RESOURCE ACCESS FILTERING SYSTEM AND METHOD

The field of the invention relates generally to a filtering system and in particular to a computer-implemented resource access filtering system and method.

Systems and software that filter content or e-mails are well known. For example, well known fire-walls and proxy servers perform some of these functions in order to protect an internal computer network, such as a corporate intranet, from hackers, malicious viruses and worms. There are also well known systems that permit a firewall/proxy server to filter unauthorized Internet access or so that users do not receive those unwanted e-mail messages. Typically, these systems operate with a server that acts as a gateway to the corporate network. The server typically has some functionality (in software or hardware) that permits the server to perform filtering operations on incoming and outgoing traffic.

Remote working is becoming more widespread across many fields and in many industries. A remote computing device is used remotely from a corporate network or LAN. In some systems, the remote device may perform its own filtering, but it is then more difficult to enforce a corporate-wide acceptable usage policy (AUP) and the device needs additional processing power in order to filter its own resource accesses. Typically, a user of the remote device may access resources from a computer network such as e-mail messages, various different files from an FTP or WWW site, a posting from a newsgroup and the like. Thus, it

is desirable to provide a system that filters a remote device's request for access to a resource from a computer network. Thus, it is desirable to provide a filtering system and method that achieves these goals and it is to this end that the present invention is directed.

According to the present invention there is provided an apparatus and method as set forth in the appended claims. Preferred features of the invention will be apparent from the dependent claims, and the description which follows.

A filtering system and method are provided that permit the monitoring and filtering of a resource access of a remote device. The preferred system enables a company to extend its corporate acceptable use policy beyond the wall of the office. In particular, the system permits a corporation to manage the resources accessed by remote devices, as such as used by mobile and remote employees and employees working from home. The invention also provides a computer and a client for the system.

In a preferred embodiment, the system comprises a client installed on a remote device that communicates with a computer. The remote device communicates remotely with the computer, e.g. is not part of the same local network. Typically, the remote device communicates over a global network or wide area network, such as the Internet. The server computer monitors and filters resource access requests of the remote device. The client has a module that gathers information about a request to access a resource by the device and a module that communicates the gathered information to the computer. The computer has a

module that categorizes the resource access of the device based on the gathered information and a module that communicates, in real-time, a resource access decision to the client. Then, the client controls the access to the resource by the device based on the resource access decision of the computer.

In a particularly preferred embodiment, the resource access decision is one of either an "allow" or "block" decision. That is, the decision either allows the device to access the requested resource, or it is blocked. Advantageously, the client requires minimal processing power and memory, and the number and type of devices able to support the filtering system is increased.

There are occasions when the client device is unable to connect with the computer. When a device loses its connection with the server of the filtering system, an offline functionality permits the client to continue to filter the resource accesses of the device according to a predetermined policy. Ideally, the predetermined policy is centrally managed at the server, and the server sets a mode of the offline filtering function. In one mode, the client may allow all access requests, and generate a log of those resource accesses. The log may be communicated back to the server once the client re-establishes a connection with the server.

Many devices are used both locally and remotely. That is, a device is used at times locally within a local network such as when the user is in a corporation's offices. At other times the same device is used remotely, such as when the user is traveling or working from home.

There is a need to efficiently manage filtering of resource access requests in these two environments. In a preferred embodiment, the system comprises a module that detects whether the requested resource is to be communicated over a corporate network and that disables the filtering for the requested resource being communicated over the corporate network.

A preferred unfiltered ports filtering functionality permits the system to specify a filtering strategy for TCP ports that are not specifically identified as filtered ports so that even the unfiltered ports may be filtered in some manner.

Also, the preferred system permits an administrator to adjust a filtering sensitivity level for each client between a high sensitivity level, a medium sensitivity level, a low sensitivity level or an automatic sensitivity level. The filtering sensitivity level may be adjusted, for example, for a device with a slow Internet connection, such as a GPRS connection for a cellular phone.

The system may provide a monitoring capability that permits the system to generate reports about the resource accesses of each device or of all of the devices connected to the server.

The preferred system may reduce a company's legal liabilities, e.g. since the company is more able to control the access to inappropriate Web sites during work times. The system may increase employee productivity as any Internet access during work time can be restricted to work-related Web sites. The system may also provide

network security in that the system is able to protect against viruses and malicious content that might enter the work place through an employee using an external modem or Internet service provider.

For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

Figure 1 is a diagram illustrating an example of a device resource access filtering and monitoring system in accordance with the invention;

Figure 2 is a diagram illustrating more details of the device resource access filtering and monitoring system shown in Figure 1;

Figure 3 is a diagram illustrating further details of a client/server embodiment of the device resource access filtering and monitoring system showing more details of the device and the server;

Figure 4 is a diagram illustrating more details of the server portion of the system of Figure 3;

Figure 5 is a diagram illustrating more details of the client portion of the system of Figure 3;

Figures 6A and 6B illustrate two different examples of an installation of the device resource access filtering and monitoring system in accordance with the invention;

Figure 7 illustrates an example of the user interface for an exemplary implementation of the client administrator module of the system; and

Figure 8 illustrates an example of the user interface for an implementation of the rules administrator module of the system.

