US 20060242294A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2006/0242294 A1

(43) Pub. Date: Oct. 26, 2006

Damick et al.

(54) ROUTER-HOST LOGGING

(76) Inventors: **Jeffrey Joseph Damick**, South Riding, VA (US); **Sean Cunningham**, Washington, DC (US)

Correspondence Address:
FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022 (US)

(21) Appl. No.: **11/395,540**

(22) Filed: **Apr. 3, 2006**

Related U.S. Application Data

(60) Provisional application No. 60/758,986, filed on Jan. 17, 2006. Provisional application No. 60/667,664, filed on Apr. 4, 2005. Provisional application No. 60/686,420, filed on Jun. 2, 2005.

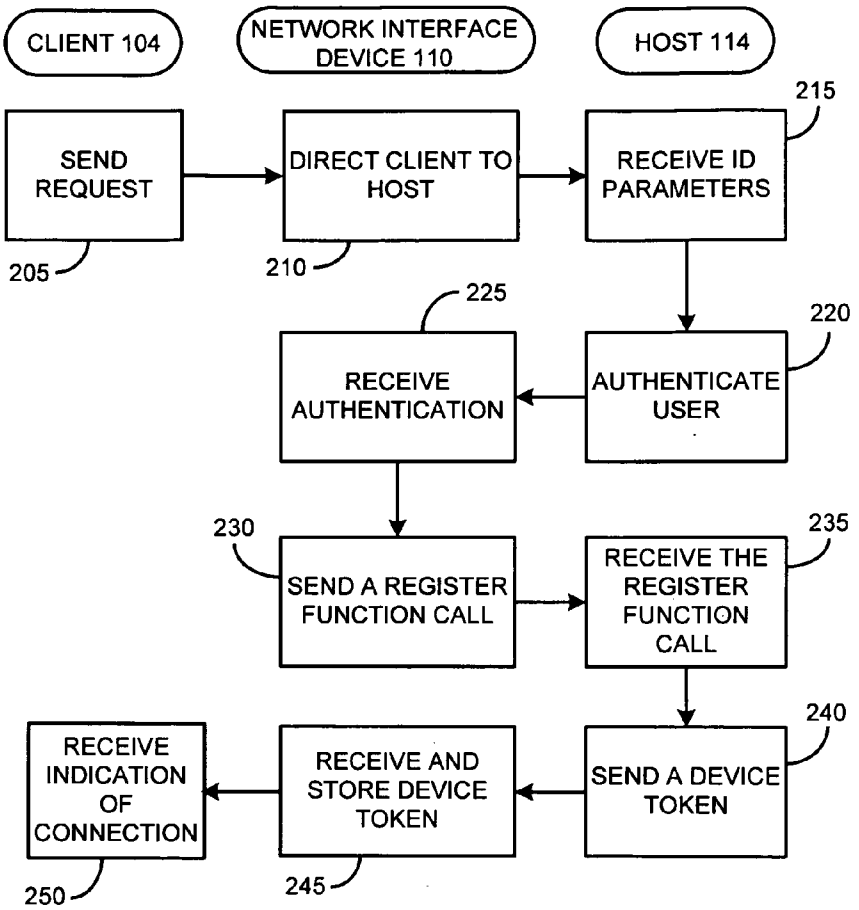
Publication Classification

(51) **Int. Cl.**
G06F 15/173 (2006.01)

(52) **U.S. Cl.** **709/224**

(57) **ABSTRACT**

According to a general aspect, a method includes receiving, at a network interface device at a user location, a request from a first machine located at the user location, the request including a first-machine identifier and a request to access through the network interface device a first location on a network. The method also includes logging, at the network interface device, the request from the first machine into a first-machine log for requests from the first machine, the logging into the first-machine log being based on the first-machine identifier. The method also includes receiving at the network interface device a request from a second machine located at the user location, the request from the second machine including a second-machine identifier and a request to access through the network interface device a second location on the network, and the network interface device, the first machine, and the second machine being located at a user location. The method further includes logging, at the network interface device, the request from the second machine into a second-machine log for all requests from the second machine, the logging into the second-machine log being based on the second-machine identifier.



FreeWheel, Ex. 1117

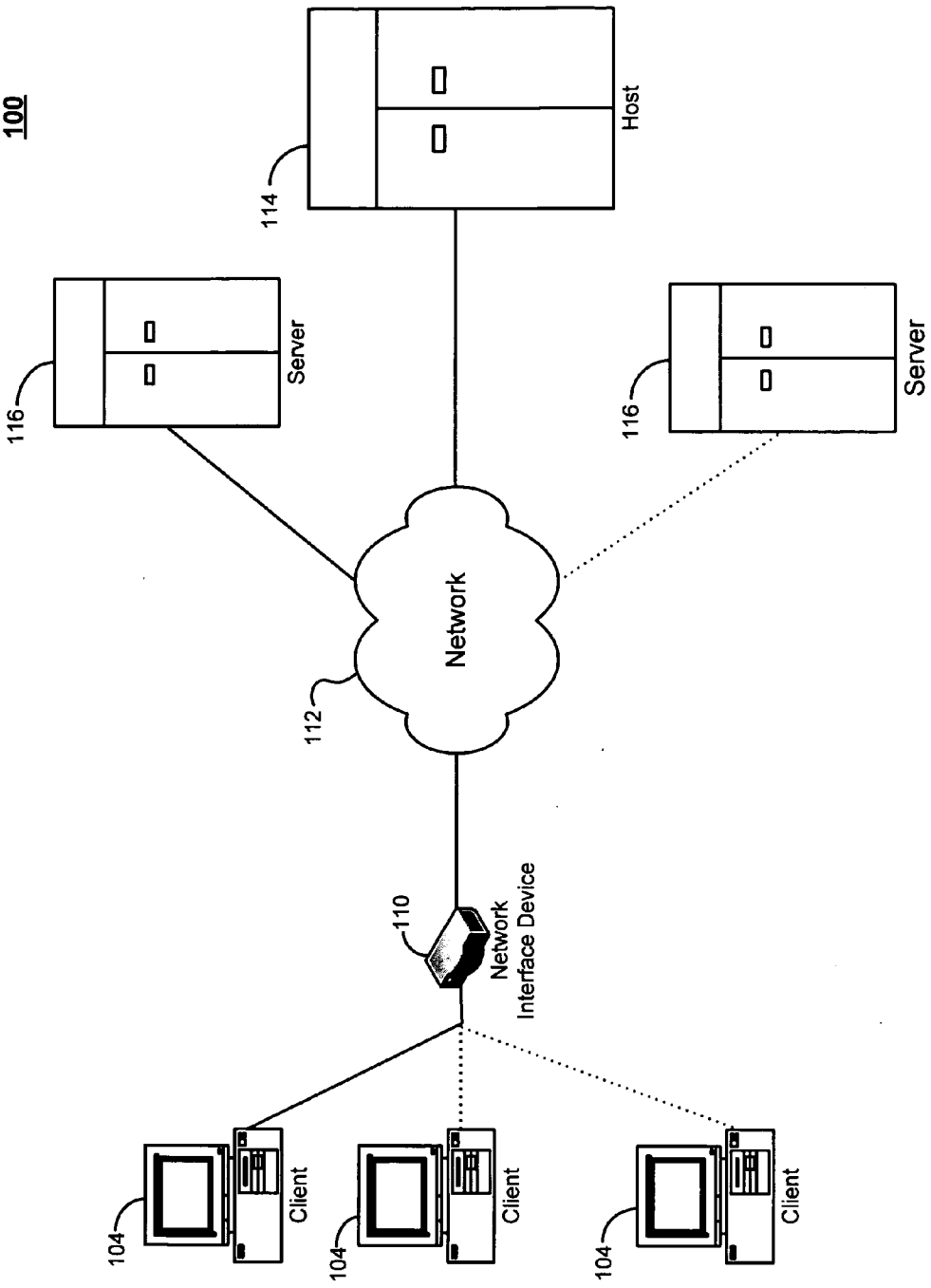

100
114
Host
116
Server
116
Server
112
Network
110
Network
Interface Device
104
Client
104
Client
104
Client

FIG. 1

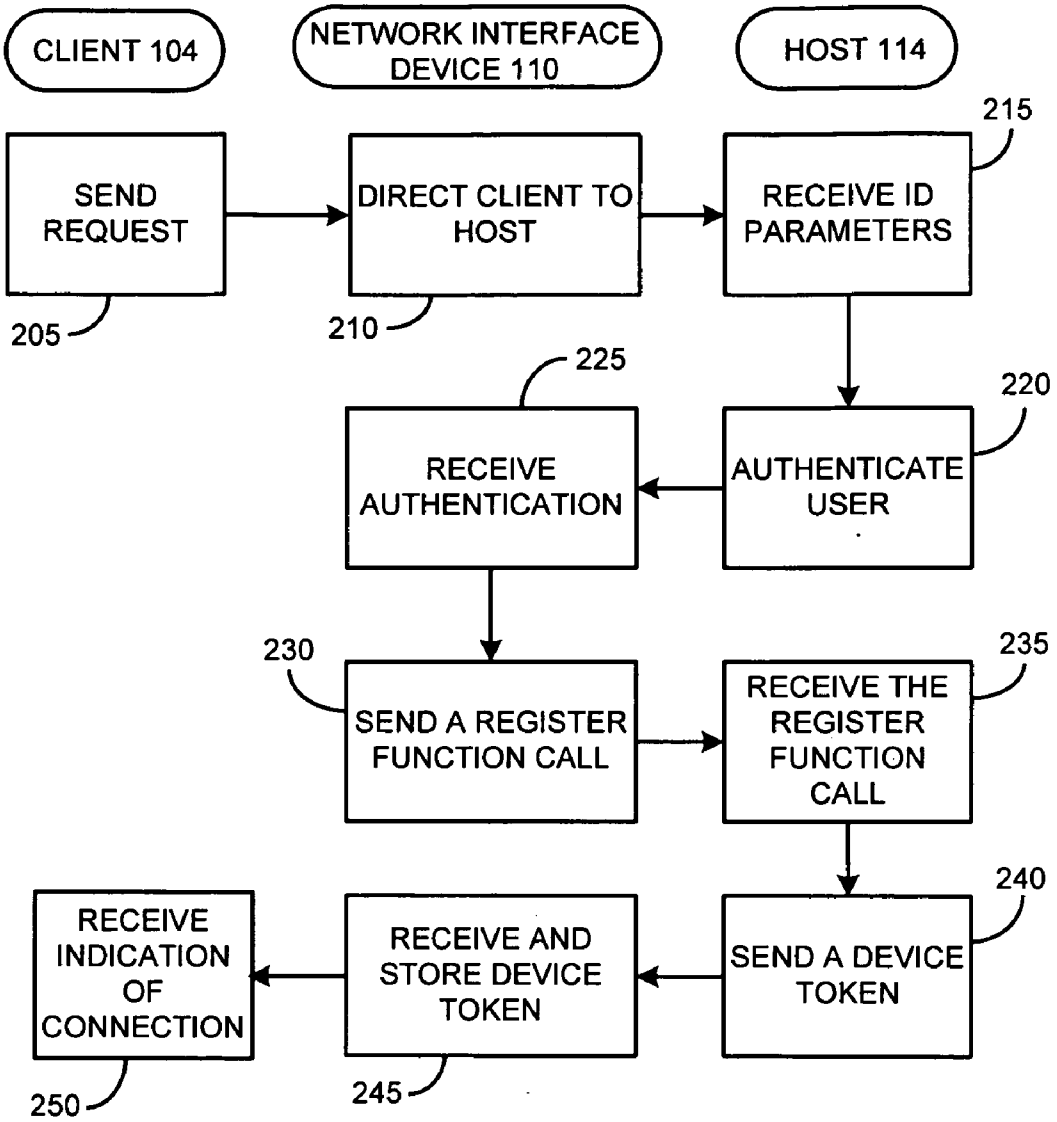

CLIENT 104
NETWORK INTERFACE DEVICE 110
HOST 114
SEND REQUEST
DIRECT CLIENT TO HOST
RECEIVE ID PARAMETERS
215
205
210
225
220
RECEIVE AUTHENTICATION
AUTHENTICATE USER
230
235
SEND A REGISTER FUNCTION CALL
RECEIVE THE REGISTER FUNCTION CALL
240
RECEIVE INDICATION OF CONNECTION
RECEIVE AND STORE DEVICE TOKEN
SEND A DEVICE TOKEN
250
245

