network technology is equally practical.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the network 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.
	an authentication accounting server connected to the database, the dial-up network server and the redirection server;	In Radia et al. Figure 1, access network control server ANCS 112 and services management system SMS 114 together are an authentication accounting server because ANCS 112 and SMS 114 are connected to the database (filtering profiles 316 within SMS 114 – see Figure 3), the dial-up network server (substituted for DHCP server 110 and login applet), and the redirection server (Coss's firewall 211 in the position of router 106 in Radia's FIG. 1). Radia et al. further disclose that the ANCS 112 and SMS 114 determine whether a user ID is authorized to access the network. For instance, Radia et al. disclose: "FIG. 9 is a flowchart showing the steps associated with a preferred embodiment of a method for **allocation of privileges to a user in a computer network**." [4:59-61, emphasis added] "Method 900 includes step **performed by SMS 114 and ANCS 112**." [9:35-36, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"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. In general, it may be appreciated that **various users of network 100 will have varying types of allowed access**." [9:46-50, emphasis added] "In FIG. 1, ANCS 112 and SMS 114 are shown as separate entities. It should be appreciated, however, that the present invention specifically anticipates that **ANCS 112 and SMS 114 may be implemented using a single computer system** that includes ANCS process 214, SMS process 314 and filtering profile database 316." [5:65-6:4, emphasis added]
	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 et al. disclose a login applet on a PC 102 and the DHCP server 110 respectively communicate a first user ID (entered using the login applet) for one of the users' computers (one of PCs 102) and a temporarily assigned network address (dynamically assigned IP address) for the first user ID to the authentication accounting server (SMS 114). For instance, Radia et al. disclose the login applet communicates from PC 102 to SMS 114: "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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		preferred embodiment of network 100, **<u>users login to network 100 using a login applet that communicates with a login server, such as SMS 114</u>**." [9:37-42, emphasis added] Radia et al. also disclose the DHCP server 110 passes the temporarily assigned network address for the first user ID to the SMS 114: "Method 700 begins with step 706 where **<u>SMS 114 waits for the allocation of an IP address to a client system 102.</u>** More specifically, for a preferred embodiment of network 100, power-on or reset of a client system 102 is followed by connection of the client system 102 to router 106. As part of this connection, the connecting client system 102 requests and receives a dynamically allocated IP address from DHCP server 110. This allocation requires that a number of messages pass between DHCP server 110 and the client system 102 requesting a new IP address. The last of these messages is a DHCPACK message sent by the DHCP server 110 to the client system 102. **<u>To monitor the allocation of IP addresses, SMS 114 monitors DHCP messages within network 100.</u>** Step 706 corresponds, in a general sense, to the methods and procedures that are executed by SMS 114 to wait for and detect DHCPACK messages within network 100." [7:21-34, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		With reference to FIG. 9, it is inherent that the SMS 114 also receives the IP address of the client system 102 from the dial-up network server because Radia et al. disclose "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**." [9:62-64, emphasis added] Radia et al. further disclose that the IP address of the client system (one of PCs 102) is temporarily assigned: "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." [7:51-55, emphasis added] However, Radia et al. do not explicitly disclose that *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. In the admitted prior art (APA) system of FIG. 1, the dial-up network server 102 communicates a first user ID for one of the users' computers 100 and a temporarily assigned network address for the first user ID to the authentication accounting server 104.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		For instance, the APA systems are described as follows: "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, Col. 1, lines 15-37, emphasis added] It would have been obvious to not remove these useful features of the APA systems when substituting the APA dial-up networking server 102 for the DHCP server 110 and login applet in FIG. 1 of Radia et al. This would have been obvious because simple substitution of the known dial-up networking server 102 for the DHCP server 110 and login applet obtains predictable results that the dial-up networking server 102 notifies the authentication accounting server of user details. It would further have been obvious that the dial-up network server should continue to behave in this way because, rather than the SMS 114 receiving the user ID and IP address respectively from the login applet and DHCP server 110, the SMS 114 would receive this information from the dial-up networking server, as suggested by the APA.
	wherein the authentication accounting server accesses the	Radia et al. disclose the ANCS 112 and SMS 114 access the database 316 and communicate the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	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	individualized rule set (sequence of filtering profiles 400) that correlates with the first user ID (identity of the user) and the temporarily assigned network address (dynamic IP address) to the router 106. For instance, Radia et al. disclose: FIG. 9: step 906 "wait for user login", step 908 "retrieve user filter profile from database", step 910 "download user profile to ancs", and step 920 "reconfigure network components" "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". [9:46-48, emphasis added] "For the present invention, these filtering profiles 400 are preferably maintained in filtering profile database 316 and **<u>retrieved using the identity of the particular user</u>**." [9:53 -56, emphasis added] "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." [9:60-64, emphasis added] "In the following step, the ANCS 112 uses each of

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		the filtering rules 404 included in the sequence of user filtering profiles 400 **<u>to establish a packet filter for IP packets originating from the client system 102 acting as a host for the user</u>**." [9:64-10:1, emphasis added] "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 102 acting as a host for the user. For example, in some cases, the packet filter may be established by reconfiguring the modem 104 connected to the client system 102. Alternatively, the packet filter may be established by reconfiguring router 106." [10:1-7, emphasis added] It is inherent that the "packet filter for IP packets originating from the client system 102" communicated to the router 106 includes the temporarily assigned (i.e., dynamic) IP address of the client system 102 in order to identify the IP packets originating from the client system 102. However, Radia et al. do not explicitly disclose the ANCS 112 and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address *to the redirection server*. It would have been obvious to have the ANCS 112

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the firewall 211 of Coss et al. A first reason is Radia et al. teach reconfiguring one or more network components that forward packets originating at the client system 102, and the firewall 211 of Coss et al. is a network component that forwards packets originating at a client system. As such, Radia et al. suggest reconfiguring the firewall 211. It would have further been obvious to use a known technique (i.e., communicating an individualized rule set to thereby reconfiguring a router 106) to improve a similar device (firewall 211) in the same way. Additionally, Coss et al. disclose dynamic rules can be loaded into the firewall 211 at any time by trusted applications to thereby authorize specific network sessions. For instance, Coss et al. teach: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31,

