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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 August 2008 (21.08.2008)

PCT

(10) International Publication Number
WO 2008/100265 A2

(51) International Patent Classification:
H04L 12/22 (2006.01)

(21) International Application Number:
PCT/US2007/011053

(22) International Filing Date: 7 May 2007 (07.05.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/429,476 5 May 2006 (05.05.2006) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, WA 98052-6399 (US).

(72) Inventor: **ROBERTS, David, A.**; c/o Microsoft Corporation, International Patents, One Microsoft Way, Redmond, WA 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *without international search report and to be republished upon receipt of that report*

(54) Title: DISTRIBUTED FIREWALL IMPLEMENTATION AND CONTROL

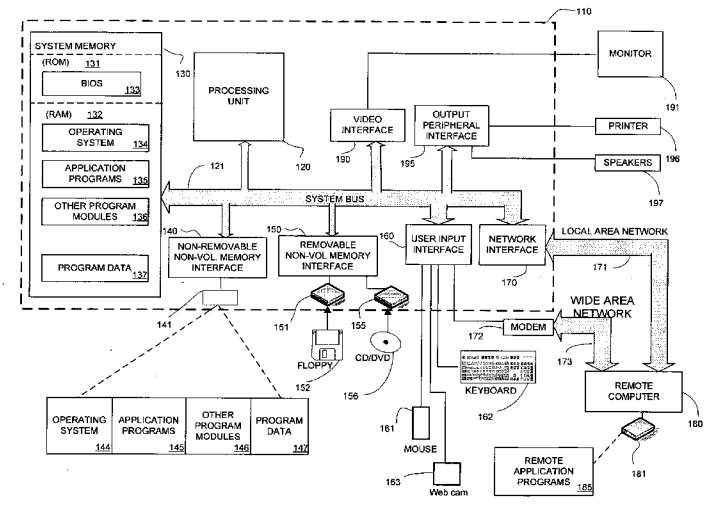

Fig. 1

(57) Abstract: A method for etching a target material in the presence of a structural material with improved selectivity uses a vapor phase etchant and a co-etchant. Embodiments of the method exhibit improved selectivities of from at least about 2-times to at least about 100- times compared with a similar etching process not using a co-etchant. In some embodiments, the target material comprises a metal etchable by the vapor phase etchant. Embodiments of the method are particularly useful in the manufacture of MEMS devices, for example, interferometric modulators. In some embodiments, the target material comprises a metal etchable by the vapor phase etchant, for example, molybdenum and the structural material comprises a dielectric, for example silicon dioxide.

WO 2008/100265 A2

DISTRIBUTED FIREWALL IMPLEMENTATION AND CONTROL

BACKGROUND

[0001] A computer connected to a network is vulnerable to attack from other computers on that network. If the network is the Internet, the attacks may include a range of acts from malicious attempts to gain access to the computer, to installing "zombie" code, to denial of service attacks. Malicious attempts to gain access to the computer may have the intent of discovering personal data, while zombie code may be used to launch denial of service attacks by overwhelming a web site with high traffic volumes from a number of computers. The attackers may include organized criminals, sophisticated but malicious computer experts, and "script kiddies" who read and repeat posted assaults on known vulnerabilities.

[0002] Most computers have addressable ports for sending and receiving data. Some of the ports may be designated for certain kinds of traffic. For example, in an Internet Protocol (IP) network, port 80 is often designated for hyptertext protocol (http) traffic, while port 443 is often designated for secure http (https) traffic. Other ports may be designated as needed for different services. Non-designated traffic on such designated ports and any traffic on unused ports may indicate attempts by attackers to gain access to the computer.

[0003] A firewall may be used to limit port traffic to certain protocols and to close unused ports from all outside traffic. The firewall may be placed on a network between computers seeking protection and "open" networks, such as the Internet, or may be integral to the computer. . In corporations, or other large private networks, firewalls may also be used to limit traffic between business units. The firewall may block traffic at a designated port having the wrong protocol, for example, file transfer protocol (FTP) may be blocked on port 80. Similarly, the firewall may block all traffic on an unused port. Both hardware and software implementations of firewalls are available.

SUMMARY

[0004] A network, such as a local area network with a variety of electronic devices, may have a first group of devices capable of providing firewall services as well as a second group of devices with limited or no firewall capability. By publishing the firewall service capabilities of those devices having such a capability or by publishing the firewall

requirements of devices needing firewall services, or both, the network may be configured to allow the first group to supply firewall service to devices of the second group.

[0005] To support such a distributed firewall service, a device may need a capability to make known its interest/ability to supply firewall services. As well, another device may need a capability to publish its desire for firewall services. Network routing changes may need to be effected to reroute data traffic such that far roll services may be rendered and a manager function may be needed to match capabilities with needs and to direct data traffic rerouting. In addition, the manager function may enforce rules for minimum levels of firewall services for those devices that may not publish their needs, or whose published capabilities do not meet other system-level minimum requirements. The manager function may be independent of other devices in the network, such as in a router, or may be incorporated in one of the devices supplying or using firewall services.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Fig. 1 is a block diagram of a computer suitable for use in a network supporting a distributed firewall environment;

[0007] Fig. 2 is a block diagram of a computer network capable of supporting a distributed firewall implementation;

[0008] Fig. 3 is a logical view of one embodiment of the distributed firewall implementation;

[0009] Fig. 4 is another logical view of the embodiment of the distributed firewall implementation of Fig. 3;

[0010] Fig. 5 is a block diagram of a computer network showing another embodiment of the distributed firewall implementation;

[0011] Fig. 6 is a logical view of the embodiment of Fig. 5;

[0012] Fig. 7 is a view of yet another embodiment of a distributed firewall implementation;

[0013] Fig. 8 is a representative block diagram of a computer suitable for participation in a distributed firewall implementation; and

[0014] Fig. 9 is representative block diagram of another computer suitable for participation in a distributed firewall implementation.

DETAILED DESCRIPTION

[0015] Although the following text sets forth a detailed description of numerous different embodiments, it should be understood that the legal scope of the description is defined by the words of the claims set forth at the end of this disclosure. The detailed description is to be construed as exemplary only and does not describe every possible embodiment since describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology devéloped after the filing date of this patent, which would still fall within the scope of the claims.

[0016] It should also be understood that, unless a term is expressly defined in this patent using the sentence "As used herein, the term '_____' is hereby defined to mean..." or a similar sentence, there is no intent to limit the meaning of that term, either expressly or by implication, beyond its plain or ordinary meaning, and such term should not be interpreted to be limited in scope based on any statement made in any section of this patent (other than the language of the claims). To the extent that any term recited in the claims at the end of this patent is referred to in this patent in a manner consistent with a single meaning, that is done for sake of clarity only so as to not confuse the reader, and it is not intended that such claim term be limited, by implication or otherwise, to that single meaning. Finally, unless a claim element is defined by reciting the word "means" and a function without the recital of any structure, it is not intended that the scope of any claim element be interpreted based on the application of 35 U.S.C. § 112, sixth paragraph.

[0017] Much of the inventive functionality and many of the inventive principles are best implemented with or in software programs or instructions and integrated circuits (ICs) such as application specific ICs. It is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein will be readily capable of generating such software instructions and programs and ICs with minimal experimentation. Therefore, in the interest of brevity and minimization of any risk of obscuring the principles and concepts in accordance to the

present invention, further discussion of such software and ICs, if any, will be limited to the essentials with respect to the principles and concepts of the preferred embodiments.