The invention is particularly applicable to a client/server based computer-implemented, software-based device resource access filtering and monitoring system and it is in this context that the invention will be described. It will be appreciated, however, that the system and method in accordance with the invention has greater utility since the system may be implemented using various different computer architectures and may be implemented with a variety of different remote devices. The system may be implemented using any computing device wherein the computing device has at least a processor, memory and an input/output device with sufficient computing power so that the computing device is capable of interacting with the system and performing the fundamental filtering functions described herein, since each client is not necessarily able to perform all of the functions described below. The system may be implemented in software or hardware. In the software embodiment, the system may comprise one or more software modules in the server and one or more modules in the client wherein each module may further comprise a plurality of lines of computer code that are executed by the processor of the server or client. Now, an embodiment of the remote device monitoring system will be described.

Figure 1 is a diagram illustrating an example of a device resource access filtering system 30 in accordance with the invention. The system 30 permits a device 32 (with a piece of software code known as a client 48) that connects to a remote computer device 33, such as a computer with server software 34 in this embodiment, over a computer network 36, such as the Internet in this embodiment, a wide area network (WAN), local area network (LAN), metropolitan area network (MAN) or the World Wide Web, to be monitored and the device's access to resources on a site 38 to be filtered. The site 38 is the source of a resource requested by the user of the device 32. In more detail, the server 34 is able to remotely filter (control and/or analyze) the device's access to resources. In accordance with the invention, the functionality to achieve this remote monitoring of the device 32 is split between the device 32 and the server 34. This reduces the network traffic between the device 32 and the server 34 and permits centralized controlling and monitoring of the access to various resources including e-mails, web pages, file transfer protocol (FTP) sites, newsgroups and the like. In accordance with the invention, the server 34 may also receive the data associated with the attempted access of the resources to determine if the device will be permitted to receive the content, download the data, etc. from the address associated with the access request to the site 38. The device and server may communicate with each other using a particular protocol that is based on a proprietary protocol. The system provides for the real-time filtering of computer network access whereby the remote computer 33, such as the server 34 in the preferred embodiment, is utilized to make and/or adjust the filtering decisions.

The protocol for the system, since the client 48 is expected to work on and in a variety of remote networks (over which the corporation may have little or no control), is compatible as possible with those remote networks so that the client 48 may operate over those remote networks. For example, the protocol is compatible with Firewalls and Proxies. The protocol handles and accommodates various different devices with different data formats and capabilities so that the protocol provides a standard data format for strings and numbers for the different devices. The protocol also is compact in size as the server may be required to handle a large number of clients using limited bandwidth and a client may have to utilize a slow internet connection to the server. In accordance with a preferred embodiment of the invention, the protocol utilizes, to increase compatibility with a wide variety of networks, hypertext transfer protocol (HTTP) over TCP port 80 using an HTTP envelope. For those networks that permit access to the Internet, the most basic access is Web access which will involve outgoing connection requests over port 80 so that port 80 is typically available and used for this protocol. Some networks only permit Internet Web access via a proxy server that expect an HTTP style request and response so that the HTTP protocol is used for this system. Furthermore, some firewalls may examine Internet accesses and raise alerts when port 80 is being used for protocols other than HTTP so that the system's protocol uses HTTP.

In accordance with the invention, the HTTP protocol may be used by the system for requests by the client 48 as well as responses from the server 34 back to the client.

As with HTTP, only the client 48 can instigate a communication and it does this by performing a well known HTTP POST to identify which operation the client is requesting along with any parameter data. An example of the format of this request is:

POSThttp://[Nomad_Module_Path]?[Operation_Code] HTTP/1.1\r\n
Host: [Host]\r\n
Content-Length: [Size_of_Encoded_Data]\r\n
Content-Type:application/x-www-form-urlencoded\r\n\r\n
[Encoded_Data]

For a response from the server to the client, the protocol again mimics the HTTP protocol so our returned data appears to be a Web Page. An example of the format of this response is:

Content-Type: text/html\r\n
<html><head><title>
SMF
</title></head><body>
[Encoded_Data]
</body></html>

The operation codes for the protocol (See [Operation_Code] variable in the request format example above) specify the various operations that may be requested using the system protocol. The [Encoded Data] provides gathered information from the client 48 to the server 34 and returns a resource access decision from the server 34 to the client 48 on the remote device 32.

Returning to Figure 1, the device 32 may be any computing device that has sufficient computing resources to perform the filtering functions specified below so that the device 32 must have at least a processor, some memory and some mechanism for accessing resources from a computer network. For example, the device 32 may be a cellular phone, a personal digital assistant, a personal computer, a laptop computer, a palmtop computer, or an appliance with the sufficient computing resources to accomplish computer network access and the like. Thus, the device may include wireless devices, cellular telephone devices, wireless e-mail devices, wireless personal digital assistant devices, such as a Palm device, a Treo device, a RIM Blackberry device, a wired personal computer, a wired laptop computer or a wirelessly connected computing device. In accordance with the invention, the system may perform various filtering functions and each device does not necessarily have to be able to support all of the filtering features described herein. For example, a cellular phone is unlikely to have sufficient memory to store a list of encrypted URLs required for the Offline mode of "Allow and Log." Thus, it is desirable to alert the system to the filtering capabilities of each device that is going to perform filtering. In accordance with the invention, a capability mask may be used for this purpose. In particular, when a device 32 logs into the system, it may communicate a capability mask for the device to the server that informs the server of the functionality that the device can and/or cannot offer based on the particular device and its characteristics.