FIG. 2

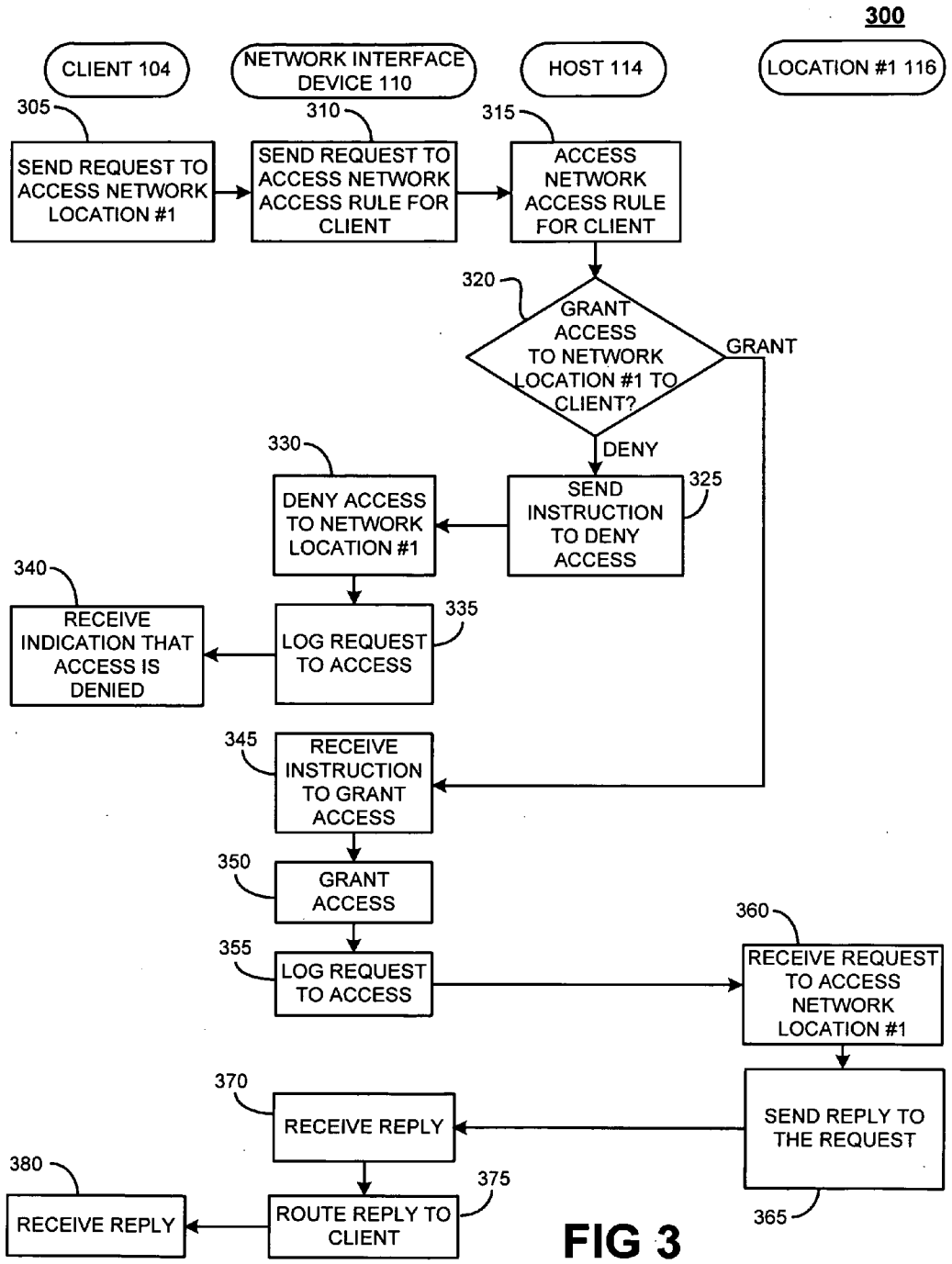

300
CLIENT 104
NETWORK INTERFACE DEVICE 110
HOST 114
LOCATION #1 116
305
SEND REQUEST TO ACCESS NETWORK LOCATION #1
310
SEND REQUEST TO ACCESS NETWORK ACCESS RULE FOR CLIENT
315
ACCESS NETWORK ACCESS RULE FOR CLIENT
320
GRANT ACCESS TO NETWORK LOCATION #1 TO CLIENT?
GRANT
DENY
325
SEND INSTRUCTION TO DENY ACCESS
330
DENY ACCESS TO NETWORK LOCATION #1
335
LOG REQUEST TO ACCESS
340
RECEIVE INDICATION THAT ACCESS IS DENIED
345
RECEIVE INSTRUCTION TO GRANT ACCESS
350
GRANT ACCESS
355
LOG REQUEST TO ACCESS
360
RECEIVE REQUEST TO ACCESS NETWORK LOCATION #1
365
SEND REPLY TO THE REQUEST
370
RECEIVE REPLY
375
ROUTE REPLY TO CLIENT
380
RECEIVE REPLY

FIG 3

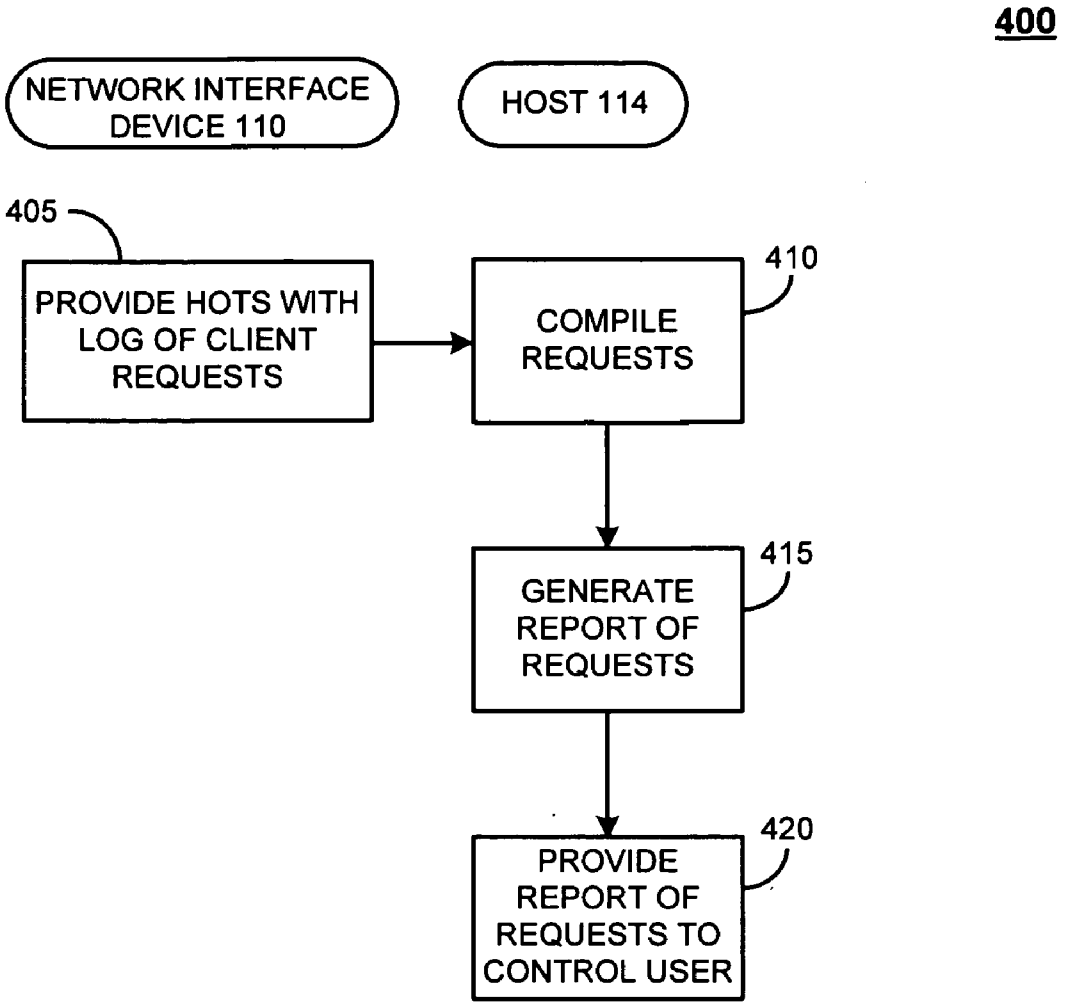

400
NETWORK INTERFACE DEVICE 110
HOST 114
405
PROVIDE HOTS WITH LOG OF CLIENT REQUESTS
410
COMPILE REQUESTS
415
GENERATE REPORT OF REQUESTS
420
PROVIDE REPORT OF REQUESTS TO CONTROL USER

