(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 July 2003 (03.07.2003)

PCT

(10) International Publication Number
WO 03/055176 A1

(51) International Patent Classification[7]: H04L 29/06, 29/12

(21) International Application Number: PCT/US02/40514

(22) International Filing Date:
17 December 2002 (17.12.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/029,708 19 December 2001 (19.12.2001) US

(71) Applicant: **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: **TANG, Puqi**; 4559 SW Silverleaf Drive, Portland, OR 97229 (US). **DIEP, Timothy**; 44 Melbourne Street, Portsmouth, NH 03801 (US). **HLASNIK, Wayne**; 22232 SW Lebeau Road, Sherwood, OR 97140 (US).

(74) Agents: **HARRIS, Scott, C.** et al.; Fish & Richardson PC, 4350 La Jolla Village Drive, Suite 500, San Diego, CA 92122 (US).

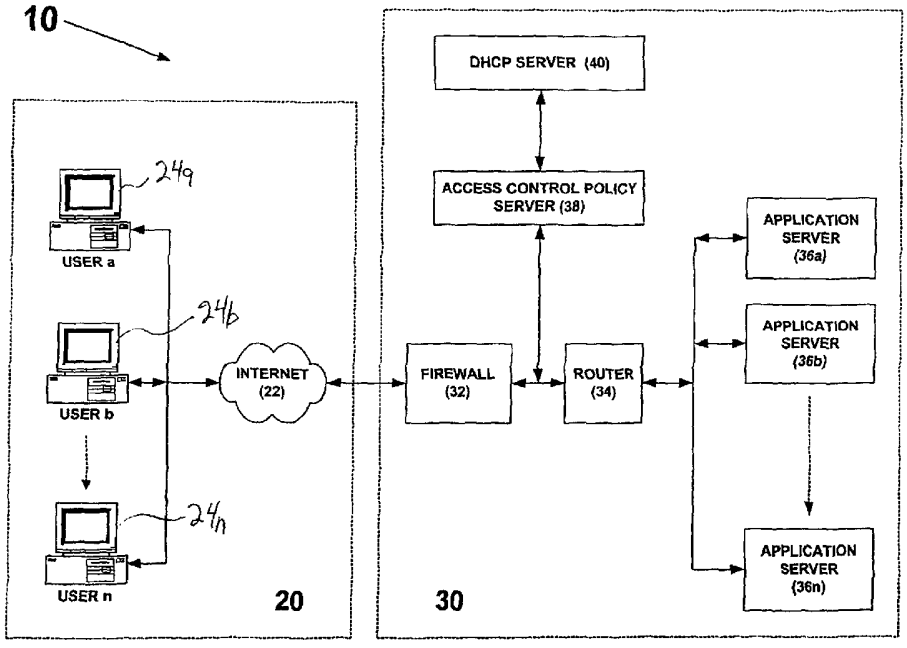
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ACCESS CONTROL MANAGEMENT



(57) Abstract: A method of access control management includes determining a private network address for a user in connection with the user accessing a network resource, determining an access control list entry for the user based on an access control policy, translating a public network address to the private network address for the user accessing the network resource, and allowing or blocking the user access based on the access control list entry, wherein determining the access control list entry is performed before translating the public network address to the private network address.

WO 03/055176 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ACCESS CONTROL MANAGEMENT

TECHNICAL FIELD

This invention relates to access control.

BACKGROUND

The Internet, which allows users to access the resources of interconnected computers, also offers the possibility of access to smaller, private networks (intranets). Intranets typically include systems that restrict access to the networked resources of the intranet to only authorized users. Networked resources refers to the hardware, software, and data included in a network and accessible to authorized users from inside or outside the network.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram.

FIG. 2 shows data and command flows in the block diagram of FIG.1.

DESCRIPTION

Referring to FIG. 1, a computer network 10 includes a public network 20, in this case the Internet 22, connected to a private network 30. External computer USERa-USERn ("users") may access the resources of the Internet 22

computers 36a-36n that provide application programs and data to authorized users.