The site 38 may store any resource that can be accessed over a computer network, such as an e-mail,

downloaded data (PDF files, text files, word documents, HTML files, zip files and the like), an FTP site or a TELNET server. The invention is not limited to any particular architecture of the system (and the relationships of the computers within the system) although a client/server architecture is shown for illustration purposes. For example, the system may be implemented using a peer-to-peer architecture in which the remote computer 34 functionality is distributed. Furthermore, the invention is not limited to any particular type of resource as the system may be configured to handle any type of resource or any new resource or type of resource.

Figure 2 is a diagram illustrating more details of an example of the system 30 shown in Figure 1. In this example, the device 32 may be a personal computer that is capable of access to resources at the site 38 (See Figure 1) and is being monitored by the computer 34 which is a typical server computer in this example. The device may comprise one or more processors 40, a persistent storage device 42 and a memory 44 that are interconnected to each other in a well known manner. The persistent storage device may comprise, for example, non-volatile memory such as flash memory, a hard disk drive, a writeable optical drive, a removable media drive or another storage mechanism that permits storage of data and instructions while the device 32 is powered down. The memory 44 may be, for example, SRAM, DRAM or another structure that temporarily stores data and instructions being executed by the processor(s) 40 while the device is powered up. The device 32 may further comprise some mechanism (not shown) for accessing the site 38 and server 34, such as a wired connection (such as a cable modem and cable for example)

or a wireless connection (such as a 802.11 link, a cellular link or GPRS link). The device 32 may further comprise an operating system 46 that resides in the memory 44 during operation of the device and is executed by the processor(s) 40 as is well known. The invention is not limited to any particular type of operating system and may be implemented with various different operating systems. In order to implement the filtering and monitoring system in accordance with the invention, the device 32 may further include a client 48 (which is shown as a software application/software module containing a plurality of lines of computer instructions and data in this example) that is stored in the memory 44 and executed by the processor(s) 40 to perform the client functions of the filtering system as described below in more detail. In the preferred embodiment of the invention, the client further comprises one or more software modules having a plurality of lines of computer code wherein each module performs different functions of the filtering system and the combination of the modules implements the client functions. The client 48 may also be implemented as a mixed hardware/software device, such as a plug-in media card that is plugged into the device 32, or as a hardware device, such as an ASIC with the client embedded into the ASIC. When the user of the device 32 attempts to access a remote resource, such as a resource on the site 38 shown in Figure 1, the client 48 intercepts the access and gathers data about the access that is then forwarded to the server 34 in one embodiment of the invention. The client 48 may also gather the data about the resource access and then make a determination about the access request itself in another embodiment of the invention.

The level of access for each user (and/or each device) may be customized for a particular user.

The server 34 may further comprise one or more processor(s) 50, a persistent storage device 52 and a memory 54 that are interconnected together as is well known. The server may further comprise a database 56 that stores the data and software code associated with the filtering system in accordance with the invention. The server may further comprise an operating system 58 as is well known and a filtering/categorization module 60, shown as a piece of software residing in the memory 54 in this example, that processes the resource access requests and determines whether or not the device 32 may access the resource on the site 38 in one embodiment of the invention. The module 60 (which preferably comprises one or more software modules) implements different functions of the filtering system including administrative functions associated with the filtering system and may interact with the database 56 to request and store data in the database associated with the filtering activities.

To uniquely identify each device 32, each device is assigned a unique identifier that ties the configuration and filtering requests to a particular device and permits the filtering logs for a particular device to be stored in the database. In addition, the combination of the unique identifier with an initial log-in by each device 32 to the server reduces the amount of data being transmitted between the device 32 and computer 34 during each resource access request when the server 34 is performing the filtering decisions. In this embodiment of the invention, the filtering system permits the filtering of access by a

device to a remote resource in real-time wherein a server is used to accomplish the filtering decisions. That is, the server performs a majority or the processing and memory workload of the system, and very little need be done at the client. In another embodiment of the invention, the device may perform it's own filtering decisions. In particular, when the server is unavailable to the device, the client operates in an offline mode specified by the server, such as for example, the client logs the accesses and then uploads a log to the server when connectivity is re-established.