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		emphasis added] It therefore would have further been obvious to have the ANCS 112 communicate the individualized rule set to the firewall 211 of Coss et al. because the ANCS 112 is a trusted application that authorizes specific network sessions, as suggested by Coss et al.
	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.	Radia et al. disclose that data directed toward the public network from the one of the users' computers (one of PCs 102) are processed by the router 106 according to the individualized rule set. For instance, Radia et al. disclose: "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." [10:11-14, emphasis added] However, Radia et al. do not explicitly disclose that data directed toward the public network from the one of the user's computers is processed *by the redirection server* according to the individualized rule set. Coss et al. disclose data directed toward the public network from the one of the users' computers are

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		processed by firewall 211 according to the individualized rule set. For instance, Coss et al. disclose: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets." [2:29-32, emphasis added] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-34, emphasis added] "The particular rule set that is applied for any packet can be determined based on information such as the **incoming and outgoing network interfaces** as well as the **network source and destination addresses**." [1:67-2:4, emphasis added] It would have been obvious that when substituting router 106 in the network of Radia et al. with the firewall 211 of Coss et al., subsequent to the firewall 211 of Coss et al. being reconfigured by the ANCS 112, data directed toward the public network from the one of the user's computers would be processed by the firewall 211 according to the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		individualized rule set. A first reason is the ANCS 112 is disclosed to reconfigure the router 106 to process data in this way, and the firewall 211 is simply another type of networking component. In other words, simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 is reconfigured to process data directed toward the public network in the same way. Another reason is it would have been obvious to use a known technique (reconfiguring a router 106 to process outgoing data according to the individualized rule set) to improve a similar device (firewall 211) in the same way.
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.	Radia et al disclose that router 106 in FIG. 1 further provides control over a plurality of data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *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. However, Coss et al. disclose that firewall 211 further provides control over a plurality of data to

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "The latter embodiment can allow the firewall techniques of the invention to provide, for example, parental control of Internet and video access in the home." [2:57-60] See FIG. 3, rule No. 10 controlling FTP data **<u>to host B</u>**, and rule No. 30 controlling Telnet data **<u>from host B</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" [4:39-43] allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
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.	Radia et al disclose that router 106 in FIG. 1 blocks the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *the redirection server* further blocks the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 3, rule No. 20 blocking data **<u>from host A</u>**; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data **<u>to host A</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', **<u>'drop'</u>**, or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 allows the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose *the redirection server* further allows the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 4, first session key rule (A, B, TELNET) allowing data **<u>to host B</u>**, and second session key rule (B, A, TELNET) allowing data **<u>from host B</u>**. Coss et al. also disclose rule set categories such as

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., '**pass**', 'drop', or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose *the redirection server further redirects the data to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "For some users and proxy applications, the connection should appear at the destination to be coming from the original source rather than the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		remote system. This applies, e.g., to services which check the source IP address to ensure that it matches the user who signed up for the requested service. **<u>This capability is provided by "dual reflection" (or "two-way reflection"), with the source address of the outgoing connection changed back from the remote proxy to the original user's source address. This change is effected at the firewall, as each packet is received from the proxy and sent to the destination.</u>**" [9:6-16, emphasis added] Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**<u>proxy</u>**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
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.	Radia et al. do not explicitly disclose *the redirection server* further redirects the data from the users' computers *to multiple destinations* as a function of the individualized rule set. However, Coss et al. disclose that firewall 211 further redirects the data from the users' computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" [9:39-42] "Proxy processes have also been developed for other special-purpose applications, e.g., to perform services such as **<u>authentication, mail handling, and virus scanning</u>**." [1:45-49, emphasis added] Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data **<u>to a Telnet proxy server</u>**. Coss et al. further state, "For example, an **<u>FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request." It is inherent that data was also redirected to the FTP proxy application as a function of the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		individualized rule set. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**<u>proxy</u>**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data from the users' computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the database entries for a plurality of the plurality of the users' IDs are correlated with a common individualized rule set. For instance, "In the above description, we have set a default profile called the default login profile. The default login profile is a static profile that **<u>applies to ALL newly connected client systems</u>**. This way the SMS does not need to be aware as new client

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		systems are connected. "**One may also consider setting the default profile to a null profile and for each client system as the client system connects**; for example, since a client system that connects may do a DHCP operation, this event can trigger the SMS to **set the login profile for the newly connected computer**." [3:23-33, emphasis added]
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.	Radia et al. disclose that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) packet. For instance, Radia et al. disclose: "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" [6:30-36, emphasis added] Radia et al. also disclose that at least one rule forwards packets associated with a DNS (domain name service): "The second of the login filtering profiles 400

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		forwards packets **<u>associated with DNS (domain name service)</u>** address resolution." [8:6-8, emphasis added] However, Radia et al. do not explicitly disclose at least one rule as a function of a type of IP *service*. Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. For instance, Coss et al. disclose: "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL". "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, **<u>a designation of a special service which can be called for in a packet</u>**, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" **<u>and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet</u>**." [4:2-11, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. For example: "The SMS maintains a series of filtering profiles, each of which includes one or more of filtering rules. **<u>The SMS sets a default filter sequence for the newly connected client system</u>** by downloading the sequence by the SMS to the ANCS. … Subsequently, the packet filter uses the rules of the login filtering profile sequence to selectively forward or discard IP packets originating from the client system. **<u>This filtering sequence will allow newly connected client systems to perform login, but nothing else</u>**." [3:5-22, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"A preferred embodiment of the present invention also generates or selects filtering profiles for users. With the login filtering profile sequence in place, a user can use the newly connected client system to login to the network. The user login is monitored by the SMS. **If the user login is successful, the SMS selects or generates a user filtering profile sequence.** The user filtering profile sequence is then downloaded by the SMS to the ANCS…. **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.**" [3:34-50, emphasis added] However, Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. For instance, Coss et al. disclose:

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"Exemplary dynamic rules include a 'one-time' rule which is only used for a single session, **a time-limited rule which is used only for a specified time period**, and a threshold rule which is used only when certain conditions are satisfied." [8:37-40, emphasis added] Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address. For instance, Radia et al. disclose: "In FIG. 5, it may be seen that each filtering rule 404 includes an action 500. Action 500 specifies the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		disposition of IP packets that match by a particular filtering rule 404. In particular, **action 500 may indicate that a matched IP packet will be forwarded**, or that a matched IP packet will be discarded." [6:14-18] "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" [6:30-36, emphasis added] "Filtering rule 404 also includes a destination IP address 502 and a destination IP mask 504. Destination IP address 502 corresponds to the destination address included in the header of an IP packet. Destination IP mask 504 is similar to destination IP address 502 but corresponds to a range of destination addresses. To match a particular filtering rule 404, an IP packet must either have a destination address that matches the destination address 502 included in the filtering rule 404 or have a destination address that is covered by the destination address mask 504 of the filtering rule 404." [6:18-29, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		However, Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on *a request type* and a destination address. Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose: Rule No. 40 in Figure 3 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
54.	The system of claim 44, wherein the individualized rule	Radia et al. do not explicitly disclose that the individualized rule set includes at least one rule

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	redirecting the data to a new destination address based on a request type and an attempted destination address. However, Coss et al. disclose that 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. For instance, Coss et al. disclose: Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
55.	The system of claim 44,	Radia et al. do not disclose that the redirection

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	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.	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. However, Coss et al. disclose that firewall 211 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. For instance, Coss et al. disclose: "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, **<u>and a specification of an action to be taken on a packet</u>**." [4:1-6, emphasis added] "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values;" [9:39-44, emphasis added] It would have been obvious to not remove these

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
56.	In a system comprising	Radia et al. Figure 1: computer network 100 is a system
	a database with entries correlating each of a plurality of user IDs with an individualized rule set;	Radia et al. Figure 3: filtering profiles 316 are a database with entries correlating each of a plurality of user IDs with an individualized rule set. For instance, Radia et al. disclose: "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**. In general, it may be appreciated that various users of network 100 will have varying types of allowed access. As a result, **different network users will require different filtering profiles 400. Generally, these filtering profiles 400 are defined separately for each user** using either automatic or manual generation techniques. For the present invention, **these filtering profiles 400 are preferably maintained in filtering profile database 316 and retrieved using the identity of the particular user**." [9:46-56, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	a dial-up network server that receives user IDs from users' computers;	Radia et al. disclose in Figure 1 that modems 104 (which may be telephone - i.e., dial-up) and DHCP server 110 establish a communications link with the user's PC. A login applet on the user's computer (one of PCs 102) allows users to login to the network 100. For instance, Radia et al. disclose: "A **<u>cable modem 104</u>** is connected to each client system 102." [1:11-12, emphasis added] "For example, an internet service provider (ISP) may have users who connect, login, logoff and disconnect to its network over time **<u>using telephone or able modems</u>**." [2:45-48, emphasis added] "The client systems, which are typically personal computers using cable modems, connect to the router. **<u>As part of the connection process, each client system receives a dynamically allocated IP address from the DHCP server.</u>**" [2:67-3:4, emphasis added] "For a preferred embodiment of network 100, user logins are handled by downloading small, specifically tailored applications, known as "login applets," to client systems 102. The login applets are downloaded from a server system, such as server system 108, or in some cases, from SMS

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		114." [8:30-34, emphasis added] "More specifically, as discussed with regard to method 700, for a preferred embodiment of network 100, **<u>users login to network 100 using a login applet that communicates with a login server, such as SMS 114</u>**." [9:39-42, emphasis added] However, Radia et al. do not explicitly disclose *a dial-up network server* that receives user IDs from users' computers. Admitted prior art (APA) systems in Figure 1 of the `118 patent include a dial-up networking server 102 that receives user IDs from users' computers 100. The APA systems are described as follows: "In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), **<u>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.</u>** 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

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		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." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] It would have been obvious to substitute the DHCP server 110 and login applet disclosed by Radia et al. with the dial-up networking server 102 included in the APA systems to thereby obtain the predictable results of: 1) allowing dial-up users to login through the dial-up networking server rather than through an applet running on the user's computer, and 2) assigning a temporary IP address to the user's computer by the dial-up networking server 102 rather than by the DHCP server 110.
	a redirection server connected between the dial-up network server and a public network, and	Radia et al. Figure 1: router 106 is connected to the dial-up network server (substituted for DHCP server 110 and login applet) and server systems 108 of the network 100. Router 106 is similar to a redirection server because router 106 is connected between the user's computer (PC 102) and the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		network's server systems 108, and controls the user's access to the network's server systems 108. Radia et al. further disclose that the network is a public network such as the Internet: "For example, assume that a company uses a router to link its internal intranet with an external network, **such as the Internet**." [2:5-7, emphasis added] However, Radia et al. do not explicitly disclose that the router 106 controls the user's access to the public network *by utilizing redirection functionality*. Coss et al. disclose a firewall that is connected between a user's computer and a public network that controls the user's access to the network by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis] "Dynamic rules are rules which are included with

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] It would be obvious to replace the router 106 of Radia et al. with the firewall 211 of Coss et al. to

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		not only allow discarding and forwarding traffic as taught by Radia et al., but to also allow controlling the user's access to the network by redirecting traffic at the firewall 211 to thereby prevent the router 106 from having to utilize application proxies, as suggested by Coss et al. Radia et al. further disclose that other networking technologies may be used instead of router 106, stating: "The use of cable router 106 and cable modems 104 is also intended to be exemplary and it should be appreciated **<u>that other networking technologies and topologies are equally practical.</u>**" [1:13-16, emphasis added] Therefore, it would have been further obvious to a person of ordinary skill in the art that the firewall 211 of Coss et al. could substitute the router 106 because the firewall 211 disclosed by Coss et al. is another type of networking technology and Radia et al. suggest other types of network technology is equally practical. It would have been further obvious that simple substitution of the known firewall 211 for the router 106 obtains predictable results that the network 100 of Radia et al. may now benefit from the redirection functionality included in firewall 211.

