US006182226B1

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

(10) **Patent No.: US 6,182,226 B1**
(45) **Date of Patent: Jan. 30, 2001**

(54) **SYSTEM AND METHOD FOR CONTROLLING INTERACTIONS BETWEEN NETWORKS**

(75) Inventors: **Irving Reid**, Toronto (CA); **Spencer Minear**, Fridley, MN (US)

(73) Assignee: **Secure Computing Corporation**, Roseville, MN (US)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) Appl. No.: **09/040,832**

(22) Filed: **Mar. 18, 1998**

(51) **Int. Cl.**[7] **H04L 9/00**
(52) **U.S. Cl.** **713/201**; 709/225; 709/229
(58) **Field of Search** 713/200, 201, 713/202; 707/9; 709/225, 229, 228, 227; 711/163

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,956,615	5/1976	Anderson et al.	235/61.7 B
4,104,721	8/1978	Markstein et al.	364/200
4,177,510	12/1979	Appell et al.	364/200
4,442,484	4/1984	Childs, Jr. et al.	364/200
4,584,639	4/1986	Hardy	364/200
4,621,321	11/1986	Boebert et al.	364/200
4,648,031	3/1987	Jenner	364/200
4,701,840	10/1987	Boebert et al.	364/200
4,713,753	12/1987	Boebert et al.	364/200
4,870,571	9/1989	Frink	364/200
4,885,789	12/1989	Burger et al.	380/25
4,914,568	4/1990	Kodosky et al.	364/200
5,093,914	3/1992	Coplien et al.	395/700
5,124,984	6/1992	Engel	370/94.1
5,153,918	10/1992	Tuai	380/25
5,204,961	4/1993	Barlow	395/725
5,228,083	7/1993	Lozowick et al.	380/9
5,263,147	11/1993	Francisco et al.	395/425
5,272,754	12/1993	Boebert	380/25
5,276,735	1/1994	Boebert et al.	380/21
5,303,303	4/1994	White	380/49
5,305,385	4/1994	Schanning et al.	380/49
5,311,593	5/1994	Carmi	380/23
5,329,623	7/1994	Smith et al.	395/275
5,333,266	7/1994	Boaz et al.	395/200
5,355,474	10/1994	Thuraisngham et al.	395/600
5,414,833	5/1995	Hershey et al.	395/575

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0 554 182 A1	4/1993	(EP)	H04L/29/06
0 743 777 A2	11/1996	(EP)	H04L/29/06
2287619	9/1995	(GB)	H04L/12/22
96/13113	5/1996	(WO)	H04L/29/06
96/35994	11/1996	(WO)	G06F/13/14
97/13340	4/1997	(WO)	H04L/9/00
97/26731	7/1997	(WO)	H04L/9/00
97/26734	7/1997	(WO)	H04L/9/00
97/26735	7/1997	(WO)	H04L/9/00
97/29413	8/1997	(WO) .	

OTHER PUBLICATIONS

Boebert, W.E., et al., "Secure Ada Target: Issues, System Design, and Verification", *Proceedings of the Symposium on Security and Privacy,* Oakland, California, pp. 59–66, (1985).

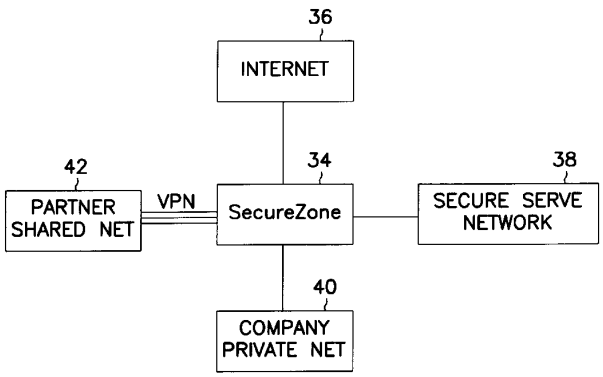
(List continued on next page.)

