INSTITUTO NACIONAL
DA PROPRIEDADE INDUSTRIAL

(11) Número de Publicação: **PT 1420564 E**

(51) Classificação Internacional:
H04L 29/06 (2006.01) ***G06F 1/00*** (2006.01)
H04L 12/24 (2006.01)

(12) **FASCÍCULO DE PATENTE DE INVENÇÃO**

(22) Data de pedido: **2003.10.28**

(30) Prioridade(s): **2002.10.28 US 0281843**

(43) Data de publicação do pedido: **2004.05.19**

(45) Data e BPI da concessão: **2006.12.13**
001/2007

(73) Titular(es):
SECURE COMPUTING CORPORATION
2675 LONG LAKE ROAD ROSEVILLE
MINNESOTA 55113 **US**

(72) Inventor(es):
THOMAS R. MARKHAM **US**
JESSICA J BOGLE **US**
CHARLES N. JR PAYNE **US**

(74) Mandatário:
ALBERTO HERMÍNIO MANIQUE CANELAS
RUA VÍCTOR CORDON, 14 1249-103 LISBOA **PT**

(54) Epígrafe: **MODELO DE POLÍTICA ASSOCIATIVA**

(57) Resumo:

RESUMO

"MODELO DE POLÍTICA ASSOCIATIVA"

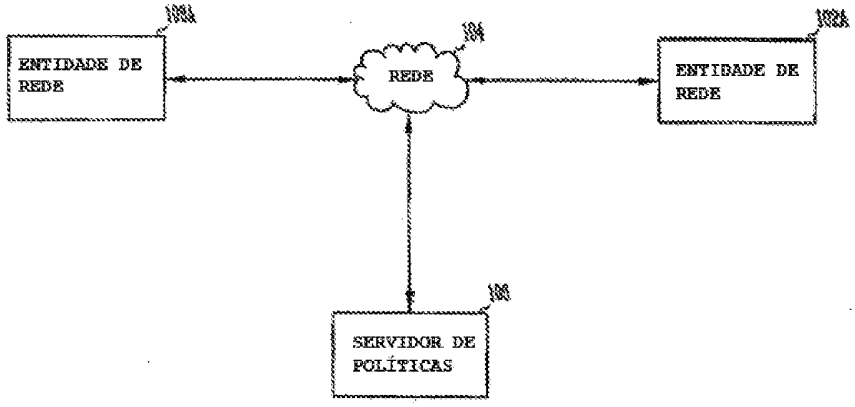


Fig.1A

São fornecido sistemas e métodos para um modelo de política associativa. Uma forma de realização da presente invenção fornece um método para implementação de uma política associativa. Nesta forma de realização, o método inclui fornecer uma política num servidor de políticas, a política tendo uma definição de serviço que contém primeiro e segundo componente relacional, fornecendo primeira e segunda entidade de rede, acoplando operacionalmente a primeira e segunda entidade de rede ao servidor de políticas, associando dinamicamente a primeira entidade de rede com a segunda entidade de rede (em que tal associação inclui associar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede, e associar o segundo componente relacional da definição de serviço na política à segunda entidade de rede), e aplicar a política na primeira e segunda entidade de rede.

DESCRIÇÃO

"MODELO DE POLÍTICA ASSOCIATIVA"

CAMPO DA INVENÇÃO

A presente invenção relaciona-se com sistemas computacionais, e mais particularmente com métodos e sistemas para implementação de um modelo de política associativa.

ANTECEDENTES DA INVENÇÃO

Existe um número crescente de utilizadores em rede (clientes). Adicionalmente, existe um número crescente de aplicações de rede (servidores) que providenciam um conjunto de serviços para estes utilizadores. Num tal ambiente, a segurança dos dados é frequentemente uma preocupação. Os utilizadores acedem continuamente aos servidores, e os servidores respondem aos pedidos que chegam através da rede.

Para ajudar na gestão das preocupações de segurança, muitos sistemas ligados à Internet ou outros sistemas de rede implementam políticas de segurança em que um servidor de políticas, por exemplo, controla a segurança para um domínio de acordo com as regras na sua política.

Desta maneira, o servidor de políticas é capaz de endereçar as necessidades de segurança para os nós no domínio aplicando as regras existentes na política.

