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

**(11) PI 0401852-4 B1**

**(22) Data do Depósito:** 27/05/2004

**(45) Data de Concessão:** 29/05/2018

**(54) Título:** MÉTODO PARA PROTEGER UMA REDE DE COMPUTADORES

**(51) Int.Cl.:** H04L 12/66

**(30) Prioridade Unionista:** 06/06/2003 US 10/456,068

**(73) Titular(es):** MICROSOFT TECHNOLOGY LICENSING, LLC

**(72) Inventor(es):** DOUGLAS KEITH BRUBACHER; HUSEYIN GOKMEN GOK

“MÉTODO PARA PROTEGER UMA REDE DE COMPUTADORES”

CAMPO DA INVENÇÃO

Esta invenção diz respeito em geral a um sistema e método para automaticamente descobrir e configurar recursos de segurança da rede, e mais particularmente diz respeito a um sistema e método para dinamicamente combinar a capacidade para descobrir recursos de barreira de proteção tanto de hardware quanto de software disponíveis a um servidor de porta de comunicação em rede e automaticamente configurar dispositivos de porta de comunicação de rede externos ou software servidor para proteger uma rede.

ANTECEDENTE

À medida que as redes de computadores tornam-se mais comuns em locais privados, comerciais, institucionais e governamentais, como também outros locais, a necessidade de proteger redes locais contra infiltração ou ataque de entidades externas tornou-se crescentemente importante. Por exemplo, redes locais freqüentemente têm uma porta de comunicação (“gateway”) ou outra entidade através da qual os clientes na rede local podem acessar uma rede de área ampla (WAN) como a Internet. Este arranjo é benéfico por muitas razões. Em um local comercial, por exemplo, um empreendimento comercial pode querer que seus empregados tenham acesso à Internet por razões de negócio, mas pode querer controlar ou monitorar esse acesso. A porta de comunicação pode executar tais funções de controle ou

110

monitoramento. Além disso, com todos os computadores na rede local sendo expostos à Internet por meio de um ou alguns portais, os administradores da rede podem mais facilmente monitorar as ameaças ou atividade suspeita que se encontram na rede local da Internet.

Crescentemente, dispositivos de porta de comunicação de hardware, como Dispositivos de Porta de comunicação para a Internet (IGDs) estão sendo preferidos em portas de comunicação de software, uma vez que às vezes são desenvolvidos em servidores que servem coma portas de comunicação. As razões para a prevalência atual de dispositivos de hardware neste papel são muitas, mas algumas das vantagens primárias dos dispositivos de porta de comunicação de hardware incluem custo de aquisição e custo de desenvolvimento.

Não obstante, tais portas de comunicação de hardware ou outros pontos de hardware de egresso e entrada não podem executar salvaguarda ou monitorar a rede local corretamente a menos que eles sejam primeiro identificados e corretamente configurados. Em particular, os ambientes de rede variam grandemente em termos de estrutura e leiaute, e o tipo de comunicações que pode ser considerado que ser suspeitoso também varia de um ambiente de rede para outro. Por isto, portas de comunicação de rede de hardware e outros pontos de acesso de hardware para a rede local são tipicamente configurados na instalação antes de serem colocados em serviço. Atualmente, a descoberta e configuração de portas de comunicação de hardware, como

também reconfiguração de tais dispositivos, têm sido executadas manualmente. Por exemplo, um administrador da rede pode estar ciente de um dispositivo recentemente instalado e especificamente comunicará e configurará aquele dispositivo, como por meio de uma aplicação de configuração na rede local. Isto não só requer do administrador estar ciente das portas de comunicação de hardware desenvolvidas, mas, além disso, o administrador deve ser instruído com relação à rotina de configuração particular e requerimentos de cada dispositivo.

BREVE SUMÁRIO DA INVENÇÃO

Nas modalidades da invenção, um sistema e método de configuração permitem seleção dinâmica entre soluções de barreira de proteção de software ou hardware, e configuração automática de qualquer solução de uma maneira ininterrupta. Em particular, a arquitetura de UPnP é alavancada para fornecer descoberta de dispositivos externos enquanto as Interfaces de Programas de Aplicação (APIs) públicas são usadas no caso de soluções de software. Em ambos os casos, a informação de configuração pode ser trocada por meio das mesmas duas técnicas (UPnP ou APIs públicas). Um sistema e método de configuração permitem descoberta e configuração simples dos Dispositivos de Porta de comunicação para a Internet. Em particular, a arquitetura de Universal Plug and Play (UPNP) é explorada para fornecer descoberta de dispositivos externos, e trocar informação de configuração para tais dispositivos. Além disso, se o Protocolo de Configuração Dinâmica do Hospedeiro (DHCP) estiver

implementado no dispositivo alvo, este protocolo pode ser usado durante a configuração dentro das modalidades da invenção.

A seleção de serviços para proteger a rede envolve usar UPnP para pesquisar além dos dispositivos locais para descobrir outros dispositivos em rede também, e usar API's para descobrir as capacidades de software disponíveis para a máquina hospedeira. Em uma modalidade da invenção, um mecanismo multidifundido é usado para facilitar a descoberta do dispositivo, enquanto API's são usadas para executar a descoberta correspondente das capacidades de software. O processo de descoberta e configuração compreende três etapas gerais em uma modalidade da invenção. Primeiro, o dispositivo e software são descobertos usando UPnP, para as soluções de hardware, e API's públicas para as soluções de software. Segundo, no caso de hardware, o dispositivo transmite sua identificação, capacidades, etc. para a unidade descoberta, enquanto que no caso de software pode haver chamadas adicionais de API para determinar as capacidades e configuração atuais da barreira de proteção do software. Por fim a solução de hardware ou software é configurada. No caso de hardware, a informação do dispositivo transmitida é usada para configurar o dispositivo, enquanto que no caso de software, as APIs são usadas para configurar o software com base na informação de configuração colhida. Em uma modalidade da invenção, um mecanismo de sondagem é usado para assegurar que a configuração do dispositivo ou software não altere, ou se

alterar, que possa ser rapidamente reajustada para seu estado anterior.

Características e vantagens adicionais da invenção tornarão evidentes da descrição detalhada a seguir das modalidades ilustrativas que prosseguem com referência às figuras em anexo.

BREVE DESCRIÇÃO DOS DESENHOS

Embora as reivindicações em anexo expõem as características da presente invenção com particularidade, a invenção, junto com seus objetivos e vantagens, pode ser melhor entendida da descrição detalhada a seguir considerada junto com os desenhos em anexo, dos quais:

Figura 1 é diagrama esquemático de um dispositivo de computação utilizável para implementar uma modalidade da invenção;

Figura 2 é um diagrama esquemático de um ambiente de rede de computadores em que uma modalidade da invenção pode ser implementada;

Figura 3A é um fluxograma que ilustra as etapas tomadas em uma modalidade da invenção para proteger uma rede local;

Figura 3B é um fluxograma que ilustra outras etapas tomadas em uma modalidade da invenção para proteger uma rede local; e

Figura 4 é uma ilustração esquemática de uma aplicação de facilitação de configuração de dispositivo e suas interfaces de acordo com uma modalidade da invenção.