[0018] Fig. 1 illustrates a computing device in the form of a computer 110 that may participate in a distributed firewall system. Components of the computer 110 may include, but are not limited to a processing unit 120, a system memory 130, and a system bus 121 that couples various system components including the system memory to the processing unit 120. The system bus 121 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnect (PCI) bus also known as Mezzanine bus.

[0019] The computer 110 typically includes a variety of computer readable media. Computer readable media can be any available media that can be accessed by computer 110 and includes both volatile and nonvolatile media, removable and non-removable media. By way of example, and not limitation, computer readable media may comprise computer storage media and communication media. Computer storage media includes volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical disk storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can accessed by computer 110. Communication media typically embodies computer readable instructions, data structures, program modules or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media includes wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency, infrared and other wireless media. Combinations of the any of the above should also be included within the scope of computer readable media.

[0020] The system memory 130 includes computer storage media in the form of volatile and/or nonvolatile memory such as read only memory (ROM) 131 and random access memory (RAM) 132. A basic input/output system 133 (BIOS), containing the basic routines that help to transfer information between elements within computer 110, such as during start-up, is typically stored in ROM 131. RAM 132 typically contains data and/or program modules that are immediately accessible to and/or presently being operated on by processing unit 120. By way of example, and not limitation, Figure 1 illustrates operating system 134, application programs 135, other program modules 136, and program data 137.

[0021] The computer 110 may also include other removable/non-removable, volatile/nonvolatile computer storage media. By way of example only, Figure 1 illustrates a hard disk drive 140 that reads from or writes to non-removable, nonvolatile magnetic media, a magnetic disk drive 151 that reads from or writes to a removable, nonvolatile magnetic disk 152, and an optical disk drive 155 that reads from or writes to a removable, nonvolatile optical disk 156 such as a CD ROM or other optical media. Other removable/non-removable, volatile/nonvolatile computer storage media that can be used in the exemplary operating environment include, but are not limited to, magnetic tape cassettes, flash memory cards, digital versatile disks, digital video tape, solid state RAM, solid state ROM, and the like. The hard disk drive 141 is typically connected to the system bus 121 through a non-removable memory interface such as interface 140, and magnetic disk drive 151 and optical disk drive 155 are typically connected to the system bus 121 by a removable memory interface, such as interface 150.

[0022] The drives and their associated computer storage media discussed above and illustrated in Figure 1, provide storage of computer readable instructions, data structures, program modules and other data for the computer 110. In Figure 1, for example, hard disk drive 141 is illustrated as storing operating system 144, application programs 145, other program modules 146, and program data 147. Note that these components can either be the same as or different from operating system 134, application programs 135, other program modules 136, and program data 137. Operating system 144, application programs 145, other program modules 146, and program data 147 are given different numbers here to illustrate that, at a minimum, they are different copies. A user may enter commands and information into the computer 110 through input devices such as a keyboard 162 and pointing device 161, commonly referred to as a mouse, trackball or touch pad. Another input device may be a

camera for sending images over the Internet, known as a web cam 163. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 120 through a user input interface 160 that is coupled to the system bus, but may be connected by other interface and bus structures, such as a parallel port, game port or a universal serial bus (USB). A monitor 191 or other type of display device is also connected to the system bus 121 via an interface, such as a video interface 190. In addition to the monitor, computers may also include other peripheral output devices such as speakers 197 and printer 196, which may be connected through an output peripheral interface 195.

[0023] The computer 110 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 180. The remote computer 180 may be a personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer 110, although only a memory storage device 181 has been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 171 and a wide area network (WAN) 173, but may also include other networks. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

[0024] When used in a LAN networking environment, the computer 110 is connected to the LAN 171 through a network interface or adapter 170. The network interface or adapter 170 may include a firewall capability, as is discussed further below. When used in a WAN networking environment, the computer 110 typically includes a modem 172 or other means for establishing communications over the WAN 173, such as the Internet. The modem 172, which may be internal or external, may be connected to the system bus 121 via the user input interface 160, or other appropriate mechanism. In a networked environment, program modules depicted relative to the computer 110, or portions thereof, may be stored in the remote memory storage device. By way of example, and not limitation, Figure 1 illustrates remote application programs 185 as residing on memory device 181. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

[0025] Fig. 2 illustrates a computer network 200 capable of supporting a distributed firewall implementation. An external network 201, such as the Internet, may be connected to

the computer network 200 by a network interface, such as router or Internet gateway device (IGD) 202. The connection between the IGD 202 and the network 201 may be referred to as the upstream connection of the IGD 202. On the opposite side of the IGD 202 may be one or more downstream connections. A first downstream connection 204 may be coupled to a printer 206 shared on the computer network 200, although it may also be made available to resources on the external network 201. A second downstream connection 208 may be coupled first to a computer 210 and subsequently to a computer 211. In this configuration, the computer 210 may share its connection with computer 211 over network connection 213 through facilities such as Internet connection sharing (ICS) available through Microsoft's Windows™ operating system. Another downstream connection 212 from the IGD 202 may couple to a wireless access point 214 supporting network access to a wireless device 216, such as a smart phone/personal digital assistant (PDA) and laptop 218 over a wireless transport 220.

[0026] In a traditional, prior art implementation, the IGD 202 may also include a firewall and perform that function for all devices on the downstream side of the IGD 202. This may result in all the downstream connections 204 208 212 and each associated device having the same firewall settings. The settings in an IGD-based firewall may default to a minimum level of protection or may not account for the different needs of some devices over others, such as printer 206 versus a wireless device 216. Current art IGD's, in addition to firewall services, often perform network address translation (NAT). IGD's supporting IPv6 will no longer provide NAT and may also minimize support for firewall services, making a distributed approach to providing firewall services more attractive, if not a necessity.

[0027] Firewall services may include a number of functions that provide a range of protective capabilities. Most firewalls have the ability to block unused ports, that is, to reject any incoming traffic on a port that is not currently associated with a particular application or service. On designated ports, the firewall may restrict traffic to an authorized protocol, such as http (hypertext transfer protocol) or ftp (file transfer protocol). Additionally, a firewall may restrict outbound traffic to specific ports, services or applications. For example, a web browser may not be able to send an outbound request on a port other than port 80. Any activity with an unknown source may be blocked. For example, a spyware program that is unknown to the firewall may be blocked from sending or receiving traffic. Firewalls may also distinguish between networks, that is, a local area network may have its traffic treated

differently from a wide-area network, such as the Internet. A firewall may act as an endpoint for a secure tunnel, such as a layer 4 virtual private network (VPN). In some cases, the firewall may require a secure tunnel for some connections or applications. The firewall may react to specific instructions to block or allow traffic as applications or services request connections.

[0028] Fig. 3 is a logical view of one embodiment of a distributed firewall implementation using the network 200 of Fig. 2. In a case where the IGD 202 does not provide suitable firewall services for a device, such as wireless device 216, computer 210, as well as IGD 202, may be configured to provide more appropriate firewall service. This may be accomplished by logically connecting the wireless access point 214 downstream from computer 210, such that all traffic intended for the wireless device 216 may be first routed through computer 210 via downstream connection 208 and logical connection 224.

[0029] Traffic for the wireless device 216 may include voice over IP (VOIP) or Internet packets. (Network agile smart phones may select a lower cost network such as WiFi when available.) The computer 210 may provide firewall services that restrict traffic to VOIP on one or more designated ports or Internet traffic to a designated wireless access protocol (WAP) port. The computer 210 may provide firewall services for itself as well. In such a case, it may publish that no services are required, so an upstream device or controller does not assign it default firewall services at another device. The logical connection 224 is discussed in more detail following with respect to Fig. 4.

