US006674743B1

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

(10) **Patent No.: US 6,674,743 B1**
(45) **Date of Patent: Jan. 6, 2004**

(54) **METHOD AND APPARATUS FOR PROVIDING POLICY-BASED SERVICES FOR INTERNAL APPLICATIONS**

(75) Inventors: **Satish Amara**, Mount Prospect, IL (US); **Michael Freed**, Arlington Heights, IL (US)

(73) Assignee: **3Com Corporation**, Santa Clara, CA (US)

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

(21) Appl. No.: **09/475,855**

(22) Filed: **Dec. 30, 1999**

(51) **Int. Cl.**[7] **H04L 12/28**
(52) **U.S. Cl.** **370/351**; 370/389; 370/392; 709/228
(58) **Field of Search** 370/229–235, 370/351, 389–392, 412–418, 428, 401, 402, 465, 466; 709/227, 228, 238, 240

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,473,607	A		12/1995	Hausman et al. 370/85.13
5,528,595	A		6/1996	Walsh et al. 370/85.13
5,530,703	A		6/1996	Liu et al. 370/85.13
5,541,911	A		7/1996	Nilakantan et al. 370/13
5,606,668	A		2/1997	Shwed 395/200.11
5,761,424	A		6/1998	Adams et al. 395/200.47
5,790,554	A		8/1998	Pitcher et al. 370/471
5,802,320	A		9/1998	Baehr et al. 395/200.79
5,835,726	A		11/1998	Shwed et al. 395/200.59
5,835,727	A		11/1998	Wong et al. 395/200.68
5,878,231	A		3/1999	Baehr et al. 395/200.75
5,884,025	A		3/1999	Baehr et al. 395/187.01
5,889,953	A		3/1999	Thebaut et al. 395/200.51
5,889,958	A		3/1999	Willens 395/200.59
5,951,649	A		9/1999	Dobbins et al. 709/238
5,983,270	A		11/1999	Abraham et al. 709/224
6,104,700	A	*	8/2000	Haddock et al. 370/235
6,157,955	A	*	12/2000	Narad et al. 709/228

FOREIGN PATENT DOCUMENTS

WO	9840987	9/1998
WO	9911003	3/1999

OTHER PUBLICATIONS

Corbridge et al, Packet Filtering in an IP Router, pp. 227–232, LISA–V—Sep. 30–Oct. 3, 1991.*
Wakeman et al, Implementing Real Time Packet Forwarding Policies using streams, pp. 1–12, Nov. 14, 1994.*
"IPSec Network Security Commands," http://www.cisco-.com/univercd/cc/td/doc/products/software/ios120/12cgcr/secur_r/srprt4/sripsec.htm, pp. 1–45 (1998).
R. Rajan, S. Kamat, Internet Engineering Task Force (IETF), Internet Draft, "A Simple Framework and Architecture for Networking Policy," draft–rajan–policy–framework–00.txt, May 23, 1999, pp. i–xxiii.
H–W. Braun, Network Working Group, Request for Comments: 1104, "Models of Policy Based Routing," Jun. 1989, pp. 1–10.
D, Estrin, Network Working Group, Request for Comments: 1125, "Policy Requirements for Inter Adminstrative Domain Routing," Nov. 1989, pp. 1–21.
D. Clark, Network Working Group, Request for Comments: 1102, "Policy Routing in Internet Protocols," May 1989, pp. 1–22.

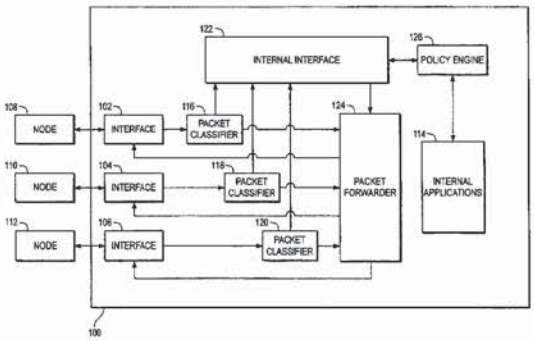
* cited by examiner

Primary Examiner—Dang Ton
Assistant Examiner—Frank Duong
(74) *Attorney, Agent, or Firm*—McDonnell Boehnen Hulbert & Berghoff

(57) **ABSTRACT**

A packet-forwarding device for providing policy-based services has at least a first interface, a second interface, and a packet forwarder for forwarding external packets between the first and second interfaces. The packet-forwarding device also runs internal applications that may be remotely accessed. The first and second interfaces transmit and receive internal and external packets, the internal packets being those packets generated or received by the internal applications during remote access, and the external packets being those packets destined for devices other than the packet-forwarding device. The packet forwarder forwards external packets between the first and second interfaces. An internal interface forwards internal packets between the internal applications and the first and second interfaces, and a policy engine logically connected to the internal interface applies a policy to the internal packets.