DESCRIÇÃO DETALHADA

Voltando para os desenhos, em que tais numerais de referência referem-se a tais elementos, a invenção é ilustrada como sendo implementada em um ambiente de computação adequado. Embora não requerido, a invenção será descrita no contexto geral de instruções executáveis por computador, como módulos de programa, sendo executados por um computador. Em geral, os módulos de programa incluem rotinas, programas, objetos, componentes, estruturas de dados, etc. que executam tarefas particulares ou implementam tipos de dados abstratos particulares. Além disso, aqueles versados na técnica apreciarão que a invenção pode ser praticada com outras configurações de sistema de computador, incluindo dispositivos portáteis, sistemas de multi-processador, eletrônicos com base em microprocessador ou programáveis pelo consumidor, PCs de rede, minicomputadores, mainframes e outros. A invenção pode ser praticada em ambientes de computação distribuídos onde as tarefas são executadas por dispositivos de processamento remotos que são ligados através de uma rede de comunicação. Em um ambiente de computação distribuído, os módulos de programa podem estar localizados em dispositivos de armazenamento de memória tanto locais quanto remotos.

Esta descrição começa com uma descrição de um dispositivo de computação de propósito geral que pode ser usado em um sistema exemplar para implementar a invenção, após a qual a invenção será descrita em maior detalhe com referência às figuras subseqüentes. Voltando agora para a Figura 1, um dispositivo de computação de propósito geral é

mostrado na forma de um computador convencional 20, incluindo uma unidade de processamento 21, uma memória do sistema 22 e um barramento do sistema 23 que acopla vários componentes do sistema incluindo a memória do sistema à unidade de processamento 21. O barramento do sistema 23 pode ser quaisquer de vários tipos de estruturas de barramento incluindo um barramento de memória ou controlador de memória, um barramento periférico e um barramento local usando qualquer de uma variedade de arquiteturas de barramento. A memória do sistema inclui memória exclusiva de leitura (ROM) 24 e memória de acesso aleatório (RAM) 25. Um sistema básico de entrada/saída (BIOS) 26, contendo as rotinas básicas que ajudam a transferir a informação entre os elementos dentro do computador 20, como durante a inicialização, é armazenado na ROM 24. O computador 20 também inclui uma unidade de disco rígido 27 para ler e escrever em um disco rígido 60, uma unidade de disco magnético 28 para ler ou escrever em um disco magnético removível 29 e uma unidade de disco óptico 30 para ler ou escrever em um disco óptico removível 31 como um CD ROM ou outros meios ópticos.

A unidade de disco rígido 27, unidade de disco magnético 28 e unidade de disco óptico 30 são conectadas ao barramento do sistema 23 por uma interface de unidade de disco rígido 32, uma interface de unidade de disco magnético 33 e uma interface de unidade de disco óptico 34, respectivamente. As unidades e seus meios legíveis por computador associados provêem armazenamento não-volátil de

instruções legíveis por computador, estruturas de dados, módulos de programa e outros dados para o computador 20. Embora o ambiente exemplar aqui descrito empregue um disco rígido 60, um disco magnético removível 29 e um disco óptico removível 31, será apreciado por aqueles versados na técnica que outros tipos de meios legíveis por computador podem armazenar dados que são acessíveis por um computador, como cassetes magnéticos, cartões de memória instantânea, discos de vídeo digital, cartuchos de Bernoulli, memórias de acesso aleatório, memórias exclusivas de leitura, redes de área de armazenamento e outros podem também ser usados no ambiente operacional exemplar.

Os vários módulos de programa podem ser armazenados no disco rígido 60, disco magnético 29, disco óptico 31, ROM 24 ou RAM 25, incluindo um sistema operacional 35, um ou mais programas de aplicação 36, outros módulos de programa 37 e dados de programa 38. Um usuário pode entrar os comandos e a informação no computador 20 através dos dispositivos de entrada como um teclado 40 e um dispositivo de apontamento 42. Outros dispositivos de entrada (não mostrados) podem incluir um microfone, joystick, acionador de jogo, disco satélite, escâner ou outros. Estes e outros dispositivos de entrada são freqüentemente conectados à unidade de processamento 21 através de uma interface de porta serial 46 que é acoplada ao barramento do sistema, mas podem ser conectados através de outras interfaces, como uma porta paralela, porta de jogo ou um barramento serial universal (USB) ou uma placa de

interface de rede. Um monitor 47 ou outro tipo de dispositivo de exibição é também conectado ao barramento do sistema 23 por meio de uma interface, como um adaptador de vídeo 48. Além do monitor, muitos computadores também incluem outros dispositivos de saída periféricos, não mostrados, como alto-falantes e impressoras.

O computador 20 preferivelmente opera em um ambiente em rede usando conexões lógicas a um ou mais computadores remotos, como um computador remoto 49. O computador remoto 49 pode ser um computador pessoal, um servidor, um roteador, um PC de rede, um dispositivo semelhante ou outro nodo de rede comum, e tipicamente inclui muitos ou todos os elementos acima descritos com relação ao computador 20, embora apenas um dispositivo de armazenamento de memória 50 tenha sido ilustrado na Figura 1. Em uma modalidade da invenção, o computador remoto 49 é um Dispositivo de Porta de comunicação para a Internet (IGD) habilitado com UPNP e tem as características tipicamente associadas a um tal dispositivo, como será apreciado por aqueles de habilidade na técnica. As conexões lógicas descritas na Figura 1 incluem uma rede local (LAN) 51 e uma rede de área ampla (WAN) 52. Tais ambientes de gestão de redes são comuns em escritórios, redes de computadores de empreendimento amplo, intranets e a Internet.

Quando usado em um ambiente de gestão de redes de LAN, o computador 20 é conectado à rede local 51 através de uma interface ou adaptador de rede 53. Quando usado em um ambiente de gestão de redes WAN, o computador 20 tipicamente

inclui um modem 54 ou outros dispositivos para estabelecer comunicações pela WAN 52. O modem 54 que pode ser interno ou externo é conectado ao barramento do sistema 23 por meio da interface de porta serial 46. Módulos de programa descritos com relação ao computador 20, ou porções destes, podem ser armazenados no dispositivo de armazenamento de memória remoto se tal estiver presente. Será apreciado que as conexões de rede mostradas são exemplares e outros dispositivos de estabelecer um link de comunicação entre os computadores podem ser usados.