[0030] Fig. 4 is another logical view of the embodiment of the distributed firewall implementation of Fig. 3. In operation, the logical connection 224 may be accomplished by changes in both the IGD 202 and computer 210. Traffic arriving from the network 201 destined for wireless device 216 may be routed first to the device 210 over logical connection 226 (physical connection 208). The traffic may be filtered in computer 210, re-addressed to the wireless device 216 and transmitted to the IGD 202 via logical connection 228. At the IGD 202, the filtered traffic may be rerouted via logical connection 230 to the wireless device 216. The IDG may therefore treat packets addressed to the wireless device 216 differently, depending on the source. Packets addressed to the wireless device 216 coming from the network 201 may be routed to the computer 210, while packets addressed to the wireless device 216 originating at the computer 210 are routed to the wireless device 216. The logical connection 230 may correspond to the physical connection 212 from the IGD 202 to the

wireless access point 214 and the over-the-air connection 220 from the wireless access point 214 to the wireless device 214.

[0031] In one embodiment, the wireless device 216 may publish a request for firewall services. The computer 210 may respond to the request and reach agreement with the wireless device 216 to provide the requested services. The IGD 202 may accept instructions from either the wireless device 216 or the computer 210 to reroute traffic as required. In some cases the IGD may accept instructions only from the device whose traffic is being rerouted. Cryptographic authentication may be required for the IGD 202 to accept such instructions. In another embodiment, the computer 210 may publish its ability to provide firewall services and the wireless device 216 may respond with a request. In both embodiments, the published data may use a peer-to-peer network discovery protocol to exchange firewall service information.

[0032] In yet another embodiment, the IGD 202, or one of the other downstream devices, may incorporate a manager that discovers firewall service requirements and firewall service capabilities and matches devices using that information. The manager may incorporate rules for identifying minimum firewall service requirements for each device, for example, by type. The manager may match firewall service providers to devices even when the device has some firewall capability, but, for example, doesn't meet the minimum firewall service requirement.

[0033] Fig. 5 is a block diagram of a computer network showing another embodiment of the distributed firewall implementation. In this exemplary embodiment, laptop 218 provides firewall services to printer 206. The printer 206 may have programmable elements, or a rudimentary processing capability, such as font or color translation. The printer 206 may then request appropriate firewall services by publishing a request to limit traffic to port 80 for printing jobs and port 443 for processing font or translation requests. The laptop 218 may respond to the request for firewall services from the printer 206 and the printer 206 may accept. After receiving a confirmation from the printer 206, the laptop 218 may direct the IGD 202 to reroute traffic for the printer as shown in Fig. 6. Turning briefly to Fig. 6, traffic from the network 201 destined for the printer 206 may be directed first to the laptop 218 over logical connection 232. As above, the laptop 218 may perform the requested firewall services on behalf of the printer 206 and forward the filtered traffic to the IGD 202 over logical connection 234. The IGD 202 may then route the traffic to printer 206 over logical connection 236.

[0034] Returning to Fig. 5, in an alternate embodiment , the IGD 202 may have a firewall capability. The laptop 218 may recognize the need for specialized firewall services for the printer 206 and direct the IGD 202 to provide the necessary services for the printer 206. In this case, the laptop 218 acts as a director, but does not actively manage traffic. In the role of director, the laptop 218 may also monitor and manage other aspects of firewall activity. For example, the laptop 218 may be programmed with parental controls, allowing firewall settings to change by user or by time of day. The embodiment of Figs. 5 and 6 use printer 206 and laptop 218 as exemplary network elements. The principals apply equally to other devices such as computer 210, PDA 216, or other devices not specifically depicted, such as a network-attached storage device.

[0035] Other sequences for firewall service discovery and agreement for services provisioning are possible, as discussed above with respect to Fig. 4.

[0036] Fig. 7 is a view of yet another embodiment of a distributed firewall implementation. Computer 210 is shown coupled to the network 201 over connection 208 via IGD 202. Computer 210 is also shown sharing its Internet connection with computer 211 over network connection 213. As mentioned above, this may be through an Internet connection sharing facility in computer 210 and may involve two network ports, one supporting connection 208 and the other supporting connection 213. Computer 211 may publish a request for firewall services and computer 210 may respond with its ability to provide the requested services. The two computers 210 211 may then agree to terms associated with providing the requested services. Such terms may include contractual or monetary considerations, but may also simply be an agreement that computer 210 will provide firewall services meeting the needs of computer 211, or a minimum requirement of the network 200. Logically, traffic received at the IGD 202 addressed to computer 211 may be transported to computer 210 over logical connection 238, filtered at computer 210 and forwarded over logical connection 240. Data from computer 211 may be sent via logical link 242 and forwarded via logical link 244 to the IGD 202 and eventually out to the network 201.

[0037] As shown in Fig. 2, other devices may exist on the downstream side of the IGD 202, including on network connection 208. The firewall services provided by computer 210 may offer protection not only from traffic on network 201, but also from undesired or unauthrorized traffic from these locally-connected devices.

[0038] Fig. 8 is a representative block diagram of a computer suitable for participation in a distributed firewall implementation. A wide area network 802 may have a network connection 804 to a router 806 or other Internet gateway connection. The router 806 may be coupled to a computer 808 via a connection 807. The computer 808 may have a network connection 810 supporting the connection 807 to the router 806. The computer 808 may also have a manager 812 or controller coupled to the network connection 810 and to a firewall service provider 814. The manager 812 may be operable to monitor published requests for firewall services from another device, such as electronic device 816. The manager 812 may then configure the network connection 810 to support receipt of traffic addressed to the electronic device 816 and route it to the firewall service 814. When traffic addressed to the electronic device 816 arrives, it may be routed to the firewall service 814 and processed according to the agreed upon firewall service requirements, resulting in filtered traffic. The network connection 810, in conjunction with the manager 812, may then return the filtered traffic from the firewall service 814 to the router 806 for delivery over network connection 818 to the electronic device 816. If the computer 808 also has some routing capability, it may send the filtered traffic directly to the electronic device 816 over connection 820. Traffic addressed to the computer 808 may also be processed by the firewall service 814.

[0039] In some cases, the manager 812 may change the level of firewall services provided, depending on requirements for compliance with standing policies or administrative rules. In many cases, the firewall services provided may be more restrictive than those requested by the electronic device 816, although less restrictive firewall services may apply. For example, less restrictive firewall services may be appropriate when the manager 812 is aware of upstream firewall services (not depicted) that reduce a local requirement.

[0040] Fig. 9 is a representative block diagram of another computer suitable for participation in a distributed firewall implementation. In an exemplary embodiment corresponding to the network configuration shown in Fig. 7, a network 902, such as the Internet, is shown coupled to computer 906 via network connection 904. The computer 906 has a first network connection 908, a manager 910 or controller, and a firewall service 912 similar to those described with respect to Fig. 8. Computer 906 is also shown having a second network connection 914 coupled via connection 916 to a network 918, and subsequently to electronic device 920. The electronic device 920 may request to firewall service, may respond to a published offer to provide firewall service by computer 906, or

may be assigned a default firewall service when the computer 906 cannot determine the firewall capability of the electronic device 920.

[0041] Traffic addressed to the electronic device 920 arriving at the network connection 908 may be directed by the manager 910 to the firewall service 912 where filtering may be performed on behalf of the device 920. The manager 910 may then direct the filtered traffic to network connection 914 for delivery to the electronic device 920.

[0042] While current networks and devices are expected to benefit from the apparatus and techniques described above, networks converted to IPv6 using lower cost and lower function Internet gateway devices maybe even bigger beneficiaries. Additionally, the use of an intelligent manager to evaluate firewall service needs and requirements, in light of administrative rules and current network architecture, may allow less duplication of functionality while maintaining or exceeding protection provided by previous firewall architectures.