Computer systems 32, 34, 36a-36n, 38 and 40, interpret data packets based on one or more functional layers of an Open Systems Interconnect (OSI) model. For example, router 34 interprets packets using the network layer of OSI, and therefore, uses a network layer ACL from policy server 38 to determine which packets are to be blocked or transmitted to a server 36a-36n.

Policy server 38 maintains the access control policy by storing application layer ACLs for server computers 36a-36n. The application layer ACLs used by server computers 36a-36n are specific to each server or specific to an application on each server. Application layer ACLs do not include the dynamically allocated private IP address from DHCP server 40, however, a network layer ACL may use the private IP address as part of a network layer ACL entry.

Whenever a private IP address is allocated from DHCP server 40 (i.e., a private IP address is assigned to a new access request), policy server 38 retrieves the appropriate application layer ACL for the access request and generates a corresponding network layer ACL. Policy server 38 then sends the generated network layer ACL to each network device, such as router 34, and also to each application server 36a-36n that supports network layer packet filtering.

through computers 24a-24n. Users may also attempt to access resources of private network 30 by sending access requests through Internet 22 to private network 30. Private network 30 determines whether to allow or block each user access request.

Private network 20 includes an access control policy server 38 that manages an access policy for private network 20. The various computers and devices included in private network 20 use access control lists (ACLs) to determine and control access to the resources of private network 20. The ACLs used by the computers and devices included in network 20 are maintained and generated by policy server 38, as will be explained.

In addition to policy server 38, private network 30 includes other inter-connected computer systems, i.e., a Dynamic Host Configuration Protocol (DHCP) server 40 that dynamically allocates a private IP address for each user of private network 30, and a firewall computer 32 that authenticates user requests received from public network 20 and translates a public IP address for each user request to the dynamically allocated private IP address from DHCP server 40. Firewall computer 32 also forwards authenticated user requests, along with the translated private IP address, to a router 34 that transports data within private network 30. Private network 30 also includes application server

Policy server 38 also sends the retrieved application layer ACL to those servers 36a-36n that do not support network layer packet filtering. As each ACL is received by a network device or computer system in network 20, the ACL is "installed" by that device or computer system, and then used to determine whether to allow or deny access to a received user access request, as will be explained. Please note that the ACL retrieval, generation and installation is performed before the allocated private IP address is sent to firewall computer 32.

Maintaining the control policy on a centralized policy server 38 avoids having to manage separate access policies (and separate ACLs) on each server computer and network device in private network 30. This also assures the horizontal consistency of ACLs that are used in each application layer throughout private network 30. Furthermore, the access control policy server 38 uses the private IP address allocated at "runtime" to dynamically generate network layer ACLs that map to application layer ACLs, both of which are then distributed to the appropriate systems in private network 30. This assures vertical consistency of ACLs logically across application layers and network layers.

An example of a user 24b attempting to access an application from server 36a and 36b is shown in FIG. 2.

Flow arrows (51-59) depict the sequence of actions required to establish a flow of data (60) for a user 24b attempting to access an application from server 36b. In this example, user 24b is allowed access to an application on server 36b, but denied access to any applications on server 36a. User 24b sends (51) a login message through Internet 22. The login message is forwarded (52) through Internet 22 to firewall computer 32. Firewall computer 32 authenticates the credentials included in the login message, and sends (53) a DHCP request to policy server 38. Policy server 38 forwards (54) the DHCP request to DHCP server 40. In response to the DHCP request, DHCP server 40 returns (55) a private IP address to policy server 38. Policy server 38 searches the application ACLs stored in access control database and finds an entry that corresponds to "user 24b is allowed to read from application server 36b, but not allowed to access other servers". Policy server 38 uses the private IP address to generate a network layer ACL entry (required by each network layer device, such as router 34) that corresponds to the found application layer ACL. Policy server retrieves the found application layer ACL for each of the server computers 36a-36n. Then policy server 38 sends (56) the generated network layer ACLs to router 34, and sends (57)(58) the retrieved application layer ACLs to servers 36a and 36b, respectively. Router 34, and servers

36a and 36b, install, respectively, the received ACLs, for use in determining access for the user access request.