Na descrição que segue, a invenção será descrita com referência às ações e representações simbólicas das operações que são executadas por um ou mais computadores, a menos que do contrário indicado. Como tal, será entendido que tais ações e operações que são às vezes referidas como sendo executadas por computador incluem a manipulação pela unidade de processamento do computador de sinais elétricos representando dados em uma forma estruturada. Esta manipulação transforma os dados ou os mantém nas localizações no sistema de memória do computador que reconfigura ou do contrário altera a operação do computador de uma maneira bem entendida por aqueles versados na técnica. As estruturas de dados onde os dados são mantidos são localizações físicas da memória que têm propriedades particulares definidas pelo formato dos dados. Porém, embora a invenção esteja sendo descrita no contexto anterior, ela não é intencionada ser limitativa como aqueles de habilidade na técnica apreciarão que muitas das ações e operações

descritas doravante podem também ser implementadas em hardware.

Voltando para a Figura 2, um ambiente operacional exemplar 201, em que as modalidades da invenção podem ser implementadas, é mostrado. Em particular, um IGD ou outra porta de comunicação de hardware 207 e/ou as capacidades de software de barreira de proteção disponíveis em um computador de porta de comunicação 208 protege uma rede local 205 contra acesso impróprio de um computador como um computador remoto 211 que pode acessar a rede 205 por meio de uma rede de área ampla (WAN) 209. A WAN 209 pode ser qualquer tipo de rede de área ampla, e irá tipicamente, embora não necessariamente, compreender a Internet. A rede local 205 pode compreender qualquer número e tipo de computadores e/ou dispositivos, mas um computador simples 203 é mostrado para fins de ilustração. Em uma modalidade da invenção, o computador 208 é um servidor de pequena empresa. Exemplos de tais servidores incluem servidores de e-mail, servidores de rede e assim por diante. A rede local 205 pode compreender recursos adicionais como diretórios, bases de dados, etc.

Em um cenário de uso típico em que o computador 208 é um servidor de e-mail, o servidor 208 transmite o e-mail de clientes na rede local 205 para os recipientes, como computador remoto 211, por meio da WAN 209. O servidor 208 também envia o e-mail recebido da WAN 209, como do computador remoto 211, para os recipientes intencionados na rede local 205. O servidor de e-mail pode ter muitas das

características debatidas com respeito ao computador 20 da Figura 1. Em um cenário de uso típico em que o computador 208 é um servidor de rede, o servidor 208 hospeda um ou mais web sites acessíveis, como para o computador remoto 211 na WAN 209. Tais sites podem ser comerciais, educacionais, etc. Além da porta de comunicação 207 ilustrado na Figura 2, pode haver qualquer número de outras portas de comunicação presentes no ambiente operacional 201. A descoberta e configuração de um dispositivo de porta de comunicação de hardware, como dispositivo 207, e uma barreira de proteção de software, como pode residir no computador de porta de comunicação 208, serão descritas em maior detalhe com referência à Figura 3.

Figuras 3A e 3B compreendem um fluxograma que ilustra as etapas tomadas para descobrir e configurar um dispositivo de porta de comunicação de hardware e/ou barreira de proteção de software de acordo com uma modalidade da invenção. O debate das Figuras 3A e 3B também se referirão quando apropriado aos elementos da arquitetura da Figura 2. Inicialmente na etapa 301, um dispositivo de porta de comunicação habilitado com UPNP 207, como um IGD padrão, é fisicamente instalado por meio da conexão à rede local 205 se tal for para ser usada. Esta etapa tipicamente envolve a conexão física de cabeamento e assim por diante, de forma que o dispositivo de porta de comunicação 207 seja capaz de enviar e receber as transmissões pela rede local 205. Neste momento, a rede local 205 ainda não está protegida pelo dispositivo recentemente instalado 207.

Nas etapas 303 a 347, a ser debatidas separadamente em maior detalhe abaixo, uma aplicação de facilitação de conexão, aqui referida como um "assistente" de conexão, descobre o dispositivo recentemente instalado 207 e/ou recursos de barreira de proteção de software e configura o dispositivo e/ou barreira de proteção de software de acordo com as seleções feitas por um usuário por meio do assistente. Um arranjo exemplar do assistente de conexão dentro da arquitetura de uma máquina de descoberta é mostrado esquematicamente na Figura 4. Em particular, o assistente de conexão 401 é uma aplicação que acessa o sistema operacional 403 do computador hospedeiro 405 para executar operações de UPNP. O assistente de conexão 401 preferivelmente é também capaz de enviar e receber transmissões usando os recursos de conexão de gestão de redes 407 do computador hospedeiro 405. O computador hospedeiro 405 quanto ao assistente de conexão 401 pode estar localizado em qualquer lugar na rede local 205, e pode ser, por exemplo, o computador 203.

Referindo novamente ao fluxograma da Figura 3A, o assistente de conexão 401 multidifunde uma mensagem de pesquisa para o endereço de multidifusão do Protocolo de Pesquisa e Descoberta Simples (SSDP) por meio de todos os adaptadores de rede (i.e. os recursos de conexão 407) do computador hospedeiro 405 na etapa 302. A multidifusão pode ser automaticamente iniciada periodicamente em um intervalo predeterminado ou pode ser automaticamente acionada após um comando ou solicitação de um usuário. Na etapa 303 é

122

determinado se qualquer dispositivo de porta de comunicação de hardware foi detectado. Se não, o processo transita para a junção A da Figura 3B. Do contrário, o processo flui para a etapa 304, onde o usuário é induzido a indicar se o(s) dispositivo(s) de porta de comunicação de hardware detectado(s) deve(m) ser usado(s). Se for determinado na etapa 304 que nenhum dispositivo de porta de comunicação detectado não deve ser usado, o processo transita para a junção A da Figura 3B. Do contrário, o processo move para a etapa 305, com apenas aqueles dispositivos de porta de comunicação que deveriam ser usados participando nesta e nas etapas subseqüentes. Assumindo que o dispositivo de porta de comunicação recentemente instalado 207 está associado a um endereço de IP válido, então ele responderá na etapa 305 transmitindo um URL ao assistente de conexão 401 no computador hospedeiro 405 para o uso na obtenção da informação de descrição do dispositivo. Será apreciado que os URLs para mais de um dispositivo podem ser recebidos no assistente de conexão 401.

Na etapa 307, o assistente de conexão 401 apresenta uma lista de dispositivos descobertos para o usuário do computador hospedeiro 405. Após o usuário selecionar um dispositivo para configurar na etapa 309, como o dispositivo 207 neste exemplo, então na etapa 311 o assistente de conexão 401 transmite uma solicitação de HTTP GET para o URL que foi enviado pelo dispositivo na etapa 305. Observe que se nenhum dispositivo for selecionado pelo usuário na etapa 309, o processo move diretamente para a

junção A da Figura 3B. Na etapa 313, o dispositivo 207 responde transmitindo um documento em XML contendo sub-dispositivos e serviços contidos no dispositivo-raiz como também URLs utilizáveis para configurar os sub-dispositivos e serviços. Na etapa 315, o assistente de conexão 401 apresenta as opções de configuração para os sub-dispositivos e serviços ao usuário e recebe as seleções de configuração do usuário para os sub-dispositivos e serviços. Tipicamente a configuração desse modo especificada compreenderá um conjunto de mapeamentos de porta especificados.