[0043] Although the forgoing text sets forth a detailed description of numerous different embodiments of the invention, it should be understood that the scope of the invention is defined by the words of the claims set forth at the end of this patent. The detailed description is to be construed as exemplary only and does not describe every possibly embodiment of the invention because describing every possible embodiment would be impractical, if not impossible. Numerous alternative embodiments could be implemented, using either current technology or technology developed after the filing date of this patent, which would still fall within the scope of the claims defining the invention.

[0044] Thus, many modifications and variations may be made in the techniques and structures described and illustrated herein without departing from the spirit and scope of the present invention. Accordingly, it should be understood that the methods and apparatus described herein are illustrative only and are not limiting upon the scope of the invention.

We claim:

1. A method of configuring firewall services in a network 200 having a plurality of devices comprising:

determining a firewall capability for a first device 210 in the network 200;

determining a firewall service requirement for a second device 216 in the network; and

configuring the first device 210 to provide firewall service for itself 210 and for the second device 216 according to the firewall service requirement of the second device 216 and the firewall capability of the first device 210.

2. The method of claim 1, further comprising configuring a router 202 to logically place the second device 216 behind the first device 210.

3. The method of claim 1, wherein determining the firewall capability for the first device 210 comprises monitoring published information corresponding to the firewall capability of the first device 210.

4. The method of claim 1, wherein determining the firewall service requirement comprises monitoring a published request for firewall services from the second device 216.

5. The method of claim 4, wherein an administrative setting requires the firewall service to be more restrictive than the published request for firewall services from the second device 216.

6. The method of claim 1, wherein determining the firewall service requirement comprises selecting a default firewall service for the second device 216 when no published information is available from the second device 216.

7. The method of claim 1, wherein an upstream device 202 sets open access for its firewall service when a downstream device 210 has a firewall capability that meets a minimum firewall capability.

8. A network 200 having a plurality of devices adapted for configurable firewall protection comprising:
a router 806 with an upstream side 804 and a downstream side 807 818 for directing data traffic with devices on the network;
a first device 808 coupled to the downstream side 807 of the router, the first device 808 having an ability to supply at least one firewall capability; and
a second device 816 coupled to the downstream side of the router 818, the second device 816 adapted to publish a request for a firewall service, wherein the first device 808 supplies the at least one firewall capability responsive to the request from the second device 816 when the at least one firewall capability of the first device 808 meets a requirement of the request for the firewall service.

9. The network of claim 8, wherein the requirement is implicit in the request.

10. The network of claim 8, wherein the router 806 accepts a signal to direct incoming traffic addressed to the second device 816 to the first device 808 for fulfilling the request for the firewall service.

11. The network of claim 8, wherein the first device 808 shares out a network connection 820 916 to the second device 816 920.

12. The network of claim 8, wherein the first device 808 publishes the ability to supply the at least one firewall capability.

13. The network of claim 12, wherein the second device 816 receives from the first device 808 the published ability to supply the at least one firewall capability and directs the request for the firewall service to the first device 808.

14. The network of claim 8, further comprising a controller 812 for monitoring a firewall capability and a firewall service requirement for each of the plurality of devices adapted for configurable firewall protection.

15. The network of claim 14, wherein the controller 812 is incorporated in one of the first device 808 and the router 806.

16. The network of claim 14, wherein the controller 812 has a communication function for publishing a firewall service requirement to each of the plurality of devices.

17. The network of claim 16, wherein the first device 808 supplies the at least one firewall capability to be more restrictive than the request for firewall service from the second device 816 when the published firewall service requirement is more restrictive than the request for firewall service from the second device 816.

18. The network of claim 14, wherein the controller 812 assigns a default firewall service for a third device 206 that does not publish a request for firewall service.

19. A computer 808 arranged and adapted to provide firewall services to an other electronic device 816 comprising:
a network connection 810 supporting bidirectional data traffic with an upstream network 804;
a manager 812 coupled to the network connection 807 operable to monitor published requests for firewall services from the other electronic device 816, and, responsive to the request, configure the network connection 810 to place the other electronic device 816 logically downstream of the computer 808, and determine a level of firewall service to provide to the other electronic device 816; and
a firewall service provider 814 coupled to the manager 812 and the network connection 810, wherein the firewall service provider supports firewall service for itself 808 and provides firewall service for data traffic addressed to the other electronic device 816 according to the level determined by the manager 812.

20. The computer of claim 19, further comprising a second network connection 916 wherein data traffic on the network connection addressed to the other electronic device 920 is filtered according to the level of firewall service and routed via the second network connection 916.

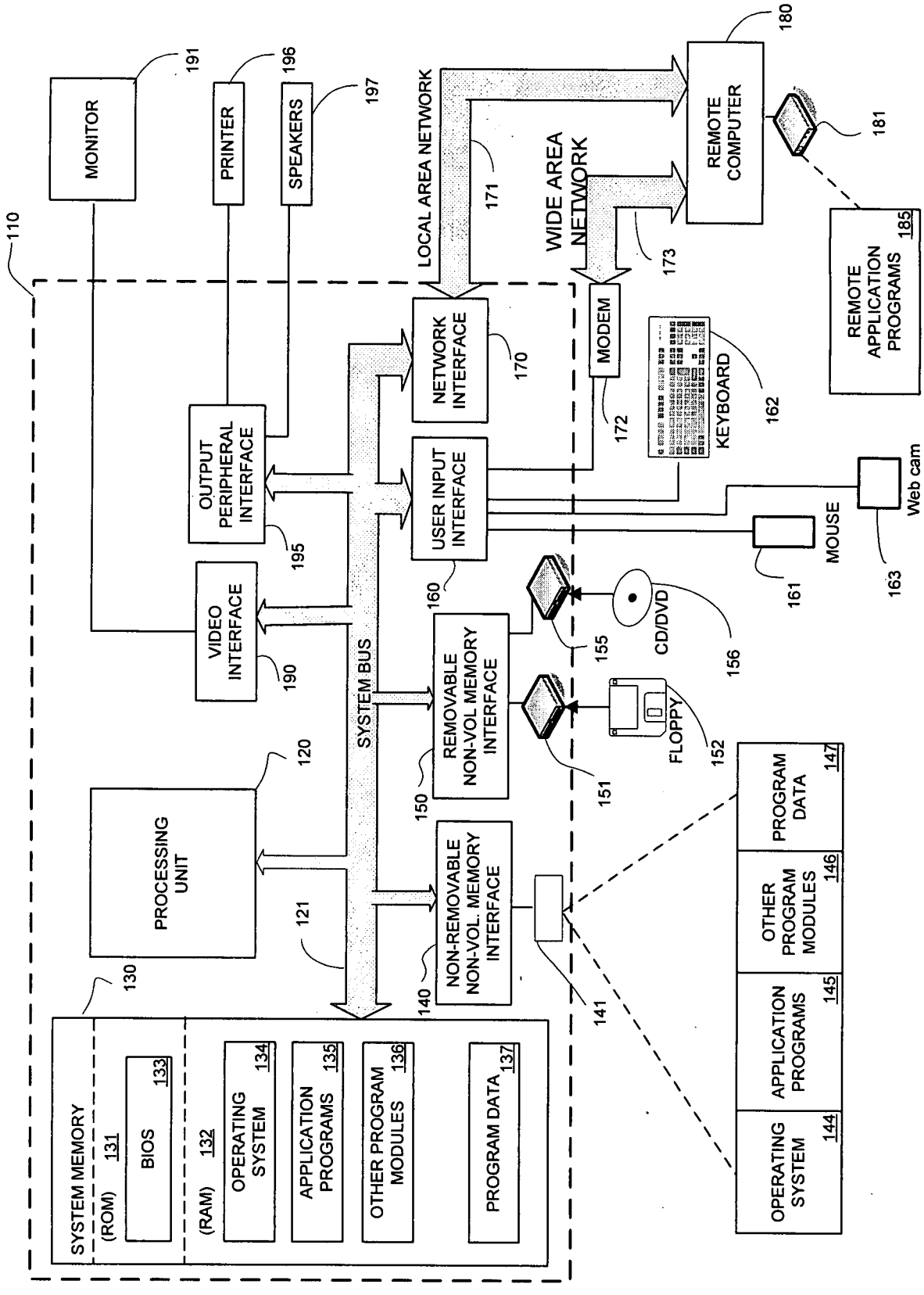
110
MONITOR
191
PRINTER
196
SPEAKERS
197
LOCAL AREA NETWORK
WIDE AREA NETWORK
171
REMOTE COMPUTER
180
181
173
REMOTE APPLICATION PROGRAMS
185
MODEM
172
NETWORK INTERFACE
170
KEYBOARD
162
OUTPUT PERIPHERAL INTERFACE
195
USER INPUT INTERFACE
160
MOUSE
161
Web cam
163
VIDEO INTERFACE
190
SYSTEM BUS
155
CD/DVD
156
REMOVABLE NON-VOL MEMORY INTERFACE
150
151
FLOPPY
152
PROCESSING UNIT
120
121
NON-REMOVABLE NON-VOL. MEMORY INTERFACE
140
141
PROGRAM DATA
147
OTHER PROGRAM MODULES
146
APPLICATION PROGRAMS
145
OPERATING SYSTEM
144
SYSTEM MEMORY
130
(ROM) 131
BIOS 133
(RAM) 132
OPERATING SYSTEM 134
APPLICATION PROGRAMS 135
OTHER PROGRAM MODULES 136
PROGRAM DATA 137