Before the installation of ACL entries in router 34 and servers 36a and 36b, policy server 38 may query the individual server computers 36a and 36b to determine their packet filtering capabilities. If policy server 38 determines that a server computer is capable of performing network layer packet filtering, policy server 38 may also send the generated network ACL entry to that server.

Continuing with the example shown in FIG. 2, policy server 38 returns (59) the private IP address for user 24b to firewall computer 32. At this point firewall computer 32 performs the required network address translation (NAT) for user 24b (i.e., translating a public IP address associated with the user on public network 20 to the allocated private IP address). Performing NAT allows a flow of data (60) to be established between user computer 24b and application server 36b. However, when user 24b attempts (61) to access server 36a, for example, the network layer ACL installed at router 34 or the application layer ACL installed at server 36a, will block the access request.

Please note that before firewall computer 32 translates ("tags") the user access request with the private IP address (via NAT), the access control ACLs, for both application layer computers and network layer devices have already been

(SIP, DIP, Proto, SPort, DPort)-> Action

The first field, SIP, stands for the source IP address (in this case the private IP address of the user in the private network 30). The second field, DIP, stands for the destination IP address of a server 36a-36n in the private network. The third field, Proto, stands for a transport layer protocol, such as TCP, UDP, etc. for which this ACL is intended. The fourth field, SPort, stands for the source port of the user request. The fifth field, DPort, stands for the destination port of the server application.

Exemplary network layer ACL entries, Entry A and Entry B, generated by policy server 38 are shown below.

ACL Entry A: (192.168.3.10,IpAddrOfAppServer36b, TCP, SPort, PortOnAppServer36b) -> "ALLOW";

ACL Entry B: (192.168.3.10, *, *, SPort, *) -> DENY.

ACL Entry A and ACL Entry B correspond to network layer ACL entries that are mapped and generated by policy server 38 for the previous example shown in FIG. 2. In more detail, ACL Entry A is generated to ALLOW access for user requests from source IP address "192.163.8.10" (the private IP address allocated to user 24b by DHCP server 40). ACL

sent by policy server 38, and installed by the respective computers and network devices of network 30.

Access control policy may be stored on a storage medium (not shown) connected to policy server 38. The access control policy may be modified by an authorized manager via a direct connection to policy server 38 (not shown) and may be modified indirectly by commands received at policy server 38 from an authorized manager associated with one of the server computers 36a-36n.

The access control policy uses "role-based" definitions to determine what level of access is allowed for a user request based on a defined role for each user. For example, access control policy may include several different roles, such as a "guest" who is denied access to any server data, a "regular user" who is allowed to read data from a specific server, a "power user" who is allowed to modify data on a specific server, and an "administrator" who is allowed to modify data on a specific server and allowed to re-boot that server.

Each entry in a network layer ACL (shown below), generated by policy server 38, includes a "5-tuple", i.e., a five (5) field filter along with a "deny" or "allow" action associated with that 5-tuple.

NETWORK LAYER ACL ENTRY:

Entry A also specifies a destination port of server computer 36b, a TCP protocol designation (the network layer of OSI), a source port corresponding to firewall computer 32 and a destination port corresponding to an application on server computer 36b. ACL Entry B would also be generated along with ACL Entry A. ACL Entry B is generated to DENY access to all user 24b requests to any other server besides server 36b. The '*' character included in ACL Entry B is a wildcard character, and is interpreted as all values allowed by the field in which the wildcard is used. In ACL Entry B, therefore, all user requests from source address "192.163.8.10" and from the source address of firewall computer 32 are denied access to any server system in private network 30.