FIG. 4

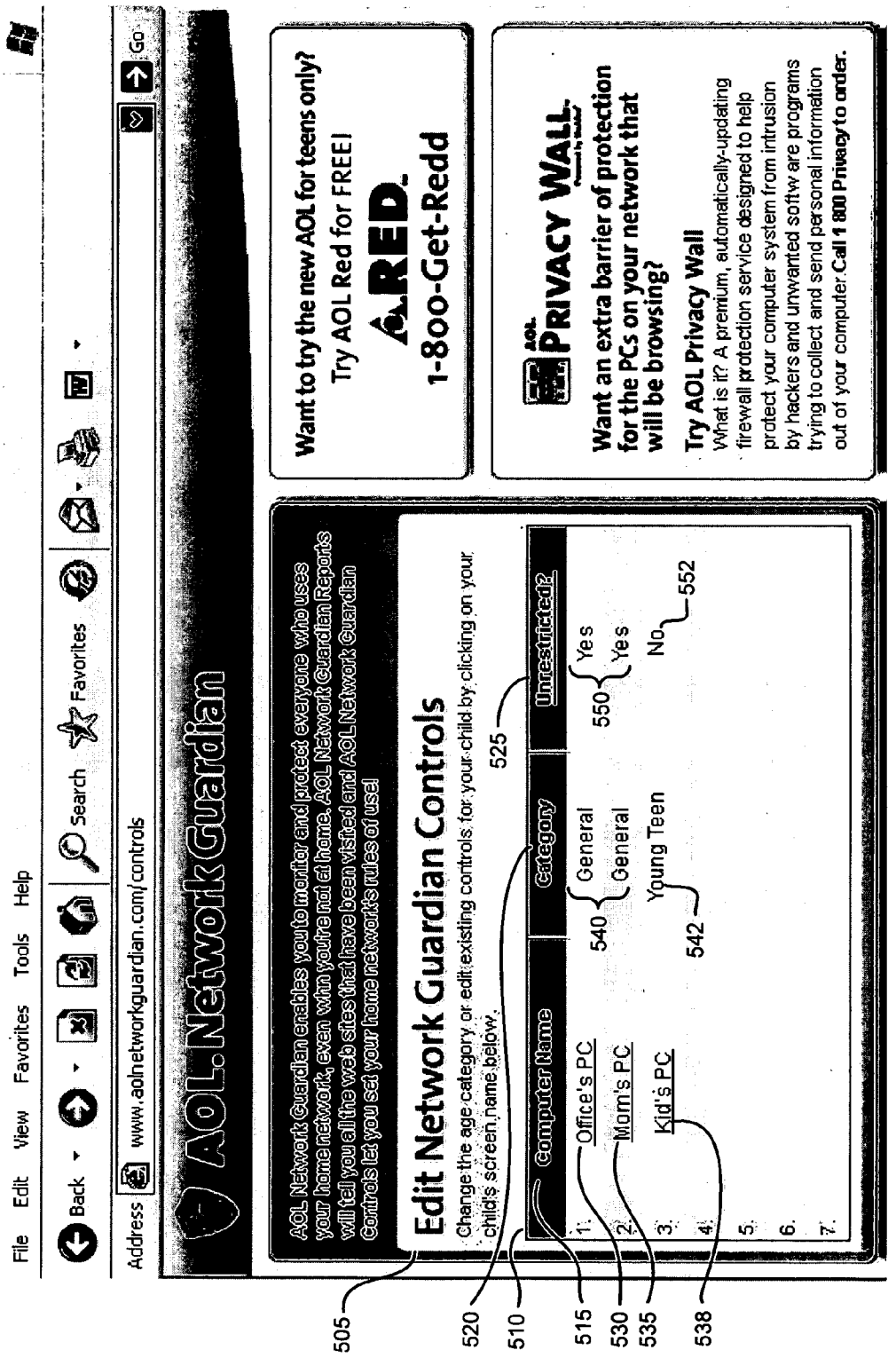

File Edit View Favorites Tools Help
Back
Search
Favorites
Address
www.aolnetworkguardian.com/controls
Go
AOL Network Guardian
AOL Network Guardian enables you to monitor and protect everyone who uses your home network, even when you're not at home. AOL Network Guardian Reports will tell you all the web sites that have been visited and AOL Network Guardian Controls let you set your home network's rules of use!
Edit Network Guardian Controls
Change the age category or edit existing controls for your child by clicking on your child's screen name below.
Computer Name
Category
Unrestricted?
1. Office's PC
2. Mom's PC
3. Kid's PC
4.
5.
6.
7.
General
General
Young Teen
Yes
Yes
No
Want to try the new AOL for teens only?
Try AOL Red for FREE!
AOL RED.
1-800-Get-Redd
AOL PRIVACY WALL
Want an extra barrier of protection for the PCs on your network that will be browsing?
Try AOL Privacy Wall
What is it? A premium, automatically-updating firewall protection service designed to help protect your computer system from intrusion by hackers and unwanted softw are programs trying to collect and send personal information out of your computer. Call 1 800 Privacy to order.
505
520
510
515
530
535
538
540
542
525
550
552

FIG. 5A

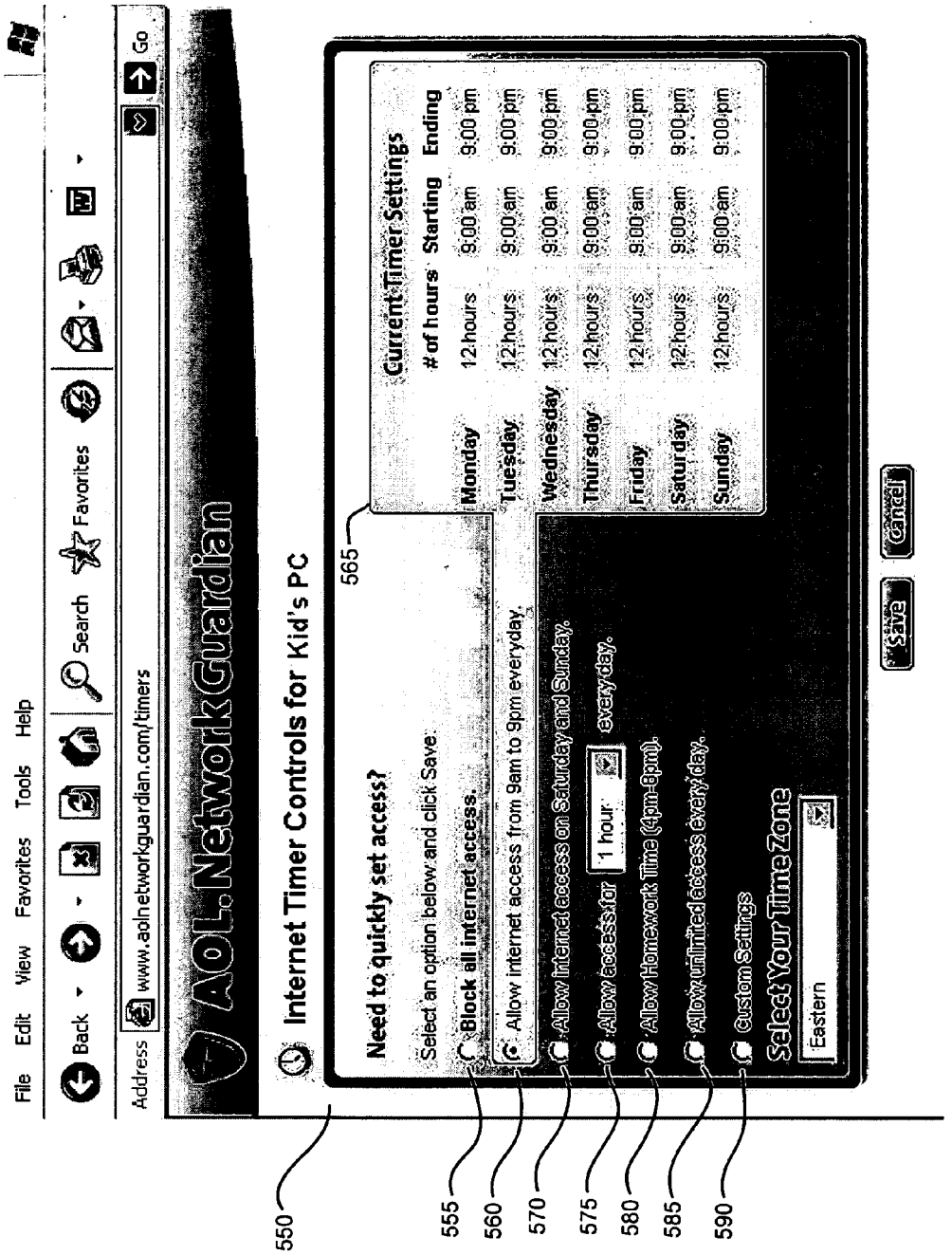

File Edit View Favorites Tools Help
Back
Search
Favorites
Address
www.aolnetworkguardian.com/timers
Go
AOL Network Guardian
Internet Timer Controls for Kid's PC
Need to quickly set access?
Select an option below and click Save:
Block all internet access.
Allow internet access from 9am to 9pm everyday.
Allow internet access on Saturday and Sunday.
Allow access for 1 hour every day.
Allow Homework Time (4pm-8pm).
Allow unlimited access every day.
Custom Settings
Select Your Time Zone
Eastern
Current Timer Settings
# of hours Starting Ending
Monday 12 hours 9:00 am 9:00 pm
Tuesday 12 hours 9:00 am 9:00 pm
Wednesday 12 hours 9:00 am 9:00 pm
Thursday 12 hours 9:00 am 9:00 pm
Friday 12 hours 9:00 am 9:00 pm
Saturday 12 hours 9:00 am 9:00 pm
Sunday 12 hours 9:00 am 9:00 pm
Save
Cancel
550
555
560
570
575
580
585
590
565