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	an authentication accounting server connected to the database, the dial-up network server and the redirection server,	Radia et al. Figure 1 disclose access network control server ANCS 112 and services management system SMS 114 together are an authentication accounting server because ANCS 112 and SMS 114 are connected to the database (filtering profiles 316 within SMS 114 – see Figure 3), the dial-up network server (substituted for DHCP server 110 and login applet), and the redirection server (Coss's firewall 211 in the position of router 106 in Radia's FIG. 1). Radia et al. further disclose that the ANCS 112 and SMS 114 determine whether a user ID is authorized to access the network. For instance, Radia et al. disclose: "FIG. 9 is a flowchart showing the steps associated with a preferred embodiment of a method for **allocation of privileges to a user in a computer network**." [4:59-61, emphasis added] "Method 900 includes step **performed by SMS 114 and ANCS 112**." [9:35-36, emphasis added] "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. In general, it may be appreciated that **various users of network 100 will have varying types of allowed**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		<u>access</u>." [9:46-50, emphasis added] "In FIG. 1, ANCS 112 and SMS 114 are shown as separate entities. It should be appreciated, however, that the present invention specifically anticipates that **<u>ANCS 112 and SMS 114 may be implemented using a single computer system</u>** that includes ANCS process 214, SMS process 314 and filtering profile database 316." [5:65-6:4, emphasis added]
	a method comprising the steps of:	Method disclosed by Radia et al. in Figure 9
	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;	Radia et al. disclose a login applet on a PC 102 and the DHCP server 110 respectively communicate a first user ID (entered using the login applet) for one of the users' computers (one of PCs 102) and a temporarily assigned network address (dynamically assigned IP address) for the first user ID to the authentication accounting server (SMS 114). For instance, Radia et al. disclose the login applet communicates from PC 102 to SMS 114: "Method 900 begins with step 906 where SMS 114 **<u>waits for a user login</u>**. More specifically, as discussed with regard to method 700, for a preferred embodiment of network 100, **<u>users login to network 100 using a login applet that communicates with a login server, such as SMS</u>**

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		114." [9:37-42, emphasis added] Radia et al. also disclose the DHCP server 110 passes the temporarily assigned network address for the first user ID to the SMS 114: "Method 700 begins with step 706 where **SMS 114 waits for the allocation of an IP address to a client system 102.** More specifically, for a preferred embodiment of network 100, power-on or reset of a client system 102 is followed by connection of the client system 102 to router 106. As part of this connection, the connecting client system 102 requests and receives a dynamically allocated IP address from DHCP server 110. This allocation requires that a number of messages pass between DHCP server 110 and the client system 102 requesting a new IP address. The last of these messages is a DHCPACK message sent by the DHCP server 110 to the client system 102. **To monitor the allocation of IP addresses, SMS 114 monitors DHCP messages within network 100.** Step 706 corresponds, in a general sense, to the methods and procedures that are executed by SMS 114 to wait for and detect DHCPACK messages within network 100." [7:21-34, emphasis added] With reference to FIG. 9, it is inherent that the SMS 114 also receives the IP address of the client system 102 from the dial-up network server because Radia

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		et al. disclose "At the same time, **<u>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</u>**." [9:62-64, emphasis added] Radia et al. further disclose that the IP address of the client system (one of PCs 102) is temporarily assigned: "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." [7:51-55, emphasis added] However, Radia et al. do not explicitly disclose 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. In the admitted prior art (APA) system of FIG. 1, the dial-up network server 102 communicates a first user ID for one of the users' computers 100 and a temporarily assigned network address for the first user ID to the authentication accounting server 104. For instance, the APA systems are described as

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		follows: "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, 1st paragraph of Background of the Invention section, emphasis added] It would have been obvious to not remove these useful features of the APA systems when substituting the APA dial-up networking server 102 for the DHCP server 110 and login applet in FIG. 1 of Radia et al. This would have been obvious because simple substitution of the known dial-up networking server 102 for the DHCP server 110 and login applet obtains predictable results that the dial-up networking server 102 continues to include the above disclosed features. It would further have been obvious that the dial-up network server should continue to behave in this way because, rather than the SMS 114 receiving the user ID and IP address respectively from the login applet and DHCP server 110, the SMS 114 would receive this information from the dial-up networking server, as suggested by the APA.
	communicating the individualized rule set that	Radia et al. disclose the ANCS 112 and SMS 114 access the database 316 and communicate the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	correlates with the first user ID and the temporarily assigned network address to the redirection server from the authentication accounting server;	individualized rule set (sequence of filtering profiles 400) that correlates with the first user ID (identity of the user) and the temporarily assigned network address (dynamic IP address) to the router 106. For instance, Radia et al. disclose: FIG. 9: step 906 "wait for user login", step 908 "retrieve user filter profile from database", step 910 "download user profile to ancs", and step 920 "reconfigure network components" "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". [9:46-48, emphasis added] "For the present invention, these filtering profiles 400 are preferably maintained in filtering profile database 316 and **<u>retrieved using the identity of the particular user</u>**." [9:53 -56, emphasis added] "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." [9:60-64, emphasis added] "In the following step, the ANCS 112 uses each of

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		the filtering rules 404 included in the sequence of user filtering profiles 400 **<u>to establish a packet filter for IP packets originating from the client system 102 acting as a host for the user</u>**." [9:64-10:1, emphasis added] "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 102 acting as a host for the user. For example, in some cases, the packet filter may be established by reconfiguring the modem 104 connected to the client system 102. Alternatively, the packet filter may be established by reconfiguring router 106." [10:1-7, emphasis added] It is inherent that the "packet filter for IP packets originating from the client system 102" communicated to the router 106 includes the temporarily assigned (i.e., dynamic) IP address of the client system 102 in order to identify the IP packets originating from the client system 102. However, Radia et al. do not explicitly disclose communicating the individualized rule set that correlates with the first user ID and the temporarily assigned network address *to the redirection server* from the ANCS 112 and SMS 114. It would have been obvious to have the ANCS 112

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		and SMS 114 access the database 316 and communicate the individualized rule set that correlates with the first user ID and the temporarily assigned network address to the firewall 211 of Coss et al. A first reason is Radia et al. teach reconfiguring one or more network components that forward packets originating at the client system 102, and the firewall 211 of Coss et al. is a network component that forwards packets originating at a client system. As such, Radia et al. suggest reconfiguring the firewall 211. It would have further been obvious to use a known technique (i.e., communicating an individualized rule set to thereby reconfiguring a router 106) to improve a similar device (firewall 211) in the same way. Additionally, Coss et al. disclose dynamic rules can be loaded into the firewall 211 at any time by trusted applications to thereby authorize specific network sessions. For instance, Coss et al. teach: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31,