When a user has finished with an established data flow to a server computer, for example, firewall computer 32 releases the private IP address allocated to that data flow and also de-installs the network layer ACLs. In more detail, firewall computer 32 sends a DHCP release request to policy server 38, and policy server 38 de-installs the network ACL entries associated with the private IP address from all "enforcement points", such as router 34 (and server 36b, if server 36b is capable of network layer filtering). In an embodiment, policy server 38 includes a cache (not shown) for storing each network layer ACL. Therefore, in

this embodiment, policy server 38 deletes the appropriate network ACL entries from its cache and forwards the DHCP release request to the DHCP server 40. DHCP server 40 responds to policy server 38 with a release acknowledgement, and policy server 38 forwards the release acknowledgement to firewall computer 32.

The process of generating ACLs according to a centralized access control policy, hereafter referred to as "process 100", is not limited to use with the hardware and software of FIG. 1. It may find applicability in any computing or processing environment. Process 100 may be implemented in hardware, software, or a combination of the two. Process 100 may be implemented in computer programs executing on programmable computers or other machines that each include a processor and a storage medium readable by the processor

The invention is not limited to the specific embodiments described above. For example, control policy server 38 and DHCP server 40 may be implemented on a single computer system performing both the allocation of private IP addresses and the generation of ACL's according to the control policy of system 10.

Other embodiments not described herein are also within the scope of the following claims.

What is claimed is:

1. A method comprising:

determining a private network address for a user in connection with the user accessing a network resource;

determining an access control list entry for the user based on an access control policy;

translating a public network address to the private network address for the user accessing the network resource; and

allowing or blocking the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

2. The method of claim 1, further comprising sending the determined access control list entry from a first computer on the network to a second computer on the network before allowing or blocking the user access.

3. The method of claim 2, further comprising:

generating an access control list entry corresponding to the access control policy, that entry including the determined private network address.

4. The method of claim 3, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

5. The method of claim 2, wherein the determined access control list entry comprises an application level access control list entry stored on storage device connected to the first computer.

6. The method of claim 3, wherein determining the network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

7. The method of claim 3, wherein the second computer comprises a network layer device, and

wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

8. The method of claim 5, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

9. The method of claim 5, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

10. The method of claim 3, further comprising:

releasing the private network address following completion of the access to the network resource.

11. The method of claim 10, further comprising:

de-installing a network layer access control entry following completion of the access to the network resource.

12. An article comprising a machine-readable medium that stores machine-executable instructions, the instructions causing a machine to:

determine a private network address for a user in connection with the user accessing a network resource;

determine an access control list entry for the user based on an access control policy;

translate a public network address to the private network address for the user accessing the network resource; and

allow or block the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

13. The article of claim 12, further comprising instructions causing a machine to:

send the determined access control list entry from a first computer on the network to a second computer on the network before allowing or blocking the user access.

14. The article of claim 13, further comprising instructions causing a machine to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

15. The article of claim 14, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

16. The article of claim 13, wherein the determined access control list entry comprises an application level access control list entry stored on storage device connected to the first computer.

17. The article of claim 14, wherein determining the network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

18. The article of claim 14, wherein the second computer comprises a network layer device, and

wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

19. The article of claim 16, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

20. The article of claim 16, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

21. The article of claim 14, further comprising:

releasing the private network address following completion of the access to the network resource.

22. The article of claim 21, further comprising:

de-installing a network layer access control entry following completion of the access to the network resource.

23. An apparatus comprising:

a first memory that stores executable instructions; and

a first processor that executes the instructions from the first memory to:

determine a private network address for a user in connection with the user accessing a network resource;

determine an access control list entry for the user based on an access control policy;

translate a public network address to the private network address for the user accessing the network resource; and

allow or block the user access based on the access control list entry,

wherein determining the access control list entry is performed before translating the public network address to the private network address.

24. The apparatus of claim 23, further comprising:

a second processor connected to the first processor, wherein the first processor executes instructions to:

send the determined access control list entry from the first processor to the second processor in a network.