Figure 3 is a diagram illustrating further details of a client/server embodiment of the device resource access filtering and monitoring system showing more details of the device 32 and the server 34. In this example, the device 32 may include one or more typical software applications that might be used on a typical personal computer, such as a web browser 70, an AOL browser 72, Outlook Express 74, Outlook 76, an FTP client (not shown), a Gopher client (not shown) and/or a news reader 78. When using any of these typical software applications that attempts to access a remote resource, the information about the remote resource access is intercepted by the client 48 so that it can be sent to the server 34 to determine if access to the particular resource should be permitted for the particular device. In one embodiment, on the server 34 side, the server further comprises a Microsoft's Internet Information Server (IIS) 80 that receives the data from the client 48 on the device 32. The invention is not limited to using the IIS and may be implemented in other manners. The IIS server 80 may then forward that information onto an IIS plug-in 82 that

forwards the data onto a categorization engine 84. The IIS plug-in 82 may determine a particular client associated with the device 32 using a client database 56a (part of the database 56 shown in Figure 2 in a preferred embodiment or a separate database) wherein the client database may be maintained using an administration module 86. The administration module may contain, for example, a list of all monitored clients that are installed on remote devices along with the settings for each client that may be stored in the client database 56a as described in more detail with reference to Figure 7.

The IIS Plug-in 82 may further comprise an offline filtering module, an unfiltered ports module and/or a filtering sensitivity module. The server 34 may then communicate the offline mode, unfiltered ports mode and filtering sensitivity settings for a particular client to the client which then implements the offline filtering, unfiltered ports filtering and filtering sensitivity levels. The client may comprise an offline filtering module, an unfiltered ports module and a filtering sensitivity module wherein each module implements the respective functions of the client and each module may be implemented as a plurality of lines of computer code that are executed by the processor of the device on which the client resides.

The categorization engine 84 may pull categorization rules from a rules database 56b (part of the database 56 in Figure 2 in a preferred embodiment or a separate database) that is maintained by a rules administration module 88. The rules administration module 88 may also be used to create a new rule as described in more detail

below with reference to Figure 8. The categorization engine may store its results in a monitor database 56c (part of the database 56 in Figure 2 in a preferred embodiment or a separate database) that is maintained by a monitor module 90. The monitor module 90 may, for example, collect and display information about the Web surfing habits of each client or of all of the clients. The monitor module 90 may also include a real-time monitor module (not shown) that permits a user of the monitoring system to show the Internet connections for remote user of the devices as the connections are requested. In accordance with the invention, the categorization engine may categorize a particular information request based upon one or more pieces of data. The information request may be categorized primarily based on the site address to be accessed by the device. The categorization engine may also use 1) the device's host name or a server-side configurable alternative name (when the device does not have a host name); and/or 2) the device's current user name or a server-side configurable alternative name (for devices that do not have a user name). Thus, the categorization criteria (and therefore the accessible resources) are configurable for a particular device/user. For example, the level of access may change depending on the employee seniority or status within the company. An administrator module (not shown) may include a scheduler that permits the user to set-up events to occur automatically on the server, such as database updates, database maintenance tasks and the like. The administrator module also permits a user to categorize/re-categorize a site. A virtual control agent (not shown) is an optional module that uses artificial intelligence to automatically visit and categorize sites that have been

accessed by the user, that at that time, did not have a category. The administrator module also has a web reporting module so that the system can generate reports on the client data and the surfing habits. The various modules of the remote computer 34 may each be a piece of software with a plurality of lines of code that implements the functions described herein.

Figure 4 is a diagram illustrating more details of the server portion 34 of the device client/server embodiment of the invention and Figure 5 is a diagram illustrating more details of the device 32 portion of the device client/server embodiment of the invention. As shown in Figure 4, an implementation of the server 34 is shown wherein an SQL database is used to store the data for the system and a web filter rules engine service. An example of a filtering rule in accordance with the invention and how a rule is created is described in more detail below with reference to Figure 8. As shown in Figure 5, the client 48 on the device further comprises a user interface portion 100, a client communications layer 102, a network interceptor layer 104 and a storage medium 106 that stores the configurations for the particular client 48 as well as any log files as described below. In a preferred embodiment, each of these portions and layers is a piece of software being executed by the processor of the device. The user interface portion 100 generates the user interface of the monitoring system that is displayed to the user and may include configuration user interface screens. The network interceptor layer 104 may gather the data from a resource access request to an external site while the client communications layer 102 may format that data into a format to send to the server 34 and receive

the server's resource access decision and implements that decision.

During normal operation of the system in accordance with the invention, the device may initiate a resource access request to a resource on a remote site, such as a web page from Amazon.com, and the client 48 captures the data associated with that request, such as the site address. The client may also gather the device identifier and other device data and then forward the resource access request data to the server 34. The server may then, based on the resource access request data, make a categorization/filtering decision to generate a resource access decision and then send the resource access decision back to the client 48 so that the client may take the appropriate actions. Thus, the remote server may perform real-time monitoring and filtering of the resource access requests of the device 32. If, however, the server 34 is not available to the device (for any reason), then the device may perform offline filtering wherein the device 32 is responsible for its own monitoring and filtering. When the device (and hence the client) is unable to connect to the server, it will attempt reconnection on a regular basis, such as every 5 minutes, while the client is connected to the Internet.