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Christopher Revak
(74) *Attorney, Agent, or Firm*—Schwegman, Lundberg, Woessner & Kluth, P.A.

(57) **ABSTRACT**

A firewall is used to achieve network separation within a computing system having a plurality of network interfaces. A plurality of regions is defined within the firewall and a set of policies is configured for each of the plurality of regions. The firewall restricts communication to and from each of the plurality of network interfaces in accordance with the set of policies configured for the one of the plurality of regions to which the one of the plurality of network interfaces has been assigned.

32 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

5,416,842		5/1995	Aziz	380/30
5,455,828		10/1995	Zisapel	370/85.3
5,485,460		1/1996	Schrier et al.	370/94.1
5,511,122		4/1996	Atkinson	380/25
5,548,646		8/1996	Aziz et al.	380/23
5,550,984		8/1996	Gelb	395/200.17
5,566,170		10/1996	Bakke et al.	370/60
5,583,940		12/1996	Vidrascu et al.	380/49
5,586,260		12/1996	Hu	395/200.2
5,604,490		2/1997	Blakley, III et al.	340/825.31
5,606,668		2/1997	Shwed	395/200.11
5,615,340		3/1997	Dai et al.	395/200.17
5,619,648		4/1997	Canale et al.	395/200.01
5,623,601	*	4/1997	Vu	713/201
5,636,371		6/1997	Yu	395/500
5,644,571		7/1997	Seaman	370/401
5,671,279		9/1997	Elgamal	380/23
5,673,322		9/1997	Pepe et al.	380/49
5,684,951		11/1997	Goldman et al.	395/188.01
5,689,566		11/1997	Nguyen	380/25
5,699,513		12/1997	Feigen et al.	395/187.01
5,706,507		1/1998	Schloss	395/615
5,708,780		1/1998	Levergood et al.	395/200.12
5,864,683	*	1/1999	Boerbert et al.	713/201
5,918,018	*	6/1999	Gooderum et al.	713/200
5,968,176	*	10/1999	Nessett et al.	713/201
5,983,350		11/1999	Minear et al.	713/201

OTHER PUBLICATIONS

Boebert, W.E., et al., "Secure Computing: The Secure Ada Target Approach", *Sci. Honeyweller,* 6(2), 17 pages, (1985).

International Search Report, PCT Application No. PCT/US 95/12681, 8 p. (mailed Apr. 9, 1996).

News Release: "100% of Hackers Failed to Break Into One Internet Site Protected by Sidewinder™", Secure Computing Corporation (Feb. 16, 1995).

News Release: "Internet Security System Given 'Product of the Year' Award", Secure Computing Corporation (Mar. 28, 1995).

News Release: "SATAN No Threat to Sidewinder™", Secure Computing Corporation (Apr. 26, 1995).

"Answers to Frequently Asked Questions About Network Security", *Secure Computing Corporation,* p. 1–41 & p. 1–16 (Sep. 25, 1994).

"Sidewinder Internals", Product information, Secure Computing Corporation, 16 p. (Oct. 1994).

"Special Report: Secure Computing Corporation and Network Security", *Computer Select,* 13 p. (Dec. 1995).

Adam. J.A., "Meta–Matrices", *IEEE Spectrum,* p. 26 (Oct. 1992).

Adam, J.A., "Playing on the Net", *IEEE Spectrum,* p. 29 (Oct. 1992).

Ancilotti, P., et al., "Language Features for Access Control", *IEEE Transactions on Software Engineering, SE–9,* 16–25 (Jan. 1983).

Badger, L., et al., "Practical Domain and Type Enforcement for UNIX", *Proceedings of the 1995 IEEE Symposium on Security and Privacy,* p. 66–77 (May 1995).

Belkin, N.J., et al., "Information Filtering and Information Retrieval: Two Sides of the Same Coin?", *Communications of the ACM,* 35, 29–38 (Dec. 1992).