25. The apparatus of claim 24, wherein the first processor executes instructions to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

26. The apparatus of claim 25, wherein the determined access control list entry comprises a network level access control list entry including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined network address, and an indication of allowed or denied access to the network resource.

27. The apparatus of claim 25, wherein determining the network address comprises assigning a network address based on a dynamic host configuration protocol (DHCP).

28. The apparatus of claim 25, further comprising:

a storage medium connected to the first processor, wherein the determined access control list entry comprises an application level access control list stored on the storage medium.

29. The apparatus of claim 24, wherein the second processor comprises a network layer device.

30. The apparatus of claim 29, wherein the network layer device executes instructions to block or allow access to the network resource based on the network level access control list entry.

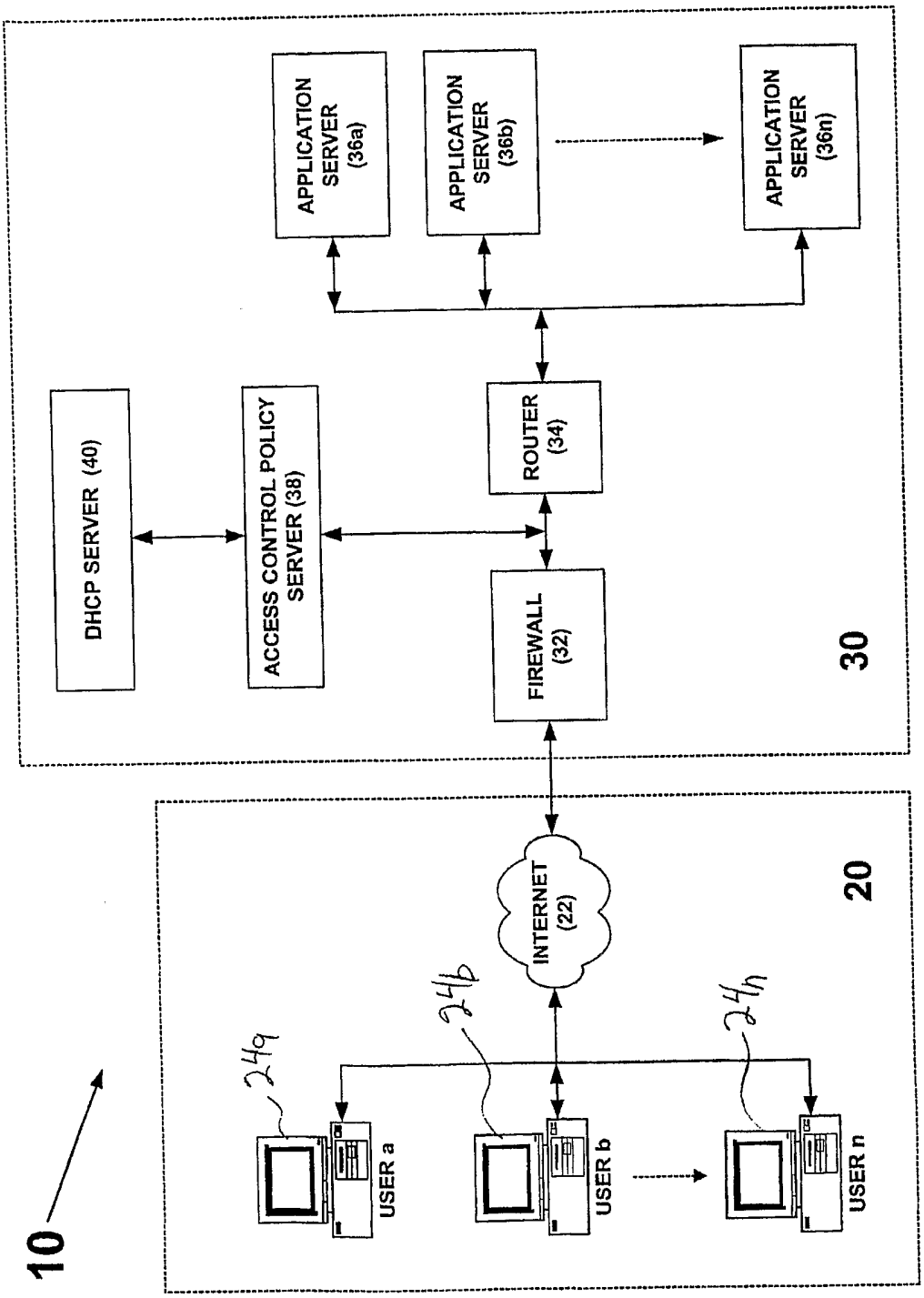

10
USER a
USER b
USER n
24a
24b
24n
INTERNET (22)
20
FIREWALL (32)
ACCESS CONTROL POLICY SERVER (38)
DHCP SERVER (40)
ROUTER (34)
APPLICATION SERVER (36a)
APPLICATION SERVER (36b)
APPLICATION SERVER (36n)
30