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		emphasis added] It therefore would have further been obvious to have the ANCS 112 communicate the individualized rule set to the firewall 211 of Coss et al. because the ANCS 112 is a trusted application that authorizes specific network sessions, as suggested by Coss et al.
	and processing data directed toward the public network from the one of the users' computers according to the individualized rule set.	Radia et al. disclose processing data directed toward the public network from the one of the users' computers (one of PCs 102) according to the individualized rule set. For instance, Radia et al. disclose: "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." [10:11-14, emphasis added]
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.	Radia et al disclose that router 106 in FIG. 1 further provides control over a plurality of data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose the step of

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		controlling a plurality of data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further provides control over a plurality of data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "The latter embodiment can allow the firewall techniques of the invention to provide, for example, parental control of Internet and video access in the home." [2:57-60] See FIG. 3, rule No. 10 controlling FTP data <u>**to host B**</u>, and rule No. 30 controlling Telnet data <u>**from host B**</u>. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or 'proxy'" [4:39-43] allowing the firewall 211 to control data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 further blocks the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose blocking the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further blocks the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 3, rule No. 20 blocking data **<u>from host A</u>**; and FIG. 4, fifth session key rule (A, C, MAIL) blocking data **<u>to host A</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', '**<u>drop'</u>**, or 'proxy'" [4:39-43, emphasis added] allowing the firewall

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		211 to block (i.e., drop) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al disclose that router 106 in FIG. 1 further allows the data from the users' computers as a function of the individualized rule set (FIG. 6, step 606, "filter IP packets in accordance with filtering profile" and col. 10, lines 6-14). Radia et al. do not explicitly disclose allowing the data *to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further allows the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: FIG. 4, first session key rule (A, B, TELNET) allowing data **to host B**, and second session key

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		rule (B, A, TELNET) allowing data **<u>from host B</u>**. Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., '**<u>pass</u>**', 'drop', or 'proxy'" [4:39-43, emphasis added] allowing the firewall 211 to allow (i.e., pass) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. do not explicitly disclose *redirecting the data to and from* the users' computers as a function of the individualized rule set. However, Coss et al. disclose firewall 211 further redirects the data to and from the users' computers as a function of the individualized rule set. For instance, Coss et al. disclose: "For some users and proxy applications, the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		connection should appear at the destination to be coming from the original source rather than the remote system. This applies, e.g., to services which check the source IP address to ensure that it matches the user who signed up for the requested service. **<u>This capability is provided by "dual reflection" (or "two-way reflection"), with the source address of the outgoing connection changed back from the remote proxy to the original user's source address. This change is effected at the firewall, as each packet is received from the proxy and sent to the destination.</u>**" [9:6-16, emphasis added] Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**<u>proxy</u>**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data to and from the users' computers as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		disclosed features.
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.	Radia et al. do not explicitly disclose *redirecting the data from the users' computers to multiple destinations* a function of the individualized rule set. However, Coss et al. disclose firewall 211 redirects the data from the user's computers to multiple destinations as a function of the individualized rule set. For instance, Coss et al. disclose: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy" [9:39-42] "Proxy processes have also been developed for other special-purpose applications, e.g., to perform services such as **<u>authentication, mail handling, and virus scanning</u>**." [1:45-49, emphasis added] Coss et al. also gives examples of redirecting data to both a Telnet proxy and an FTP proxy. For example, Figure 3, rule No. 30 redirects TELNET data to a **<u>Telnet proxy server</u>**. Coss et al. further state, "For example, an **<u>FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request."

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		Coss et al. also disclose rule set categories such as "Source host group identifier or IP address", "Destination host group identifier or IP address", and "Rule action, e.g., 'pass', 'drop', or '**proxy**'" [4:39-43, emphasis added] allowing the firewall 211 to redirect (i.e., proxy) data from the users' computers to multiple destinations as a function of the individualized rule set. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. The reason is simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose 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. For instance, "In the above description, we have set a default profile called the default login profile. The default login profile is a static profile that **applies to ALL newly connected client systems**. This way the SMS does not need to be aware as new client

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		systems are connected. "**<u>One may also consider setting the default profile to a null profile and for each client system as the client system connects</u>**; for example, since a client system that connects may do a DHCP operation, this event can trigger the SMS to **<u>set the login profile for the newly connected computer</u>**." [3:23-33, emphasis added]
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.	Radia et al. disclose that the individualized rule set includes at least one rule as a function of a type of IP (Internet Protocol) packet. For instance, Radia et al. disclose: "Filtering rule 404 also includes **<u>a protocol type 506</u>**. **<u>Protocol type 506 corresponds to the protocol type of an IP packet</u>**. 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" [6:30-36, emphasis added] Radia et al. also disclose that at least one rule forwards packets associated with a DNS (domain name service): "The second of the login filtering profiles 400

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		forwards packets **associated with DNS (domain name service)** address resolution." [8:6-8, emphasis added] However, Radia et al. do not explicitly disclose at least one rule as a function of *a type of IP service*. Coss et al. disclose that the individual rule set includes at least one rule as a function of a type of IP service. For instance, Coss et al. disclose: "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL". "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, **a designation of a special service which can be called for in a packet**, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" **and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet**." [4:2-11, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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 initial period of time and to thereafter utilize the standard rule set.	Radia et al. disclose the individualized rule set includes a default filter sequence for a newly connected client system that allows the newly connected client system to perform login. Radia et al. also disclose that after a user of the newly connected client logs in, the filter sequence associated with the client device is changed to another sequence. For example: "The SMS maintains a series of filtering profiles, each of which includes one or more of filtering rules. **<u>The SMS sets a default filter sequence for the newly connected client system</u>** by downloading the sequence by the SMS to the ANCS. … Subsequently, the packet filter uses the rules of the login filtering profile sequence to selectively forward or discard IP packets originating from the client system. **<u>This filtering sequence will allow newly connected client systems to perform login, but nothing else</u>**." [3:5-22, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"A preferred embodiment of the present invention also generates or selects filtering profiles for users. With the login filtering profile sequence in place, a user can use the newly connected client system to login to the network. The user login is monitored by the SMS. **If the user login is successful, the SMS selects or generates a user filtering profile sequence.** The user filtering profile sequence is then downloaded by the SMS to the ANCS…. **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.**" [3:34-50, emphasis added] However, Radia et al. do not explicitly disclose utilizing the login filtering sequence *for an initial period of time*. (Instead Radia et al. only disclose utilizing the login filtering sequence until the user logs in.) Coss et al. disclose that the individualized rule set includes an initial temporary rule set and a standard rule set, and wherein the firewall 211 is configured to utilize the temporary rule set for an initial period of time and to thereafter utilize the standard rule set. For instance, Coss et al. disclose:

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		"Exemplary dynamic rules include a 'one-time' rule which is only used for a single session, **a time-limited rule which is used only for a specified time period**, and a threshold rule which is used only when certain conditions are satisfied." [8:37-40, emphasis added] Accordingly, Coss et al. disclose utilizing an initial rule set being a set of rules including the time-limited rule before the specified time period has expired, and utilizing a standard rule set being the set of rules not including the time-limited rule after the specified time period has expired. It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
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.	Radia et al. disclose that the individualized rule set includes at least one rule allowing access based on a type of IP (Internet Protocol) packet and destination address. For instance, Radia et al. disclose: "In FIG. 5, it may be seen that each filtering rule 404 includes an action 500. Action 500 specifies the

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		disposition of IP packets that match by a particular filtering rule 404. In particular, **<u>action 500 may indicate that a matched IP packet will be forwarded</u>**, or that a matched IP packet will be discarded." [6:14-18, emphasis added] "Filtering rule 404 also includes **<u>a protocol type 506</u>**. **<u>Protocol type 506 corresponds to the protocol type of an IP packet</u>**. 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" [6:30-36, emphasis added] "Filtering rule 404 also includes a destination IP address 502 and a destination IP mask 504. Destination IP address 502 corresponds to the destination address included in the header of an IP packet. Destination IP mask 504 is similar to destination IP address 502 but corresponds to a range of destination addresses. To match a particular filtering rule 404, an IP packet must either have a destination address that matches the destination address 502 included in the filtering rule 404 or have a destination address that is covered by the destination address mask 504 of the filtering rule 404." [6:18-29, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		However, Radia et al. do not explicitly disclose the individualized rule set includes at least one rule allowing access based on *a request type* and a destination address. Coss et al. disclose that the individualized rule set includes at least one rule allowing access based on a request type and a destination address. For instance, Coss et al. disclose: Rule No. 40 in Figure 3 allowing access (i.e., action = "PASS") based on a request type of "MAIL" and a destination host of "D". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
66.	The method of claim 56, wherein the individualized rule	Radia et al. do not explicitly disclose that the individualized rule set includes at least one rule

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	set includes at least one rule redirecting the data to a new destination address based on a request type and an attempted destination address.	redirecting the data to a new destination address based on a request type and an attempted destination address. However, Coss et al. disclose that 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. For instance, Coss et al. disclose: Rule No. 30 in Figure 3 redirecting data (i.e., action = "PROXY") based on a request type of "TELNET" and attempted destination host of "C". "In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet." [4:2-11, emphasis added] It would have been obvious to not remove these useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.
67.	The method of claim 56,	Radia et al. do not disclose that the redirection

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
	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.	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. However, Coss et al. disclose that the firewall 211 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. For instance, Coss et al. disclose: "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, **<u>and a specification of an action to be taken on a packet</u>**." [4:1-6, emphasis added] "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values;" [9:39-44, emphasis added] It would have been obvious to not remove these

Claim No.	Claim language	Corresponding features disclosed by Radia et al. in view of the APA, and further in view of Coss et al.
		useful features of the firewall 211 disclosed by Coss et al. when substituting the firewall 211 for the router 106 in FIG. 1 of Radia et al. Simple substitution of the known firewall 211 for the router 106 obtains predictable results that the firewall 211 continues to include the above disclosed features.

3 Claim chart showing how each of claims 16-24, 26-27, 36-43 and 68-90 of the `118 patent are unpatentable under 35 U.S.C. § 103(a) as being obvious over Coss et al. in view of the APA

As show in the attached reexamination certificate of the `118 patent, independent claim 25 is cancelled but dependent claims 26-27 remain enforceable. As dependent claims 26-27 include all limitations of original base claim 25, the limitations of original claim 25 are also addressed in the below table.

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
16.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing."

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		[Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		ID and password. The dial-up networking server then passes the user ID and password, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **dynamic rules allow a given rule set to be modified** based on events happening in the network

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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:

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	of time, data transmitted to or from the user, or location the user accesses; and	"In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a specified time period,** and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **an FTP proxy application** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>control session</u>, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
	wherein the redirection server is configured to allow modification of at least a portion of the rule set as a function of time.	Coss et al. disclose the firewall 211 is configured to allow modification of at least a portion of the rule set as a function of time: "a time-limited rule which is **<u>used only for a specified time period</u>**" [2:35-36] "The dynamic rule in this example would typically not be loaded until a data request is made over the FTP control session, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
17.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>” [8:24-31, emphasis added] “To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing.” [Abstract, emphasis added] “Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**.” [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		described in the `118 patent as follows: "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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host=”A”) and a public network (destination host=“*” which includes all hosts on the Internet 105).
	wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated to the temporarily assigned	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address:

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	network address;	"Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</u>** Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host group can be modified to add or drop different hosts</u>** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **<u>until a data request is made over the FTP control session</u>**, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
	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.	Coss et al. disclose the firewall 211 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: "The dynamic rule in this example would typically **<u>not be loaded until a data request is made over the FTP control session</u>**, and could be limited to one use and made active for only a limited time period." [8:48-52]
18.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port**." [Coss et al., col. 8, lines 56-65, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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, <u>**along with a temporary Internet Protocol (IP) address for use by the user**</u> 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 <u>**to allow the user to use the temporary IP address assigned to**</u>

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>that user by the dial-up networking server</u> 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **dynamic rules allow a given rule set to be modified** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</u>** Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>group can be modified to add or drop different hosts</u> without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **<u>until a data request is made over the FTP control session</u>**, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
	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.	Coss et al. disclose the firewall 211 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: "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] "Other types of dynamic rules include rules which define a host group, such that **<u>the host group can be modified to add or drop different hosts</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		without altering other aspects of the access rule set." [8:37-52, emphasis added]
19.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		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**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	wherein the rule set contains at	Coss et al. disclose the rule set contains at least one