Na etapa 317, o assistente de conexão 401 localiza um serviço de configuração como um serviço de WANIpConnection suportado pelo dispositivo 207 descoberto como também o URL de configuração associado ao serviço de WANIpConnection. Tanto o serviço de WANIpConnection quanto o URL associado podem ser localizados na lista recebida do dispositivo na etapa 313. Por fim, na etapa 319, o assistente de conexão 401 envia as solicitações do Protocolo de Acesso de Objeto Simples (SOAP) para o URL de configuração para implementar os mapeamentos de porta de acordo com a configuração selecionada pelo usuário. Desse modo, o dispositivo recentemente instalado 207 foi automaticamente descoberto e facilmente configurado pelo usuário, e a rede está agora protegida pelo dispositivo 207 conforme a configuração selecionada pelo usuário. Após a etapa 319, o processo flui para a junção A da Figura 3B para descoberta e configuração de qualquer barreira ou barreiras de proteção de software que são para ser usadas. Em uma

modalidade da invenção, se uma barreira de proteção de hardware foi configurada como acima debatido, então o processo termina após a etapa 319 sem configurar uma barreira de proteção de software.

Na etapa 329, o processo determina se um servidor como representado pelo computador de porta de comunicação 208 é configurado para agir como um computador de porta de comunicação, ao invés de simplesmente ser um cliente na rede local 205. Se for determinado que o servidor é configurado para agir como um computador de porta de comunicação, então na etapa 331, o assistente de conexão 401 chama as APIs conhecidas para descobrir as capacidades da barreira de proteção de software disponíveis no servidor. Em uma modalidade da invenção, duas soluções de barreira de proteção de software são suportadas. Nesta modalidade da invenção, primeiro as APIs do Microsoft® Internet Security and Acceleration Server (ISA) pela Microsoft® Corporation of Redmond, Washington são chamadas para determinar se ISA está instalada. Se ISA não estiver instalada então as APIs do Microsoft Windows Server Routing and Remote Access Service são chamadas. Se for determinado que o servidor não é configurado para agir como um computador de porta de comunicação, o processo termina da etapa 329.

Na etapa 333, o processo determina se quaisquer capacidades da barreira de proteção de software foram descobertas na máquina inerente. Se não houve, então o processo termina. Do contrário, o processo flui para a etapa 335, onde o usuário é induzido a indicar se as capacidades

da barreira de proteção de software descobertas devem ser usadas. Se for determinado que as capacidades da barreira de proteção de software descobertas não devem ser usadas, então o processo termina. Do contrário, o processo flui para a etapa 337, onde o assistente de conexão 401 usa as APIs conhecidas como acima debatido para colher a informação descritiva com relação às capacidades da barreira de proteção de software descobertas.

Na etapa 339, o assistente de conexão 401 apresenta uma lista de barreiras de proteção de software descobertas ao usuário do computador hospedeiro. Na etapa 341, o usuário seleciona uma barreira de proteção de software para configuração. Subseqüentemente, o assistente de conexão 401 chama as APIs conhecidas para colher a informação com relação aos sub-dispositivos e serviços da barreira de proteção selecionada na etapa 343. Na etapa 345, o assistente de conexão 401 apresenta as opções de configuração ao usuário e recebe as seleções de configuração do usuário para sub-dispositivos e serviços da barreira de proteção selecionada. Por fim na etapa 347, o assistente de conexão 401 chama as APIs para configurar os sub-dispositivos de barreira de proteção de software e serviços de acordo com as seleções do usuário.

Em uma modalidade da invenção, um dos serviços suportados pelo dispositivo recentemente instalado 207 é o Protocolo de Configuração Dinâmica de Hospedeiro (DHCP). DHCP é um protocolo da Internet tipicamente usado para configurar computadores que estão usando TCP/IP. DHCP pode

ser usado para atribuir os endereços de IP, fornecer informação de configuração de pilha, como também fornecer outra informação de configuração. Se o dispositivo 207 suportar DHCP, então este comportamento pode ser também configurado.

Em uma modalidade da invenção, o assistente de conexão 401 periodicamente sonda a rede local 205 para determinar se quaisquer dispositivos de rede de hardware externos novos foram adicionados. Tipicamente, até mesmo quando tais dispositivos são habilitados com UPNP, não há nenhuma notificação dada quando um dispositivo novo for instalado. Em uma outra modalidade da invenção, o assistente de conexão 401 avalia periodicamente a informação de configuração dos dispositivos conhecidos para detectar qualquer alteração na configuração que pode colocar em risco a segurança da rede 205. Se uma alteração na configuração for detectada, o assistente de conexão 401 reconfigura o dispositivo inerente para sua configuração selecionada pelo usuário.

Embora aqueles de habilidade na técnica apreciarão que as APIs acima referidas podem ser substituídas por quaisquer APIs adequadas, o seguinte é uma listagem de APIs exemplares conhecidas do Microsoft® Routing and Remote Access Service que são úteis na implementação das modalidades da invenção.

MprAdminBufferfree

MprAdminDeregisterConnectionNotification

MDrAdminGetErrorString

MprAdminInterfaceConnect

MprAdminInterfaceCreate

MprAdminInterfaceDelete

MprAdminInterfaceDeviceGetinfo

MprAdminInterfaceDeyiceSetInfo

MprAdminInterfaceDisconnect

MprAdminInterfaceEnum

MprAdminInterfaceGetCredentials

MprAdminInterfaceGetCredentialsEx

MprAdminInterfaceGetHandle

MprAdminInterfaceGetInfo

MprAdminInterfaceOueryUpdateResult

MprAdminInterfaceSetCredentials

MprAdminInterfaceSetCredentialsEx

MprAdminInterfaceSetInfo

MprAdminInterfaceTansportAdd

MprAdminInterfaceTransportGetInfo

MprAdminInterfaceTransportRemove

MprAdminInterfaceTransportSetInfo

MprAdminInerfaceUndatePhonebookInfo

MprAdminInterfacepdateRoutes

MprAdminServiceRunning

MprAdminRegisterConnectionNotification

MprAdminServerConnect

MprAdminServerDisconnect

MprAdminServerGetCredentials

MprAdminServerGetInfo

MprAdminServerSetCredentials

MprAdminTransportCreate

MprAdminTransportGetInfo

MprAdminTransportSetInfo

MprConfigBufferFree

MprConfigGetFriendlyName

MprConfigGetGuidName

MprConfigInterfaceCreate

MprConfigInterfaceDelete

MprConfigInterfaceEnum

MprConfigInterfaceGetHandle

MprConfigInterfaceGetInfo

MprConfigInterfaceSetInfo

MprConfigInterfaceTransportAdd

MprConfigInterfaceTransportEnum

MprConfigInterfaceTransportGetHandle

MprConfigInterfaceTransportGetInfo

MprConfigInterfaceTransportRemove

MprConfigInterfaceTransportSetInfo

MprConfigServerBackup

MprConfigServerConnect

MprConfigServerDisconnect

MprConfigServerGetInfo

MprConfigServerInstall

MprConfigServerRestore

MprConfigTransportCreate

MprConfigTransportDelete

MprConfigTransportEnum

MprConfigTransportGetHandle

MprConfigTransPortGetInfo

MprConfigTransPortSetInfo.