48 Claims, 3 Drawing Sheets



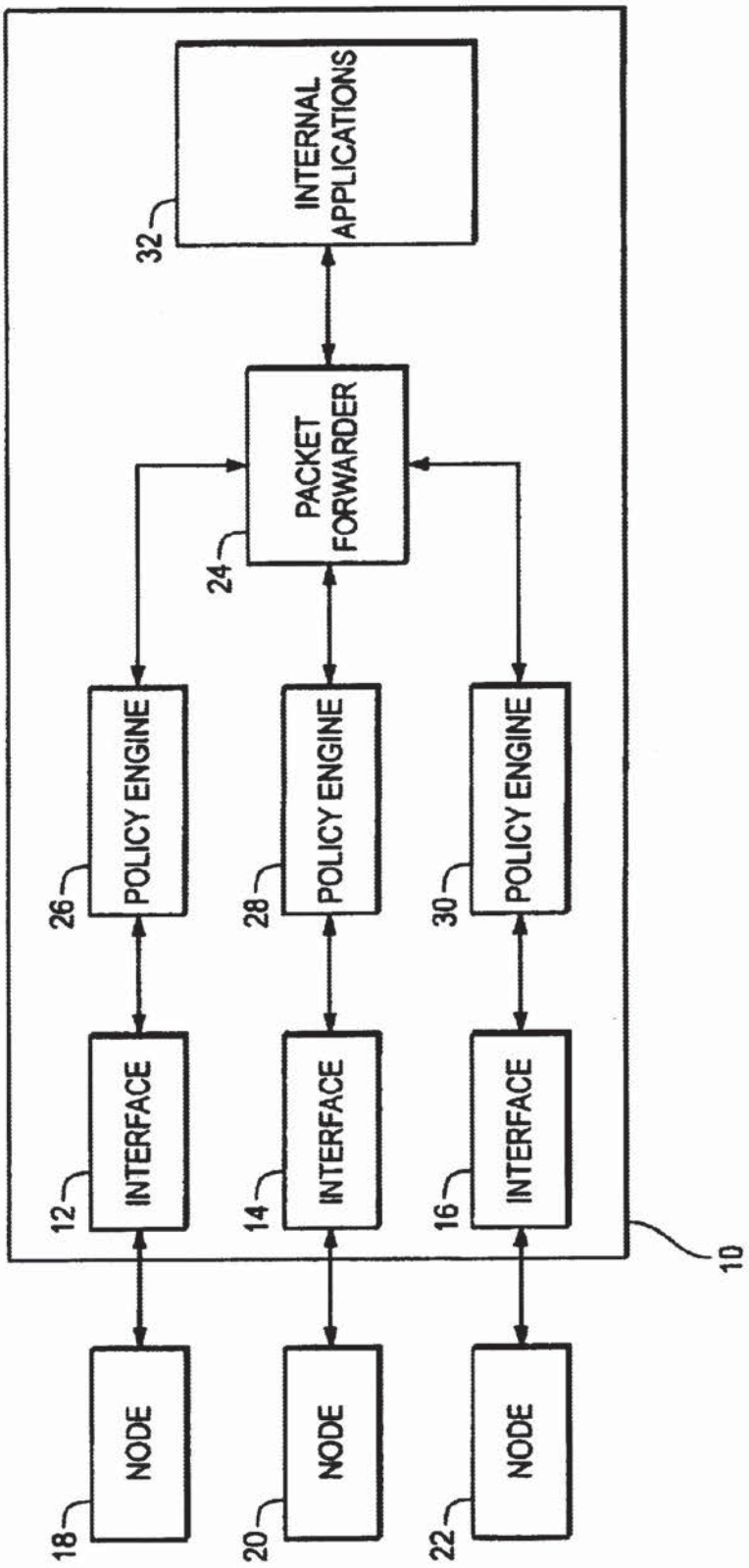