Bellovin, S.M., et al., "Network Firewalls", *IEEE Communications Magazine,* 32, 50–57 (Sep. 1994).

Bevier, W.R., et al., "Connection Policies and Controlled Interference", *Proceedings of the Eighth IEEE Computer Security Foundations Workshop,* Kenmare, Ireland, p. 167–176 (Jun. 13–15, 1995).

Bowen, T.F., et al., "The Datacycle Architecture", *Communications of the ACM,* 35, 71–81 (Dec. 1992).

Bryan, J., "Firewalls For Sale", *BYTE,* 99–100, 102, 104–105 (Apr. 1995).

Cobb, S., "Establishing Firewall Policy", *IEEE,* 198–205 (1996).

Damashek, M., "Gauging Similarity with n–Grams: Language–Independent Categorization of Text", *Science,* 267, 843–848 (Feb. 10, 1995).

Dillaway, B.B., et al., "A Practical Design For A Multilevel Secure Database Management System", *American Institute of Aeronautics and Astronautics, Inc.,* p. 44–57 (Dec. 1986).

Fine, T., et al., "Assuring Distributed Trusted Mach", *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy,* p. 206–218 (1993).

Foltz, P.W., et al., "Personalized Information Delivery: An Analysis of Information Filtering Methods", *Communications of the ACM,* 35, 51–60 (Dec. 1992).

Gassman, B., "Internet Security, and Firewalls Protection on the Internet", *IEEE,* 93–107 (1996).

Goldberg, D., et al., "Using Collaborative Filtering to Weave an Information Tapestry", *Communications of the ACM,* 35, 61–70 (Dec. 1992).

Grampp, F.T., "UNIX Operating System Security", *AT&T Bell Laboratories Technical Journal,* 63, 1649–1672 (Oct. 1984).

Greenwald, M., et al., "Designing an Academic Firewall: Policy, Practice, and Experience with SURF", *IEEE,* 79–92 (1996).

Haigh, J.T., et al., "Extending the Noninterference Version of MLS for SAT", *Proceedings of the 1986 IEEE Symposium on Security and Privacy,* Oakland, CA, p. 232–239 (Apr. 7–9, 1986).

Karn, P., et al., "The ESP DES–CBC Transform", Network Working Group, Request for Comment No. 1829, http//ds.internic.net/rfc/rfc1829.txt, 9 p. (Aug. 1995).

Kent, S.T., "Internet Privacy Enhanced Mail", *Communications of the ACM*, 36, 48–60 (Aug. 1993).

Lampson, B.W., et al., "Dynamic Protection Structures", *AFIPS Conference Proceedings,* 35, 1969 Fall Joint Computer Conference, Las Vegas, NV, 27–38 (Nov. 18–20, 1969).

Lee, K.C., et al., "A Framework for Controlling Cooperative Agents", *Computer,* 8–16 (Jul. 1993).

Lodin, S.W., et al., "Firewalls Fend Off Invasions from the Net", *IEEE Spectrum,* 26–34 (Feb. 1998).

Loeb, S., "Architecting Personalized Delivery of Multimedia Information", *Communications of the ACM,* 35, 39–48 (1992).

Loeb, S., et al., "Information Filtering", *Communications of the ACM,* 35, 26–28 (Dec. 1992).

McCarthy, S.P., "Hey Hackers? Secure Computing Says You Can't Break into This Telnet Site", *Computer Select,* 2 p. (Dec. 1995).

Merenbloom, P., "Network 'Fire Walls' Safeguard LAN Data from Outside Intrusion", *Infoworld,* p. 69 & addnl. page (Jul. 25, 1994).

Metzger, P., et al., "IP Authentication using Keyed MD5", Network Working Group, Request for Comments No. 1828, http//ds.internic.net/rfc/rfc1828.txt, 5 p. (Aug. 1995).