Embora aqueles de habilidade na técnica apreciarão que as APIs acima referidas podem ser substituídas por quaisquer APIs adequadas, o seguinte é uma listagem de interfaces exemplares conhecidas de Microsoft® Internet Security and Acceleration COM, cada uma compreendendo uma ou mais APIs que são úteis em implementar as modalidades da invenção.

FPC Object

FPCAccessControlEntry Object

FPCAccessControlList Collection

FPCAccount Object

FPCAceounts Collection

FPCActiveCacheConfiguration Object

FPCAdapter Object

FPCAdapters Collection

FPCAlert Object

FPCAlerts Collection

FPCAlertAction Object

FPCAlertActions Collection

FPCAlertInfo Object

FPCAlertNotification Object

FPCApplicatoinFilter Object

FPCApplicationFilters Collection

FPCArray Object

FPCArrays Collection

FPCArrayPolicyConfig Object

FPCArrayPolicyConfigs Collection

FPCAutoDial Object

FPCBackupRoute Object

FPCBandwidthPriority Object

FPCBandwidthPriorities Collection

FPCBandwidthRule Object

FPCBandwidthRules Collection

FPCCache Object

FPCCacheConfiguration Object

FPCCacheContents Object

FPCCacheDrive Object

FPCCacheDrives Collection

FPCClientAddressSet Object

FPCClientAddressSets Collection

FPCClientAutoScript Object

FPCClientBackupRoute Object

FPCClientConfig Object

FPCClientConfigSettings Collection

FPCClientSettingsSection Object

FPCContentGroup Object

FPCContentGroups Collection

FPCCredentials Object

FPCDeniedMethod Object

FPCDeniedMethods Collection

FPCDestination Object

FPCDestinationSet Collection

FPCDestinationSets Collection

FPCDialupEntry Object

FPCDialupEntries Collection

FPCDialupNetworkConnections Collection

FPCDirectAddressDestination Object

FPCDirectAddressDestinations Collection

FPCDirectIpDestination Object

FPCDirectIpDestinations Collection

FPCDiskDrive Object

FPCDiskDrives Collection

FPCEnterprise Object

FPCEnterprisePolicy Object

FPCEnterprisePolicies Collection

FPCEventDefinition Object

FPCEventDefinitions Collection

FPCExtensions Object

FPCFilterProtocol Object

FPCFilterProtocols Collection

FPCFirewallClientConfig Object

FPCFirewallChaining Object

FPCFirewallSession Object

FPCFirewallSessions Collection

FPCFirewallSessionConnection Object

FPCFirewallSessionConnections Collection

FPCFTPCacheConfiguration Object

FPCHTTPCacheConfiguration Object

FPCIpPacketFilter Object

FPCIpPacketFilters Collection

FPCIpRange Object

FPCLAT Collection

FPCLATEntry Object

FPCLDT Collection

FPCLDTEntry Object

FPCListenEntry Object

FPCListenEntries Collection

FPCLog Object

FPCLogs Collection

FPCNetworkConfiguration Object

FPCPolicyElements Object

FPCPrimaryRoute Object

FPCProtocolConnection Object

FPCProtocolConnections Collection

FPCProtocolDefnition Object

FPCProtocolDefinitions Collection

FPCProtocolRule Object

FPCProtocolRules Collection

FPCSenserPublishingRule Object

FPCServerPublishingRules Collection

FPCPublishing Object

FPCRef Object

FPCRefs Collection

FPCRoutingRule Object

FPCRoutingRules Collection

FPCSchedule Object

FPCSchedules Collection

FPCScheduledContentDownload Collection

FPCScheduledContentDownloadConfig Object

FPCSecurityDescriptor Object

FPCServer Object

FPCServers Collection

FPCSignaledAlert Object

FPCSignaledAlerts Collection

FPCSiteAndContentRule Object

FPCSiteAndContentRules Collection

FPCSnapinNode Object

FPCSSLCertificate Object

FPCSSLCertificates Collection

FPCTunnelPortRange Object

FPCTunnelPortRanges Collection

FPCVendorParametersSet Object

FPCVendorParametersSets Collection

FPCWebBrowserClientConfig Object

FPCWebFilter Object

FPCWebFilters Collection

FPCWebProxy Object

FPCWebPublishingRule Object

FPCWebPublishingRules Collection

FPCWebReQuestConfiguration Object

FPCWebSession Obiect

FPCWebSessions Collection

FPCWebSessionAdditionalInfo Obiect

Será apreciado que um sistema e método melhorados para descobrir e configurar topologias de rede seguras que respondem aos ambientes de gestão de redes existentes e abrangem a detecção e configuração dinâmicas de um hardware apropriado ou solução de software foram descritos. Devido às

muitas possíveis modalidades às quais os princípios desta invenção podem ser aplicados, deve ser reconhecido que as modalidades aqui descritas com respeito às figuras do desenho são intencionadas ser ilustrativas apenas e não devem ser consideradas como limitativas do escopo da invenção. Por exemplo, aqueles de habilidade na técnica reconhecerão que alguns elementos das modalidades ilustradas mostradas em software podem ser implementados em hardware e vice-versa ou que as modalidades ilustradas podem ser modificadas em arranjo e detalhe sem divergir do espírito da invenção. Portanto, a invenção conforme aqui descrita contempla todas tais modalidades que podem encaixar dentro do escopo das reivindicações a seguir e seus equivalentes.

REIVINDICAÇÕES

1. Método de proteger uma rede de computadores local (51, 205) com respeito a uma rede de computadores de área ampla (52, 209), o método sendo **CARACTERIZADO** pelo fato de que compreende:

detectar se um dispositivo de porta de comunicação de hardware utilizável está instalado entre a rede de computadores local (51, 205) e a rede de computadores de área ampla (52, 209);

se for determinado que um dispositivo de porta de comunicação de hardware utilizável está instalado, comunicar com o dispositivo de porta de comunicação de hardware (207) pela rede local (51, 205) para recuperação da informação de descrição com relação ao dispositivo (207), apresentando a informação relacionada à informação de descrição do dispositivo (207) a um usuário, receber uma seleção do usuário para configuração do dispositivo (207) e automaticamente configurar o dispositivo (207) de acordo com a seleção do usuário; e

se for determinado que um dispositivo de porta de comunicação de hardware (207) utilizável não está instalado, detectar se uma barreira de proteção de software utilizável está instalada entre a rede de computadores local (51, 205) e a rede de computadores de área ampla (52, 209), e se uma barreira de proteção de software utilizável estiver instalada, colher a informação de descrição com relação à barreira de proteção, apresentando a informação relacionada à informação de descrição da barreira de proteção ao

usuário, receber uma seleção do usuário para configurar a barreira de proteção e automaticamente configurar a barreira de proteção de acordo com a seleção do usuário.

2. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a detecção se um dispositivo de porta de comunicação de hardware (207) utilizável está instalado entre a rede de computadores local (51, 205) e a rede de computadores de área ampla (52, 209) adicionalmente compreende:

transmitir automaticamente uma transmissão de descoberta de multidifusão por meio da rede local (51, 205); e

receber uma resposta para a transmissão de descoberta de multidifusão do dispositivo de porta de comunicação (207), em que a resposta compreende um localizador para uso no contato do dispositivo de porta de comunicação na rede local (51, 205).

3. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a comunicação com o dispositivo de porta de comunicação de hardware (207) na rede local (51, 205) para recuperar a informação de descrição com relação ao dispositivo (207) adicionalmente compreende:

transmitir automaticamente uma solicitação de descrição do dispositivo (207) por meio da rede local (51, 205) para o dispositivo de porta de comunicação (207); e

em resposta à transmissão da solicitação de descrição do dispositivo (207), receber do dispositivo de

porta de comunicação (207) uma listagem dos serviços suportados pelo dispositivo de porta de comunicação (207).

4. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a listagem dos serviços suportados pelo dispositivo de porta de comunicação (207) adicionalmente compreende uma listagem dos sub-dispositivos suportados pelo dispositivo de porta de comunicação (207).

5. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a detecção se um dispositivo de porta de comunicação de hardware (207) utilizável está instalado entre a rede de computadores local (51, 205) e a rede de computadores de área ampla (52, 209) adicionalmente compreende receber uma indicação do usuário da utilidade de um dispositivo de porta de comunicação de hardware (207).

6. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que a listagem dos serviços suportados pelo dispositivo de porta de comunicação (207) adicionalmente compreende um respectivo localizador associado a cada serviço, por meio do qual o respectivo localizador associado a um serviço é utilizável para configurar aquele serviço.

7. Método, de acordo com a reivindicação 6, **CARACTERIZADO** pelo fato de que o respectivo localizador associado a cada serviço compreende um URL.

8. Método, de acordo com a reivindicação 2, **CARACTERIZADO** pelo fato de que a transmissão automática de uma transmissão de descoberta de multidifusão por meio da rede local (51, 205) compreende:

esperar por um período predeterminado para expirar; e

na expiração do período predeterminado, transmitir a transmissão de descoberta de multidifusão por meio da rede local (51, 205).

9. Método, de acordo com a reivindicação 3, **CARACTERIZADO** pelo fato de que a listagem dos serviços suportados pelo dispositivo de porta de comunicação (207) compreende uma listagem correspondendo ao Protocolo de Configuração Dinâmica do Hospedeiro.

10. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a detecção se uma barreira de proteção de software utilizável está instalada entre a rede de computadores local (51, 205) e a rede de computadores de área ampla (52, 209) adicionalmente compreende receber uma indicação do usuário da utilidade de uma barreira de proteção de software.

11. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a coleta da informação de descrição com relação à barreira de proteção adicionalmente compreende chamar uma API e receber a informação de descrição em resposta à chamada da API.

12. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a configuração automática da barreira de proteção de acordo com a seleção do usuário adicionalmente compreende chamar uma API, em que a chamada pela API compreende a informação de configuração.

13. Método, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o recebimento de uma resposta à transmissão de descoberta de multidifusão compreende receber uma pluralidade de respostas de uma pluralidade de dispositivos incluindo o dispositivo de porta de comunicação.

14. Método, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que a transmissão automática de uma solicitação de descrição do dispositivo por meio da rede local (51, 205) para o dispositivo de porta de comunicação (207) adicionalmente compreende:

apresentar uma listagem da pluralidade de dispositivos a um usuário do computador hospedeiro (405); e

receber do usuário do computador hospedeiro (405) uma seleção do dispositivo de porta de comunicação (207).

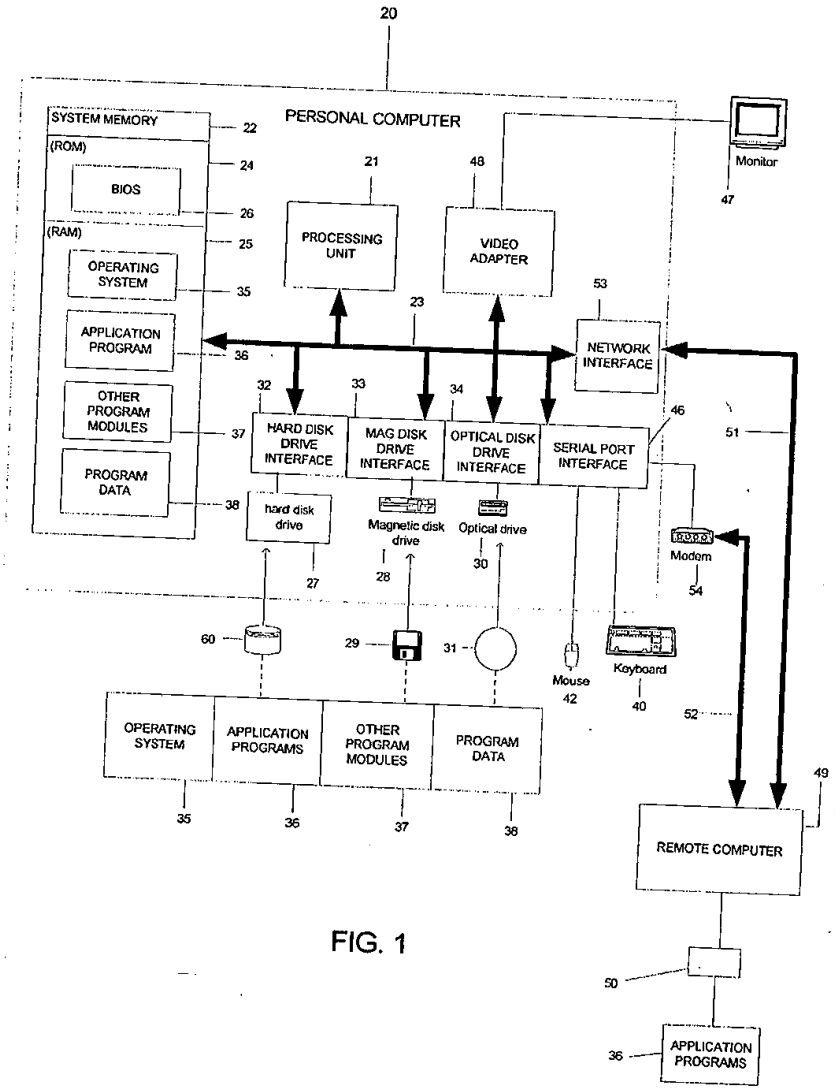
20
PERSONAL COMPUTER
SYSTEM MEMORY
22
(ROM)
24
BIOS
26
(RAM)
25
OPERATING SYSTEM
35
APPLICATION PROGRAM
36
OTHER PROGRAM MODULES
37
PROGRAM DATA
38
21
PROCESSING UNIT
48
VIDEO ADAPTER
23
53
NETWORK INTERFACE
Monitor
47
32
33
34
HARD DISK DRIVE INTERFACE
MAG DISK DRIVE INTERFACE
OPTICAL DISK DRIVE INTERFACE
SERIAL PORT INTERFACE
46
51
hard disk drive
27
Magnetic disk drive
28
Optical drive
30
Modem
54
60
29
31
Mouse
42
Keyboard
40
52
OPERATING SYSTEM
APPLICATION PROGRAMS
OTHER PROGRAM MODULES
PROGRAM DATA
35
36
37
38
49
REMOTE COMPUTER
50
36
APPLICATION PROGRAMS