FIG. 5B

600

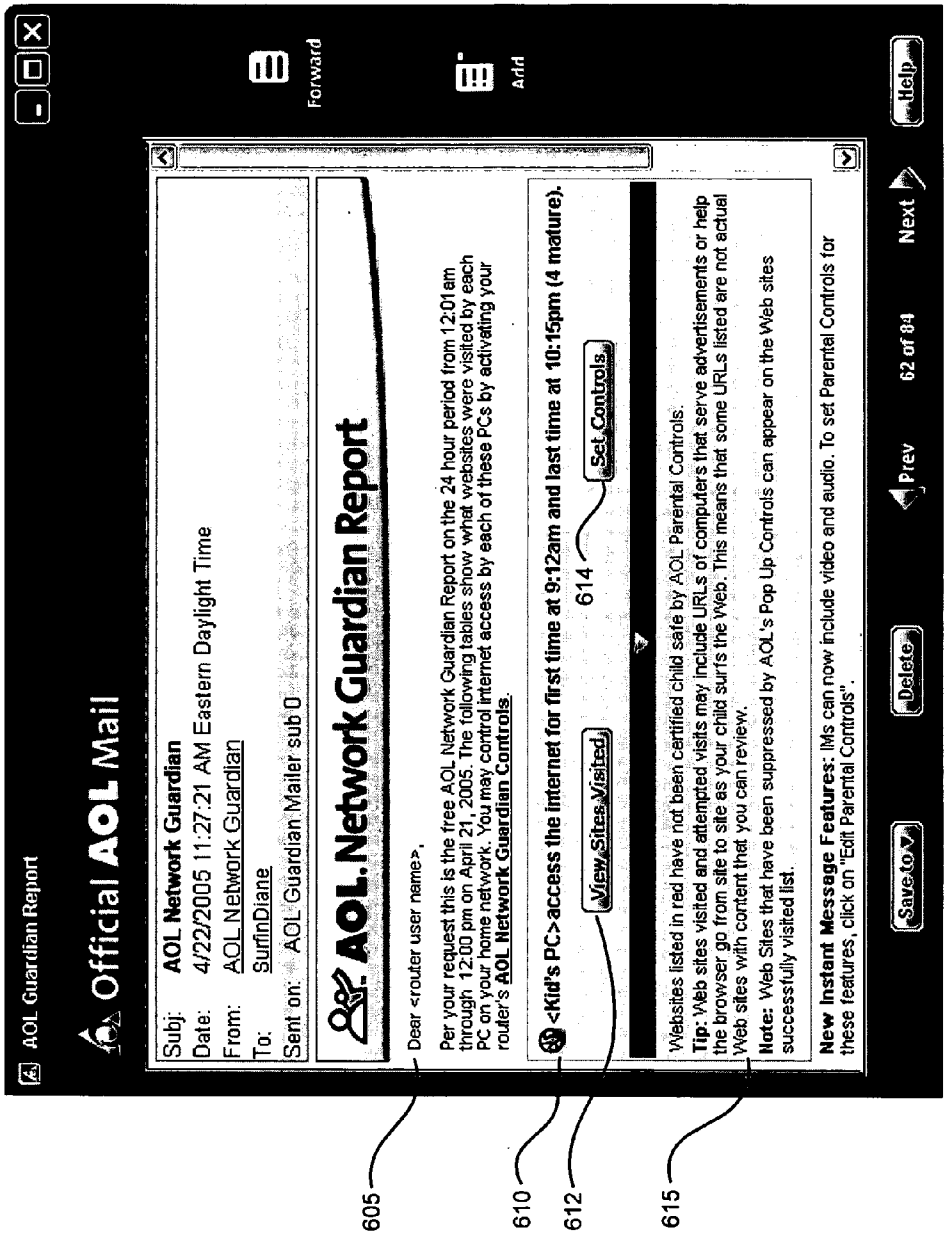

AOL Guardian Report
Official AOL Mail
Forward
Add
Subj: AOL Network Guardian
Date: 4/22/2005 11:27:21 AM Eastern Daylight Time
From: AOL Network Guardian
To: SurfinDiane
Sent on: AOL Guardian Mailer sub 0
AOL Network Guardian Report
Dear <router user name>,
Per your request this is the free AOL Network Guardian Report on the 24 hour period from 12:01am through 12:00 pm on April 21, 2005. The following tables show what websites were visited by each PC on your home network. You may control internet access by each of these PCs by activating your router's AOL Network Guardian Controls.
<Kid's PC>access the internet for first time at 9:12am and last time at 10:15pm (4 mature).
View Sites Visited
614
Set Controls
Websites listed in red have not been certified child safe by AOL Parental Controls.
Tip: Web sites visited and attempted visits may include URLs of computers that serve advertisements or help the browser go from site to site as your child surfs the Web. This means that some URLs listed are not actual Web sites with content that you can review.
Note: Web Sites that have been suppressed by AOL's Pop Up Controls can appear on the Web sites successfully visited list.
New Instant Message Features: IMs can now include video and audio. To set Parental Controls for these features, click on "Edit Parental Controls".
Save to
Delete
Prev
62 of 84
Next
Help
605
610
612
615

FIG. 6A

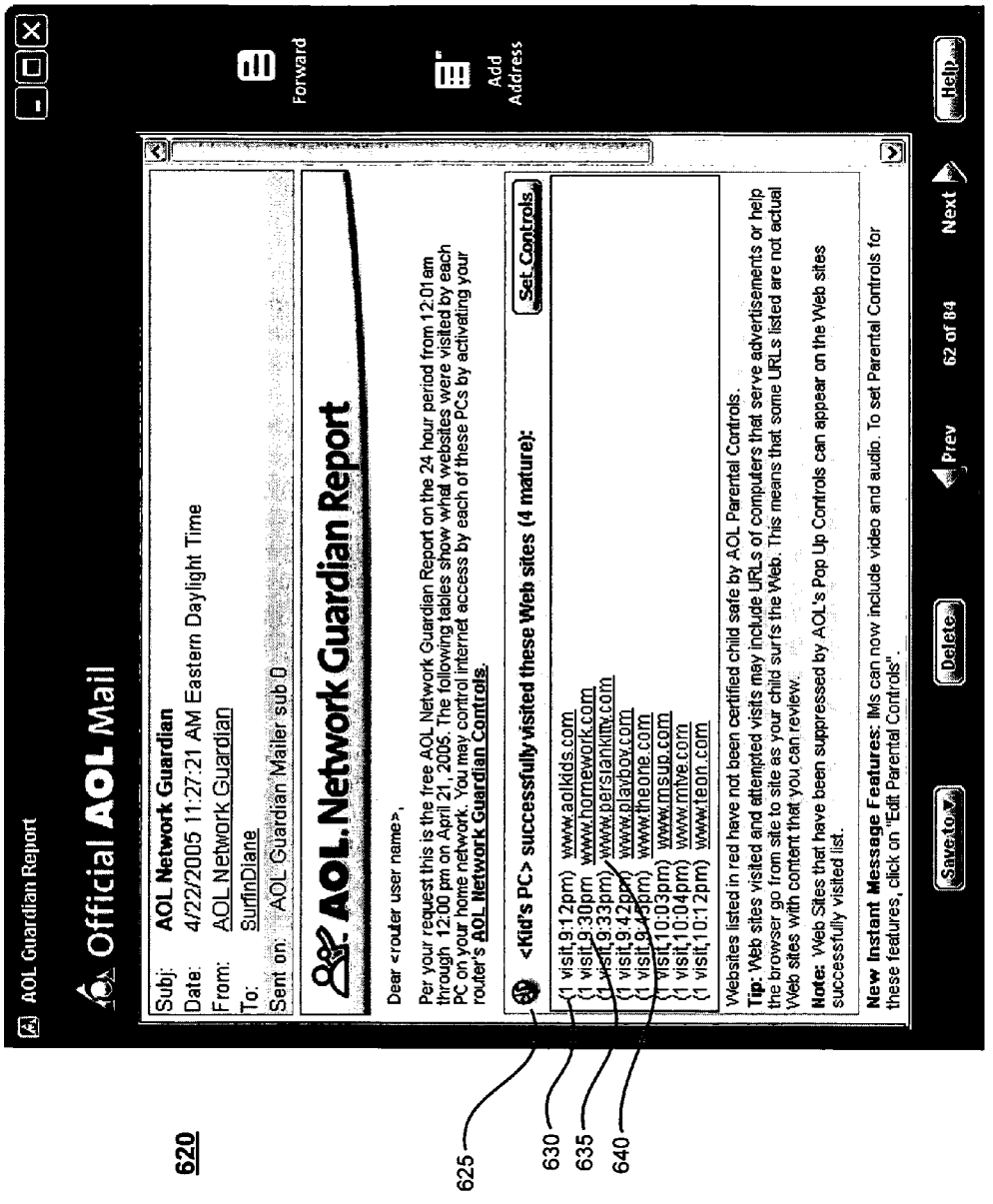

620
625
630
635
640
AOL Guardian Report
Official AOL Mail
Subj: AOL Network Guardian
Date: 4/22/2005 11:27:21 AM Eastern Daylight Time
From: AOL Network Guardian
To: SurfinDiane
Sent on: AOL Guardian Mailer sub 0
Forward
Add Address
AOL Network Guardian Report
Dear <router user name>,
Per your request this is the free AOL Network Guardian Report on the 24 hour period from 12:01 am through 12:00 pm on April 21, 2005. The following tables show what websites were visited by each PC on your home network. You may control internet access by each of these PCs by activating your router's AOL Network Guardian Controls.
<Kid's PC> successfully visited these Web sites (4 mature):
Set Controls
(1 visit,9:12pm) www.aolkids.com
(1 visit,9:30pm) www.homework.com
(1 visit,9:33pm) www.persiankitty.com
(1 visit,9:42pm) www.playboy.com
(1 visit,9:48pm) www.theone.com
(1 visit,10:03pm) www.msun.com
(1 visit,10:04pm) www.mtve.com
(1 visit,10:12pm) www.teen.com
Websites listed in red have not been certified child safe by AOL Parental Controls.
Tip: Web sites visited and attempted visits may include URLs of computers that serve advertisements or help the browser go from site to site as your child surfs the Web. This means that some URLs listed are not actual Web sites with content that you can review.
Note: Web Sites that have been suppressed by AOL's Pop Up Controls can appear on the Web sites successfully visited list.
New Instant Message Features: IMs can now include video and audio. To set Parental Controls for these features, click on "Edit Parental Controls".
Save to
Delete
Prev
62 of 84
Next
Help

FIG. 6B

650

Subj: Network Guardian
Date: 6/22/2005 11:27:21 AM Eastern Daylight Time
From: NetworkGuardian
To: SurfinDiana
Sent on: Guardian Mailer sub 0

LINKSYS Guardian Report
powered by AOL Parental Controls

Dear Admin,

Per your request this is the free AOL Network Guardian Report on the 24 hour period from 12:01am through 12:00 pm on April 21, 2005. The following tables show what websites were visited by each PC on your home network. You may control internet access by each of these PCs by activating your router's **Network Guardian Controls**.

655

Kitchen PC — Set Controls

First browsed the web at 9:09 am
Last browsed the web at 11.36 pm
Top 5 websites visited:
http://www.google.com (25 times)
http://www.friendster.com (15 times)
http://www.apple.com/itunes (10 times)
http://www.askjeeves.com (1 time)
http://www.mapquest.com (5 times)

Number of sites that may have contained mature content: 6
Click here to see full details of the day's web browsing for this PC

Office PC — Set Controls

First browsed the web at 7:29 am
Last browsed the web at 9:36 pm
Top 5 websites visited:
http://www.staples.com (5 times)
http://www.bestbuy.com (10 times)
http://www.mapquest.com (2 times)
http://www.apple.com/ipod (10 times)
http://www.google.com (20 times)

Number of sites that may have contained mature content: 10
Click here to see full details of the day's web browsing for this PC

Fred Jr's PC — Set Controls

660 First browsed the web at 3:39 pm
Last browsed the web at 10.16 pm
665 Top 5 websites visited:
http://www.mtv.com (25 times)
http://www.myspace.com (15 times)
http://www.gamersonline.com (10 times)
http://www.nickelodeon.com (5 times)
http://www.spiderman.com (25 times)
670 Number of sites that may have contained mature content: 20
675 **Click here to see full details of the day's web browsing for this PC**

Tip: Web sites visited and attempted visits may include URLs of computers that serve advertise the browser go from site to site as your child surfs the Web. This means that some URLs listed Web sites with content that you can review.

Note: Web Sites that have been suppressed by AOL's Pop Up Controls can appear on the Web successfully visited list.