Obraczka, K., et al., "Internet Resource Discovery Services", *Computer,* 8–22, (Sep. 1993).
Peterson, L.L., et al., In: *Computer Networks,* Morgan Kaufmann Publishers, Inc., San Francisco, CA, p. 218–221, 284–286 (1996).
Press, L., "The Net: Progress and Opportunity", *Communications of the ACM,* 35, 21–25 (Dec. 1992).
Schroeder, M.D., et al., "A Hardware Architecture for Implementing Protection Rings", *Communications of the ACM,* 15, 157–170 (Mar. 1972).
Schwartz, M.F., "Internet Resource Discovery at the University of Colorado", *Computer,* 25–35 (Sep. 1993).
Smith, R.E., "Constructing a High Assurance Mail Guard", Secure Computing Corporation (Appeared in the Proceedings of the National Computer Security Conference), 7 p. (1994).
Smith, R.E., "Sidewinder: Defense in Depth Using Type Enforcement", *International Journal of Network Management,* p. 219–229 (Jul.–Aug. 1995).
Stadnyk, I., et al., "Modeling User's Interests in Information Filters", *Communications of the ACM,* 35, 49–50 (Dec. 1992).
Stempel, S., "IpAccess—An Internet Service Access System for Firewall Installations", *IEEE,* 31–41 (1995).
Stevens, C., "Automating the Creation of Information Filters", *Communications of the ACM,* 35, 48 (Dec. 1992).
Thomsen, D., "Type Enforcement: The New Security Model", *SPIE,* 2617, 143–150 (1995).
Warrier, U.S., et al., "A Platform for Heterogeneous Interconnection Network Management", *IEEE Journal on Selected Areas in Communications,* 8, 119–126 (Jan. 1990).
White, L.J., et al., "A Firewall Concept for Both Control–Flow and Data–Flow in Regression Integration Testing", *IEEE,* 262–271 (1992).
Wolfe, A., "Honeywell Builds Hardware for Computer Security", *Electronics,* 14–15 (Sep. 2, 1985).