Fig. 1

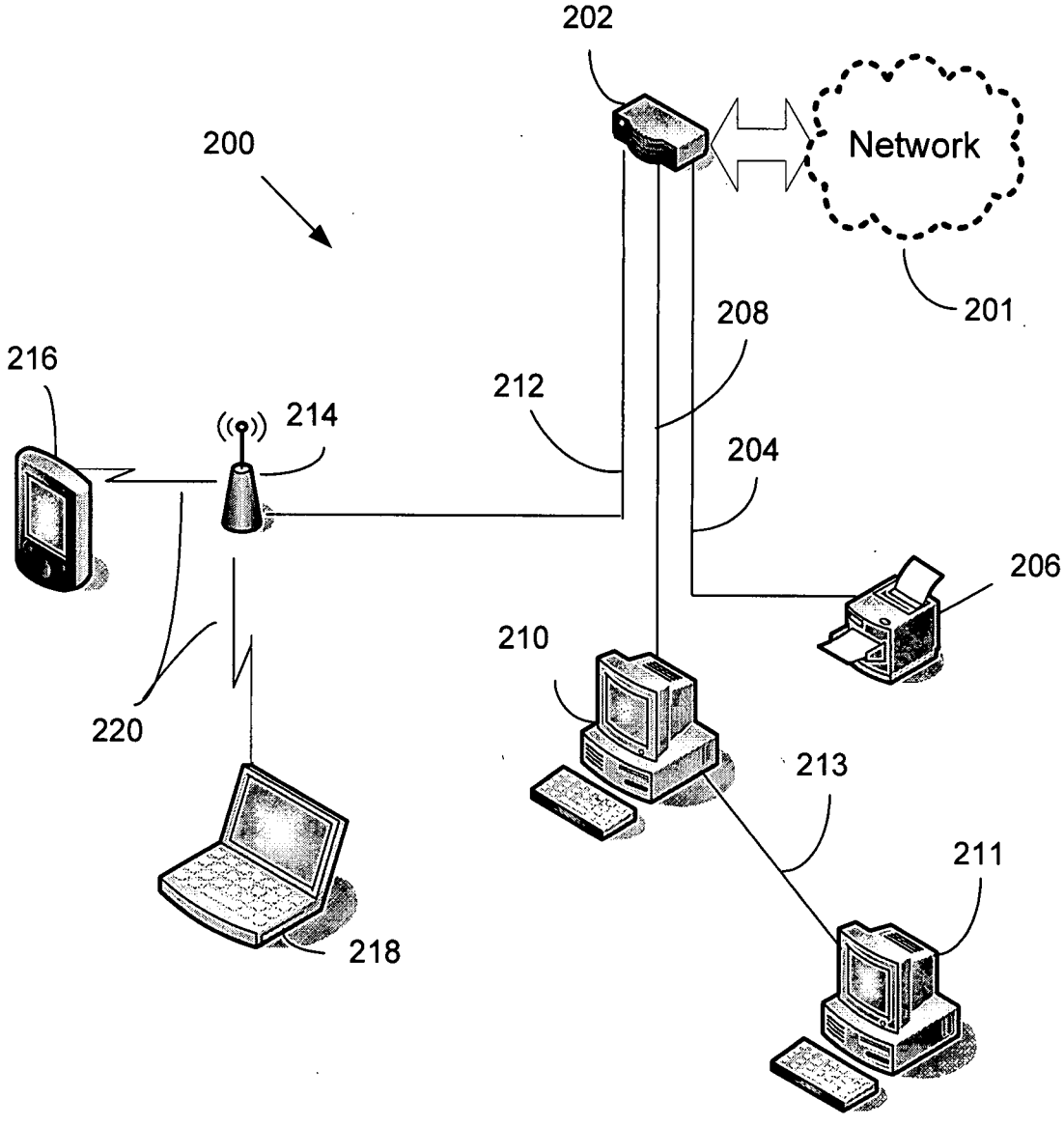

FIG. 2

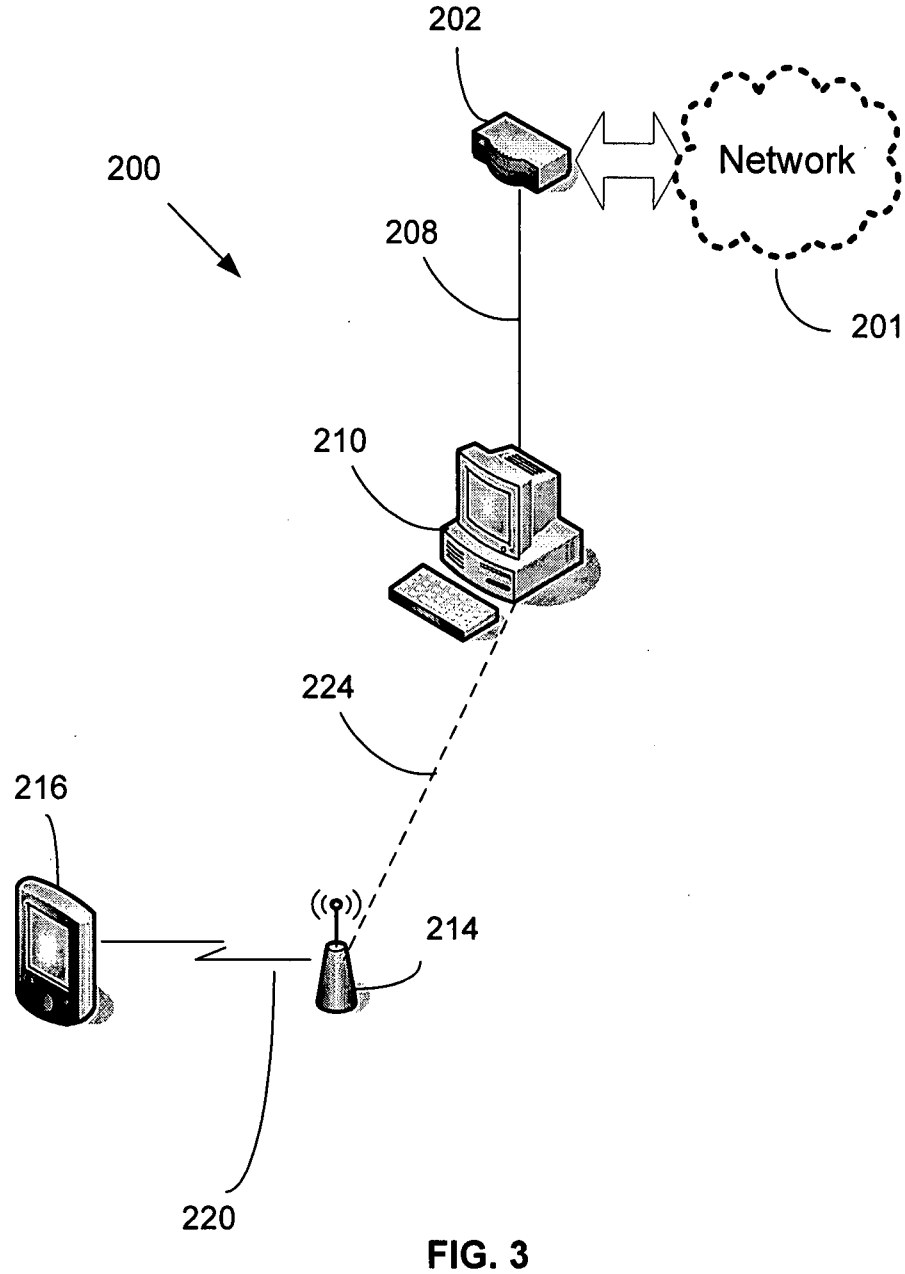

FIG. 3

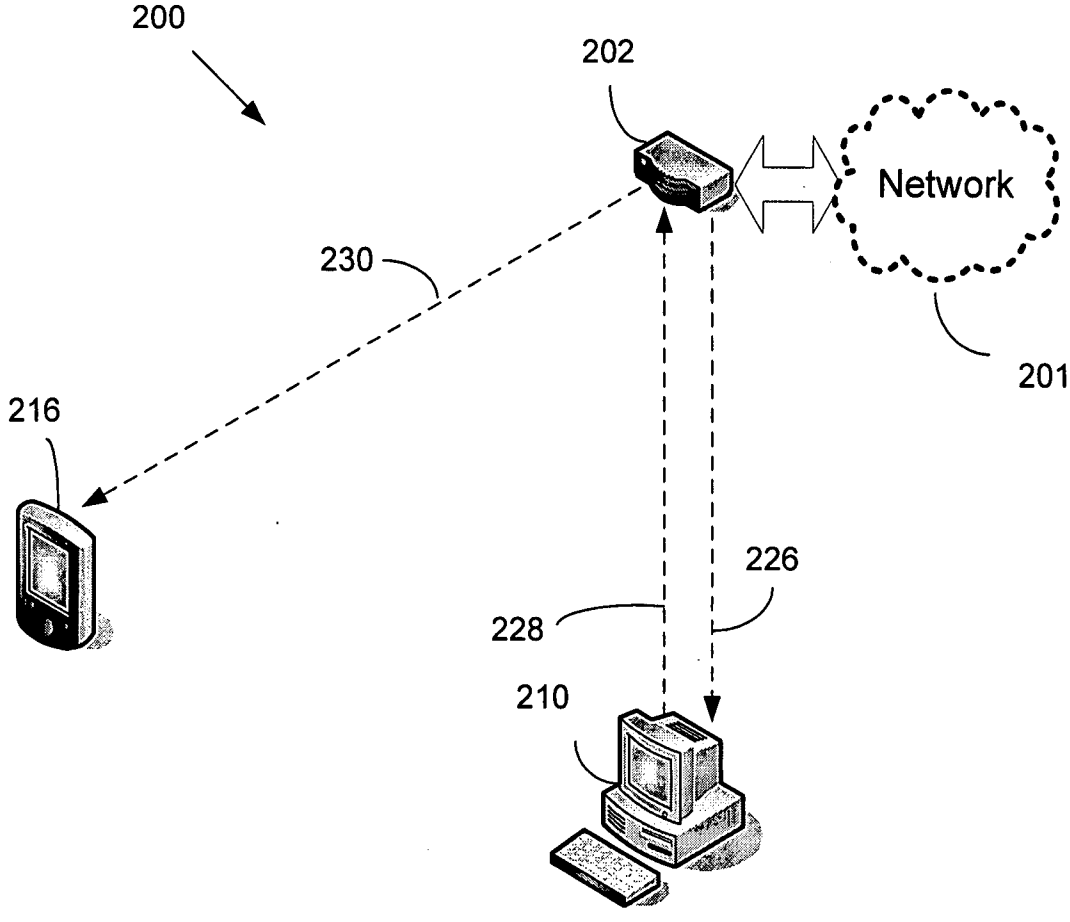

FIG. 4