FIG. 1
PRIOR ART

FIG. 2

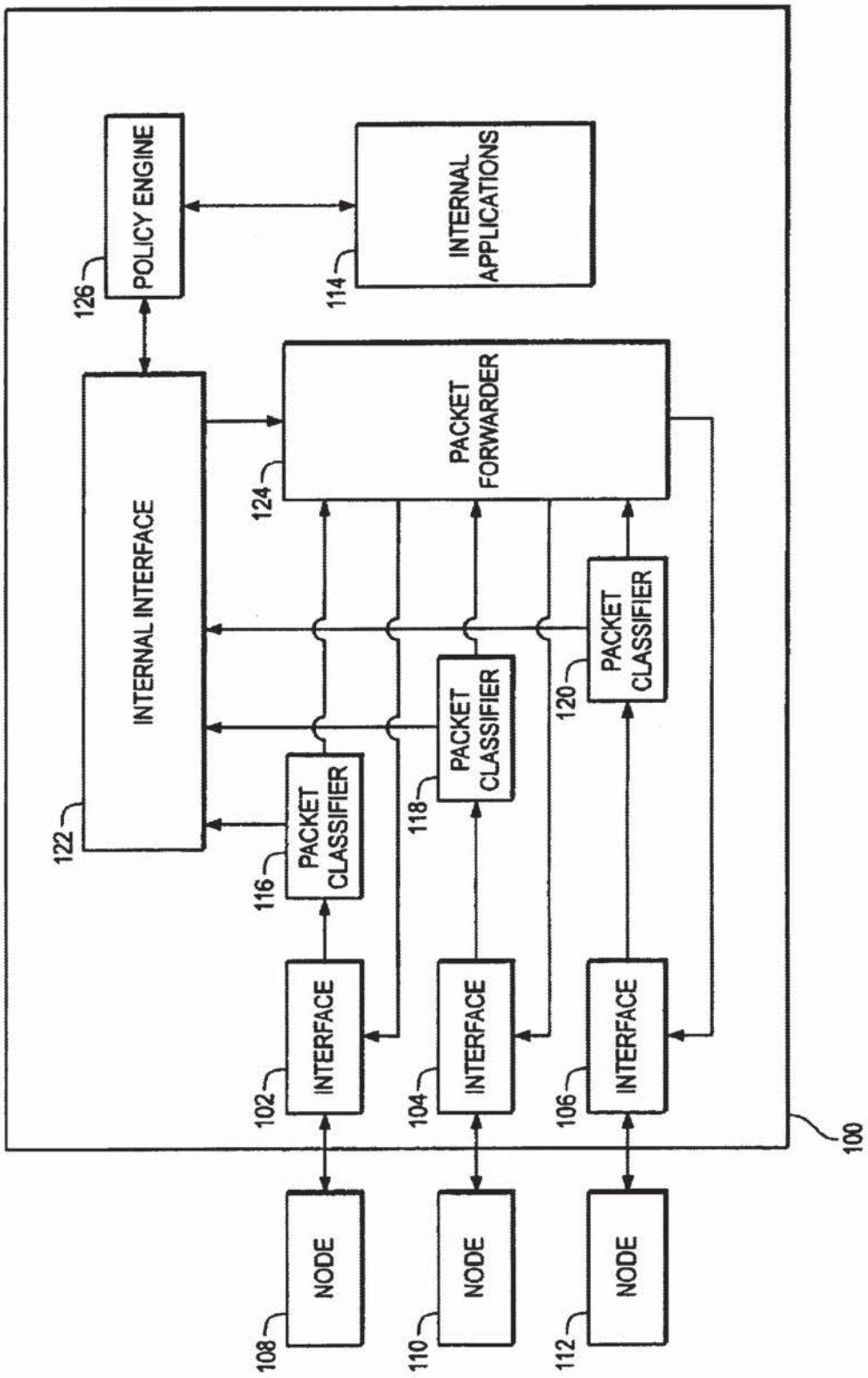