Finding the perfect gift for Dad's Day is possible at Best Buy.
BEST BUY

FIG. 6C

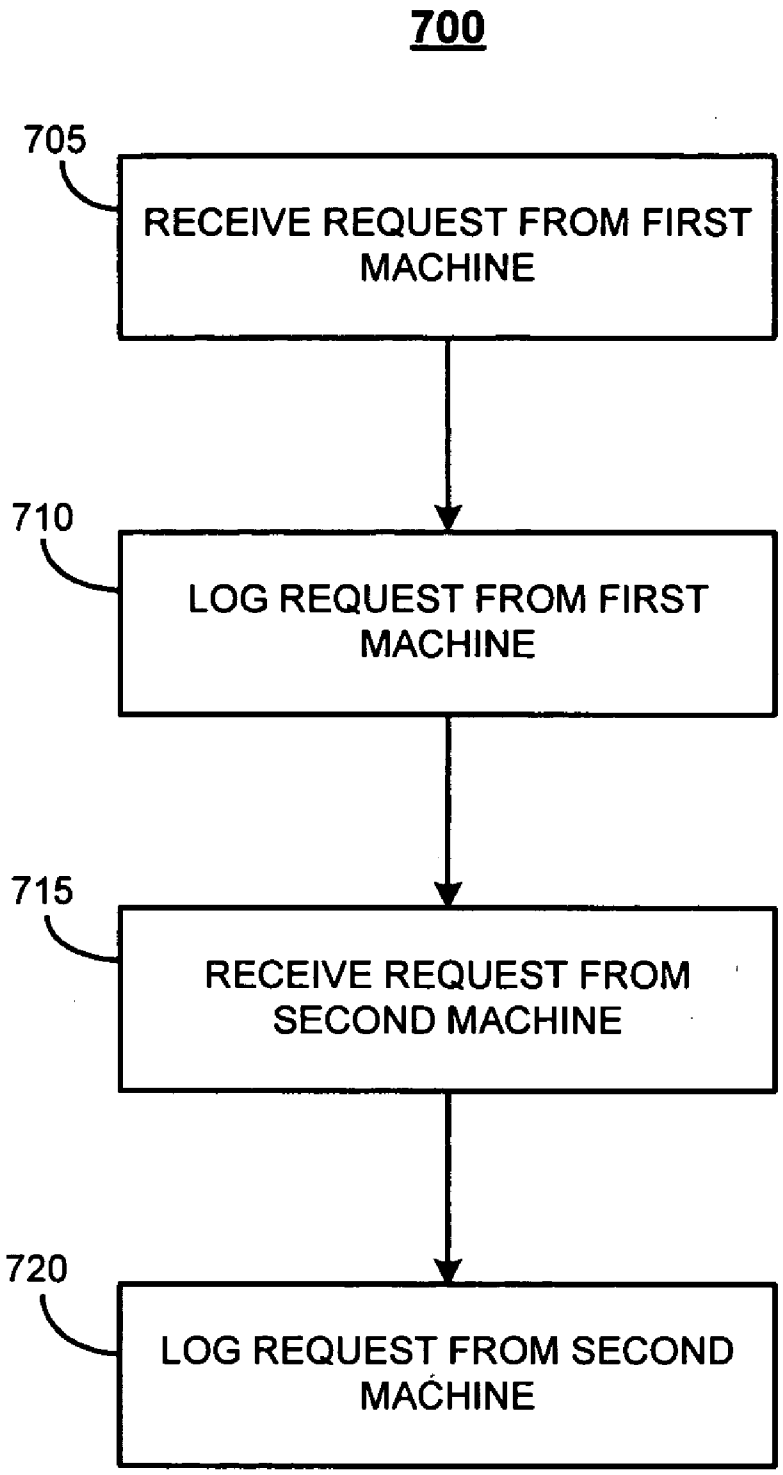

700
705
RECEIVE REQUEST FROM FIRST MACHINE
710
LOG REQUEST FROM FIRST MACHINE
715
RECEIVE REQUEST FROM SECOND MACHINE
720
LOG REQUEST FROM SECOND MACHINE

FIG. 7

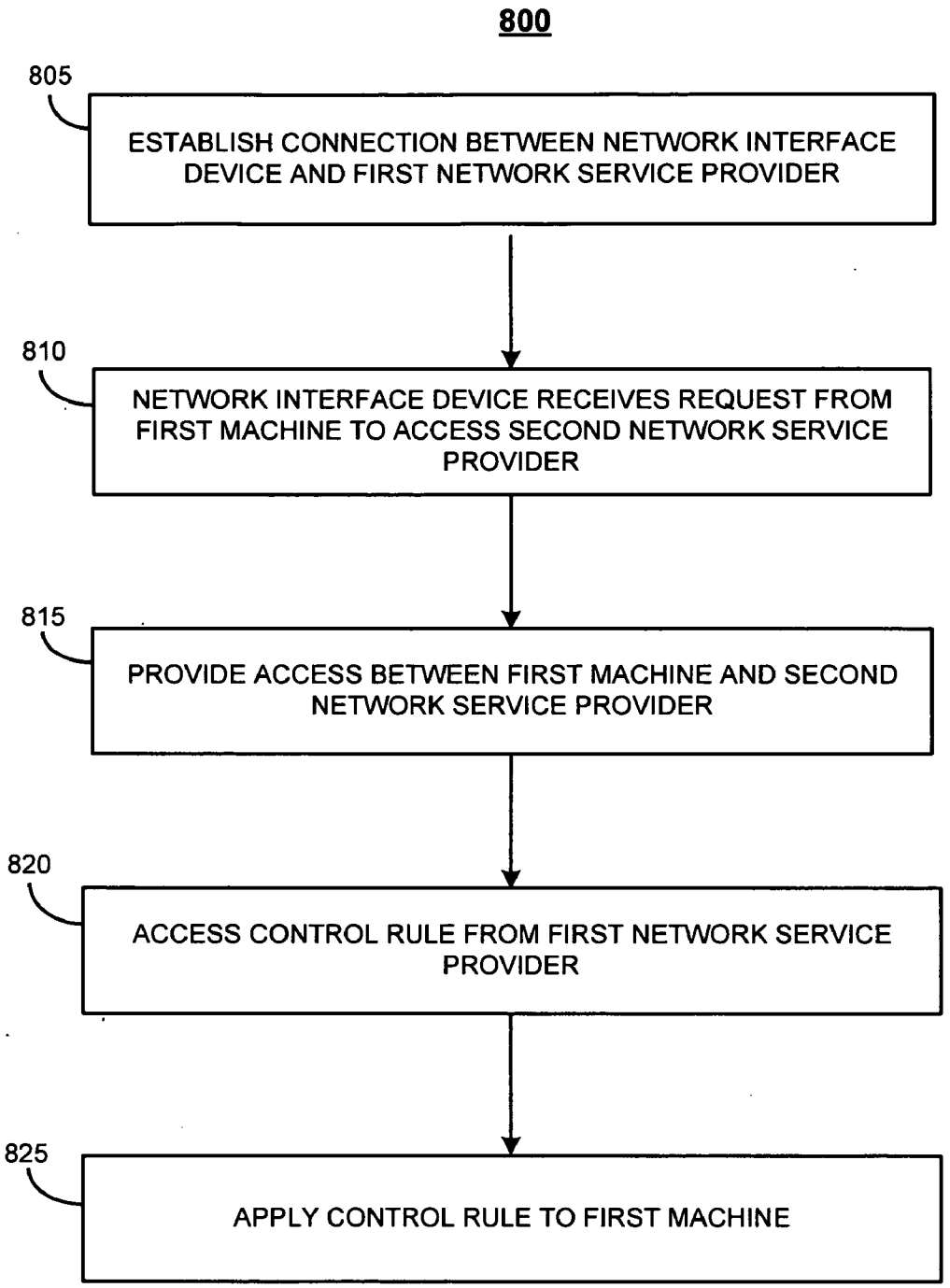

800
805
ESTABLISH CONNECTION BETWEEN NETWORK INTERFACE DEVICE AND FIRST NETWORK SERVICE PROVIDER
810
NETWORK INTERFACE DEVICE RECEIVES REQUEST FROM FIRST MACHINE TO ACCESS SECOND NETWORK SERVICE PROVIDER
815
PROVIDE ACCESS BETWEEN FIRST MACHINE AND SECOND NETWORK SERVICE PROVIDER
820
ACCESS CONTROL RULE FROM FIRST NETWORK SERVICE PROVIDER
825
APPLY CONTROL RULE TO FIRST MACHINE

FIG. 8

ROUTER-HOST LOGGING

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Provisional Application No. 60/758,986, filed Jan. 17, 2006 and titled "Router-Host Logging," which is incorporated by reference. This application claims priority to U.S. Provisional Application No. 60/686,420, filed Jun. 2, 2005 and titled "Internet Safety Device," which is incorporated by reference.

TECHNICAL FIELD

[0002] This disclosure relates, in part, to logging network communications.

BACKGROUND

[0003] Users may access content from a network, such as the Internet. In various systems, users make requests for content, using for example a browser. Systems are available to log these user requests, and provide the log to one or more interested parties. In addition to logging the requests from the users, the requests may also be screened to determine if the content that is requested is suitable for the user. If the content is deemed not to be suitable for the user, then the content may be blocked.

SUMMARY

[0004] According to a general aspect, a method includes receiving, at a network interface device at a user location, a request from a first machine located at the user location, the request including a first-machine identifier and a request to access through the network interface device a first location on a network. The method also includes logging, at the network interface device, the request from the first machine into a first-machine log for requests from the first machine, the logging into the first-machine log being based on the first-machine identifier. The method also includes receiving at the network interface device a request from a second machine located at the user location, the request from the second machine including a second-machine identifier and a request to access through the network interface device a second location on the network, and the network interface device, the first machine, and the second machine being located at a user location. The method further includes logging, at the network interface device, the request from the second machine into a second-machine log for all requests from the second machine, the logging into the second machine log being based on the second-machine identifier.

[0005] According to another general aspect, a method includes establishing a connection between a network interface device and a first network service provider having network access control rules. The method further includes receiving, at the network interface device, a request from a machine to access a second network service provider through the network interface device, the second network service provider being different from the first network service provider. The method further includes providing, by the network interface device, access between the machine and the second network service provider through the network interface device. The method further includes accessing, by the network interface device, a network access control rule from the first network service provider that governs service provided to the machine from any network service provider. The method also includes applying, by the network interface device, the network access control rule to the machine while the machine is connected with the second network service provider, to limit the service provided to the machine from the second network service provider.

[0006] According to another general aspect, a method includes receiving, at a network interface device at a user location, a request from a first machine located at the user location, the request including a first-machine identifier and a request to access through the network interface device a first location on a network. The method also includes accessing a first-machine network access rule. The method also includes determining, based on the accessed first-machine network access rule, whether to grant the first machine access to the first location on the network. The method further includes receiving at the network interface device a request from a second machine located at the user location, the request from the second machine including a second-machine identifier and a request to access through the network interface device a second location on the network, and the network interface device, the first machine, and the second machine being located at a user location. The method also includes accessing a second-machine network access rule. The method further includes determining, based on the accessed second-machine network access rule, whether to grant the second machine access to the second location on the network.

[0007] Implementations of the above general aspects may include one or more of a variety of features, such as those described elsewhere in this disclosure. Further, the claims that are listed at the end of this disclosure are to be considered as part of the specification for all purposes. Accordingly, the content of the claims is included in the specification for all purposes.

[0008] The various aspects, implementations, and features may be implemented in a variety of manners, even if only described herein in, for example, a single manner. The various aspects, implementations, and features may be implemented using, for example, one or more of: a method; an apparatus; an apparatus for performing a method; a program or other set of instructions for performing one or more aspects, implementations, or features; an apparatus that includes a program or other set of instructions; a computer readable medium; or a propagated signal. The computer readable medium or propagated signal may include, for example, instructions, software, and other data. The various aspects, implementations, and features may also include additional components, such as, for example, a computer, a router, a server, or a peripheral device.

[0009] The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

[0010] **FIG. 1** illustrates an exemplary system configured to provide network access control and logging.

[0011] **FIG. 2** illustrates an exemplary process for registering a network interface device.

[0012] **FIG. 3** illustrates an exemplary process for organizing a network interface access request.

[0013] **FIG. 4** illustrates an exemplary process for organizing an access request log report.

[0014] **FIG. 5A** illustrates an exemplary graphic user interface for configuring controls.

[0015] **FIG. 5B** illustrates an exemplary graphic user interface for configuring controls.