* cited by examiner

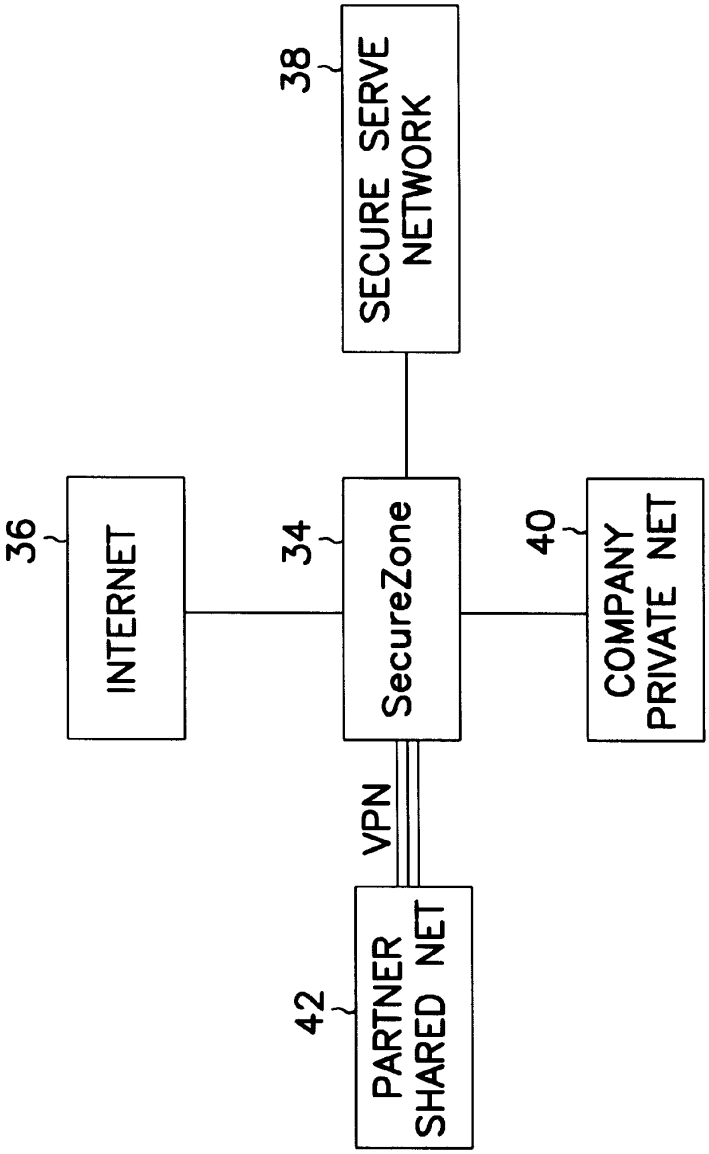


Figure 1

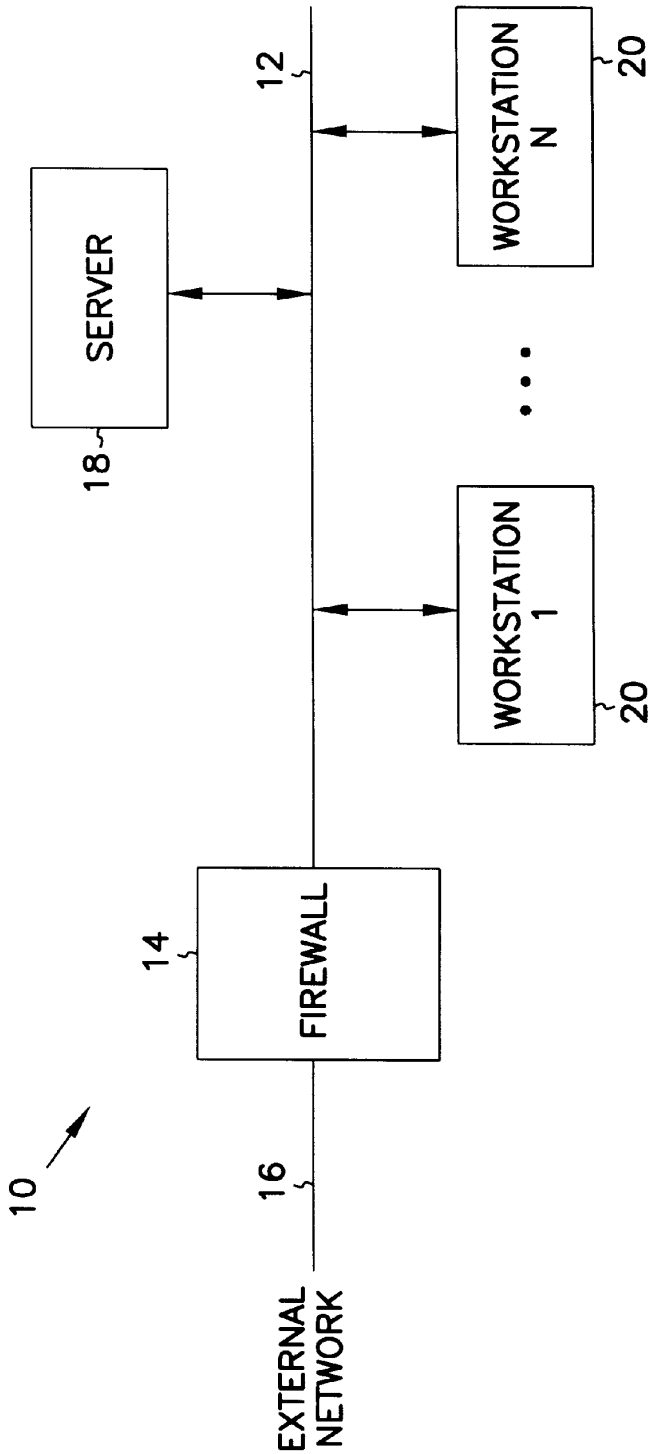


Figure 1a

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.