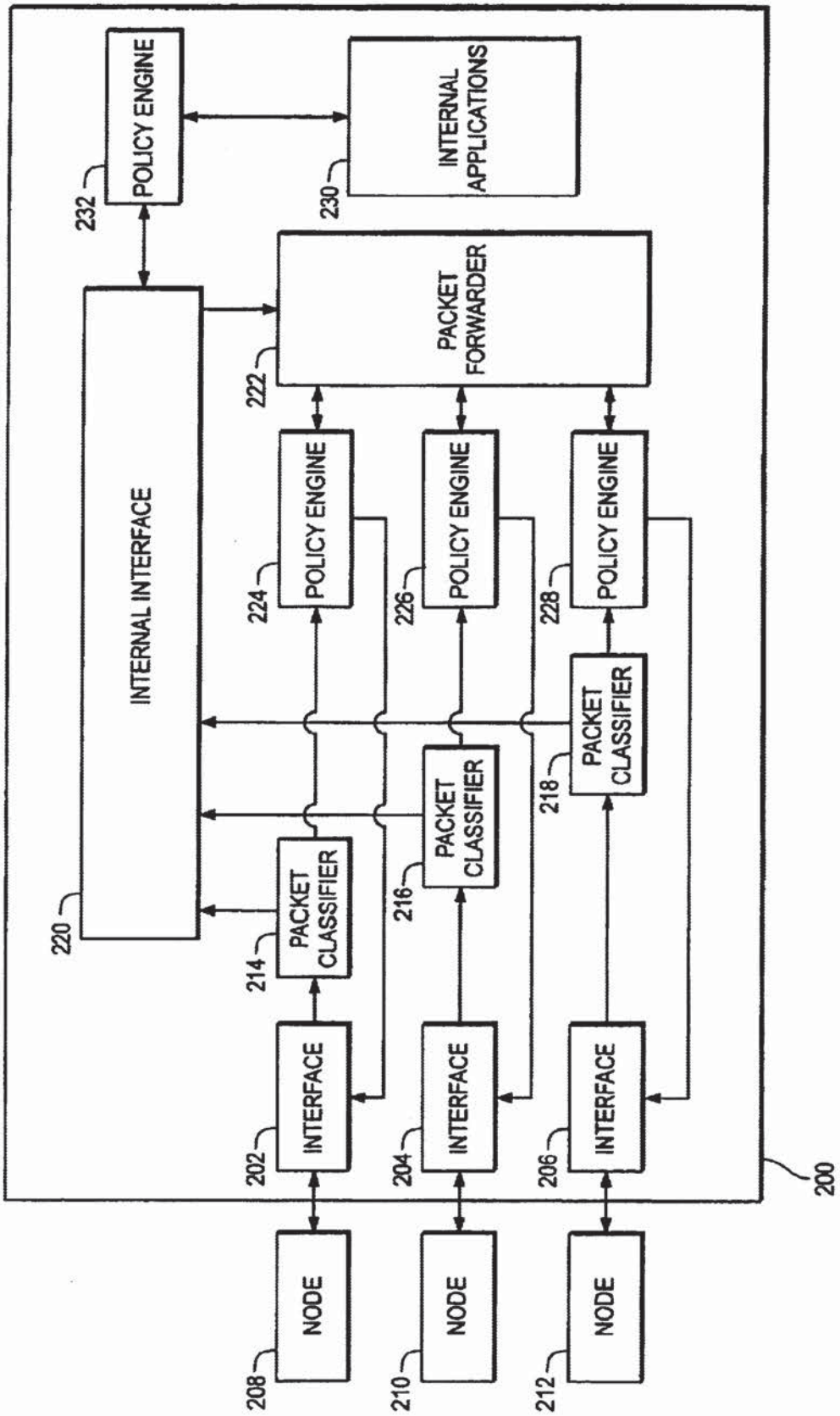