FIG. 1

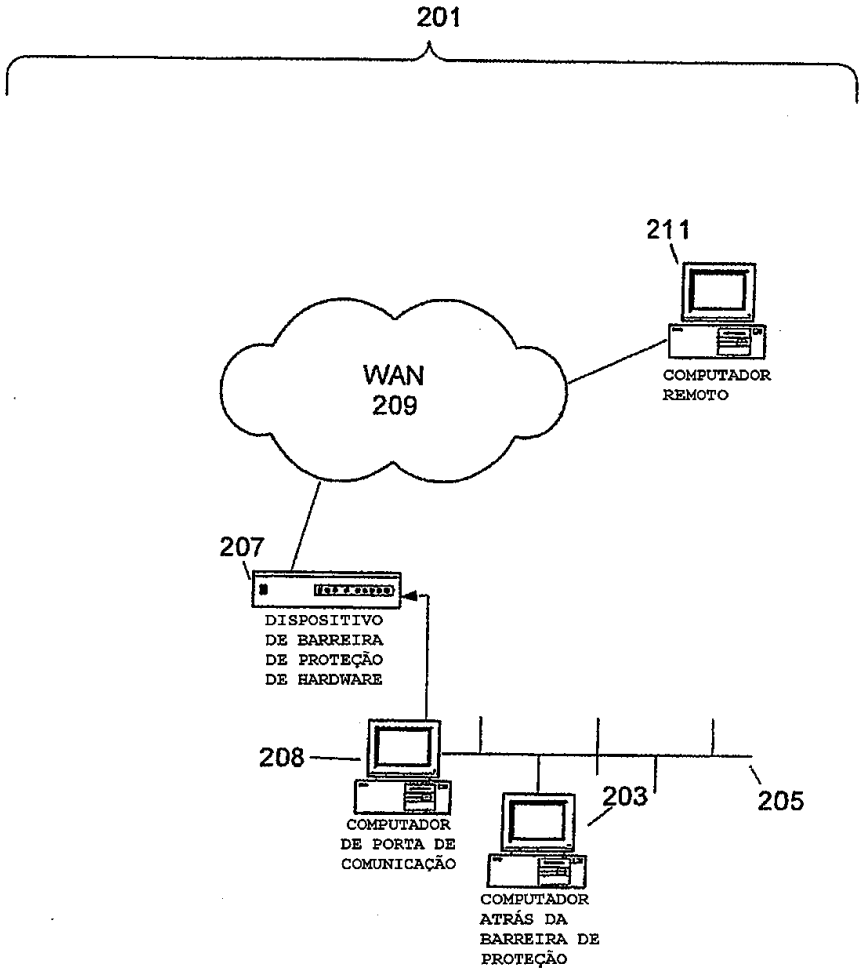
201
211
WAN
209
COMPUTADOR
REMOTO
207
DISPOSITIVO
DE BARREIRA
DE PROTEÇÃO
DE HARDWARE
208
COMPUTADOR
DE PORTA DE
COMUNICAÇÃO
203
205
COMPUTADOR
ATRÁS DA
BARREIRA DE
PROTEÇÃO

FIG. 2

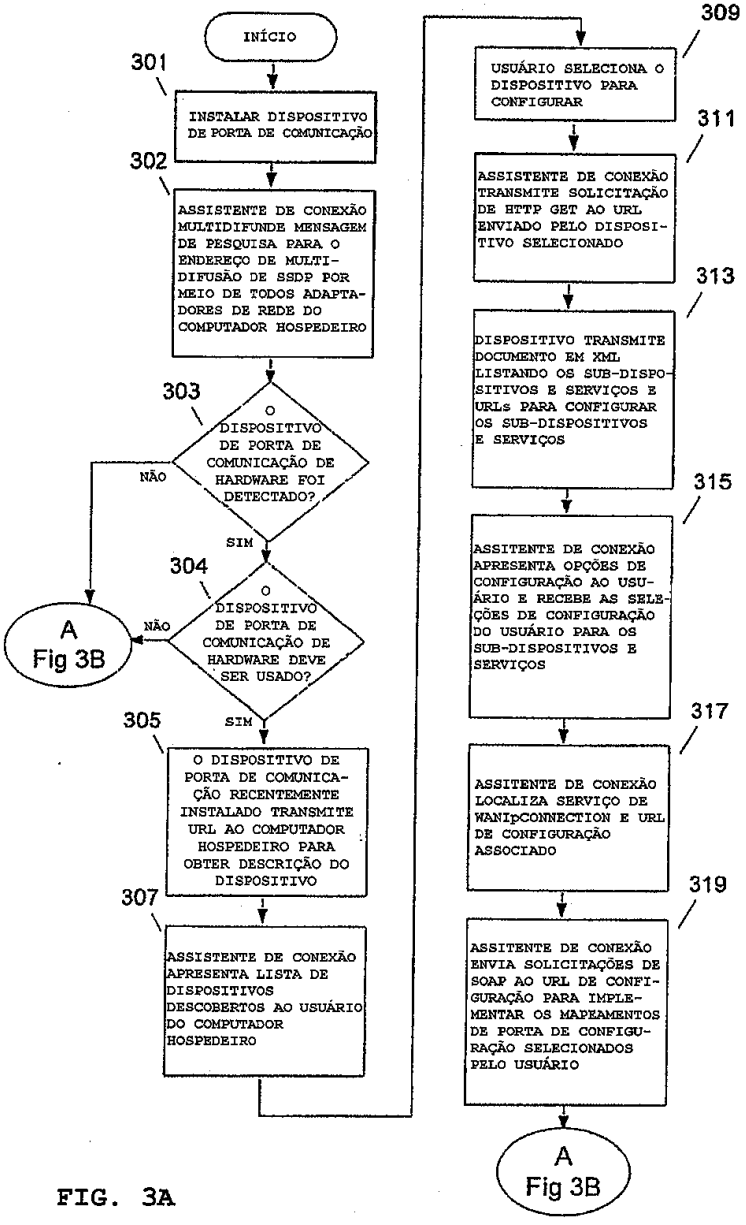
INÍCIO
301
INSTALAR DISPOSITIVO DE PORTA DE COMUNICAÇÃO
302
ASSISTENTE DE CONEXÃO MULTIDIFUNDE MENSAGEM DE PESQUISA PARA O ENDEREÇO DE MULTI-DIFUSÃO DE SSDP POR MEIO DE TODOS ADAPTA-DORES DE REDE DO COMPUTADOR HOSPEDEIRO
303
O DISPOSITIVO DE PORTA DE COMUNICAÇÃO DE HARDWARE FOI DETECTADO?
NÃO
SIM
304
O DISPOSITIVO DE PORTA DE COMUNICAÇÃO DE HARDWARE DEVE SER USADO?
NÃO
SIM
A Fig 3B
305
O DISPOSITIVO DE PORTA DE COMUNICA-ÇÃO RECENTEMENTE INSTALADO TRANSMITE URL AO COMPUTADOR HOSPEDEIRO PARA OBTER DESCRIÇÃO DO DISPOSITIVO
307
ASSISTENTE DE CONEXÃO APRESENTA LISTA DE DISPOSITIVOS DESCOBERTOS AO USUÁRIO DO COMPUTADOR HOSPEDEIRO
309
USUÁRIO SELECIONA O DISPOSITIVO PARA CONFIGURAR
311
ASSISTENTE DE CONEXÃO TRANSMITE SOLICITAÇÃO DE HTTP GET AO URL ENVIADO PELO DISPOSI-TIVO SELECIONADO
313
DISPOSITIVO TRANSMITE DOCUMENTO EM XML LISTANDO OS SUB-DISPO-SITIVOS E SERVIÇOS E URLs PARA CONFIGURAR OS SUB-DISPOSITIVOS E SERVIÇOS
315
ASSITENTE DE CONEXÃO APRESENTA OPÇÕES DE CONFIGURAÇÃO AO USU-ÁRIO E RECEBE AS SELE-ÇÕES DE CONFIGURAÇÃO DO USUÁRIO PARA OS SUB-DISPOSITIVOS E SERVIÇOS
317
ASSITENTE DE CONEXÃO LOCALIZA SERVIÇO DE WANIpCONNECTION E URL DE CONFIGURAÇÃO ASSOCIADO
319
ASSITENTE DE CONEXÃO ENVIA SOLICITAÇÕES DE SOAP AO URL DE CONFI-GURAÇÃO PARA IMPLE-MENTAR OS MAPEAMENTOS DE PORTA DE CONFIGU-RAÇÃO SELECIONADOS PELO USUÁRIO
A Fig 3B