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	least one of a plurality of functions used to control data passing between the user and a public network;	of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>on events happening in the network without requiring that the entire rule set be reloaded.</u> Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host group can be modified to add or drop different hosts</u>** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **<u>until a data request is made over the FTP control session</u>**, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
	wherein the redirection server is configured to allow the removal	Coss et al. disclose the firewall 211 is configured to allow the removal or reinstatement of at least a

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	or reinstatement of at least a portion of the rule set as a function of time.	portion of the rule set as a function of time: Dynamic rule may specify: "Rule Timeout – Number of seconds of inactivity before rule is removed from rule list" [4:48-49, emphasis added] "a time-limited rule which is **<u>used only for a specified time period</u>**" [2:35-36] "The dynamic rule in this example would typically not be loaded until a data request is made over the FTP control session, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added] "Once a dynamic rule has served its function, it can be removed from the rule set." [8:32-34, emphasis added]
20.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet 105).
	wherein the redirection server is configured to allow automated modification of at least a portion of the rule set correlated	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	to the temporarily assigned network address;	address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **dynamic rules allow a given rule set to be modified** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a specified time period,** and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **an FTP proxy application** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added]
	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.	Coss et al. disclose the firewall 211 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 dynamic rule in this example would typically **not be loaded until a data request is made over the FTP control session**, and could be limited to one use and made active for only a limited time period." [8:48-52] "Once a dynamic rule has served its function, it can be removed from the rule set." [8:32-34, emphasis added]
21.	A system comprising:	Coss et al. illustrate a system in Figure 2

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		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**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host=”A”) and a public network (destination host=“*” which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: “Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.” [8:26-31] “The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded.” [8:34-36, emphasis added] “Source host group identifier or **<u>IP address</u>**” [4:39, emphasis added] “Destination host group identifier or **<u>IP address</u>**” [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		specified time period, and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **an FTP proxy application** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added]
	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.	Coss et al. disclose the firewall 211 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: "Destination host group identifier or **IP address**"

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		[4:40, emphasis added] Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [8:37-52, emphasis added] "Once a dynamic rule has served its function, it can be removed from the rule set." [8:32-34, emphasis added]
22.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		The security policies can be represented by **<u>sets of access rules which are represented in tabular form and which are loaded into the firewall</u>** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **<u>designations of source and destination hosts</u>**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] "This invention relates to the **<u>prevention of unauthorized access in computer networks</u>** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator,

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		to authorize specific network sessions." [8:26-31] "The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	wherein the redirection server is configured to allow automated	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	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	of the rule set as a function of some combination of time, data transmitted to or from the user, or location the user accesses: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a specified time period,** and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **an FTP proxy application** could use a dynamic rule to authorize establishment of an

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added]
	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.	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a specified time period,** and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added] "Once a dynamic rule has served its function, it can be removed from the rule set." [8:32-34, emphasis added]
23.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>access rules which are represented in tabular form and which are loaded into the firewall</u> by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **<u>designations of source and destination hosts</u>**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] "This invention relates to the **<u>prevention of unauthorized access in computer networks</u>** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.</u>**" [8:24-31, emphasis added] "To unburden the firewall of application proxies,

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to that user by the dial-up networking server</u>** 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host="A") and a public network (destination host="*" which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	wherein the redirection server is configured to allow automated modification of at least a	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set as a function of some combination of

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	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	time, data transmitted to or from the user, or location the user accesses: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</u>** Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host group can be modified to add or drop different hosts</u>** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added]
	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	Coss et al. disclose that firewall 211 has a user side that is connected to a user site 201, and a network side connected to a computer network (Internet 105): "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] However, Coss et al. do not explicitly disclose that the firewall 211 has a user side *that is connected to a computer using the temporarily assigned network address*. It is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to program the firewall 211 with the rule set correlated to the assigned IP address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server.	Coss et al. disclose user site 201 is connected to the computer network through the firewall 211: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] However, Coss et al. do not explicitly disclose *the computer using the temporarily assigned network address* is connected to the computer network through the redirection server. As explained above, it is inherent that user site 201 includes the computer utilizing the assigned IP address and therefore it is also inherent that the computer is connected to the Internet 105 through the firewall 211. As explained above, it would also have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
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.	Coss et al. disclose instructions to the firewall 211 to modify the rule set are received by one or more of the user side of the firewall 211 and the network side of the firewall 211. For instance, Coss et al disclose: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by</u>** **<u>trusted parties</u>**, e.g., a trusted application, remote proxy or **<u>firewall administrator</u>**, to authorize specific network sessions." [8:26-31] Figure 1 illustrates Administrator processor 115 is on the **<u>network side</u>** of the firewalls 111, 113, 114. Figure 2 illustrates Administrator processor (ADM) 215 is on the **<u>user side</u>** of firewall 211.
25.	In a system comprising	Coss et al. illustrate a system in Figure 2
	a redirection server containing a user's rule set correlated to a temporarily assigned network address	Firewall 211 contains a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple users, each with a separate security policy**." [3:31-33, emphasis added] The security policies can be represented by **sets of access rules which are represented in tabular form and which are loaded into the firewall** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **designations of source and destination hosts**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] "This invention relates to the **prevention of unauthorized access in computer networks** and, more particularly, to firewall protection within

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions.**" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port**." [Coss et al., col. 8, lines 56-65, emphasis added]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "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, **<u>along with a temporary Internet Protocol (IP) address for use by the user</u>** 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 **<u>to allow the user to use the temporary IP address assigned to</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>that user by the dial-up networking server</u> 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, **<u>the end user would be identified by the temporarily assigned IP address</u>**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP) data passing between the user (Source host="A") and a public network (destination host="*" which

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		includes all hosts on the Internet 105).
	the method comprising the step of:	Coss et al. illustrates a method (e.g., flowcharts of Figures 5A, 5B, 7, 9, 10A, 10B)
	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	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **<u>dynamic rules allow a given rule set to be modified</u>** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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	Coss et al. disclose that firewall 211 has a user side that is connected to a user site 201, and a network side connected to a computer network (Internet 105): "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] However, Coss et al. do not explicitly disclose that the firewall 211 has a user side *that is connected to a computer using the temporarily assigned network address*. It is inherent that user site 201 includes a computer utilizing the assigned IP address because if there were no such computer at user site 201 there would be no reason for Coss et al. to program the firewall

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		211 with the rule set correlated to the assigned IP address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	wherein the computer using the temporarily assigned network address is connected to the computer network through the redirection server and	Coss et al. disclose user site 201 is connected to the computer network through the firewall 211: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] However, Coss et al. do not explicitly disclose *the computer using the temporarily assigned network address* is connected to the computer network through the redirection server. As explained above, it is inherent that user site 201 includes the computer utilizing the assigned IP address and therefore it is also inherent that the computer is connected to the Internet 105 through the firewall 211.