During the offline filtering, the device/client may operate in different modes of operation depending on the configuration of the particular client by the server. For example, the client 48 may permit all Internet accesses, but log each resource access request into a local log file (a "Log & Allow" mode) that may then be later uploaded to the server. Alternatively, the client may block all

Internet access (a "Block All" mode) or allow all Internet access with no logging (an "Allow All" mode). In accordance with the invention, the offline logs recorded on the client may be stored in the local storage of the device, such as the memory or persistent storage device as described above. If the log is later uploaded to the server, the log file may then be deleted on the device. In a preferred embodiment, the log file may be encrypted. The log file may further include some basic monitoring capabilities to detect unauthorized tampering of the client. In accordance with the invention, the offline log uploading may include bandwidth throttling so that when the server comes back online, it is not overloaded by numerous clients all trying to upload their logs to the server.

In accordance with the invention, the server may include the administrator module 86 that permits a system administrator, such as a Chief Information Officer for a corporation, or the client itself (using an automated algorithm) to adjust the operation of the filtering and monitoring system in accordance with the invention. For example, the filtering sensitivity of the system (the level at which Internet accesses are filtered on a particular device) for each device may be customized/adjusted so that the amount of Internet traffic being filtered may be reduced for a particular device which reduces the amount of bandwidth of the device dedicated to the monitoring and filtering operations. For example, a device with a slow Internet connection, such as GPRS for a cellular phone, may have its sensitivity adjusted. In accordance with the invention, the filtering sensitivity for any device may be adjusted based on any

particular characteristics of the device. In a preferred embodiment of the system, there may be a high filtering level, a medium filtering level, a low filtering level and an automatic filtering level. At the high filtering sensitivity level, the system may, for example, filter all non-hypertext transfer protocol (HTTP) ports and all HTTP requests so that this setting filters all resources including, for example, pop-up ads. The high filtering sensitivity provides a very thorough filtering, but may impact filtering speed and performance if the device is making a lot of resource access requests. At the medium level of sensitivity, all non-HTTP ports are categorized, but only HTTP page requests are categorized while image files, sound files, style sheets and XML requests are not categorized. At a low sensitivity level, all non-HTTP ports are categorized, but only the server address part of the HTTP request is categorized and the results may be cached for a very short time. At the automatic level of sensitivity, the client chooses the high, medium or low level based on the average server response times (response latency) and pre-configured thresholds. For the automatic mode, the client may include a piece of code that adjusts the sensitivity. For example, the high level may be used while the response latency is less than a predetermined period of time and then be reset to a medium level.

In accordance with the invention, the system may filter all TCP/IP ports wherein some of the ports are treated as HTTP web requests either made directly to the resource at the site 38 or via a Proxy Server. In order to reduce needless communications with the server for device access to ports that a particular company is not interested in filtering or monitoring, the device 32 may

be informed (by the server) of which ports are to be communicated to the server and which of those ports are to be treated as HTTP web requests. Thus, the server may be configured, for a particular company, with unfiltered ports (the list of ports that are not to be communicated to the server.) In accordance with the invention, the list of ports to filter and/or treat as HTTP requests are communicated to the device during the login procedure of the device. The client may then perform an unfiltered port action which is an automatic action taken when an application executing on the device attempts to access an unfiltered port. In a current implementation and one embodiment of the system, the list of filtering ports and HTTP ports are hard coded into the server software. In another embodiment of the invention, the server may analyze a set/list of rules (which may be adjusted/customized) and the list of monitored ports is automatically generated from the rules. The unfiltered port actions may include, for example, an allow all option in which all of these port requests are allowed (an "Allow All" mode), a block all option (a "Block All" mode) is which access to all unfiltered ports is blocked and a filter option (a "Filter" mode) in which the port request is communicated to the server which is useful for rules that in a typical Web filter usually affects all ports, such as block everyone from adult content.

Figures 6A and 6B are two different examples of an installation of the filtering system in accordance with the invention. For each installation, the server 34 is positioned so that the devices 32 (with the clients) may access the server over TCP port 80. In Figure 6A, the server 34 may be positioned external to a main protected

network 112 (with its internal computing devices 114) and connected to the corporate network via bridge/router/firewall device 110 as shown so that the devices 32 may access the server 34. In the example shown in Figure 6B, the server 34 may be located within the network 112 and then the firewall 110 must be configured to allow traffic on TCP port 80 as long as the traffic is directed to server 34. In both cases, the device 32 are able to communicate with the server 34 and therefore the server can perform the remote monitoring and filtering operations.

Figure 7 illustrates an example of the user interface 120 for an exemplary implementation of the client administrator module. The administrator is the main management point for the system and provides a customizable description of each remote device and the settings for each particular device. The user interface 120 includes a summary portion 122 and a client detail portion 124 wherein the summary portion 122 lists all of the clients currently entered into or logged into the system (only one is shown in this example for simplicity.) When the user of the administrator module selects a particular client from the summary portion, the client detail portion 124 shows the detailed settings and other information for the particular client and the device on which the client is being executed. The client detail portion 124 may further include a client information portion 126 and a client settings portion 128 wherein the client information portion lists information about the particular selected client/device and the client settings portion permits the administrator to adjust/set/reset the settings of the filtering/monitoring for the particular

client/device. As shown in the client information portion, each client has a unique identification (the Client Id shown in Figure 7) that uniquely identifies each client installation so that the settings for each client may be stored in the database.

