República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial.

(21) **PI0710933-4 A2**

BRPI0710933A2

(22) Data de Depósito: 07/05/2007
(43) Data da Publicação: 31/05/2011
(RPI 2108)

(51) Int.Cl.:
H04L 12/22 2006.01
G06F 21/20 2006.01

(54) Título: **IMPLEMENTAÇÃO DE FIREWALL DISTRIBUÍDO E CONTROLE**

(30) Prioridade Unionista: 05/05/2006 US 11/429.476

(73) Titular(es): Microsoft Corporation

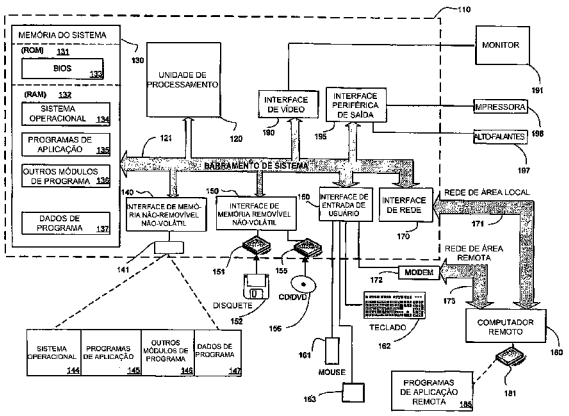
(72) Inventor(es): David A. Roberts

(74) Procurador(es): Nellie Anne Daniel-shores

(86) Pedido Internacional: PCT US2007011053 de 07/05/2007

(87) Publicação Internacional: WO 2008/100265de 21/08/2008

(57) Resumo: IMPLEMENTAÇÃO DE FIREWALL DISTRIBUÍDO E CONTROLE Um método para gravar um material alvo na presença de um material estrutural com seletividade aperfeiçoada utiliza um gravador de fase de vapor e um co-gravador. Modalidades do método apresentam seletividades aperfeiçoadas a partir de ao menos aproximadamente 2 vezes a ao menos aproximadamente 100 vezes em comparação com um pro- cesso de gravação similar não utilizando um co-gravador. Em algumas modalidades, o material alvo compreende um metal que pode ser gravado por intermédio do gravador de fase de vapor. Modalidades do método são particularmente úteis na fabricação de dispositivos MEMS, por exemplo, moduladores interferométricos. Em algumas modalidades, o material alvo compreende um metal que pode ser gravado pelo gravador de fase de vapor, por e- xemplo, molibdênio; e o material estrutural compreende um material dielétrico, por exemplo, diáxido de silício.



"IMPLEMENTAÇÃO DE FIREWALL DISTRIBUÍDO E CONTROLE"

ANTECEDENTES

Um computador conectado a uma rede está vulnerável a ataque a partir de outros computadores naquela rede. Se a rede é a Internet, os ataques podem incluir uma gama de ações a partir de tentativas maliciosas para obter acesso ao computador, para instalar código "zumbi", para negativa de ataques de negativa de serviço. Tentativas maliciosas para obter acesso ao computador podem ter a intenção de descobrir dados pessoais, enquanto que o código zumbi ode ser usado para lançar ataques de negativa de serviço mediante neutralização de um local da Rede com elevados volumes de tráfego a partir de um número de computadores. Os violadores podem incluir criminosos organizados, peritos em computador sofisticados, porém maliciosos, e "script kiddies" que lêem e repetem os ataques postados em vulnerabilidades conhecidas.

A maioria dos computadores tem portas endereçáveis para enviar e receber dados. Algumas das portas podem ser designadas para certos tipos de tráfego. Por exemplo, em uma rede de Protocolo Internet (IP), a porta 80 freqüentemente é designada para tráfego de protocolo de hipertexto (http), enquanto que a porta 443 freqüentemente é designada para tráfego http seguro (https). Outras portas podem ser designadas conforme necessário para diferentes serviços. Tráfego não-designado em tais portas designadas e qualquer tráfego em portas não-utilizadas pode indicar tentativas pelos violadores em obter acesso ao computador.

Um firewall pode ser usado para limitar o tráfego de porta para certos protocolos e para fechar portas não utilizadas a partir de todo o tráfego externo. O firewall pode ser colocado em uma rede entre computadores procurando proteção e redes "abertas", tal como a Internet, ou pode ser integral ao computador. Nas corporações, ou grandes redes privadas, firewalls podem também ser usados para limitar o tráfego entre unidades comerciais. O firewall pode bloquear o tráfego em uma porta designada tendo o protocolo errado, por exemplo, protocolo de transferência de arquivo (FTP) pode ser bloqueado na porta 80. Similarmente, o firewall pode bloquear todo o tráfego em uma porta não utilizada. Implementações não somente de hardware, mas também de software dos firewalls estão disponíveis.

SUMÁRIO

Uma rede, tal como uma rede de área local com uma variedade de dispositivos eletrônicos, pode ter um primeiro grupo de dispositivos capaz de prover serviços de firewall assim como um segundo grupo de dispositivos com capacidade limitada ou nenhuma capacidade de firewall. Mediante publicação das capacidades de serviço de firewall desses dispositivos tendo tal capacidade ou mediante publicação das exigências de firewall dos dispositivos precisando de serviços de firewall, ou ambos, a rede pode ser configurada para permitir que o primeiro grupo forneça serviço de firewall aos dispositivos do segundo grupo.

Para suportar tal serviço de firewall distribuído, um dispositivo pode precisar de uma capacidade para tornar conhecido o seu interesse/capacidade em fornecer serviços de firewall. Do mesmo modo, outro dispositivo pode precisar de uma capacidade para publicar seu desejo pelos serviços de firewall. Mudanças de roteamento de rede podem precisar ser realizadas para re-encaminhar o tráfego de dados de tal modo que serviços de processamento distante possam ser executados e uma função de gerenciador pode ser necessária para combinar as capacidades com as necessidades e dirigir o re-roteamento de tráfego de dados. Além disso, a função de gerenciador pode impor regras para níveis mínimos de serviços de firewall para aqueles dispositivos que podem não publicar suas necessidades, ou cujas capacidades publicadas não atendem outras exigências mínimas a nível de sistema. A função de gerenciador pode ser independente de outros dispositivos na Rede, tal como em um roteador, ou pode ser incorporada em um dos dispositivos fornecendo ou utilizando os serviços de firewall.

DESCRIÇÃO RESUMIDA DOS DESENHOS

A Figura 1 é um diagrama de blocos de um computador adequado para uso em uma rede suportando um ambiente de firewall distribuído;

A Figura 2 é um diagrama de blocos de uma rede de computador capaz de suportar uma implementação de firewall distribuído;

A Figura 3 é uma vista lógica de uma modalidade da implementação de firewall distribuído;

A Figura 4 é outra vista lógica da modalidade da implementação de firewall distribuído da Figura 3;

A Figura 5 é um diagrama de blocos de uma rede de computador mostrando outra modalidade da implementação de firewall distribuído;

A Figura 6 é uma vista lógica da modalidade da Figura 5;

A Figura 7 é uma vista de ainda outra modalidade de uma implementação de firewall distribuído;

A Figura 8 é um diagrama representativo de blocos de um computador adequado para participação em uma implementação de firewall distribuído; e

A Figura 9 é um diagrama representativo de blocos de outro computador adequado para participação em uma implementação de firewall distribuído.

DESCRIÇÃO DETALHADA

Embora o texto a seguir ilustre uma descrição detalhada de várias modalidades diferentes, deve ser entendido que o escopo legal da descrição é definido pelos termos das reivindicações apresentadas no fim dessa revelação. A descrição detalhada deve ser considerada apenas como exemplar e não descreve cada modalidade possível uma vez que descrever cada modalidade possível seria impraticável, se não impossível. Várias modalidades

alternativas poderiam ser implementadas, utilizando quer seja tecnologia atual ou tecnologia desenvolvida após a data de depósito dessa patente, a qual ainda estaria abrangida pelo escopo das reivindicações.

Também deve ser entendido que, a menos que um termo seja expressamente definido nessa patente utilizando a frase "como aqui usado, o termo "_____" é definido aqui como significando..." ou uma frase similar, não existe a intenção de limitar o significado daquele termo, seja expressamente ou mediante implicação, além de seu significado simples ou comum, e tal termo não deve ser interpretado como limitado em escopo com base em qualquer declaração feita em qualquer seção desta patente (exceto a linguagem das reivindicações). Até o ponto em que qualquer termo citado nessas reivindicações no fim dessa patente é referido nessa patente de uma maneira compatível com um único significado, isto é feito com o propósito apenas de clareza de modo a não confundir o leitor, e não se pretende que tal termo da reivindicação seja limitado, mediante implicação ou de outro modo, aquele único significado. Finalmente, a menos que o elemento da reivindicação seja definido mediante exposição da palavra - "meios", e uma função sem a exposição de qualquer estrutura, não se pretende que o escopo de qualquer elemento da reivindicação seja interpretado com base na aplicação de 35 U.S.C. § 112, parágrafo sexto.