FIG. 3A

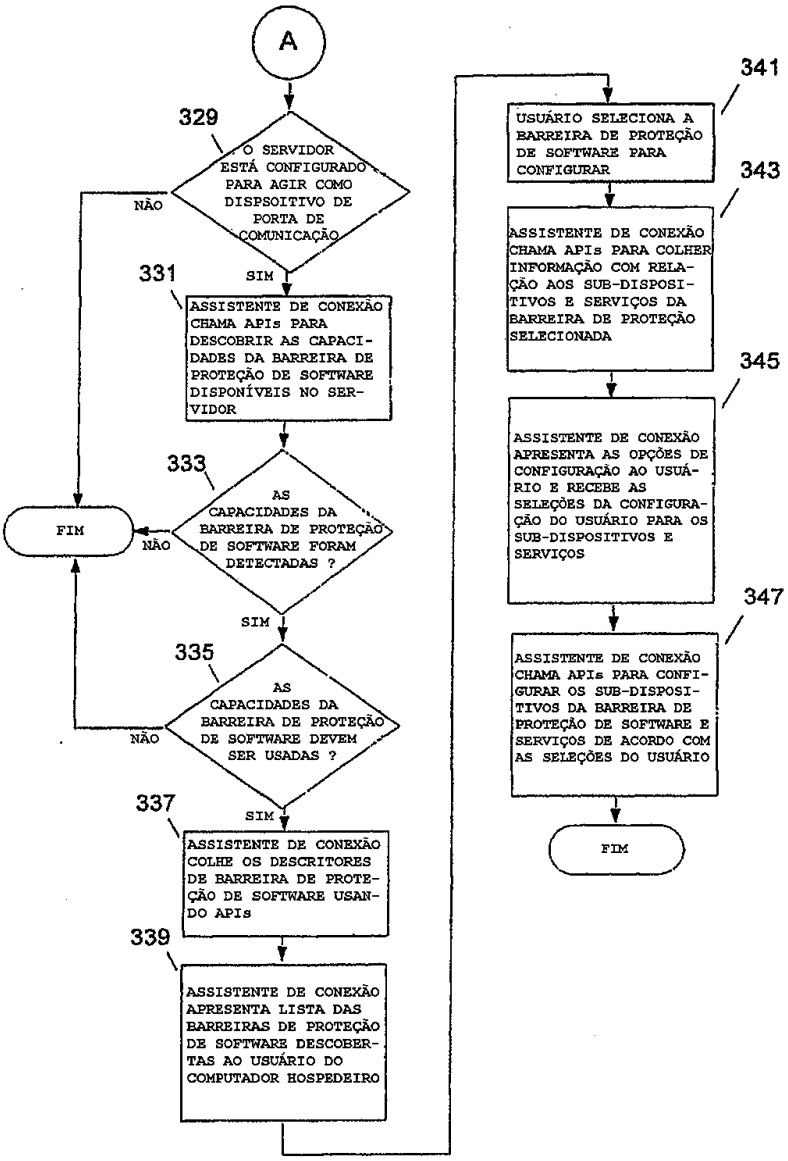


FIG. 3B

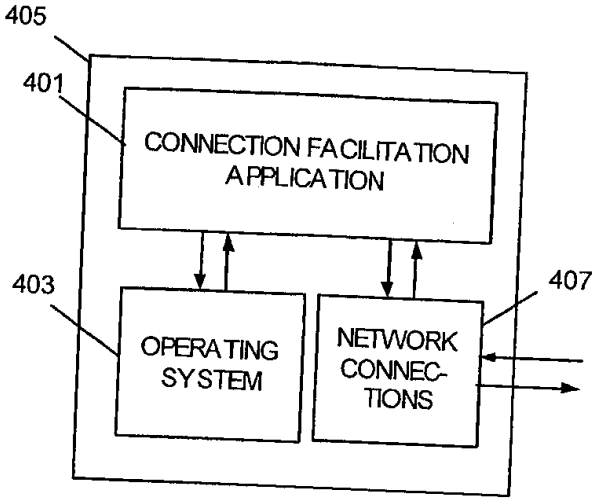
405
401
CONNECTION FACILITATION APPLICATION
403
407
OPERATING SYSTEM
NETWORK CONNEC-TIONS

FIGURE 4