Os modelos típicos de especificação de políticas requerem uma especificação explícita dos elementos de rede num dado domínio de segurança. A especificação explícita pode incluir os nomes dos nós ou endereços do Protocolo Internet (IP) (do inglês "IP - Internet Protocol") dos elementos de rede, e tal informação frequentemente necessita de ser previamente introduzida no modelo de política. Se o nome ou o endereço IP de um dado elemento de rede muda ao longo do tempo (tal como quando é utilizado o Protocolo de Configuração Dinâmica de Nós (DHCP) (do inglês "DHCP - Dynamic Host Configuration Protocol)), ou se são adicionados ou apagados elementos de rede de um domínio, o modelo de política pode necessitar de ser actualizado manualmente, e a informação apontada por cada um dos elementos de rede pode também necessitar de mudar. Isto requer um esforço adicional, e introduz um maior potencial de erro e inconsistência. Adicionalmente, o modelo de política em tais implementações está muitas vezes dependente da topologia de rede. Por exemplo, se a política utiliza endereços IP fixos, a política deve mudar frequentemente para permanecer consistente com as alterações dos endereços IP.

A patente GB2356763 divulga métodos e equipamentos para gestão de políticas. Uma política é

definida como um conjunto de regras para controlar a utilização ou o acesso a serviços de rede. São descritas diversas regras para atribuição de políticas a serviços de rede especificados. Estas técnicas incluem associar grupos de serviços de rede especificados com grupos de políticas, e fornecer utilizadores e nomes de nós com endereços de rede associados identificados pela política e mapeados dinamicamente a processos de clientes.

A patente WO00/69145 divulga modelos de políticas de segurança de rede generalizados para implementação de políticas de segurança de rede similares através de redes múltiplas. Uma política de segurança de rede compreende regras de segurança de rede, cada uma delas especificada com respeito a um ou mais pseudónimos. Para cada pseudónimo, é recebida uma lista de um ou mais elementos de rede servindo a função representada pelo pseudónimo. Cada pseudónimo no modelo de política de segurança de rede é substituído com a lista recebida de dispositivos de segurança de rede especificados para o pseudónimo produzir uma política de segurança de rede adaptada para utilização numa rede.

SUMÁRIO DA INVENÇÃO

Várias formas de realização da presente invenção são aqui providenciadas. Uma forma de realização providencia um método para implementar uma política associativa. Nesta forma de realização, o método inclui

fornecer uma política num servidor de políticas, a política tendo uma definição de serviço que contém primeiro e segundo componente relacional e em que cada componente relacional tem um ou mais conjuntos de regras em que cada um contém um ou mais termos, fornecer primeira e segunda entidade de rede, acoplando operacionalmente a primeira e segunda entidade de rede ao servidor de políticas, associando dinamicamente a primeira entidade de rede com a segunda entidade de rede (em que uma tal associação inclui ligar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede, e ligar o segundo componente relacional da definição de serviço na política à segunda entidade de rede, e aplicar a política na primeira e segunda entidade de rede.

Esta forma de realização, assim como outras formas de realização, irá ser descrita na descrição detalhada abaixo.

BREVE DESCRIÇÃO DOS DESENHOS

A FIG.1A ilustra um diagrama de blocos de um sistema possuindo múltiplas entidades de rede e um servidor de políticas para implementar várias formas de realização da presente invenção.

A FIG.1B ilustra um diagrama de blocos para uma forma de realização do sistema mostrado na FIG.1A, em que cada uma das entidades de rede inclui um computador com um componente de software.

A FIG.1C ilustra um diagrama de blocos para uma forma de realização do sistema mostrado na FIG.1A, em que cada uma das entidades de rede inclui um computador e um dispositivo de interface de rede.

A FIG.2 ilustra um diagrama de blocos de um sistema cliente-servidor e servidor de políticas para implementar várias formas de realização da presente invenção.

A FIG.3 ilustra um diagrama de blocos de um modelo de política associativa, de acordo com uma forma de realização da presente invenção.

A FIG.4 ilustra um diagrama de blocos de uma definição de serviço com componentes de cliente e servidor, de acordo com uma forma de realização da presente invenção.

A FIG.5A e a FIG.5B ilustram diagramas de blocos de várias definições de serviços tendo componentes de cliente e servidor, de acordo com determinadas formas de realização da presente invenção.

A FIG.6 ilustra um diagrama de blocos da distribuição de especificações de políticas a partir de um escritório corporativo para filiais, de acordo com uma forma de realização da presente invenção.

DESCRIÇÃO DETALHADA

Na descrição detalhada seguinte das formas de realização, é feita referência aos desenhos acompanhantes que formam parte dela, e nos quais são mostradas por meio de ilustrações formas de realização específicas nas quais a invenção pode ser praticada. Estas formas de realização são descritas em detalhe suficiente para permitir aos especialistas na técnica praticarem a invenção. Deverá ser compreendido que as várias formas de realização da invenção, embora diferentes, não são necessariamente mutuamente exclusivas. Por exemplo, uma funcionalidade, estrutura ou característica específica descrita numa forma de realização pode ser incluída noutras formas de realização.