Grande parte da funcionalidade inventiva e muitos dos princípios inventivos são mais bem implementados com ou nos programas de software ou instruções e circuitos integrados (ICs) tal como os ICs de aplicação específica. Espera-se que aqueles versados na técnica, não obstante possivelmente esforço significativo e muitas escolhas de projeto motivadas, por exemplo, pelo tempo disponível, tecnologia atual, e considerações econômicas, quando orientados pelos conceitos e princípios aqui revelados serão facilmente capazes de gerar tais instruções e programas de software e os ICs com experimento mínimo. Portanto, no interesse de brevidade e minimização de qualquer risco de obscurecer os princípios e conceitos de acordo com a presente invenção, discussão adicional de tal software e dos ICs, se houver, será limitada aos elementos indispensáveis com relação aos princípios e conceitos das modalidades preferidas.

A Figura 1 ilustra um dispositivo de computação na forma de um computador 110 que pode participar em um sistema de firewall distribuído. Os componentes do computador 110 podem incluir, mas não são limitados a uma unidade de processamento 20, uma memória de sistema 130, e um barramento de sistema 121 que acopla vários componentes de sistema incluindo a memória do sistema à unidade de processamento 120. O barramento de sistema 121 pode ser qualquer um de vários tipos de estruturas de barramento incluindo um barramento de memória ou controlador de memória, um barramento periférico, e um barramento local utilizando qualquer uma de uma variedade de arquiteturas de barramento. Como exemplo e não como limitação, essas arquiteturas incluem: barramento de Arquitetura

Padrão da Indústria (ISA); barramento de Arquitetura de Microcanal (MCA); barramento de ISA Otimizada (EISA); barramento local da Associação de Padrões de Eletrônica de Vídeo (VESA); e barramento de Interconexão de Componentes Periféricos (PCI) também conhecido como barramento Mezzanine.

O computador 110 inclui tipicamente uma variedade de meios legíveis por computador. Meios legíveis por computador podem ser quaisquer meios disponíveis que possam ser acessados pelo computador 110 e incluem não só meios voláteis como também meios não-voláteis, meios removíveis e meios não-removíveis. Por intermédio de exemplo, e não limitação, meios legíveis por computador podem compreender meios de armazenamento de computador e meios de comunicação. Meios de armazenamento de computador incluem meios voláteis e não-voláteis, removíveis e não-removíveis implementados em qualquer método ou tecnologia para armazenamento de informação tal como instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados. Meios de armazenamento de computador incluem, mas não são limitados a, RAM, ROM, EEPROM, memória flash ou outra tecnologia de memória, CD-ROM, discos digitais versáteis (DVD) ou outro armazenamento de disco ótico, cassetes magnéticos, fita magnética, armazenamento de disco magnético ou outros dispositivos de armazenamento magnético, ou qualquer outro meio que possa ser usado para armazenar a informação desejada e o qual possa ser acessado pelo computador 110. Os meios de comunicação incorporam tipicamente instruções legíveis por computador, estruturas de dados, módulos de programa ou outros dados em um sinal modulado de dados tal como uma onda portadora ou outro mecanismo de transporte e inclui quaisquer meios de fornecimento de informação. O termo "sinal modulado de dados" significa um sinal que tem uma ou mais de suas características definidas ou alteradas de tal modo a codificar informação no sinal. Como exemplo, e não como limitação, meios de comunicação incluem meios cabeados tal como uma rede cabeada, ou conexão cabeada direta; e meios sem fio tais como meios acústicos, de radiofreqüência, de infravermelho e outros. Combinações de quaisquer dos mencionados acima também podem estar incluídas dentro do escopo de meios legíveis por computador.

A memória de sistema 130 inclui meios de armazenamento de computador na forma de memória volátil e/ou não-volátil tal como memória de leitura (RAM) 131 e memória de acesso aleatório RAM 132. Um sistema de entrada/saída básico 133 (BIOS), contendo as rotinas básicas que ajudam a transferir informação entre elementos dentro do computador 110, tal como durante a partida, é tipicamente armazenado na ROM 131. A RAM 132 contém tipicamente módulos de dados e/ou programas que são imediatamente acessíveis e/ou presentemente sendo operados pela unidade de processamento 120. Como exemplo, e não como limitação, a Figura 3 ilustra o sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137.

O computador 110 também pode incluir outros meios de armazenamento de computador removíveis/não-removíveis, voláteis/não-voláteis. Apenas como exemplo, a Figura 1 ilustra uma unidade de disco rígido 140 que lê a partir dos meios magnéticos não-removíveis, não-voláteis, ou grava nos mesmos, uma unidade de disco magnético 151 que lê a partir de um disco magnético removível, não-volátil 152 ou grava no mesmo, e uma unidade de disco ótico 155 que lê a partir do disco ótico removível, não-volátil 156 ou grava no mesmo, tal como um CD-ROM ou outros meios óticos. Outros meios de armazenamento de computador removíveis/não-removíveis, voláteis/não-voláteis que podem ser usados no ambiente de operação exemplar incluem, mas não são limitados a, cassetes de fita magnética, cartões de memória flash, discos versáteis digitais, fita de vídeo digital, RAM de estado sólido, ROM de estado sólido, e semelhante. A unidade de disco rígido 141 é conectada tipicamente ao barramento de sistema 121 através de uma interface de memória não-removível tal como interface 140, e unidade de disco magnético 151 e unidade de disco ótico 155 são conectadas tipicamente ao barramento de sistema 121 por intermédio de uma interface de memória removível, tal como a interface 150.

As unidades e seus meios de armazenamento de computador associados discutidos acima, ilustrados na Figura 1, proporcionam armazenamento de instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 110. Na Figura 1, por exemplo, a unidade de disco rígido 141 é ilustrada como armazenando o sistema operacional 144, programas de aplicação 145, outros módulos de programa 146, e dados de programa 147. Observar que esses componentes podem ser ou idênticos ou diferentes do sistema operacional 134, programas de aplicação 135, outros módulos de programa 136, e dados de programa 137. O sistema operacional 144, programas de aplicação 145, outros módulos de programa 146, e dados de programa 147 recebem aqui números diferentes para ilustrar que, no mínimo, eles são cópias diferentes. Um usuário pode introduzir comandos e informação no computador 110 através dos dispositivos de entrada tal como um teclado 162 e um dispositivo indicador 161, comumente referido como um mouse, trackball ou elemento sensível ao toque. Outro dispositivo de entrada pode ser uma câmera para enviar imagens através da Internet, conhecida como web cam 163. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, joystick, elemento de jogos, prato de satélite, scanner, ou semelhantes. Esses e outros dispositivos de entrada freqüentemente são conectados à unidade de processamento 120 através de uma interface de entrada de usuário 160 que é acoplada ao barramento de sistema, mas pode ser conectada por outra interface e estruturas de barramento, tal como uma porta paralela, porta de jogos ou um barramento serial universal (USB). Um monitor 191 ou outro tipo de dispositivo de exposição também é conectado ao barramento de sistema 121 por intermédio de uma interface, tal como uma interface de vídeo 190. Além do monitor, os computadores também podem incluir

outros dispositivos periféricos de saída tais como alto-falantes 197 e impressora 196, que podem ser conectados através de uma interface periférica de saída 195.

O computador 110 pode operar em um ambiente de rede utilizando conexões lógicas para um ou mais computadores remotos, tal como um computador remoto 180. O computador remoto 180 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo não-hierárquico ou outro nó de rede comum e, tipicamente, inclui vários ou todos os elementos descritos acima em relação ao computador 110, embora apenas um dispositivo de armazenamento de memória 181 tenha sido ilustrado na Figura 1. As conexões lógicas ilustradas na Figura 1 incluem uma rede de área local (LAN) 171 e uma rede de área remota (WAN) 173, mas pode incluir também outras redes. Tais ambientes de rede são comuns em escritórios, redes de computadores empresariais, intranets e a Internet.

Quando usado em um ambiente de rede LAN, o computador 110 é conectado à LAN 171 através de uma interface ou adaptador de rede 170. A interface ou adaptador de rede 170 pode incluir uma capacidade de firewall, conforme discutido adicionalmente abaixo. Quando usado em um ambiente de rede WAN, o computador 110 inclui tipicamente um modem 172 ou outro meio para estabelecer comunicações através da WAN 173, tal como a Internet. O modem 172, o qual pode ser interno ou externo, pode ser conectado ao barramento de sistema 121 por intermédio da interface de entrada de usuário 160, ou outro mecanismo apropriado. Em um ambiente de rede, os módulos de programa ilustrados em relação ao computador 110, ou porções do mesmo, podem ser armazenados no dispositivo de armazenamento de memória remoto. Como exemplo, e não como limitação, a Figura 1 ilustra os programas de aplicação remota 185 como residindo no dispositivo de memória 181. Será considerado que as conexões de rede mostradas são exemplares e que outros meios de estabelecer um link de comunicação entre os computadores podem ser usados.