FIG. 3



METHOD AND APPARATUS FOR PROVIDING POLICY-BASED SERVICES FOR INTERNAL APPLICATIONS

BACKGROUND OF THE INVENTION

A. Field of the Invention

This invention relates to the field of digital telecommunications. More particularly, this invention relates to a method and apparatus for applying policies in packet forwarding devices, such as routers and remote access servers.

B. Description of Related Art

Packet-switched networks, such as the Internet, typically include one or more packet forwarding devices, such as routers or remote access servers. Viewed at the simplest level, a router is a device having a plurality of interfaces, with each interface typically connected to a wide area network (WAN), a local area network (LAN), or a host. Internally, the router forwards packets from one interface to another based on the destination address contained in the header of each packet. A remote access server is similar to a router, except that, in addition to interfaces to WANs and/or LANs, a remote access server also includes one or more interfaces to the public switched telephone network (PSTN) to provide dial-in access to the network. Remote access servers also forward packets from one interface to another based on the destination addresses of the packets.

Increasingly, routers and remote access servers are also performing more sophisticated handling of packets than simply routing them on the basis of destination address. In particular, some packets may be selected for special treatment in order to provide "policy-based services." "Policy-based services" encompass any disposition of packets that involves more than simply routing them based on their destination addresses. For example, routers and remote access servers may perform packet filtering, in which certain packets are dropped, diverted, and/or logged. The router or remote access server may also perform network address translation (NAT), in which the source and/or destination addresses are changed. Certain packets may be encrypted or decrypted, such as provided for in the IPsec protocols. Finally, certain packets may be prioritized in the queue of the router or remote access server in order to provide a particular quality of service (QoS) level. Many other types of special handling of packets could also be performed.

To identify the packets that are to be subject to such special handling, the router or remote access server typically examines more than the destination address of the packet. In general, the packet-forwarding device examines one or more "selector fields" within each packet, such as the source address, destination address, source port, destination port, and protocol type. User name, more particularly the IP address allocated to a particular user, may also be used as a selector filed in remote access servers. The packet-forwarding device then enforces a "policy" by applying a set of rules to packets whose selector fields meet predefined criteria. The rules specify how the packets are to be handled. As a result of this policy enforcement, packets may be dropped, logged, translated, encrypted, decrypted, or prioritized, if the selector fields within the packets match certain predefined criteria.

Typically, the "policy" is applied to all interfaces of the packet-forwarding device. For example, Abraham et al., U.S. Pat. No. 5,983,270 discloses a network server through which all traffic between a LAN and the Internet passes. A filter engine in the network server applies a policy, embodied in a set of rules, to all outbound packets transmitted from the LAN to the Internet and to all inbound packets from the Internet to the LAN.

Similarly, Haddock et al., PCT Publication No. WO 99/11003 discloses a packet-forwarding device having a comparison engine. The comparison engine examines the packets arriving at each input port to determine with which traffic group each packet is associated, the traffic groups defining different QoS levels.

A packet-forwarding device **10** that typifies the prior art approach of applying policies to packets is shown in FIG. **1**. FIG. **1** is a functional block diagram in which arrows illustrate the flow of packets between functional blocks. Device **10** may be a router, a remote access server, or other such device that forwards packets. Device **10** includes interfaces **12**, **14**, and **16**, that connect device **10** to nodes **18**, **20**, and **22**, respectively. Nodes **18–22** may represent hosts connected via a LAN or WAN or via the PSTN. Nodes **18–22** may also represent other packet forwarding devices. Although device **10** is shown in FIG. **1** with three interfaces, device **10** may, in general, have a greater or fewer number of interfaces.

As indicated by the double-headed arrows, interfaces **12–16** are able to send packets to and to receive packets from nodes **18–22**, respectively. Interfaces **12–16**, in turn, are logically connected to a packet forwarder **24** via policy engines **26**, **28**, and **30**. Internal applications **32** are also logically connected to packet forwarder **24**. Internal applications **32** include the applications on device **10**, such as applications for controlling and configuring device **10**, that are accessible remotely, such as by SNMP or by Telnet.

Packet forwarder **24** receives packets forwarded by interfaces **12–16**, via policy engines **26–30**, and by internal applications **32**. Packet forwarder **24**, in turn, is able to forward packets to internal interfaces **12–16**, via policy engines **26–30**, and to internal applications **32**. Packet forwarder **24** performs a routing functionality. Specifically, packet forwarder **24** determines, for each packet it receives, whether to forward the packet to one or more of interfaces **12–16** and/or internal applications **32**. Packet forwarder **24** makes this routing determination for each packet based on the packet's destination address. Typically, packet forwarder **24** has access to routing tables that specify where to send each destination address. Normally, packet forwarder **24** will forward a packet to internal applications **32** when the packet's destination address matches one of the packet-forwarding device's own IP addresses.

Policy engines **26–30** apply policies to all packets forwarded between interfaces **12–16** and packet forwarder **24**. In this process, policy engines **26–30** trap each packet and examine various selector fields in each packet, such as source address, destination address, source port, destination port, and protocol type. Based on this information, policy engines **26–30** apply a set of rules that specify the manner in which the packets are to be handled. In general, policy engines **26–30** may be separately configured so as to apply different policies.

The problem with this approach is that there is a high overhead associated with applying policies to all incoming and outgoing packets. This high overhead may increase the latency of each packet and may degrade the throughput of the packet-forwarding device. Another disadvantage with the prior art approach is the time and effort required to develop and manage policies for each interface. Finally, the overhead and management difficulties serve to limit the complexity of the policies that a packet-forwarding device can apply.

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.