FIGURE 1

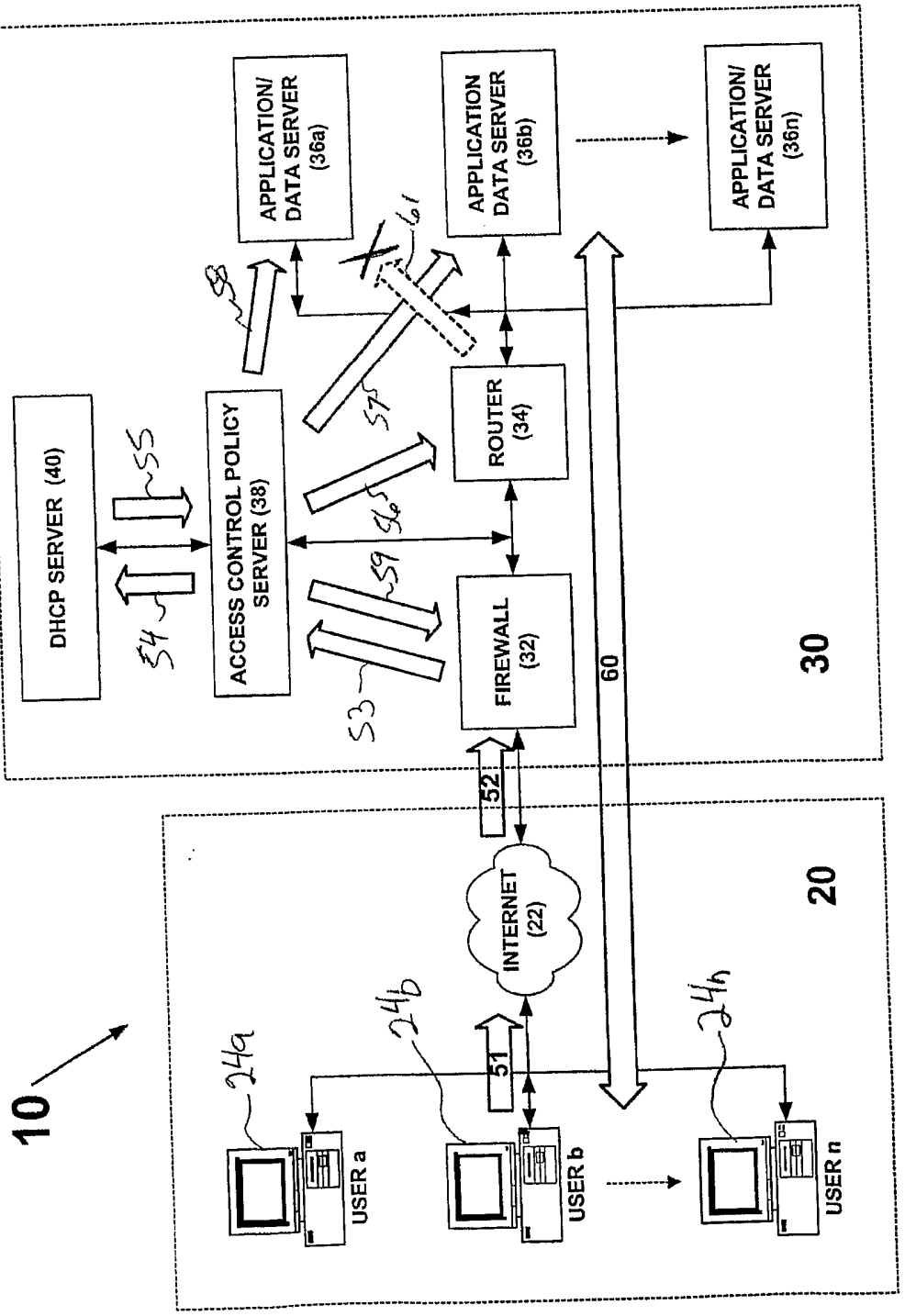

10
20
30
USER a
USER b
USER n
INTERNET (22)
FIREWALL (32)
ROUTER (34)
ACCESS CONTROL POLICY SERVER (38)
DHCP SERVER (40)
APPLICATION/ DATA SERVER (36a)
APPLICATION DATA SERVER (36b)
APPLICATION/ DATA SERVER (36n)
60
51
52
53
54
55
57
59
61
24a
24b
24n

FIGURE 2

INTERNATIONAL SEARCH REPORT

International cation No
PCT/US 02/40514

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 199 24 575 A (SUN MICROSYSTEMS INC) 2 December 1999 (1999-12-02) abstract column 3, line 21 - line 53 column 10, line 42 -column 11, line 4 claim 1 figure 1 --- -/--	1-30

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 2003	14/04/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bub, A

INTERNATIONAL SEARCH REPORT

International ation No
PCT/US 02/40514

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 941 947 A (GREENBERG RICHARD G ET AL) 24 August 1999 (1999-08-24) abstract figures 1,3A,7 column 2, line 59 - line 66 column 3, line 26 - line 36 column 7, line 38 -column 8, line 18 column 9, line 12 - line 26 column 16, line 19 - line 27 column 24, line 1 - line 7 column 27, line 44 - line 58	1-30