A Figura 2 ilustra uma rede de computador 200 capaz de suportar uma implementação de firewall distribuído. Uma rede externa 201, tal como a Internet, pode ser conectada à rede de computador 200 por intermédio de uma interface de rede, tal como um roteador ou o dispositivo de portal da Internet (IGD) 202. A conexão entre o IGD 202 e a rede 201 pode ser referida como uma conexão a montante do IGD 202. No lado oposto do IGD 202 pode estar uma ou mais conexões a jusante. Uma primeira conexão a jusante 204 pode ser acoplada a uma impressora 206 compartilhada na rede de computador 200, embora ela também possa ser disponibilizada para recursos na rede externa 201. A segunda conexão a jusante 208 pode ser acoplada primeiramente a um computador 210 e subseqüentemente a um computador 211. Nessa configuração, o computador 210 pode compartilhar sua conexão com o computador 211 através da conexão de rede 213 através de recursos tais como o compartilhamento de conexão com Internet (ICS) disponível através do sistema operacional Windows™ da Microsoft. Outra conexão a jusante 212 a partir do IGD 202 pode acoplar um

ponto de acesso sem fio 214 suportando acesso de rede a um dispositivo sem fio 216, tal como um fone inteligente/assistente pessoal digital (PDA) e laptop 218 através de um transporte sem fio 220.

Em uma implementação tradicional da técnica anterior, o IGD 202 também pode incluir um firewall e realizar essa função para todos os dispositivos no lado a jusante do IGD 202. Isso pode resultar em todas as conexões a jusante 204, 208, 212, e cada dispositivo associado tendo as mesmas configurações do firewall. As configurações em um firewall baseado em IGD podem ter como padrão um nível mínimo de proteção ou podem não considerar as diferentes necessidades de alguns dispositivos em relação a outros, tal como a impressora 206 versus um dispositivo sem fio 216. Os IGD da técnica atual, além dos serviços de firewall, freqüentemente realizam conversão de endereço de rede (NAT). Os IGD suportando IPv6 não mais proporcionarão NAT e também podem minimizar o suporte para os serviços de firewall, tornando mais atraente uma abordagem distribuída de prover serviços de firewall, se não uma necessidade.

Os serviços de firewall podem incluir um número de funções que proporcionam uma gama de capacidades de proteção. A maioria dos firewalls tem a capacidade de bloquear as portas não utilizadas, isto é, rejeitar qualquer tráfego que chega a uma porta que não esteja atualmente associado com uma aplicação ou serviço específico. Nas portas designadas, o firewall pode limitar o tráfego a um protocolo autorizado, tal como http (protocolo de transferência de hipertexto) ou ftp (protocolo de transferência de arquivo). Adicionalmente, um firewall pode limitar o tráfego de saída para portas, serviços ou aplicações específicos. Por exemplo, um navegador da Rede pode não ser capaz de enviar uma solicitação de ida em uma porta exceto a porta 80. Qualquer atividade com uma fonte desconhecida pode ser bloqueada. Por exemplo, um programa spyware que é desconhecido do firewall pode ser bloqueado em termos de enviar ou receber tráfego. Os firewalls podem também distinguir entre redes, isto é, uma rede de área local pode ter seu tráfego tratado diferentemente a partir de uma rede de área remota, tal como a Internet. Um firewall pode atuar como um ponto de extremidade para um túnel seguro, tal como uma rede privada virtual de camada 4 (VPN). Em alguns casos, o firewall pode exigir um túnel seguro para algumas conexões ou aplicações. O firewall pode reagir às instruções específicas para bloquear ou permitir o tráfego como conexões de solicitação de aplicações ou serviços.

A Figura 3 é uma vista lógica de uma modalidade de uma implementação de firewall distribuído utilizando a rede 200 da Figura 2. Em um caso onde o IGD 202 não proporciona serviços de firewall adequados para um dispositivo, tal como dispositivo sem fio 216, computador 210, assim como IGD 202, pode ser configurado para prover serviço de firewall mais apropriado. Isto pode ser realizado mediante conexão de forma lógica do ponto de acesso sem fio 214 a jusante do computador 210, de tal modo que todo o tráfego destinado

ao dispositivo sem fio 216 pode ser primeiramente encaminhado através do computador 210 por intermédio da conexão a jusante 208 e conexão lógica 224.

O tráfego para o dispositivo sem fio 216 pode incluir pacotes de voz sobre IP (VOIP) ou da Internet. (Fones inteligentes ágeis de rede podem selecionar uma rede de custo inferior, tal como WiFi quando disponível). O computador 210 pode prover serviços de firewall que limitam o tráfego para VOIP em uma ou mais portas designadas ou tráfego de Internet para uma porta de protocolo de acesso sem fio (WAP), designada. O computador 210 também pode prover serviços de firewall para ele próprio. Em tal caso, ele pode publicar que nenhum serviço é exigido, de modo que um dispositivo a montante ou controlador não atribua a ele serviços de firewall padrão em outro dispositivo. A conexão lógica 224 é discutida em mais detalhe a seguir com relação à Figura 4.

A Figura 4 é outra vista lógica da modalidade da implementação de firewall distribuído da Figura 3. Em operação, a conexão lógica 224 pode ser realizada mediante mudanças não somente no IGD 202 como também no computador 210. O tráfego que chega a partir da rede 201 destinado ao dispositivo sem fio 216 pode ser encaminhado primeiramente para o dispositivo 210 através da conexão lógica 226 (conexão física 208). O tráfego pode ser filtrado no computador 210, re-endereçado para o dispositivo sem fio 216 e transmitido para o IGD 202, por intermédio de conexão lógica 228. No IGD 202, o tráfego filtrado pode ser re-encaminhado, por intermédio da conexão lógica 230, para o dispositivo sem fio 216. O IGD, portanto, pode tratar os pacotes endereçados ao dispositivo sem fio 216 diferentemente, dependendo da fonte. Os pacotes endereçados ao dispositivo sem fio 216 provenientes da rede 201 podem ser encaminhados para o computador 210, enquanto que os pacotes endereçados ao dispositivo sem fio 216, originados no computador 210 são encaminhados para o dispositivo sem fio 216. A conexão lógica 230 pode corresponder à conexão física 212 a partir do IGD 202 para o ponto de acesso sem fio 214 e da conexão pelo ar 220 a partir do ponto de acesso sem fio 214 para o dispositivo sem fio 214.

Em uma modalidade, o dispositivo sem fio 216 pode publicar uma solicitação de serviços de firewall. O comutador 210 pode responder à solicitação e obter acordo com o dispositivo sem fio 216 para prover os serviços solicitados. O IGD 202 pode aceitar as instruções seja a partir do dispositivo sem fio 216 ou do computador 210 para re-encaminhar o tráfego conforme exigido. Em alguns casos o IGD pode aceitar as instruções apenas a partir do dispositivo cujo tráfego está sendo re-encaminhado. Autenticação criptográfica pode ser exigida para o IGD 202 para aceitar tais instruções. Em outra modalidade, o computador 210 pode publicar a sua capacidade de prover serviços de firewall e o dispositivo sem fio 216 pode responder com uma solicitação. Em ambas as modalidades, os dados publicados podem utilizar um protocolo de descoberta de rede não-hierárquica para permutar informação de serviço de firewall.

Em ainda outra modalidade, o IGD 202, ou um dos outros dispositivos a jusante, pode incorporar um gerenciador que descobre exigências de serviço de firewall e capacidades de serviço de firewall e combina os dispositivos utilizando essa informação. O gerenciador pode incorporar regras para identificar exigências mínimas de serviço de firewall para cada dispositivo, por exemplo, pelo tipo. O gerenciador pode combinar provedores de serviço de firewall com dispositivos mesmo quando o dispositivo tiver alguma capacidade de firewall, mas, por exemplo, não atende à exigência mínima de serviço de firewall.

A Figura 5 é um diagrama de blocos de uma rede de computador mostrando outra modalidade da implementação de firewall distribuído. Nessa modalidade exemplar, o laptop 218 provê serviços de firewall para impressora 206. A impressora 206 pode ter elementos programáveis, ou uma capacidade de processamento rudimentar, tal como conversão de fonte ou cor. A impressora 206 pode então solicitar serviços de firewall apropriados mediante publicação de uma solicitação para limitar o tráfego para a porta 80 para trabalhos de impressão e porta 443 para processar solicitações de fonte ou de conversão. O laptop 218 pode responder à solicitação por serviços de firewall a partir da impressora 206 e a impressora 206 pode aceitar. Após receber uma confirmação a partir da impressora 206, o laptop 218 pode direcionar o IGD 202 para re-encaminhar o tráfego para a impressora conforme mostrado na Figura 6. Voltando-se resumidamente para a Figura 6, o tráfego a partir da rede 201 destinado à impressora 206 pode ser direcionado primeiramente para o laptop 218 através da conexão lógica 232. Como acima, o laptop 218 pode realizar os serviços de firewall solicitados em benefício da impressora 206 e enviar o tráfego filtrado para o IGD 202 através da conexão lógica 234. O IGD 202 pode então encaminhar o tráfego para a impressora 206 através da conexão lógica 236.

Retornando à Figura 5, em uma modalidade alternativa, o IGD 202 pode ter uma capacidade de firewall. O laptop 218 pode reconhecer a necessidade de serviços especializados de firewall para a impressora 206 e direcionar o IGD 202 para prover os serviços necessários para a impressora 206. Nesse caso, o laptop 218 atua como um diretor, mas não gerencia ativamente o tráfego. Na função de diretor, o laptop 218 também pode monitorar e gerenciar outros aspectos da atividade de firewall. Por exemplo, o laptop 218 pode ser programado com controles paternos, permitindo que configurações de firewall mudem pelo usuário ou de acordo com a hora do dia. A modalidade das Figuras, 5 e 6, utiliza a impressora 206 e o laptop 218 como elementos exemplares de rede. Os pontos fundamentais também se aplicam igualmente a outros dispositivos, tal como computador 210, PDA 216, ou outros dispositivos não ilustrados especificamente, tal como um dispositivo de armazenamento ligado à rede.