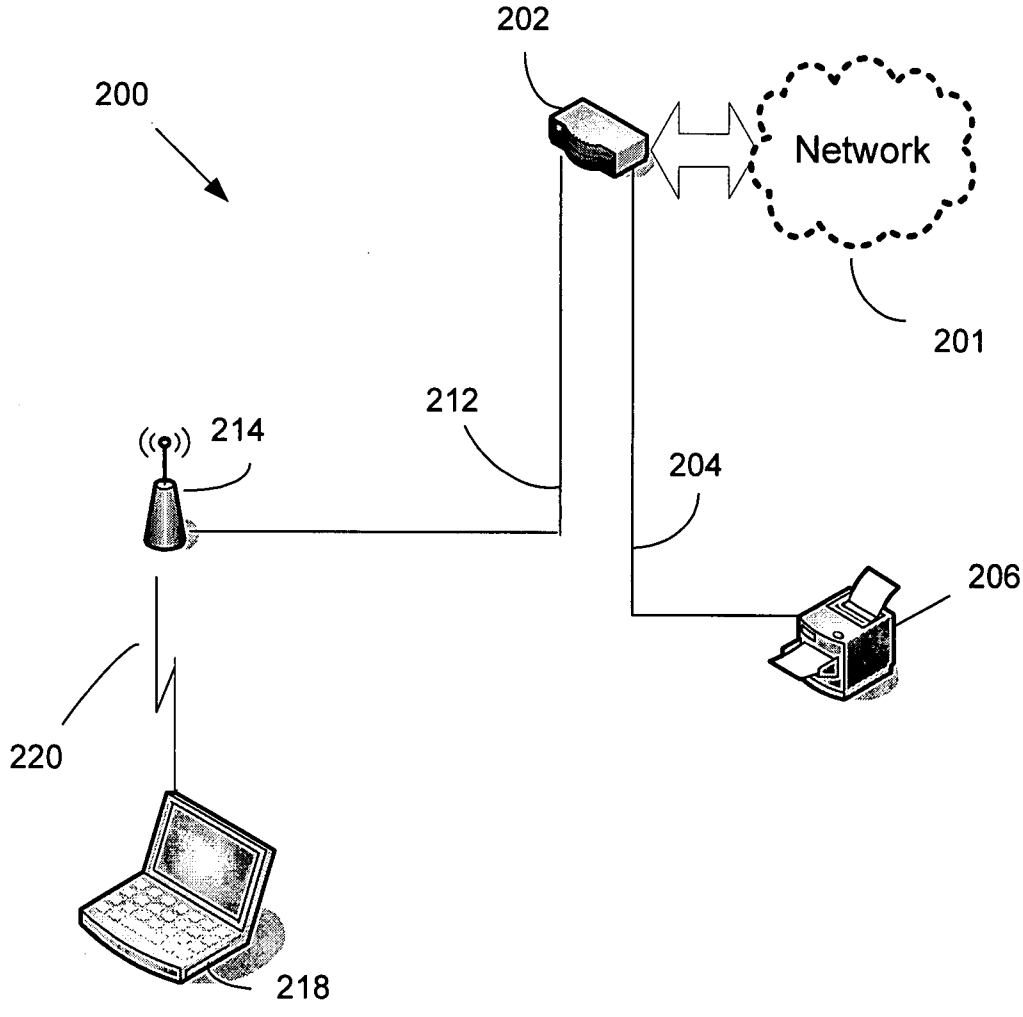

FIG. 5

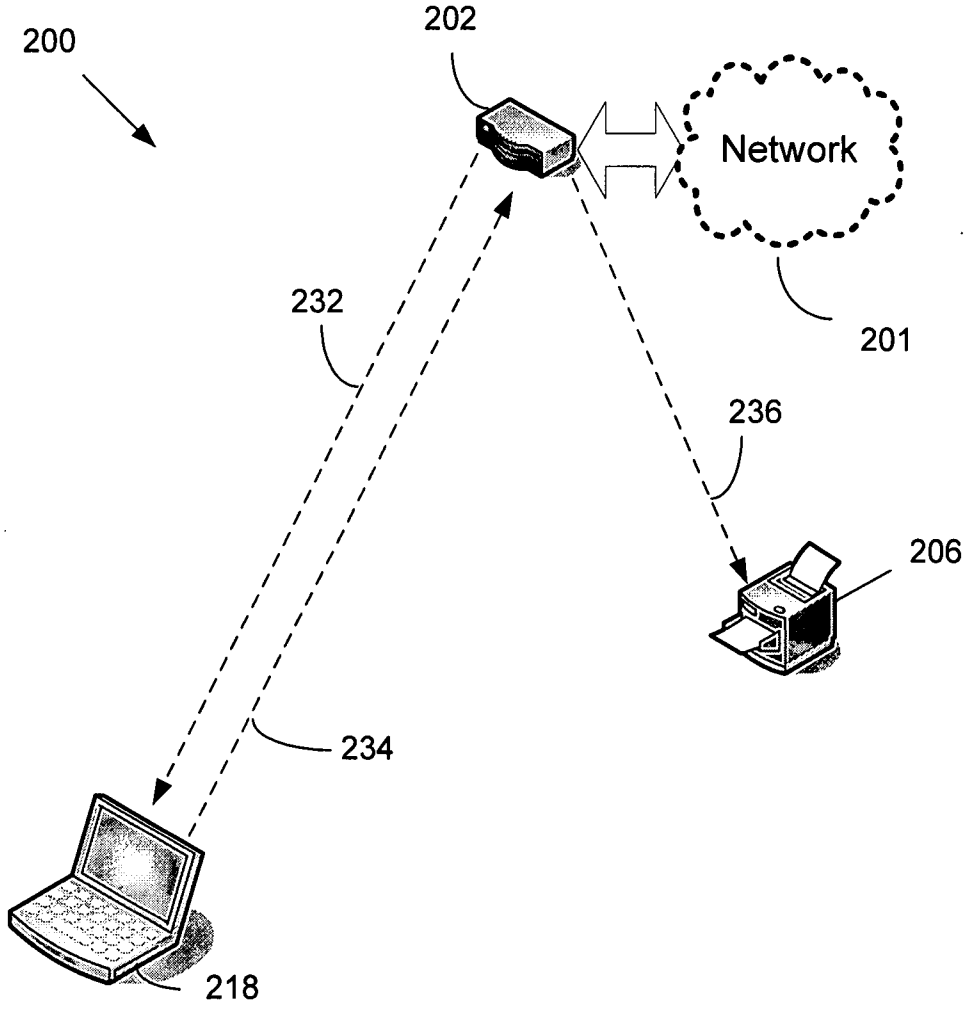

FIG. 6

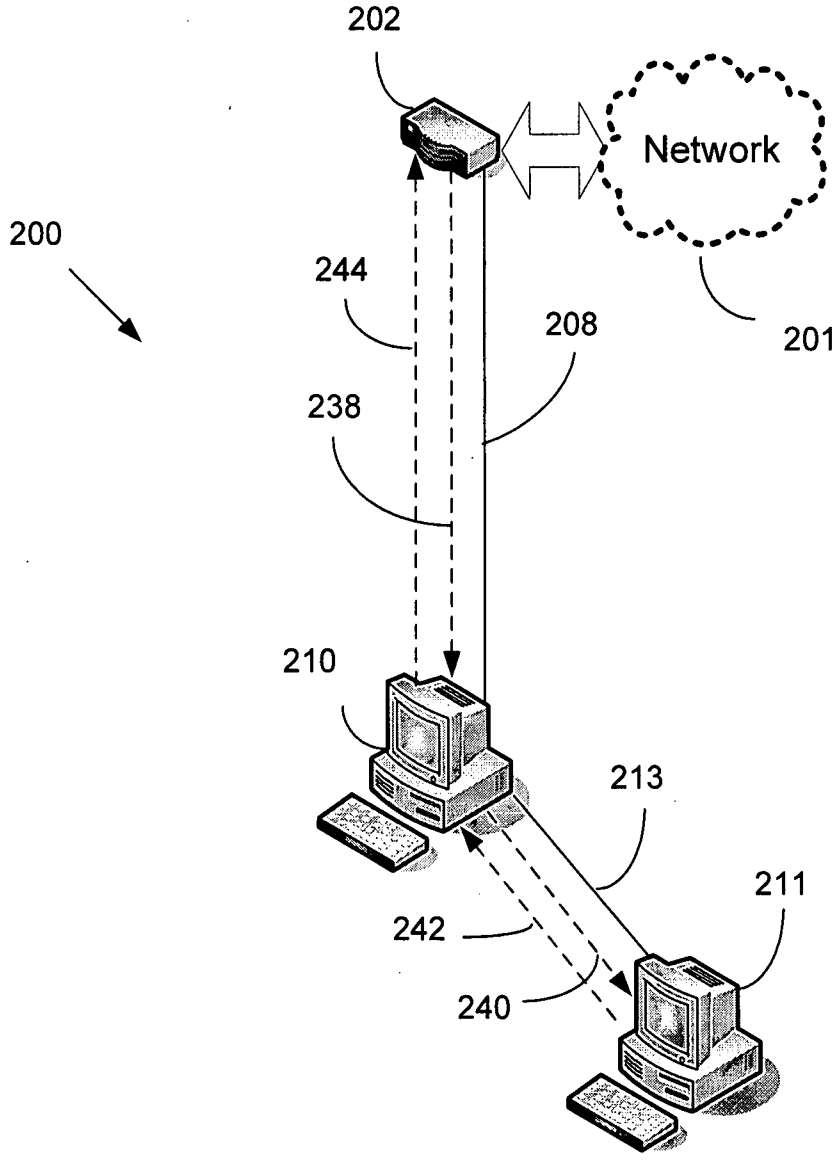

FIG. 7

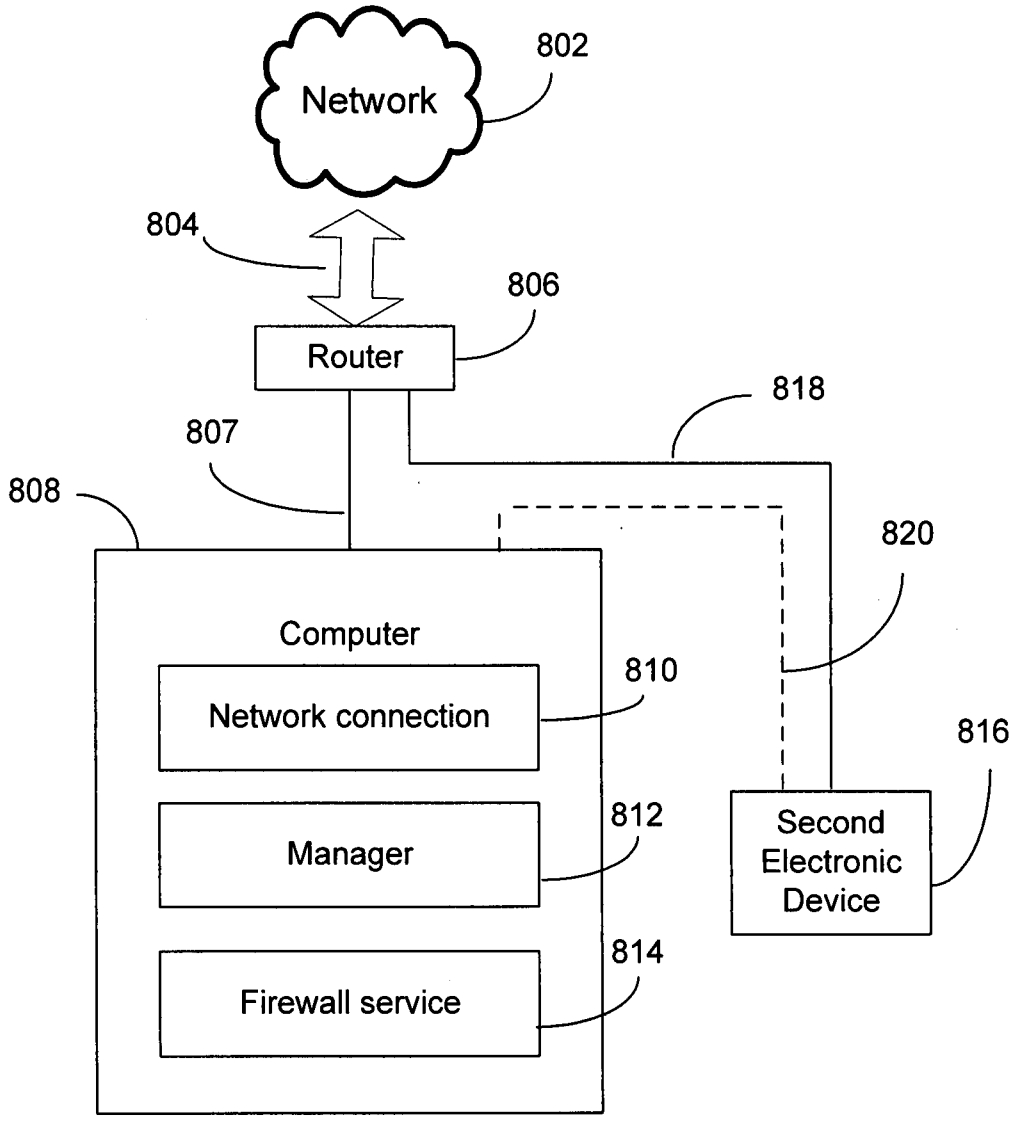