[0016] **FIG. 6A** illustrates an exemplary log report of access requests.

[0017] **FIG. 6B** illustrates an exemplary log report of access requests.

[0018] **FIG. 6C** illustrates an exemplary log report of access requests.

[0019] **FIG. 7** illustrates an exemplary process for providing network access control and logging.

[0020] **FIG. 8** illustrates an exemplary process for providing network access control and logging.

DETAILED DESCRIPTION

[0021] In one implementation, a system includes multiple computers in a home that are connected to a router that is also in the home. The computers access the Internet through the router, and the router keeps a log of Internet activity for each of the computers. The router uploads the log on a regular basis to a host computer on the Internet, and the host computer makes the logs available to an authorized viewer in one or more of a variety of useful formats that are configurable by the authorized viewer. The router also controls access to the Internet for each of the computers by applying access rules to determine whether to grant or to deny access to any particular Internet site that is requested at one of the computers. The access rules may be varied based on the computer or the user that is using the computer.

[0022] Referring to **FIG. 1**, system **100** is shown to be configured to provide network communication. System **100** includes several clients **104** coupled to a network interface device **110** that is coupled to a network **112**. The network **112** also is coupled to a host **114** and servers **116**. The host **114** may be configured to provide network access rules and the servers **116** may be configured to provide content for a user of client **104**. The dashed lines in **FIG. 1** indicate optional connections.

[0023] A client **104** may include devices with which the user interacts in order to send a request to access a network location. For example, a client **104** may be a personal computer, laptop, cell phone, or personal data assistant. A client **104** also, or alternatively, may include an application, a piece of software, or a set of instructions, with which the user interacts in order to send a request to access a network location. Multiple clients **104** may all be co-located in one building, home, or other user location.

[0024] A client **104** may be configured to communicate with the network interface device **110** through various methods, such as wireless networking or Ethernet cable. The network interface device **110** may include, for example, a router, and it may be utilized to link multiple clients **104** to the network **112**. The network **112** may include, for example, the Internet, and servers **116**, and the host **114** may include devices connected to the Internet.

[0025] In one implementation, system **100** is configured to provide Internet access for one or more of the clients **104**. The host **114** provides network access rules (or simply access rules) that result in the network interface device **110** granting or denying a request, received through the network **112** from a user of a client **104**, to access resources hosted at or available through servers **116**. The access rules are stored on the host **114** and may be transferred to the network interface device **110**. Access rules on the host **114** may be accessed for all requests. In other implementations, access rules on the host **114** are accessed only for some requests.

[0026] Note that the access rules may be static rules that are created once and not changed. Alternatively, the access rules may be rules that are (1) updated regularly, (2) updated automatically using, for example, new votes/ratings that are received from users, and/or (3) updated automatically using, for example, various forms of artificial intelligence.

[0027] Referring to **FIG. 2**, a process **200** involves a network interface device establishing an initial connection with a host. Process **200** focuses, in part, on establishing a connection between the network interface device and the host because later figures provide additional detail to illustrate aspects of the network interface device performing a variety of services while in communication with the host.

[0028] The process **200** may be used in conjunction with the system **100** of **FIG. 1** and, accordingly, the discussion below and **FIG. 2** itself describe the process **200** in the context of the system **100**. However, other systems may be used.

[0029] Moreover, implementations of the process **200** may be performed, for example, only one time at the initial configuration of the network interface device **110** (as indicated in the description below of the process **200**), or each time the network interface device **110** is powered on. Implementations of the process **200** may be initiated, for example, by a request for content from the client **104** (as indicated in **FIG. 2**), or by a self-initiated request for connection or configuration by the network interface device **110**. The following therefore describes one exemplary implementation of a process for establishing an initial connection with a host.

[0030] Process **200** includes the client **104** sending a request for content to the host **114** through the network interface device **110** (**205**). The request, also referred to as an initiation request, is intended to establish initial communications between the client **104** and the host **114**, and serves as a useful vehicle for prompting the network interface device **110** to establish an initial connection with the host **114** and perform configuration procedures. The initiation request may be sent, for example, automatically when the client **104** is turned on or may be sent as a result of the user manually launching a software program on the client **104**. The initiation request contains an identifier of the client **104** such as, for example, a media access control or internet protocol address.

[0031] The initiation request is received by the network interface device **110** which then directs the client **104** to the host **114** and sends to the host **114** identification parameters of the network interface device **110** (**210**). The identification parameters may be, for example, a media access control (i.e., MAC) or IP (Internet Protocol) address. The identification

parameters allow the host **114** to identify the network interface device **110** and allow the host **114** to store a profile for the network interface device **110**.

[**0032**] The host **114** receives the identification parameters (**215**) and authenticates the user (**220**). Authenticating the user (**220**) may be conducted automatically or it may require user input, such as a password or login number. A notice of authentication, which may optionally include a reservation number, is generated and then sent to the network interface device **110**. The reservation number also is associated with the network interface device **110**.

[**0033**] Upon receipt of the authentication (**225**), the network interface device **110** sends a register function call to the host **114** (**230**). The register function call may include the reservation number as well as a network interface device **110** identification number. The register function call is the mechanism by which the network interface device initially registers with the host **114** so that the host **114** will be configured to receive log reports and access rule requests from the network interface device **110**, as described in more detail below. Implementations may wait, as in the process **200**, for user authentication to be complete before sending a register function call, for security purposes. However, other implementations, for example, send a register function call without authenticating a user.

[**0034**] In response to receiving the register function call (**235**), the host **114** generates and sends a device token to the network interface device **110** (**240**). The device token is generated based on some identifying information for the network interface device **110**, such as, for example, the identification parameters earlier received (see **215**). By generating the device token based on stored information for the network interface device **110**, the host **114** is able to regenerate the device token as explained with respect to **FIG. 3** below.

[**0035**] The device token instructs the network interface device **110** to conduct a grant-or-deny procedure for each of the access requests generated by the client **104**. The network interface device **110** receives the device token and stores the device token locally on the network interface device **110** (**245**). Optionally, an indication of connection between the network interface device **110** and the host **114** based on the device token may be sent to the client **104** (**250**).

[**0036**] Establishing the initial connection of the network interface device **110** may be conducted differently or not at all. For example, the process **200** may be conducted automatically when the network interface device **110** first establishes a connection to the network **112**. In another implementation, a user may initiate the process **200** by manually selecting initiation options on the client **104**, in which case the selection options are later sent to the host **114** through the network interface device **110**.

[**0037**] Various system configuration options may be configured by a user during initiation, such as during the authentication of the user (**220**), which may be interactive between the user and the host **114**. The configuration options may allow the user to limit access through the network interface device **110** to the host **114** or one or more servers **116**, which represent locations accessible through the network **112**. Such configuration options may apply to all clients **104** connected to the network interface device **110**. The configuration options may allow access to be limited based on, for example, network locations, time of day, bandwidth, or content. Upon receiving a request for content from a client **104**, the network interface device **110** may access the configuration options on the host **114** and make a decision to grant or deny access to the requested content.

[**0038**] Referring to **FIG. 3**, a process **300** includes a network interface device **110** granting or denying an access request from a client **104**. The process **300** may be used in conjunction with the system **100** of **FIG. 1**, and the discussion below and **FIG. 3** itself describe the process **300** in the context of the system **100**. However, other systems may be used.

[**0039**] Process **300** includes a client **104** sending a request to access network location #**1** (**305**). The access request is generated when, for example, the user navigates to a website or launches a file sharing program. The access request contains an identifier of the client **104** such as a MAC or IP address. The access request is sent to the network interface device **110** which in turn sends a request to the host **114** to access network access rules for the client **104** (**310**). The network access rules contain information pertaining to a particular machine (the client **104**) and enable a determination of a grant-or-deny decision.

[**0040**] In sending the request to access network access rules, the network interface device **110** includes its device token as well as some additional descriptive information, such as, for example, the identification parameters provided to the host **114** in the process **200**. The host **114** receives the request for network access rules, including the device token and the additional descriptive information. The host **114** then verifies the device token by generating the device token again based on the additional descriptive information. In this way, the network interface device **110** must have its device token as well as the particular additional descriptive information in order to be recognized and serviced by the host **114**. The verification, by the host **114**, of the device token provides a security measure that other implementations need not provide or may provide in a different manner.

[**0041**] The host **114** accesses the access rules pertaining to the client **104** (**315**). Using the accessed rules, the host **114** determines whether to grant or deny access to network location #**1** to the client **104** (**320**).

[**0042**] If a decision to deny access is determined (**320**), instructions to deny client **104** access to network location #**1** are sent to the network interface device **110** (**325**). The instructions to deny access are commands that instruct the network interface device **110** not to deliver content at network location #**1**. The network interface device **110** denies the client **104** access (**330**) by, for example, canceling the request for access from the client **104**, and generates a log of the request from the client **104** to access network location #**1** (**335**). An indication that access to network location #**1** has been denied is sent to, and received (**340**) by, the client **104** (**340**).

[**0043**] If a decision to grant access is determined (**320**), instructions to grant access to network location #**1** are sent to, and received by (**345**), the network interface device **110**. The instructions to grant access are commands that instruct the network interface device **110** to deliver the content at network location #**1**. The network interface device **110**

grants the client **104** access (**350**) by, for example, approving the request, and generates a log of the request by the client **104** to access network location #**1** (**355**). The request to access network location #**1** is sent to network location #**1** (**365**). A reply, to the request to access, which includes content from location #**1116**, is generated by network location #**1** and is sent to the network interface device **110** (**365**). The reply from location #**1116** is received by the network interface device **110** (**370**) and is routed by the network interface device **110** to the client **104** (**375**). The client **104** receives the reply to the request (**380**).

[**0044**] The previous description is an example implementation of the grant-or-deny process **300** and other or different operations may be included. For example, logging of the access requests may be performed by the host **114** and determining whether to grant-or-deny access may be performed at the network interface device **110**. Multiple clients **104** used by different users may concurrently be involved in separate grant-or-deny processes **300** through the network interface device **110**.

[**0045**] Referring to **FIG. 4**, a process **400** may be used for organizing an access request log report. The process **400** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below, as well as **FIG. 4** itself, describe the process **400** in the context of the system **100**. However, other systems may be used. In one implementation, the process **400** is carried out once per week. In other implementations, the process **400** is carried out after every grant-or-deny decision is determined.

[**0046**] In process **400**, a network interface device **110** provides a log of requests from the client **104** to the host **114** (**405**). The log of requests from the client **104** includes data associated with the access requests and the grant-or-deny decision accompanying each access request. The log tracks all requests from the client **104** regardless of which user may have been using the client **104**.

[**0047**] The host **114** receives and compiles the log of requests (**410**). Compiling the requests includes processing to simplify data such as, for example, combining access requests into a group associated with all access requests for a particular network location.

[**0048**] A report of the log of requests is generated by the host **114** (**415**). The report is provided to a user having the appropriate rights to view the report (**420**). Such a user is referred to as a control user. The report contains information described in the compiled requests and may be provided in various forms, such as, for example, in a webpage or an email.