Outras seqüências para descoberta de serviço de firewall e acordos para provisionamento de serviço são possíveis, conforme discutido acima com relação à Figura 4.

A Figura 7 é uma vista de ainda outra modalidade de uma implementação de firewall distribuído. O computador 210 é mostrado acoplado à rede 201 através da conexão 208 por intermédio de IGD 202. O computador 210 também é mostrado compartilhando sua conexão com a Internet com o computador 211 através da conexão de Internet 213. Conforme mencionado acima, isso pode ser feito através de um recurso de compartilhamento de conexão com a Internet no computador 210 e pode envolver duas portas de rede, uma suportando conexão 208 e a outra suportando conexão 213. O computador 211 pode publicar uma solicitação para serviços de firewall e o computador 210 pode responder com sua capacidade de prover os serviços solicitados. Os dois computadores 210, 211 podem então concordar com os termos associados à provisão dos serviços solicitados. Tais termos podem incluir considerações contratuais ou monetárias, mas também podem simplesmente ser um acordo de que o computador 210 proporcionará serviços de firewall atendendo às necessidades do computador 211, ou uma exigência mínima da rede 200. Logicamente, o tráfego recebido no IGD 202 endereçado ao computador 211 pode ser transportado para o computador 210 através de conexão lógica 238, filtrado no computador 210 e enviado através de conexão lógica 240. Os dados a partir do computador 211 podem ser enviados por intermédio do link lógico 242 e enviados através do link lógico 244 para o IGD 202 e eventualmente para fora da rede 201.

Conforme mostrado na Figura 2, outros serviços podem existir pelo lado a jusante do IGD 202, incluindo na conexão de rede 208. Os serviços de firewall providos pelo computador 210 podem oferecer proteção não apenas a partir do tráfego na rede 201, mas também a partir de tráfego indesejado ou não autorizado a partir desses dispositivos localmente conectados.

A Figura 8 é um diagrama representativo de blocos de um computador adequado para a participação em uma implementação de firewall distribuído. Uma rede de área remota 802 pode ter uma conexão de rede 804 para um roteador 806 ou outra conexão de portal da Internet. O roteador 806 pode ser acoplado a um computador 808 por intermédio de uma conexão 807. O computador 808 pode ter uma conexão de rede 810 suportando a conexão 807 para o roteador 806. O computador 808 também pode ter um gerenciador 812 ou controlador acoplado à conexão de rede 810 e a um provedor de serviço de firewall 814. O gerenciador 812 pode ser operável para monitorar as solicitações publicadas para serviços de firewall a partir de outro dispositivo, tal como dispositivo eletrônico 816. O gerenciador 812 pode então configurar a conexão de rede 810 para suportar o recebimento do tráfego endereçado ao dispositivo eletrônico 816 e encaminhar o mesmo para o serviço de firewall 814. Quando o tráfego endereçado ao dispositivo eletrônico 816 chega, ele pode ser encaminhado para o serviço de firewall 814 e processado de acordo com as exigências de serviço de firewall acordadas, resultando em tráfego filtrado. A conexão de rede 810, em conjunto com

o gerenciador 812, pode então retornar o tráfego filtrado a partir do serviço de firewall 814 para o roteador 816 para fornecimento através da conexão de rede 818 ao dispositivo eletrônico 816. Se o computador 808 também tiver alguma capacidade de roteamento, ele pode enviar o tráfego filtrado diretamente para o dispositivo eletrônico 816 através da conexão 820. O tráfego endereçado ao computador 808 também pode ser processado pelo serviço de firewall 814.

Em alguns casos, o gerenciador 812 pode mudar o nível de serviços de firewall providos, dependendo das exigências para obediência às políticas e regras administrativas em vigor. Em muitos casos, os serviços de firewall providos podem ser mais restritivos do que aqueles solicitados pelo dispositivo eletrônico 816, embora se possam empregar serviços de firewall menos restritivos. Por exemplo, serviços de firewall menos restritivos podem ser apropriados quando o gerenciador 812 tem conhecimento dos serviços de firewall a montante (não ilustrados) que reduzem a exigência local.

A Figura 9 é um diagrama representativo de blocos de outro computador adequado para participação em uma implementação de firewall distribuído. Em uma modalidade exemplar correspondendo à configuração de rede mostrada na Figura 7, uma rede 902, tal como a Internet, é mostrada acoplada ao computador 906 por intermédio da conexão de rede 904. O computador 906 tem uma primeira conexão de rede 908, um gerenciador 910 ou controlador, e um serviço de firewall 912 similar àqueles descritos com relação à Figura 8. O computador 906 também é mostrado tendo uma segunda conexão de rede 914, acoplada por intermédio da conexão 916, a uma rede 918, e subseqüentemente ao dispositivo eletrônico 920. O dispositivo eletrônico 920 pode solicitar que o serviço de firewall possa responder a uma oferta publicada para prover serviço de firewall pelo computador 906, ou pode ser atribuído um serviço de firewall padrão quando o computador 906 não pode determinar a capacidade de firewall do dispositivo eletrônico 920.

O tráfego endereçado ao dispositivo eletrônico 920 chegando à conexão de rede 908 pode ser direcionado pelo gerenciador 910 para o serviço de firewall 912 onde filtração pode ser realizada no interesse do dispositivo 920. O gerenciador 910 pode então dirigir o tráfego filtrado para conexão de rede 914 para fornecimento ao dispositivo eletrônico 920.

Embora redes e dispositivos atuais devam, conforme esperado, se beneficiar do aparelho e técnicas descritas acima, redes convertidas para IPv6 utilizando dispositivos de portal da Internet de custo inferior e de função inferior podem ser ainda os maiores beneficiários. Adicionalmente, o uso de um gerenciador inteligente para avaliar as exigências e necessidades do serviço de firewall, a luz das regras administrativas e arquitetura de rede atual, podem permitir menos duplicação da funcionalidade enquanto mantendo ou excedendo a provisão provida pelas arquiteturas de firewall anteriores.

Embora o texto anterior ilustre uma descrição detalhada de várias modalidades dife-

rentes da invenção, deve ser entendido que o escopo da invenção é definido pelos termos das reivindicações apresentados no fim desta patente. A descrição detalhada deve ser considerada apenas como exemplar e não descreve cada possível modalidade da invenção porque descrever cada modalidade possível seria impraticável, senão impossível. Diversas modalidades alternativas poderiam ser implementadas, utilizando quer seja a tecnologia atual ou a tecnologia desenvolvida após a data de depósito dessa patente, as quais ainda estariam abrangidas pelo escopo das reivindicações definindo a invenção.

Desse modo, muitas modificações e variações podem ser feitas nas técnicas e estruturas aqui descritas e ilustradas sem se afastar do espírito e escopo da presente invenção. Conseqüentemente, deve ser entendido que os métodos e aparelho aqui descritos são apenas ilustrativos e não são limitadores do escopo da invenção.

REIVINDICAÇÕES

1. Método de configurar serviços de firewall em uma rede (200) tendo uma pluralidade de dispositivos, **CARACTERIZADO** por compreender:

determinar uma capacidade de firewall para um primeiro dispositivo (210) na rede (200);

determinar uma exigência de serviço de firewall para um segundo dispositivo (216) na rede; e

configurar o primeiro dispositivo (210) para prover serviço de firewall para ele próprio (210) e para o segundo dispositivo (216) de acordo com a exigência de serviço de firewall do segundo dispositivo (216) e a capacidade de firewall do primeiro dispositivo (210).

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** por compreender ainda configurar um roteador (202) para colocar logicamente o segundo dispositivo (216) atrás do primeiro dispositivo (210).

3. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que determinar a capacidade de firewall para o primeiro dispositivo (210) compreende monitorar informação publicada correspondendo à capacidade de firewall do primeiro dispositivo (210).

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que determinar a exigência de serviço de firewall compreende monitorar uma solicitação publicada para serviços de firewall a partir do segundo dispositivo (216).

5. Método, de acordo com a reivindicação 4, **CARACTERIZADO** pelo fato de que uma configuração administrativa requer que o serviço de firewall seja mais restritivo do que a solicitação publicada para serviços de firewall a partir do segundo dispositivo (216).

6. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que determinar a exigência de serviço de firewall compreende selecionar um serviço de firewall padrão para o segundo dispositivo (216) quando nenhuma informação publicada estiver disponível a partir do segundo dispositivo (216).

7. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que um dispositivo a montante (202) define acesso aberto para seu serviço de firewall quando um dispositivo a jusante (210) tiver uma capacidade de firewall que atende a uma capacidade de firewall mínima.

8. Rede (200) tendo uma pluralidade de dispositivos adaptados para proteção de firewall configurável, **CARACTERIZADA** por compreender:

um roteador (806) com um lado a montante 804 e um lado a jusante (807), (818) para dirigir o tráfego de dados com dispositivos na rede;

um primeiro dispositivo (808) acoplado ao lado a jusante (807) do roteador, o primeiro dispositivo (808) tendo a capacidade de fornecer ao menos uma capacidade de firewall; e

um segundo dispositivo (816) acoplado ao lado a jusante do roteador (818), o segundo dispositivo (816) adaptado para publicar uma solicitação para um serviço de firewall, em que o primeiro dispositivo (808) fornece ao menos uma capacidade de firewall responsivo à solicitação a partir do segundo dispositivo (816) quando a ao menos uma capacidade de firewall do primeiro dispositivo (808) atende uma exigência da solicitação para o serviço de firewall.