In the client settings portion 128, the administrator may set various filtering and monitoring settings including, for example, an offline action setting 130, an unfiltered ports setting 132, a filter sensitivity setting 134, a user name setting 136 and a host name setting 138. As described above, the offline action setting 130 permits the administrator to select an option of how the client will operate when the server becomes unavailable to the client and the offline actions, in a preferred embodiment, may be selected from "Allow All", "Block All" or "Log and Allow". The unfiltered ports setting 132 permits the administrator to set how the particular client should behave when ports not included in the filtered ports are accessed by the user of the device. In a preferred embodiment of the invention, a selected list of TCP ports are chosen to be monitored in order to reduce the total traffic between the client and the server. The actual selection of ports being monitored may be modified using the administrator modules. The list of default TCP ports may include, for example:

PORT	APPLICATION	NUMBER
HTTP	Web traffic	80, 8000, 8080
HTTPS	Secure web traffic	443
FTP	File transfers	21
NNTP	Newsgroups	119
POP3	E-mail (receiving)	110
SMTP	E-mail (sending)	25
AOL	American Online	11523

Thus, for any port not specified as filtered or added into the monitored ports by the administrator, the unfiltered ports setting will apply. As described above, the unfiltered port selections, in a preferred embodiment, may include the Allow All, Block All and Filter modes. The filter sensitivity setting 134 permits the administrator to set the level of sensitivity of the filtering for the client. As described above, the selections may include, in a preferred embodiment, a high filtering level, a medium filtering level, a low filtering level and an automatic filtering level.

In general, the filtering rules may be based on a user name or host name. Thus, if a user name is specified by a rule, then regardless of the device being used by the user, the user filtering rules are applied. If a host name is specified in a rule, then regardless of which user logs into a particular device, the rules based on the host name are applied to that particular device. Thus, the user name setting 136 permits the administrator to set the user that is applied to the particular device. This user name is used by the server for all filtering decisions for the client device. The name can then be used to check against the rules in the rules database to determine the appropriate filtering for the particular client user. The user name setting permits the administrator to choose, in the preferred embodiment, from a client specified name mode, a server override mode or a server default mode. In the client specified mode, when the user logs into the device executing the client, the client sends the user log in name to the server which is used as the user name. In the server override mode, the administrator can specify a

name to identify this user as a member of an organization, such as engineering, secretary, mobile employee, etc…, without specifically defining the user as an individual so that the filtering rules for the organization will apply to the particular user. For example, a company may have a collection of mobile devices used for traveling insurance salesmen, and anyone using those mobile devices should be filtered according to the role of 'salesman', rather than their individual user name. Therefore rules can be created that allow 'salesman' to go to particular sites needed for the job. This mode may also be used when the client is unable to supply a user name, such as a mobile phone. The server default mode is used when the client specified mode and server override mode are not used so that the device may still be filtered at some level. The host name setting 138 specifies the actual device (in contrast to a user of the device) so that devices or groups of devices (with particular characteristics) can be grouped together, recognized and filtered according to the filtering rules for that group of devices regardless of the individual using the device. The host name settings permits the administrator to select, in a preferred embodiment, from a client specified host name mode, a server override mode and a server default mode. In the client specified mode, the client of a device, when the user logs into the device, provides the network name of the device to the server. In the server override mode, the host name is used to identify the device as a member of a group which is useful for devices, such as a mobile phone, that cannot supply a host name. In the server default mode, this is the host name used when the client specified mode and server override mode are not used so that the device may still be filtered at some level.

Figure 8 illustrates an example of the user interface 150 for an implementation of the rules administrator module. The rules administrator permits an authorized user of the system to create one or more filtering rules. The user interface shows each rule 152 as a row in the display with the different characteristics/settings of each rule, such as the type of rule, the user/device to which the rule applies, the type of content to which the rule applies, the threshold for the rule and the notification characteristics of the rule arranged in different columns of the display. The types of rules include ALLOW (allow the content specified by the rule), DISALLOW (do not allow the content specified by the rule) or THRESHOLD (allow the content specified by the rule if it is within the threshold values). For the threshold rules, a user specified by the rule may be permitted to access the Internet for a set period of time, for example. For each rule, the administrator may specify the clients/devices or groups of clients or devices to which the rule is applied during filtering operations. For each rule, the administrator may specify the type of content to be filtered. For example, as shown in Figure 8, the content may be adult/sexually explicit, travel, gambling, executables, etc.. although a rule may be created to filter any type of content and any type of content may be added into the system so that a new type of content may be filtered in the future. Each rule also specifies the time during which the rule is applied, such as ANYTIME, After Work and Weekends, Worktime, etc.. wherein different time periods may be given a new name and then the time period specified by the user. Each rule may also have a threshold as described above as well as a notification

characteristic that specifies who in the system is notified when certain content is being accessed by a user.