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		As explained above, it would also have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	the method further includes the step of	The method of Coss et al. 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.	Coss et al. disclose instructions to the firewall 211 to modify the rule set are received by one or more of the user side of the firewall 211 and the network side of the firewall 211. For instance, Coss et al disclose: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by</u>** **<u>trusted parties</u>**, e.g., a trusted application, remote proxy or **<u>firewall administrator</u>**, to authorize specific network sessions." [8:26-31] Figure 1 illustrates Administrator processor 115 is on the **<u>network side</u>** of the firewalls 111, 113, 114. Figure 2 illustrates Administrator processor (ADM)

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		215 is on the **<u>user side</u>** of firewall 211.
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 accesses.	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</u>** Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host group can be modified to add or drop different hosts</u>** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator,

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		to authorize specific network sessions." [8:26-31] "For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **<u>until a data request is made over the FTP control session</u>**, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
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 a location or locations the user accesses.	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **<u>The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</u>** Exemplary dynamic rules include a **<u>"one-time" rule which is only used for a single session</u>**, a **<u>time-limited rule which is used only for a specified time period,</u>** and a **<u>threshold rule which is used only when certain conditions are satisfied</u>**. Other types of dynamic rules include rules which define a host group, such that **<u>the host</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		group can be modified to add or drop different hosts without altering other aspects of the access rule set." [2:29-41, emphasis added] "The dynamic rule in this example would typically not be loaded **until a data request is made over the FTP control session**, and could be limited to one use and **made active for only a limited time period**." [8:48-52, emphasis added] "Once a dynamic rule has served its function, it can be removed from the rule set." [8:32-34, emphasis added]
36.	A system comprising:	Coss et al. illustrate a system in Figure 2
	a redirection server programmed with a user's rule set correlated to a temporarily assigned network address;	Coss et al. disclose firewall 211 is programmed with a user's rule set correlated to an assigned network address. Firewall 211 is also connected between the user's computer (at user site 201) and the Internet 105, and controls the user's access to the Internet 105 by utilizing redirection functionality. For instance, Coss et al. disclose: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211." [3:53-54] "With a capability for supporting multiple security domains, **a single firewall can support multiple**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>users, each with a separate security policy</u>." [3:31-33, emphasis added] The security policies can be represented by **<u>sets of access rules which are represented in tabular form and which are loaded into the firewall</u>** by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, **<u>designations of source and destination hosts</u>**, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. "Source host group identifier or **<u>IP address</u>**" [4:39, emphasis added] "Destination host group identifier or **<u>IP address</u>**" [4:40, emphasis added] "This invention relates to the **<u>prevention of unauthorized access in computer networks</u>** and, more particularly, to firewall protection within computer networks." [1:6-8, emphasis added] "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. **<u>They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall</u>**

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		<u>administrator, to authorize specific network sessions.</u>" [8:24-31, emphasis added] "To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing." [Abstract, emphasis added] "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, **<u>the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port</u>**." [Coss et al., col. 8, lines 56-65, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is programmed with a user's rule set correlated to a *temporarily assigned* network address. It is well known that dial-up users are often provided with a temporarily assigned IP address. For example, admitted prior art (APA) systems are described in the `118 patent as follows: "In prior art systems as shown in FIG. 1 when an

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		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**." [`118 patent, 1st paragraph of Background of the Invention section, emphasis added] Firewall 211 is programmed with a user's rule set correlated to an IP address. It would have been

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.
	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;	Coss et al. disclose the rule set contains at least one of a plurality of functions used to control data passing between the user and a public network. For instance, the rule set (rule table of Figure 3) contains at least one (Rule No. 20) of a plurality of functions (categories listed in column 4, line 35 to column 5, line 35) used to control (action=DROP in this example) data passing between the user (Source host=”A”) and a public network (destination host="*" which includes all hosts on the Internet 105).
	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;	Coss et al. disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the assigned network address: "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31] "The **dynamic rules allow a given rule set to be modified** based on events happening in the network without requiring that the entire rule set be reloaded." [8:34-36, emphasis added] "Source host group identifier or **IP address**" [4:39, emphasis added] "Destination host group identifier or **IP address**" [4:40, emphasis added] However, Coss et al. do not explicitly disclose the firewall 211 is configured to allow automated modification of at least a portion of the rule set correlated to the *temporarily assigned* network address. Firewall 211 is programmed with a user's rule set correlated to an IP address. As explained above, it would have been obvious that this IP address may be temporarily assigned. A first reason is this is simply combining prior art elements (temporary IP addresses) to known methods (assigning a user with an IP address) to yield predictable results. A second reason is this would allow dial-up users to temporarily connect their computers to the user site 201, as suggested by the APA systems.

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
	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	Coss et al. disclose the firewall 211 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: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. **The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.** Exemplary dynamic rules include a **"one-time" rule which is only used for a single session**, a **time-limited rule which is used only for a specified time period,** and a **threshold rule which is used only when certain conditions are satisfied**. Other types of dynamic rules include rules which define a host group, such that **the host group can be modified to add or drop different hosts** without altering other aspects of the access rule set." [2:29-41, emphasis added] "Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions." [8:26-31]

Claim No.	Claim language	Corresponding features disclosed by Coss et al. in view of admitted prior art (APA)
		"For example, **<u>an FTP proxy application</u>** could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded **<u>until a data request is made over the FTP control session</u>**, and could be limited to one use and **<u>made active for only a limited time period</u>**." [8:48-52, emphasis added]
	wherein the modified rule set includes at least one rule as a function of a type of IP (Internet Protocol) service.	Coss et al. disclose that the rule set includes at least one rule as a function of a type of IP service. For instance, Coss et al. disclose: "Service" column in rule table of Figure 3 providing rules as a function of types of IP services such as "FTP", "TELNET", and "MAIL". "As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, **<u>a designation of a special service which can be called for in a packet</u>**, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" **<u>and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet</u>**." [4:2-11, emphasis