9. Rede, de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que a exigência é implícita na solicitação.

10. Rede, de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que o roteador (806) aceita um sinal para dirigir o tráfego que chega endereçado ao segundo dispositivo (816) para o primeiro dispositivo (808) para atender à solicitação para o serviço de firewall.

11. Rede, de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que o primeiro dispositivo (808) compartilha uma conexão de rede (820), (916) com o segundo dispositivo (816), (920).

12. Rede, de acordo com a reivindicação 8, **CARACTERIZADA** pelo fato de que o primeiro dispositivo (808) publica a capacidade de fornecer ao menos uma capacidade de firewall.

13. Rede, de acordo com a reivindicação 12, **CARACTERIZADA** pelo fato de que o segundo dispositivo (816) recebe a partir do primeiro dispositivo (808) a capacidade publicada de fornecer a ao menos uma capacidade de firewall e dirige a solicitação para o serviço de firewall para o primeiro dispositivo (808).

14. Rede, de acordo com a reivindicação 8, **CARACTERIZADA** por compreender ainda um controlador (812) para monitorar uma capacidade de firewall e uma exigência de serviço de firewall para cada um da pluralidade de dispositivos adaptados para proteção de firewall configurável.

15. Rede, de acordo com a reivindicação 14, **CARACTERIZADA** pelo fato de que o controlador (812) é incorporado em um entre o primeiro dispositivo (808) e o roteador (806).

16. Rede, de acordo com a reivindicação 14, **CARACTERIZADA** pelo fato de que o controlador (812) tem uma função de comunicação para publicar uma exigência de serviço de firewall para cada um da pluralidade de dispositivos.

17. Rede, de acordo com a reivindicação 16, **CARACTERIZADA** pelo fato de que o primeiro dispositivo (808) fornece ao menos uma capacidade de firewall para ser mais restritiva do que a solicitação de serviço de firewall, a partir do segundo dispositivo (816), quando a exigência de serviço de firewall publicada é mais restritiva do que a solicitação para o serviço de firewall a partir do segundo dispositivo (816).

18. Rede, de acordo com a reivindicação 14, **CARACTERIZADA** pelo fato de que o

controlador (812) atribui um serviço de firewall padrão para um terceiro dispositivo (206) que não publica uma solicitação para serviço de firewall.

19. Computador (808) arranjado e adaptado para prover serviços de firewall para outro dispositivo eletrônico (816), **CARACTERIZADO** por compreender:

uma conexão de rede (810) suportando tráfego bidirecional de dados com uma rede a montante (804);

um gerenciador (812) acoplado à conexão de rede (807) operável para monitorar as solicitações publicadas de serviços de firewall a partir de outro dispositivo eletrônico (816) e, em resposta à solicitação, configurar a conexão de rede (810) para colocar o outro dispositivo eletrônico (816) logicamente a jusante do computador (808), e determinar um nível de serviço de firewall para prover ao outro dispositivo eletrônico (816); e

um provedor de serviço de firewall (814) acoplado ao gerenciador (812) e à conexão de rede (810), em que o provedor de serviço de firewall suporta o serviço de firewall para ele próprio (808) e provê o serviço de firewall para tráfego de dados endereçado ao outro dispositivo eletrônico (816), de acordo com o nível determinado pelo gerenciador (812).

20. Computador, de acordo com a reivindicação 19, **CARACTERIZADO** por compreender ainda uma segunda conexão de rede (916), em que o tráfego de dados na conexão de rede endereçado para o outro dispositivo eletrônico (920) é filtrado de acordo com o nível de serviço de firewall e encaminhado por intermédio da segunda conexão de rede (916).

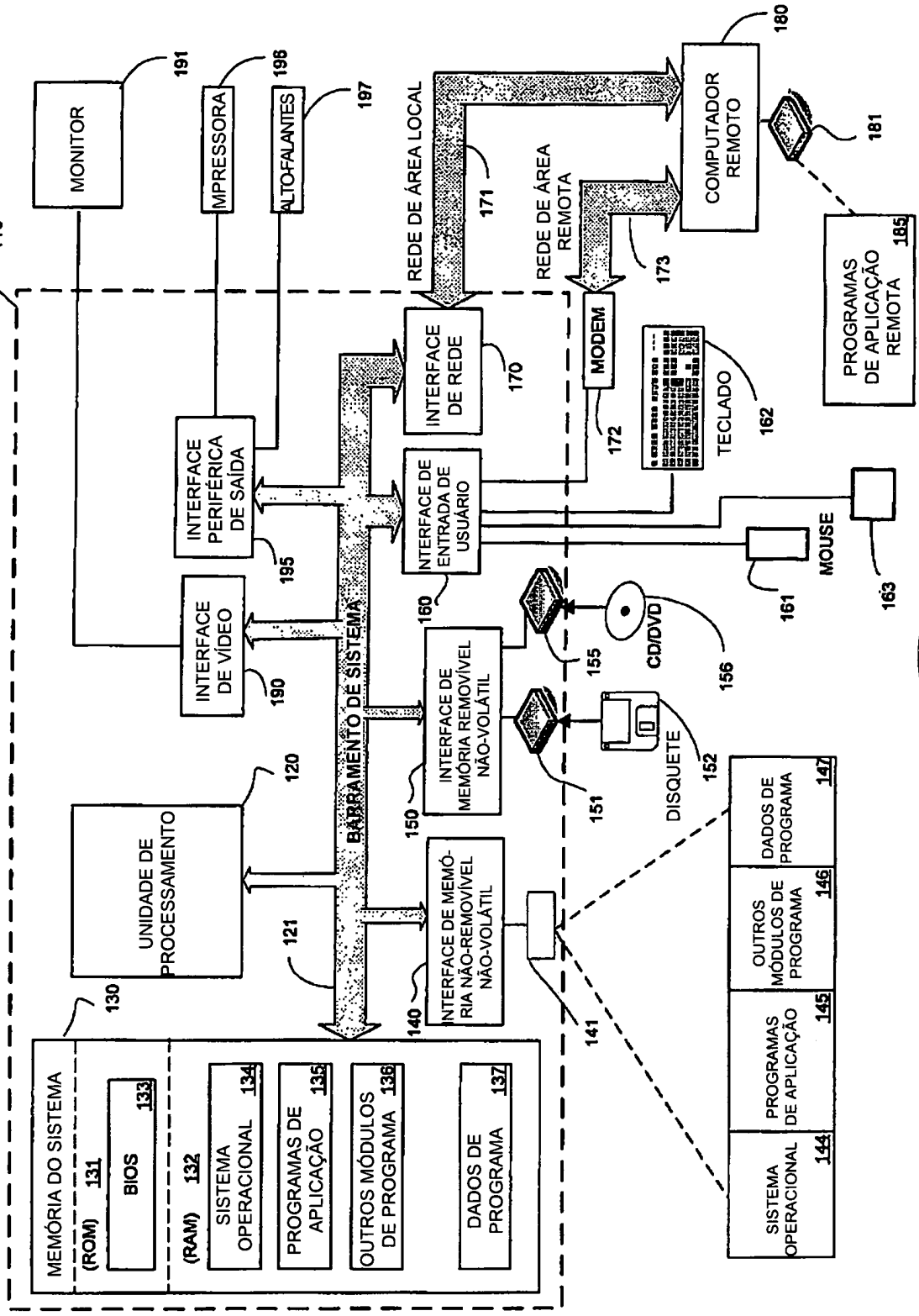

110
MONITOR
191
IMPRESSORA
196
ALTO-FALANTES
197
REDE DE ÁREA LOCAL
171
REDE DE ÁREA REMOTA
173
COMPUTADOR REMOTO
180
181
PROGRAMAS DE APLICAÇÃO REMOTA
185
INTERFACE PERIFÉRICA DE SAÍDA
195
INTERFACE DE REDE
170
MODEM
172
TECLADO
162
INTERFACE DE ENTRADA DE USUÁRIO
160
MOUSE
161
163
INTERFACE DE VÍDEO
190
BARRAMENTO DE SISTEMA
CD/DVD
155
156
UNIDADE DE PROCESSAMENTO
120
INTERFACE DE MEMÓRIA REMOVÍVEL NÃO-VOLÁTIL
150
151
DISQUETE
152
121
INTERFACE DE MEMÓRIA NÃO-REMOVÍVEL NÃO-VOLÁTIL
140
141
130
MEMÓRIA DO SISTEMA
(ROM) 131
BIOS 133
(RAM) 132
SISTEMA OPERACIONAL 134
PROGRAMAS DE APLICAÇÃO 135
OUTROS MÓDULOS DE PROGRAMA 136
DADOS DE PROGRAMA 137
SISTEMA OPERACIONAL 144
PROGRAMAS DE APLICAÇÃO 145
OUTROS MÓDULOS DE PROGRAMA 146
DADOS DE PROGRAMA 147