In accordance with the invention, the filtering rules generated by the rules administrator may govern who can access what areas of the Internet at what time of day. The rules may be positive (allowing access to sites, a category of sites such as "sexually explicit" or resources) or negative (denying access to sites, a category of sites or resources). In general, each rule may contain a Type, Who, Where, When, Notify, Threshold and HTTP Deny objects (only some of which are shown in Figure 8) that specify different characteristics of each filtering rule. The Type object contains data that specifies when the rule is allow, disallow or threshold rule. The Who object contains data that specifies the individual to which the rule will be applied wherein the object may specify an individual, a group of people, anybody, nobody, etc... The Where object contains data that specifies the origin (such as a web site) of the requested resource, but may also specify a category of sites, such as "Sexually explicit" or "ftp" for example. The When object contains data that specifies the time and/or days when the resource request is permitted or denied. The Notify object contains data that specifies one or more individuals that might be notified, such as by email, when a particular resource request triggers that rule. The Threshold object contains data that specifies the limit of the amount of data or the time spent surfing during a particular time period. The HTTP Deny object contains data that specifies that a particular type of deny page (harsh, strong or mild) is sent to the user when the rule is triggered. For each new rule, the rules administrator

permits the user to specify these characteristics of the rule by entering information and utilizing drop down menus.

In accordance with the invention, the system filters devices remote from the corporate network. It is desirable that, when a particular device transitions back onto the corporate network, such as a laptop being used on the road and then being plugged back into the corporate network, that the filtering policy of the corporate network (for the static employees, for example) will be used for the particular device as long as it is within the corporate network. In accordance with the invention, the client may include a software module that detects whether a particular resource request of the device is going to be communicated over a corporate network (such as when the device on which the client resides has been connected to the corporate network) to disable the client filtering functions for those resource requests being communicated over the corporate network so that the corporate network filtering policy may be used. As another example, a device may be connected to the corporate network but also connected to a wireless modem and the client filtering may be used for resource requests communicated over the wireless modem, but not for resource requests communicated over the corporate network.

Although a few preferred embodiments have been shown and described, it will be appreciated by those skilled in the art that various changes and modifications might be made without departing from the scope of the invention, as defined in the appended claims.

Attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings) may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

CLAIMS

1. A resource access filtering system, comprising:

a computer (33);

a client (48) on a device (32) wherein the client (48) establishes a remote connection to the computer (33), the client (48) further comprising a module that gathers information about a request to access a resource by the device (32) and a module that communicates the gathered information to the computer (33); and

the computer (33) further comprising a module that categorizes the resource access of the device (32) based on the gathered information and a module that communicates, in real-time, a resource access decision to the client (48) so that the client (48) controls the access to the resource by the device (32) based on the resource access decision of the computer (33).

2. The method of claim 1, wherein the resource access decision provides either an allow decision or a block decision to the client (48), whereby the client (48) either allows or blocks access to the requested resource.

3. The system of claim 1 or 2, wherein the client (48) further comprises a module that detects whether the requested resource is to be communicated over a corporate network and that disables the client filtering for the requested resource being communicated over the corporate network.

4. The system of claim 1, 2 or 3, wherein the client (48) further comprises an offline filtering module that controls the resource accesses of the device (32) when the client (48) is unable to communicate with the computer (33).

5. The system of claim 4, wherein the offline filtering module provides one or more modes including an allow all resource access mode, a block all resource access mode and an allow all resource access with logging mode.

6. The system of claim 5, wherein the allow all resource access with logging mode further comprises a module for throttling the offline logs uploaded to the computer (33) in order to control the bandwidth utilized by the offline logs.

7. The system of claim 4, 5 or 6, wherein a mode of offline filtering module is selected by the computer (33).

8. The system of any preceding claim, wherein the client (48) has a filtered port list downloaded from the computer (33) that indicates the ports to be filtered and the ports to be treated as HTTP ports.

9. The system of claim 8, wherein the client (48) further comprises an unfiltered ports module that controls the resource accesses of the device (32) for a port not specifically identified as a filtered port.

10. The system of claim 9, wherein the unfiltered port module further comprises an allow all resource access

mode, a block all resource access mode and a send to computer (33) for possible filtering and/or logging mode.

11. The system of claim 8, 9 or 10, wherein a mode of unfiltered port module is selected by the computer (33).

12. The system of any preceding claim, wherein the client (48) further comprises a filtering sensitivity module that controls a level of filtering of resource accesses for the client (48), whereby the client (48) determines whether or not to provide the gathered information to the computer (33) based upon the level of filtering.

13. The system of claim 12, wherein the filtering sensitivity module further comprises a high sensitivity level mode, a medium sensitivity level mode, a low sensitivity level mode and an automatic sensitivity level mode.

14. The system of claim 12 or 13, wherein a mode of the filtering sensitivity module is selected by the computer (33).

15. The system of any preceding claim, wherein the computer (33) further comprises a monitor module that monitors the resource accesses of the devices connected to the computer (33) to generate a summary of the resource accesses of the devices.

16. The system of any preceding claim, wherein the resource being accessed comprises any one of a web page, a

file transfer protocol site, an e-mail site, a secure web site, and a news site.

17. The system of any preceding claim, wherein the device (32) comprises any one of a personal digital assistant, a cellular phone, a personal computer, a laptop computer, a palmtop computer and an appliance.