A	US 6 249 873 B1 (KNIPE BRUCE ET AL) 19 June 2001 (2001-06-19) abstract figures 5,12 column 8, line 5 - line 59 column 9, line 11 - line 18	1-30
A	US 6 219 706 B1 (FAN SERENE ET AL) 17 April 2001 (2001-04-17) abstract column 2, line 52 -column 3, line 21 column 3, line 44 -column 4, line 7 column 7, line 20 - line 51 column 8, line 11 - line 48 column 9, line 57 - line 59 column 14, line 53 - line 63 column 14, line 66 -column 15, line 18 figures 1,4,6,9,10A-C	1-30
A	US 5 793 763 A (MAYES JOHN C ET AL) 11 August 1998 (1998-08-11) abstract	1-30

INTERNATIONAL SEARCH REPORT

Inform] on patent family members

International cation No
PCT/US 02/40514

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19924575 A	02-12-1999	DE 19924575 A1	02-12-1999
		FR 2782873 A1	03-03-2000
		GB 2340702 A ,B	23-02-2000
		JP 2000049867 A	18-02-2000
US 5941947 A	24-08-1999	NONE	
US 6249873 B1	19-06-2001	US 5922074 A	13-07-1999
		AU 739898 B2	25-10-2001
		AU 5627898 A	03-09-1998
		CA 2230304 A1	28-08-1998
		EP 0862105 A2	02-09-1998
		JP 10308733 A	17-11-1998
US 6219706 B1	17-04-2001	NONE	
US 5793763 A	11-08-1998	US 6510154 B1	21-01-2003
		US 6298063 B1	02-10-2001
		US 6317775 B1	13-11-2001
		US 6061349 A	09-05-2000
		US 6104717 A	15-08-2000