[**0049**] Implementations may perform the operation of providing the host **114** with logs of requests (**405**) multiple times prior to the host **114** generating a report of the log of requests. For example, the network interface device **110** may provide a log of requests for the client **104** to the host **114** (**405**) after every request for content from the client **104**, or every few seconds so as, for example, not to unnecessarily consume bandwidth at critical times. Further, the host **114** may receive the numerous logs, but only generate the log of requests (**415**) once every twenty-four hours, or whenever specifically requested by an authorized user. Note that the generated report may be provided automatically to an authorized user by, for example, the host **114** sending the report by e-mail automatically every twenty-four hours.

[**0050**] The previous description is an example implementation of organizing an access request log report. Other, or different, operations may be included. For example, the compiling of requests (**410**) for the client **104** and the generation of a report of the log of requests (**415**) may be conducted at the network interface device **110** instead of the host **114**.

[**0051**] Referring to **FIG. 5***a*, a graphic user interface (GUI) **500** for configuring controls is illustrated. The GUI **500** may be an interface to controls on, for example, one or more of the host **114** or the network interface device **110**. The GUI **500** may be used in connection with the system **100** of **FIG. 1** and the discussion below describes the GUI **500** in the context of the system **100**. However, other systems may be used

[**0052**] The GUI **500** includes edit instructions **505** and a client table **510**. The client table **510** includes a computer name list **515**, a category list **520**, and a restriction decision list **525**.

[**0053**] The edit instructions **505** include instructions pertaining to available control options and direct the user to available configuration options in the client table **510**. The client table **510** describes the client **104** profiles that are associated with the network interface device **110**.

[**0054**] Client **104** profiles may be associated with the network interface device **110** in various ways. For example, merely by entering a particular client **104** profile in the GUI **500**, the particular client **104** profile (as well as the particular client **104**) may be associated with the network interface device **110**. Alternatively, or in addition, a particular client **104** profile (or, in some implementations, the particular client **104**) may be associated with the network interface device **110** by having the network interface device **110** automatically associate those clients **104** that are in communication with the network interface device **110** to access content over the network **112**. Alternatively, or in addition, consent from a particular client **104** may be required before associating the particular client **104** with the network interface device **110**.

[**0055**] Note that the network interface device **110** may still apply access rules (and/or logging) to a client **104** that is not associated with the network interface device **110**. For example, the network interface device **110** may apply access rules from a profile designated for "non-associated clients **104**," or may apply default access rules that may apply to any client **104** (associated or not) for which a profile has not designated a specific category list **520** and/or a specific restriction decision list **525**. The network interface device **110** also, or alternatively, may apply no access rules and allow access to all requested content, or may allow no access to any requested content. Further, the network interface device **110** may apply access rules (and/or logging) to a client **104**, whether associated with the network interface device **110** or not, regardless of whether the client **104** has, for example, (1) received an Internet Protocol address from the network address device **110** or (2) self-generated an Internet Protocol address.

[**0056**] The client table **510** displays the client profile that includes the computer name list **515**, the category list **520**, and the restriction decision list **525**. The computer name list **515** lists the names of the clients **104**. The category list **520**

lists the assigned categories of user access level. The assigned category of user access level is associated with predetermined network access rules, as described below. The restricted decision list **525** reflects whether a client **104** is granted unrestricted access for all access requests.

[**0057**] The computer name list **515** shows that three devices (three clients **104**) are controlled by the table **510** and are associated with the network interface device **110**. The computer name list **515** includes an Office's PC **530**, a Mom's PC **535**, and a Kid's PC **538**. Office's PC **530** and Mom's PC **535** both are listed as having the category list **520** entry of "general"**540**. Because both Office's PC **530** and Mom's PC **535** are associated with the same category, the network access rules associated with both clients are identical. The restricted decision for the general category **540** is unrestricted **550**. All access requests will be granted for all users of either office's PC **530** or Mom's PC **535**.

[**0058**] In contrast, however, Kid's PC **538** has a category of Young Teen **542** with a restricted decision list **525** of "No"**552**. The "No"**552** indicates that the Kid's PC **538** is restricted, and the category of Young Teen **542** indicates that content not suitable for a young teen will be blocked for all users on Kid's PC **538**.

[**0059**] The previous description is an example implementation of the GUI **500** for configuring controls, and other or different features may be included. For example, other details may be included in the client table **510** such as a numbered restriction level associated with a predetermined scale of restrictions.

[**0060**] Referring to **FIG. 5***b,* a GUI **550** for configuring controls is illustrated. The GUI **550** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below describes the GUI **550** in the context of the system **100**. However, other systems may be used.

[**0061**] The GUI **550** includes various access control options for a client **104**, specifically the Kid's PC **538**.

[**0062**] Included in the access control options are various options that determine when, or how long, Internet access may be granted to a user of client **104**. The options include (i) an option **555** to block all Internet access, which never allows an access request, (ii) an option **560** to allow Internet access by time of day which may grant an access request during predetermined times of specified days, (iii) an option **570** to allow Internet access on particular days only (Saturday and Sunday are shown in **FIG. 5B**), (iv) an option **575** to allow Internet access for a specified amount of time each day (1 hour is shown in **FIG. 5B**), (v) an option **580** to allow homework time, which may grant access requests from 4 pm-8 pm to allow use of the Internet for homework, or may block access requests from 4 pm-8 pm so that a user will not be distracted from homework, (vi) an option **585** to allow unlimited access every day, and (vii) an option **590** to allow custom settings, which may grant access requests according to a combination of the above access control options and/or access control options other than those previously mentioned.

[**0063**] After selecting access control options, sub-options are displayed. For example, after selecting the option **560** to allow Internet access by time of day, a chart **565** of days of the week and allowable access times is displayed. The chart **565** allows a user to select sub-options available for the access control options.

[**0064**] The previous description is an example implementation of the GUI **550** for configuring controls, and other or different access control options may be included. For example, an option may allow access when the control user is online using Kid's PC **538**, thus providing an override of the standard access rules. As another example, an option may block all clients **104** that do not have a profile, thus precluding an unidentified machine from using the network interface device **110** to access content.

[**0065**] Referring to **FIG. 6***a,* a log report of access requests **600** is illustrated. The log report of access requests **600** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below describes the log report of access requests **600** in the context of the system **100**. However, other systems may be used.

[**0066**] The log report of access requests **600** includes a log introduction **605**, a client options section **610**, and a further information section **615**. The log introduction **605** describes current log options such as the periodicity of the report generation. The client options **610** includes options that are directed towards information in the log report of access requests **600** that the user may choose to view. The further information section **615** includes other information deemed appropriate to the log report **600**. For example, the further information section **615** may include notes and tips specific to information contained in the log report **600**.

[**0067**] The client options section **610** includes options that enable the user to view different types of information. The client options section **610** relates to the client Kid's PC **538**. The client options section **610** includes a selection **612** to view sites visited by Kid's PC **538** during the selected duration of the log report of access requests **600**. The client options section **610** also includes a selection **614** to set controls, allowing the user to set or change access control options for Kid's PC **538**.

[**0068**] The previous description is an example implementation of the log report of access requests **600** for configuring controls, and other or different access control options may be included. The report can be accessed in a variety of ways, such as by email or a webpage. The report can be sent periodically or continuously as the access requests are received. The log report of access requests **600** may also show information pertaining to denied or granted access requests. The log report of access requests **600** may include information pertaining to multiple clients **104** or may be generated for each client **104**.

[**0069**] Referring to **FIG. 6***b,* a portion **620** of the log report of access requests is illustrated that shows sites visited by Kid's PC **538**. The portion **620** is displayed in response to an user selecting option **612** to view the sites visited by Kid's PC **538**. The portion **620** includes a client log **625**. The client log **625** includes a number of visits, such as, for example, an entry **630** showing one visit to www.aolkids.com at 9:12 pm. Each entry (e.g., entry **630**) includes a frequency **635** showing the number of times a client **104** has accessed a particular URL, a time **635** showing the time of day at which the client **104** accessed the particular URL, and a location **640** showing a URL for the web address of the network location accessed by the client **104**.

[**0070**] The previous description is an example implementation of the portion **620** showing sites visited. The portion

620 may display information for multiple clients **104** in separate client logs **625** or together as one client log **625**. The information within the client log **625** may detail a summary of access requests such as the most frequently accessed sites or the most mature sites. The portion **620** may also show information pertaining to denied access requests.

[**0071**] Referring to **FIG. 6***c*, a log report of access requests **650** for multiple clients is illustrated. The log report of access requests **650** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below describes the log report of access requests **650** in the context of the system **100**. However, other systems may be used.

[**0072**] The log report of access requests **650** includes a multiple client log **655**. The multiple client log **655** includes a time feature **660** showing the time of the first and last browsing of the web. The multiple client log **655** also includes a list **665** of the top five websites visited, an indicator **670** of the number of mature sites viewed, and an option **675** to view full details of the browsing activity.

[**0073**] The time feature **660** indicates the time of the first access request during the time period of the log report of access requests **650** and the time of the last access request during the time period of the log report of access requests **650**. The list **665** of the top five websites visited indicates the five websites which had the most access requests generated by the client **104** during the time period of the log report of access requests **650**. The top five websites may be displayed, for example, in order of most recently visited. The indicator **670** of the number of mature sites viewed indicates the total number of access requests for mature sites by the client **104** during the time period of the log report of access requests **650**. The option **675** to expand details enables a user to view further details included within the log report of access requests **650**.

[**0074**] Implementation of the log report of access requests **650** may vary. For example, the log report of access requests **650** may also show information pertaining to denied access requests.

[**0075**] Referring to **FIG. 7**, a process **700** is illustrated for providing network access control and logging. The process **700** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below describes the process **700** in the context of the system **100**. However, other systems may be used.

[**0076**] In the process **700**, a network interface device **10** at a user location receives (**705**) a request from a first machine **104** at the user location. The request may include a first-machine identifier and a request to access through the network interface device **110** a first location on a network. In one implementation, receiving the request (**705**) is analogous to receiving the request sent in operation **305** of process **300**

[**0077**] The network interface device **110** logs the request from the first-machine **104** into a first-machine log for requests from the first machine (**710**). The log into the first-machine log is based on the first-machine identifier. In one implementation, logging the request (**710**) is analogous to operation **355** of process **300**.

[**0078**] The network interface device **110** at the user location receives a request from a second machine **104** at the user location (**715**). The request includes a second-machine identifier and a request to access through the network interface device **110** a second location on the network. In one implementation, receiving the request (**715**) is analogous to operation **705**.

[**0079**] The network interface device **110** logs the request from the second-machine **104** into a second-machine log for requests from the second machine (**720**). The log into the second-machine log is based on the second-machine identifier. In one implementation, logging the request (**720**) is analogous to operation **355** of process **300**.

[**0080**] The process **700** may, but need not, include performing access control. Analogously, implementations may perform a process that performs access control without logging, such as, for example, by performing the process **400** without performing logging operations **335** or **355**.

[**0081**] Referring to **FIG. 8**, a process **800** is illustrated for providing network access control and logging. The process **800** may be used in conjunction with the system **100** of **FIG. 1** and the discussion below describes the process **800** in the context of the system **100**. However, other systems may be used.

[**0082**] Process **800** includes establishing a connection between a network interface device **110** and a first network service provider (**805**). The network service provider includes network access control rules.

[**0083**] The network interface device **110** receives a request from a first machine **104** to access a second network service provider through the network interface device **110** (**810**). The second network service provider is different from the first network service provider.