18. The system of any preceding claim, wherein the client (48) further comprises a module that generates a capability mask for the device (32) and communicates that capability mask to the computer (33), the capability mask containing information about the filtering capabilities of the device (32).

19. The system of any preceding claim, wherein the gathered information and the resource access decision are communicated between the client (48) and computer (33) using a hypertext transfer protocol over TCP port 80.

20. The system of claim 19, wherein the protocol for gathered information further comprises a hypertext transfer protocol POST operation.

21. The system of any preceding claim, wherein the protocol for the resource access decision further comprises data in a web page format.

22. A resource access filtering method using a computer (33) and a client (48) on a device (32) that establishes a connection to the computer (33), the method comprising:

gathering information by the client (48) about a request to access a resource by the device (32);

communicating the gathered information to the computer (33) by remote communication;

categorizing, at the computer (33), the resource access of the device (32) based on the gathered information; and

communicating, in real-time, a resource access decision to the client (48) so that the client (48) controls the access to the resource by the device (32) based on the resource access decision of the computer (33).

23. The method of claim 22, wherein the resource access decision provides either an allow decision or a block decision to the client (48), whereby the client (48) either allows or blocks access to the requested resource.

24. The method of claim 22 or 23, wherein the client (48) further comprises a module that detects whether the requested resource is to be communicated over a corporate network and that disables the client filtering for the requested resource being communicated over the corporate network.

25. The method of claim 22, 23 or 24, wherein the client (48) further comprises an offline filtering module that controls the resource accesses of the device (32) when the client (48) is unable to communicate with the computer (33).

26. The method of claim 25, wherein the offline filtering module provides one or more modes including an allow all resource access mode, a block all resource access mode and an allow all resource access with logging mode.

27. The method of claim 26, wherein the allow all resource access with logging mode further comprises a module for throttling the offline logs uploaded to the computer (33) in order to control the bandwidth utilized by the offline logs.

28. The method of claim 25, 26 or 27, wherein a mode of offline filtering module is selected by the computer (33).

29. The method of any of claims 22 to 28, wherein the client (48) has a filtered port list downloaded from the computer (33) that indicates the ports to be filtered and the ports to be treated as HTTP ports.

30. The method of claim 29, wherein the client (48) further comprises an unfiltered ports module that controls the resources accesses of the device (32) for a port not specifically identified as a filtered port.

31. The method of claim 30, wherein the unfiltered port module further comprises an allow all resource access mode, a block all resource access mode and a send to computer (33) for possible filtering and/or logging mode.

32. The method of claim 29, 30 or 31, wherein a mode of unfiltered port module is selected by the computer (33).

33. The method of any of claims 22 to 32, wherein the client (48) further comprises a filtering sensitivity module that controls a level of filtering of resource accesses for the client (48), whereby the client (48) determines whether or not to provide the gathered information to the computer (33) based upon the level of filtering.

34. The method of claim 33, wherein the filtering sensitivity module further comprises a high sensitivity level mode, a medium sensitivity level mode, a low sensitivity level mode and an automatic sensitivity level mode.

35. The method of claim 33 or 34, wherein mode of the filtering sensitivity module is selected by the computer (33).

36. The method of any of claims 22 to 35, wherein the computer (33) further comprises a monitor module that monitors the resource accesses of the devices connected to the computer (33) to generate a summary of the resource accesses of the devices.

37. The method of any of claims 22 to 36, wherein the resource being accessed further comprises one of a web page, a file transfer protocol site, an e-mail site, a secure web site, and a news site.

38. The method of any of claims 22 to 37, wherein the device (32) further comprises one of a personal digital assistant, a cellular phone, a personal computer, a laptop computer, a palmtop computer and an appliance.

39. The method of any of claims 22 to 38, wherein the client (48) further comprises a module that generates a capability mask for the device (32) and communicates that capability mask to the computer (33), the capability mask containing information about the filtering capabilities of the device (32).

40. The method of any of claims 22 to 39, wherein the gathered information and the resource access decision are communicated between the client (48) and computer (33) using a hypertext transfer protocol over TCP port 80.

41. The method of claim 40, wherein the protocol for gathered information further comprises a hypertext transfer protocol POST operation.

42. The method of any of claims 22 to 41, wherein the protocol for the resource access decision further comprises data in a web page format.

43. A computer for a resource access filtering system, comprising:

a module that receives information about a request to access a resource by a remote device (32), wherein the information about the resource access request is remotely communicated from a client (48) on the remote device (32);

a module that categorizes the resource access of the remote device (32) based on the gathered information; and

a module that communicates, in real-time, a resource access decision to the client (48) so that the client (48) controls the access to the resource by the remote device (32) based on the resource access decision of the computer (33).

44. A remote access filtering client (48) located on a device (32) that communicates with a remote computer (33), the client (48) comprising:

a module that gathers information about a request to access a resource by the device (32);

a module that communicates the gathered information to the computer (33); and

a module that receives a resource access decision from the computer (33) and controls the access to the resource by the device (32) based on the resource access decision of the computer (33).