Network
802
804
806
Router
818
807
808
820
Computer
Network connection
810
816
Manager
812
Second Electronic Device
Firewall service
814

FIG. 8

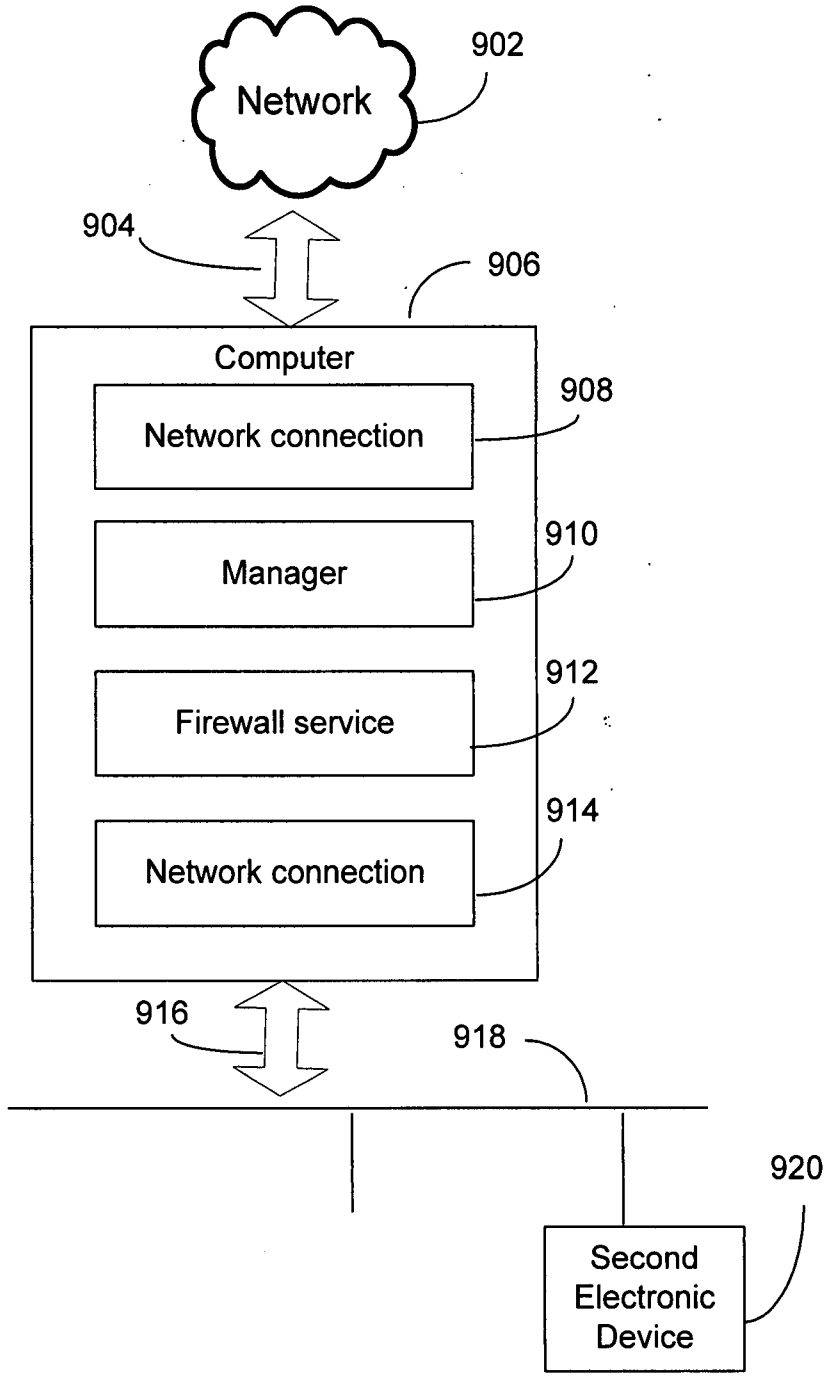
Network
902
904
906
Computer
908
Network connection
910
Manager
912
Firewall service
914
Network connection
916
918
920
Second Electronic Device

FIG. 9