[**0084**] Process **800** includes providing, through the network interface device **100**, access between the machine **104** and the second network service provider (**815**). The network interface device **110** accesses a control rule from the first network services provider that governs service provided to the machine **104** from any network service provider (**820**). The network interface device **110** applies the access control rule to the machine **104** while the machine **104** is connected with the second network service provider in order to limit the service provided to the machine **104** from the second network service provider (**825**).

[**0085**] In one implementation of process **800**, a client device connects to the Internet through a router at a user location. The client device requests content through an Internet Service Provider (ISP). The router, on the other hand, governs access based on rules and information stored with a host computer that is remote and distinct from the ISP. Thus, two logical connections are used-one between the client device and the ISP, and one between the router and the host.

[**0086**] Another example of an implementation according to process **800** involves a home that includes a PC and a wireless router, in wireless communication with each other. The router connects to the Internet and provides access, for the PC, to content on the Internet. The access is typically provided through a host, and the host also stores network access rules that are used to govern access to online content from any computer that connects to the Internet through the router. In practice, the users at the PC would ordinarily

log-in to the host, and access to the Internet would be provided through the host. The router communicates with the host to access the rules and determine, based on the rules, whether or not to allow access to the requested content. In this scenario (other scenarios and implementations may differ), the host provides access to the Internet without screening, and relies on the router to do the screening based on the access rules stored on the host. In this example, however, the router also is able to log and screen content requests from a computer that during its offline operation and during operations not involving the host.

[0087] For example, a father may set up the host account to block objectionable content for all users of the PC at home. However, a son's friend may come over to the house with a laptop and use the wireless router to access the Internet through an Internet Service Provider (ISP) other than the host, such that the friend does not log-in to the host. In this case, the router still does communicate with the host to determine what access rules to apply to the presumably unrecognized laptop. The router also is able to apply those rules to the laptop even though the laptop does not use the host to get to the Internet. Accordingly, the router logs the friend's attempt to access objectionable content, and/or blocks the friend's attempt to access objectionable content (so that the content is not delivered through the router to the laptop). Additionally, the father can access a log report that will indicate the exact websites that the friend attempted to access, the number of times the friend attempted to access those websites, and the times of day at which the attempts were made.

[0088] Referring again to **FIG. 1**, other implementations of the system **100** may provide that the server **116** is accessible through the host **114**, with or without being directly accessible from the network **112** without going through the host **114**.

[0089] Referring again to **FIG. 3**, other implementations of the process **300** include storing the grant/deny decision for a particular network location so that subsequent requests from a user to access the particular network location can be decided by accessing the stored decision. Further implementations of **FIG. 3** also provide a bypass option so that the access rules for a given client are not applied to an authorized user. For example, the client may provide on an Internet browser an option labeled "bypass" that, when selected, allows an authorized user to enter a password. After the authorized user is verified, the network interface device no longer applies the normal access rules for that client but, rather, applies no rules at all or applies another set of rules that applies to the authorized user.

[0090] Referring again to **FIGS. 6***a-c,* other implementations may allow an authorized user to tailor the log reports so that reports for each client have a different format, or reports for each user have a different format.

[0091] As is evident from the breadth of the disclosure, implementations, features, and techniques described herein, as well as variations or combinations of them, may be implemented at least in part, for example, in an operating system or in a stand-alone application or utility, running on one or more of a variety of devices. Such devices may include, for example, a personal computer, a server, a router, a gateway, or a special-purpose computer or machine. A device also may include, for example, discrete or integrated hardware, firmware, and software. A device may include, for example, a processor, which refers to processing devices in general, including, for example, a microprocessor, an integrated circuit, a programmable logic device, and a device containing a software application.

[0092] Such a device may be configured to perform one or more processes. For example, implementations may be embodied in a device that includes one or more computer readable media having instructions for carrying out one or more processes. The computer readable medium may include, for example, a storage device such as, for example, a hard disk, a compact diskette, a random access memory ("RAM"), and a read-only memory ("ROM"). A computer readable medium also may include, for example, formatted electromagnetic waves encoding or transmitting instructions. Instructions may be, for example, in hardware, firmware, software, and in an electromagnetic wave. Instructions may be found in, for example, an operating system, a separate application, or a combination of the two. A processor may be, for example, both a device configured to carry out a process and a device including computer readable media having instructions for carrying out a process.

[0093] A number of implementations have been described. Nevertheless, it will be understood that various modifications may be made. For example, elements of different implementations may be combined, supplemented, modified, or removed to produce other implementations. Further, various technologies may be used, combined, and modified to produce an implementation. Accordingly, other implementations are within the scope of the following claims

What is claimed is:

1. A method comprising:

receiving, at a network interface device at a user location, a request from a first machine located at the user location, the request including a first-machine identifier and a request to access through the network interface device a first location on a network;

logging, at the network interface device, the request from the first machine into a first-machine log for requests from the first machine, the logging into the first-machine log being based on the first-machine identifier;

receiving, at the network interface device, a request from a second machine located at the user location, the request from the second machine including a second-machine identifier and a request to access through the network interface device a second location on the network, where the network interface device, the first machine, and the second machine are located at a user location; and

logging, at the network interface device, the request from the second machine into a second-machine log for requests from the second machine, the logging into the second-machine log being based on the second-machine identifier.

2. The method of claim 1 further comprising:

accessing a first-machine network access rule;

determining, based on the accessed first-machine network access rule, whether to grant the first machine access to the first location on the network;

accessing a second-machine network access rule; and

determining, based on the accessed second-machine network access rule, whether to grant the second machine access to the second location on the network.

3. The method of claim 1 wherein receiving the request from the second machine comprises receiving the request from the second machine while the network interface device is coupled to both the first machine and the second machine.

4. The method of claim 1 further comprising:

receiving, at the network interface device, a second request from the first machine, the second request from the first machine including the first-machine identifier and a request to access through the network interface device a third location on a network; and

logging, at the network interface device, the second request from the first machine into the first-machine log, the logging into the first-machine log being based on the first-machine identifier; and wherein:

the first request from the first machine is sent using a first user identity that is logged in to a first account in a network service provider, and

the second request from the first machine is sent using a second user identity that is logged in to a second account in the network service provider.

5. The method of claim 4 further comprising:

accessing a first-machine network access rule;

determining, based on the accessed first-machine network access rule, whether to grant the first machine access to the first location on the network; and

determining, based on the accessed first-machine network access rule, whether to grant the first machine access to the third location on the network.

6. The method of claim 1 further comprising:

determining, based on the first-machine identifier, that the first machine is associated with the network interface device; and

determining, based on the second-machine identifier, that the second machine is not associated with the network interface device.

7. The method of claim 2 wherein the second-machine network access rule provides that the second machine is prohibited from accessing the second location on the network based on the determination that the second machine is not associated with the network device.

8. The method of claim 1 further comprising providing the first-machine log and the second-machine log to a recipient device.

9. The method of claim 8 further comprising receiving at the network interface device a token from the recipient device, the token configured to verify the identity of the network interface device, and

wherein providing the first-machine log to the recipient device further comprises transmitting a communication to the recipient device based on the token.

10. The method of claim 1 wherein the first-machine log includes multiple requests from the first machine, the second-machine log includes multiple requests from the second machine, and the method further comprises:

providing the first-machine log and the second-machine log to a recipient device;

receiving at the recipient device settings from a control user associated with the network interface device, wherein the settings include:

first-machine report compilation instructions specifying how to compile requests from the first machine in the first-machine log, and

second-machine report compilation instructions specifying how to compile requests from the second machine in the second-machine log;

compiling requests from the first-machine log according to the first-machine report compilation settings;

compiling requests from the second-machine log according to the second-machine report compilation settings;

generating at least one report based on the compiled requests from the first-machine log and the compiled requests from the second-machine log; and

providing the at least one report to the control user.

11. The method of claim 10 wherein providing the at least one report to the control user comprises sending the report to the control user in an email.

12. The method of claim 10 wherein providing the at least one report to the control user comprises making the report accessible to the control user on a web page.

13. The method of claim 10 wherein:

the first-machine report compilation instructions and the second-machine report compilation instructions are different;

generating at least one report comprises:

generating a first report based on the compiled requests from the first-machine log, and

generating a second report based on the compiled requests from the second-machine log; and

providing the at least one report comprises:

providing the first report to the control user, and

providing the second report to the control user.

14. The method of claim 1 wherein the logged request from the first machine includes the time at which the first request was received at the network interface device.

15. An apparatus comprising:

a first portion configured for:

receiving a request from a first machine, the request including a first-machine identifier and a request to access a first location on a network, and

receiving a request from a second machine, the request including a second-machine identifier and a request to access a second location on the network, the first machine and the second machine being located at a user location; and

a second portion configured for:

logging the request from the first machine into a first-machine log for requests from the first machine, the logging into the first-machine being based on the first-machine identifier, and

logging the request from the second machine into a second-machine log for requests from the second machine, the logging into the second-machine being based on the second-machine identifier.

16. The apparatus of claim 15 wherein:

the first portion of the apparatus comprises a first portion of a computer readable medium having instructions for performing:

the receiving of the request from the first machine, and

the receiving of the request from the second machine, and

the second portion of the apparatus comprises a second portion of the computer readable medium having instructions for performing:

the logging of the request from the first machine into the first-machine log for requests from the first machine, and

the logging of the request from the second machine into a second-machine log for requests from the second machine.

17. The apparatus of claim 15 wherein:

the first portion comprises hardware configured to perform:

the receiving of the request from the first machine, and

the receiving of the request from the second machine; and

the second portion comprises hardware configured to perform:

the logging of the request from the first machine into the first-machine log for requests from the first machine, and

the logging of the request from the second machine into a second-machine log for requests from the second machine.

18. A method comprising:

establishing a connection between a network interface device and a first network service provider having network access control rules;

receiving at the network interface device, a request from a machine to access a second network service provider through the network interface device, the second network service provider being different from the first network service provider;

providing, by the network interface device, access between the machine and the second network service provider through the network interface device;

accessing, by the network interface device, a network access control rule from the first network service provider that governs service provided to the machine from any network service provider; and

applying, by the network interface device, the network access control rule to the machine while the machine is connected with the second network service provider, to limit the service provided to the machine from the second network service provider.

19. The method of claim 18 further comprising:

receiving, at the network interface device, a request from the machine to access through the second network service provider a location on a network;

verifying, based on the network access control rule, that the machine is permitted to access the location on the network;

transmitting, based on the verification that the machine is permitted to access the location on the network, to the second network service provider the request from the machine to access the location on the network;

receiving, at the network interface device, data from the location based on the request from the machine to access the location; and

transmitting the data to the machine.

20. A method comprising:

receiving, at a network interface device at a user location, a request from a first machine located at the user location, the request including a first-machine identifier and a request to access through the network interface device a first location on a network;

accessing a first-machine network access rule;

determining, based on the accessed first-machine network access rule, whether to grant the first machine access to the first location on the network;

receiving at the network interface device a request from a second machine located at the user location, the request from the second machine including a second-machine identifier and a request to access through the network interface device a second location on the network, and the network interface device, the first machine, and the second machine being located at a user location;

accessing a second-machine network access rule; and

determining, based on the accessed second-machine network access rule, whether to grant the second machine access to the second location on the network.

* * * * *