Fig. 1

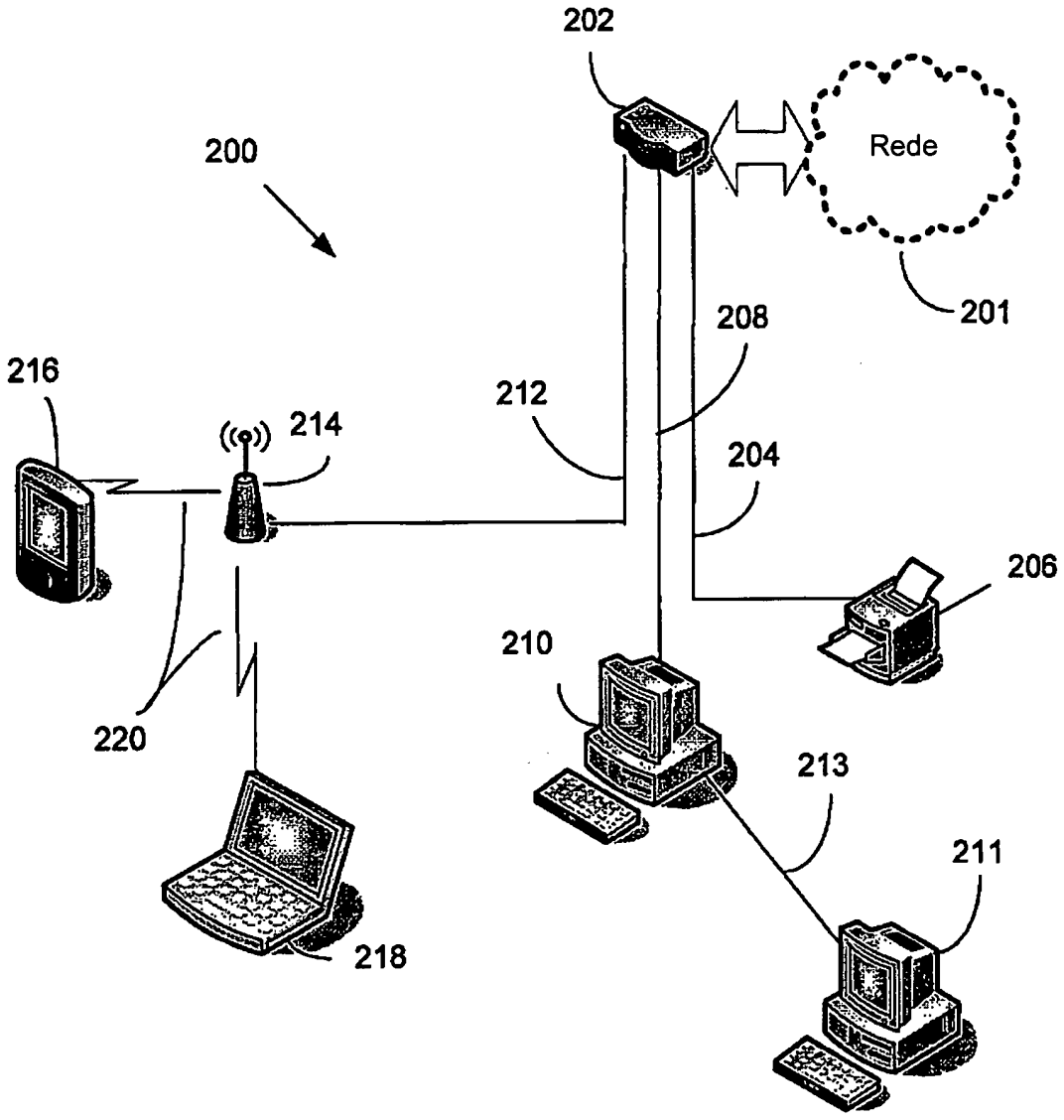


FIG. 2

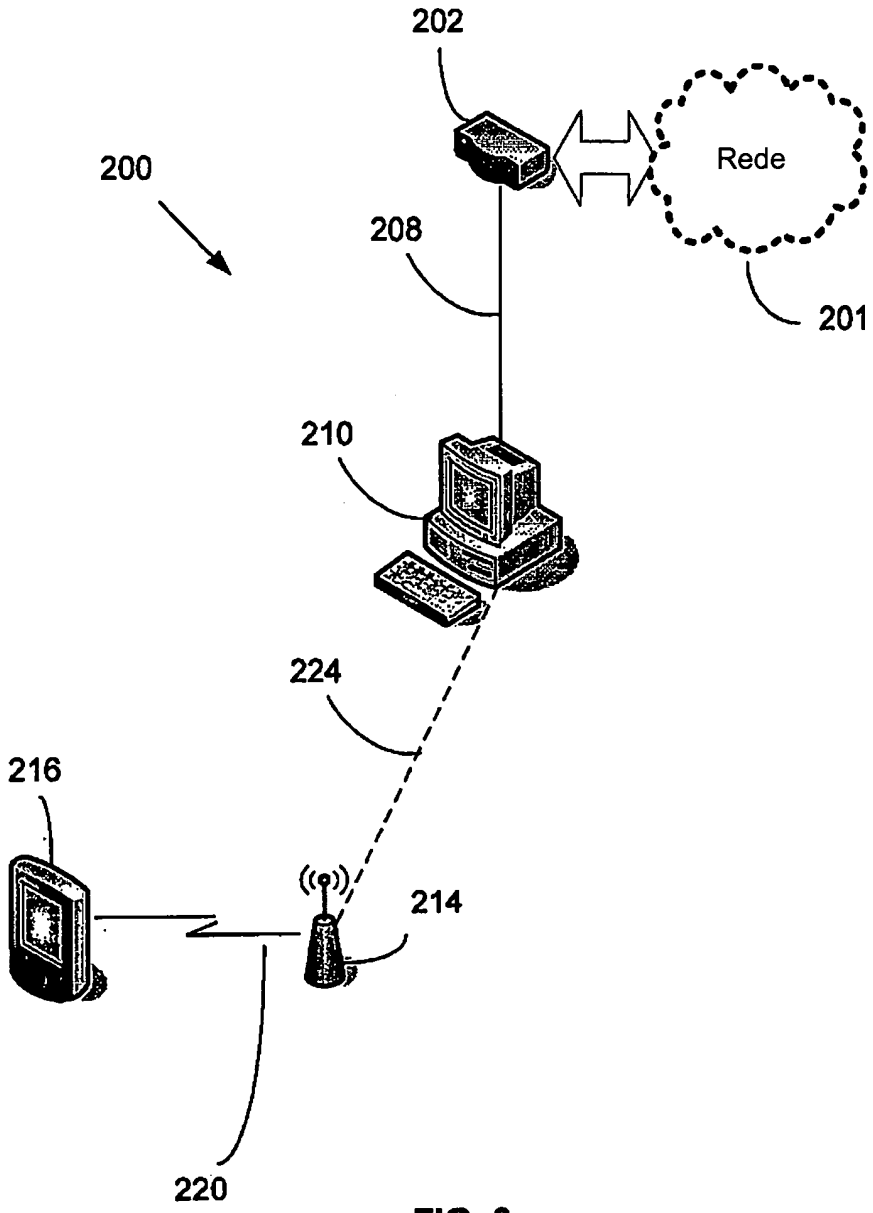


FIG. 3

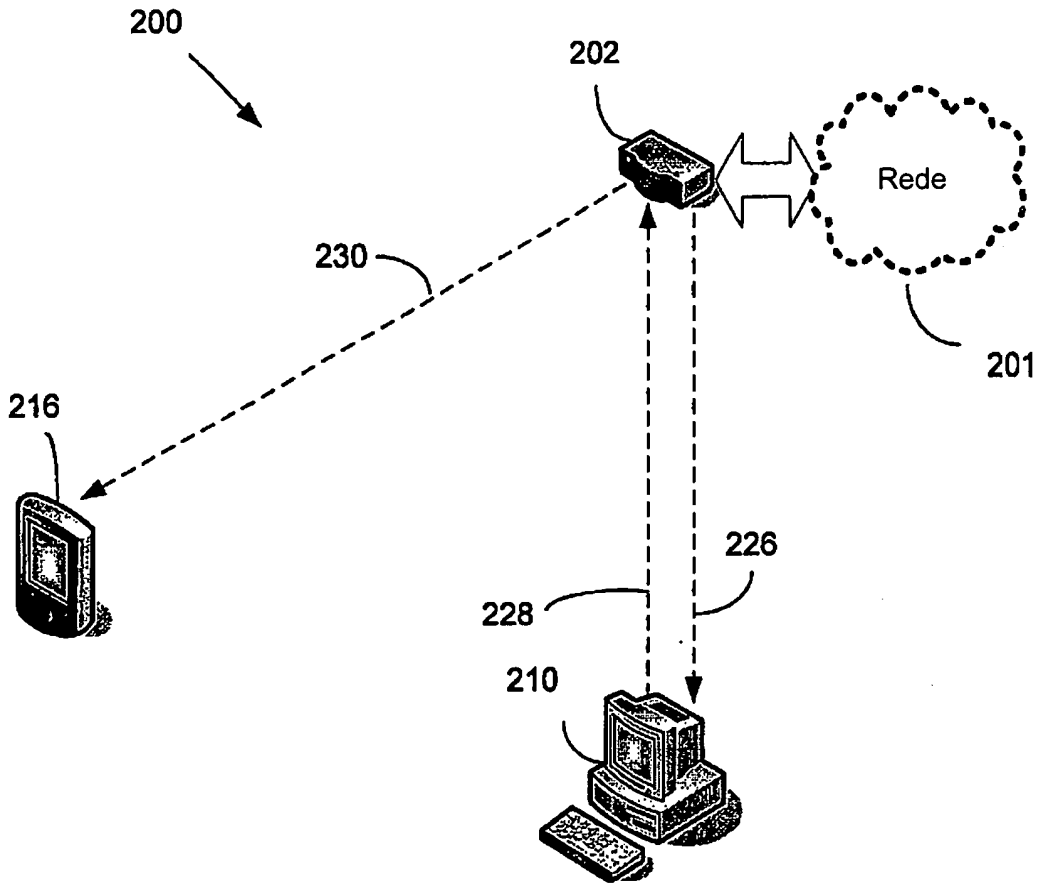


FIG. 4

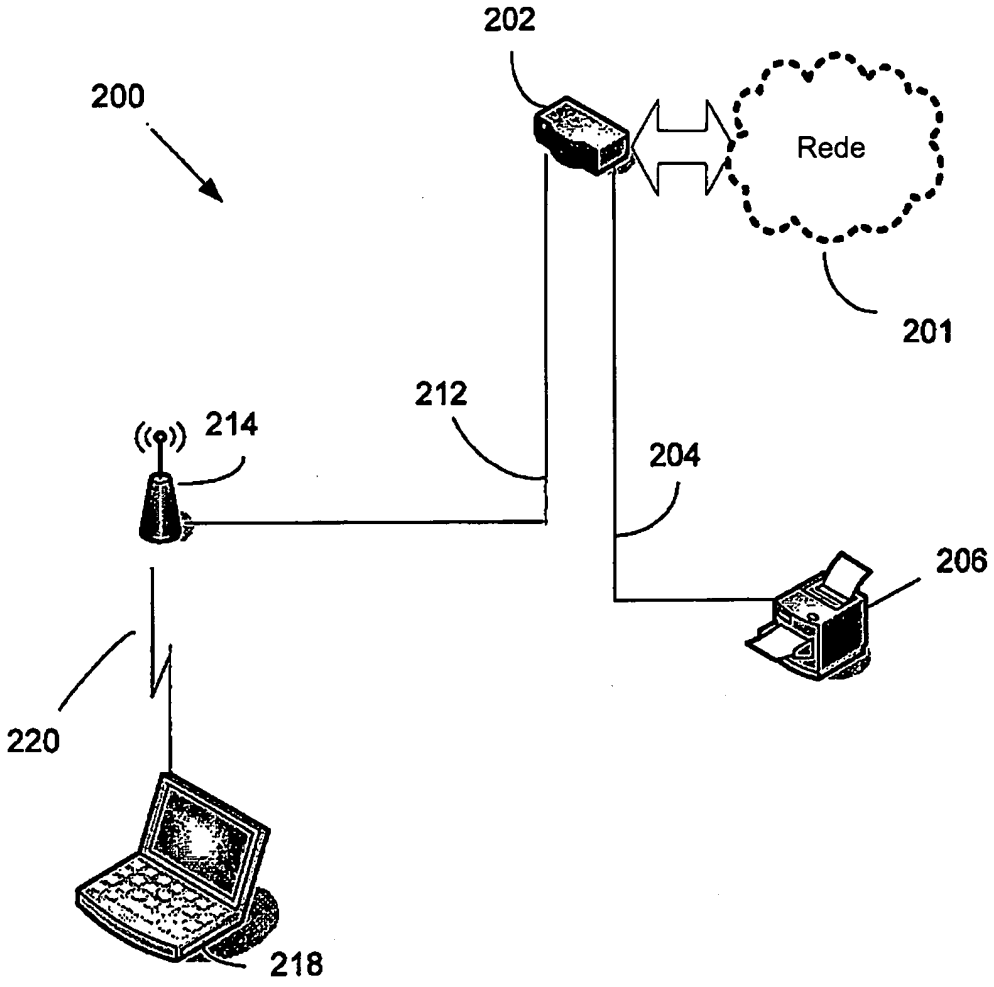


FIG. 5

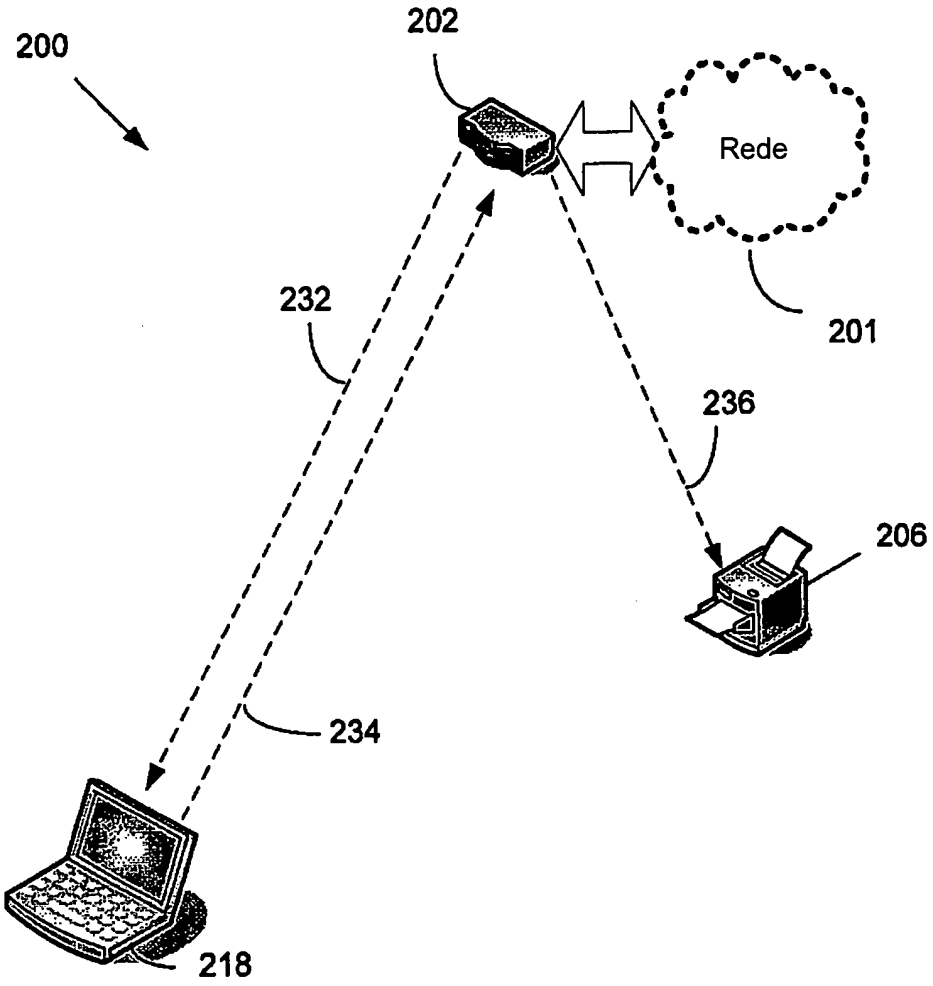


FIG. 6

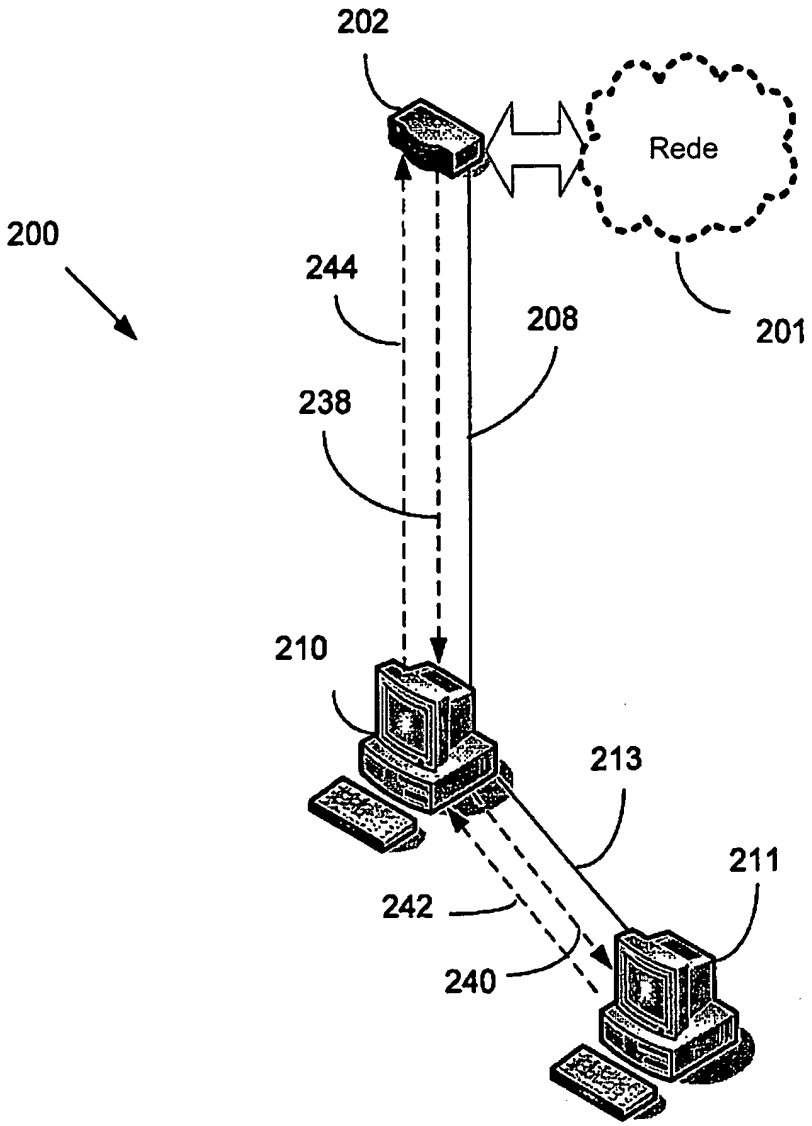


FIG. 7

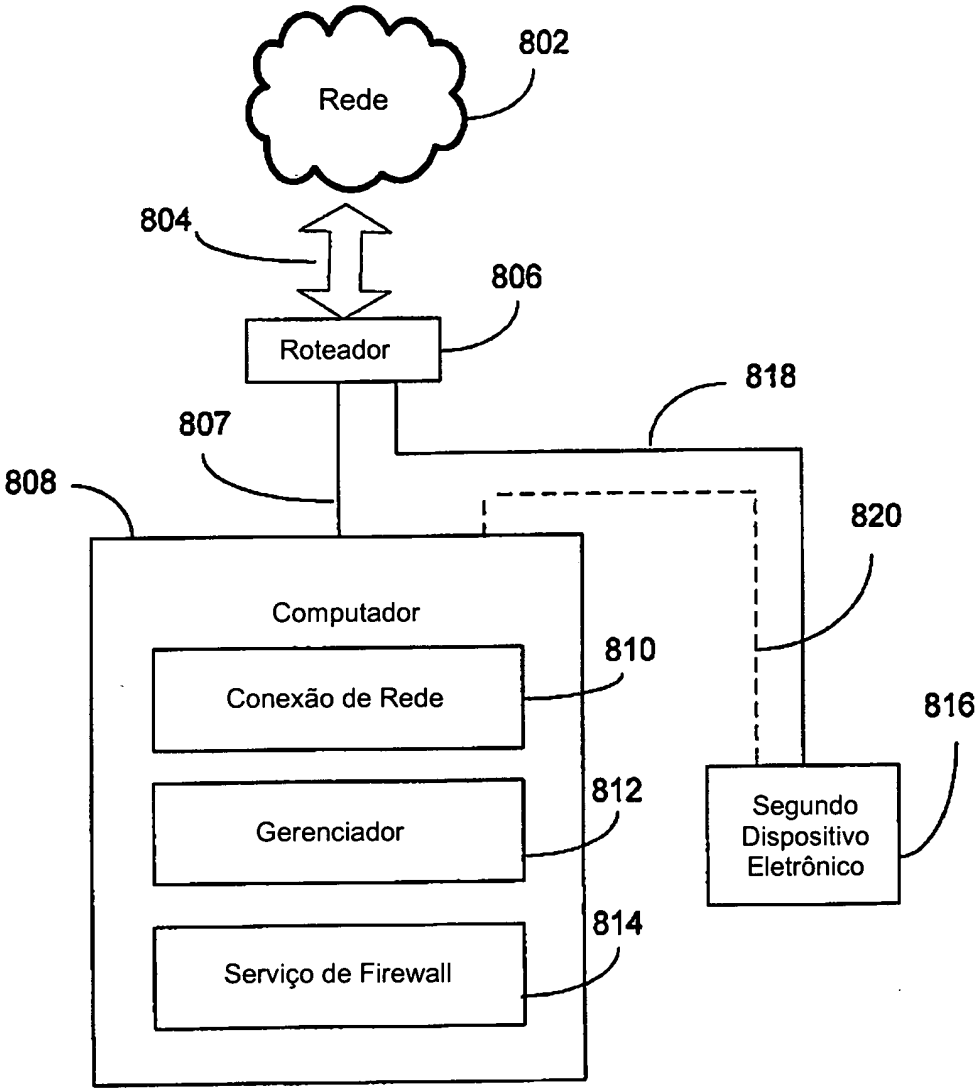

Rede
802
804
806
Roteador
818
807
808
820
Computador
810
Conexão de Rede
816
812
Gerenciador
Segundo
Dispositivo
Eletrônico
814
Serviço de Firewall

FIG. 8

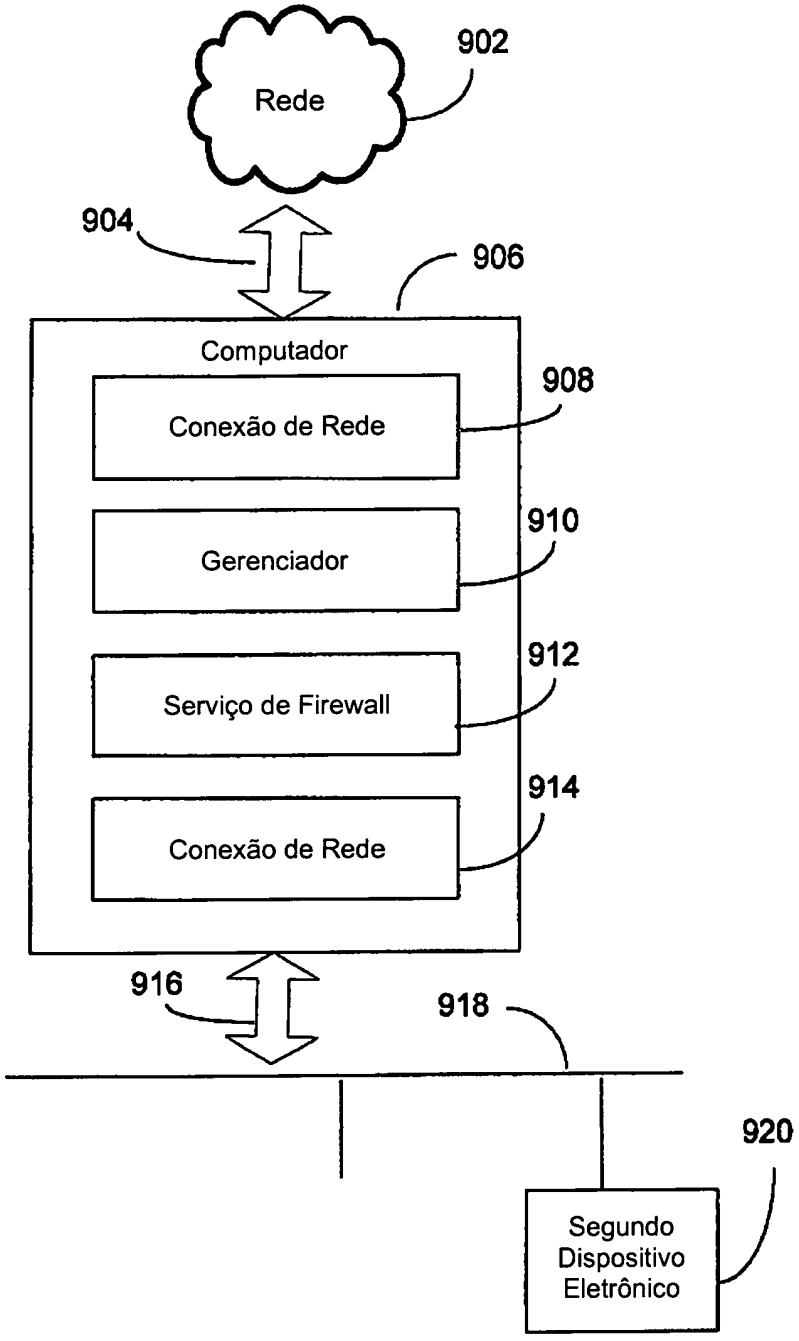

Rede
902
904
906
Computador
908
Conexão de Rede
910
Gerenciador
912
Serviço de Firewall
914
Conexão de Rede
916
918
920
Segundo
Dispositivo
Eletrônico

FIG. 9

RESUMO

"IMPLEMENTAÇÃO DE FIREWALL DISTRIBUÍDO E CONTROLE"

Um método para gravar um material alvo na presença de um material estrutural com seletividade aperfeiçoada utiliza um gravador de fase de vapor e um co-gravador. Modalidades do método apresentam seletividades aperfeiçoadas a partir de ao menos aproximadamente 2 vezes a ao menos aproximadamente 100 vezes em comparação com um processo de gravação similar não utilizando um co-gravador. Em algumas modalidades, o material alvo compreende um metal que pode ser gravado por intermédio do gravador de fase de vapor. Modalidades do método são particularmente úteis na fabricação de dispositivos MEMS, por exemplo, moduladores interferométricos. Em algumas modalidades, o material alvo compreende um metal que pode ser gravado pelo gravador de fase de vapor, por exemplo, molibdênio; e o material estrutural compreende um material dielétrico, por exemplo, dióxido de silício.