| Claim No. | Claim language | Corresponding features disclosed by Coss et al. in view of admitted prior art (APA) |
|---|---|---|
| | | added]<br><br>However, 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.<br><br>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. |
| 37. | 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.<br><br>For instance, Coss et al. disclose:<br><br>"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]<br><br>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.<br><br>"Source host group identifier or **IP address**" [4:39, emphasis added]<br><br>"Destination host group identifier or **IP address**" [4:40, emphasis added]<br><br>"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]<br><br>"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) |
|---|---|---|
| | | **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]<br><br>"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]<br><br>"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]<br><br>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.<br><br>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:<br><br>"In prior art systems as shown in FIG. 1 when an Internet user establishes a connection with an Internet Service Provider (ISP), the user first makes a physical connection between their computer 100 and a dial-up networking server 102, the user provides to the dial-up networking server their user ID and password. The dial-up networking server then passes the user ID and password, **along with a temporary Internet Protocol (IP) address for use by the user** to the ISP's authentication and accounting server 104. A detailed description of the IP communications protocol is discussed in Internetworking with TCP/IP, 3rd ed., Douglas Comer, Prentice Hall, 1995, which is fully incorporated herein by reference. The authentication and accounting server, upon verification of the user ID and password using a database 106 would send an authorization message to the dial-up networking server 102 **to allow the user to use the temporary IP address assigned to that user by the dial-up networking server** and then logs the connection and assigned IP address. For the duration of that session, whenever the user would make a request to the Internet 110 via a gateway 108, **the end user would be identified by the temporarily assigned IP address**." [`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]<br><br>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.<br><br>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: |

DOCKET ALARM

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

**LAW FIRMS**
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

**FINANCIAL INSTITUTIONS**
Litigation and bankruptcy checks for companies and debtors.

**E-DISCOVERY AND LEGAL VENDORS**
Sync your system to PACER to automate legal marketing.