Uma forma específica da invenção providencia um modelo de política associativa. Uma política associativa é uma política que é baseada sobre uma associação de alto nível entre um par de entidades. Por exemplo, associações de entidades poderão incluir: (1) cliente de correio electrónico e servidor de correio electrónico, (2) pessoa de vendas e base de dados de vendas; (3) cliente de Sistema Básico de Entrada e Saída da Rede (NetBIOS) (do inglês "NetBIOS - Network Basic Input/Output System") e servidor de NetBIOS; ou cliente *Web* e proxy *Web*. Um modelo de política associativa é um modelo que é utilizado para definir e aplicar uma política de segurança a conjuntos de tais entidades com base na sua associação. Um tal modelo é

capaz de implementar uma especificação de política independente da topologia de rede ou dos endereços das máquinas envolvidas. A especificação da política pode ser utilizada para especificar um acordo de serviços entre entidades ou pode ser utilizado para definir uma política de segurança para as entidades. As políticas associativas permitem uma fácil criação e gestão das políticas de segurança (filtragem de pacotes e associações criptográficas). Isto torna uma política auto-suficiente com respeito ao Protocolo Internet (IP), e providencia suporte flexível aos endereços IP baseados no Protocolo de Configuração Dinâmica de Nós (DHCP). É também providenciado suporte para utilizadores (ou entidades) tanto em ambientes com fios como sem fios que possam incluir computadores portáteis, assistentes digitais pessoais (PDA's) (do inglês "PDA - Personal Digital Assistants"), e afins.

Esta forma de realização da invenção permite uma maior atribuição dinâmica de uma política (ou políticas) a um dispositivo. Por exemplo, um computador portátil pode ser atribuído à equipa de engenharia num dia, mas deslocado para a equipa de gestão no dia seguinte. O modelo de política associativa pode automaticamente (sem intervenção manual do administrador) resolver os serviços a serem providenciados ao computador portátil e carregar a informação de endereçamento IP correcta no computador portátil e em todos os servidores associados.

Numa forma de realização, um modelo de política associativa é implementado numa rede com fios, em que as

entidades de rede incluem Placas de Interfaces de Rede (NIC's) (do inglês "NIC - Network Interface Cards"). Numa forma de realização, o modelo é implementado numa rede sem fios. Numa forma de realização, o modelo é implementado utilizando software em nós em vez dos NIC's. Implementando uma solução de software dentro dos servidores, encaminhadores, PDA's, ou telefones celulares permite uma especificação de endereços explícita, e pode requerer menos trabalho por parte do administrador das políticas.

A FIG.1A ilustra um diagrama de blocos de um sistema com múltiplas entidades de rede e um servidor de políticas para implementação de várias formas de realização da presente invenção. Na FIG.1A, o sistema 100A inclui a entidade de rede 108A, a rede 104, o servidor de políticas 106, e a entidade de rede 102A. A entidade de rede 108A, o servidor de políticas 106, e a entidade de rede 102A são acoplados à rede 104. Numa forma de realização, a rede 104 é uma rede com fios. Numa forma de realização, a rede 104 é uma rede sem fios. Numa forma de realização, a rede 104 é uma rede baseada na Internet. Numa forma de realização, o servidor de políticas 106 tem uma política de segurança que inclui um primeiro conjunto de regras e um segundo conjunto de regras, e cada um dos conjuntos de regras tem um ou mais termos. Quando o sistema 100A está operacional, a política 106 actua para converter a política de segurança numa política da primeira entidade inserindo informação de entidade para a entidade de rede 102A nos termos do segundo conjunto de regras, enviando a política da primeira

entidade à entidade de rede 108A, e enviando a política da segunda entidade à entidade de rede 102A.

A FIG.1B ilustra um diagrama de blocos para uma forma de realização do sistema mostrado na FIG.1A, em que cada uma das entidades de rede inclui um computador com um componente de software. Na FIG.1B, o sistema 100B inclui a entidade de rede 108B, a rede 104, o servidor de políticas 106, e a entidade de rede 102B. A entidade de rede 108B, o servidor de políticas 106, e a entidade de rede 102B são cada um deles acoplados à rede 104. Nesta forma de realização, a entidade de rede 108B inclui o computador 110, e a entidade de rede 102B inclui o computador 114. O computador 110 inclui o componente de software 112, e o computador 114 inclui o componente de software 116. Esta forma de realização providencia uma solução de software para a implementação da política associativa.

A FIG.1C ilustra um diagrama de blocos para uma forma de realização do sistema mostrado na FIG.1A, em que cada uma das entidades de rede inclui um computador e um dispositivo de interface de rede. Na FIG.1C, o sistema 100C inclui a entidade de rede 108C, a rede 104, o servidor de políticas 106, e a entidade de rede 102C. A entidade de rede 108C, o servidor de políticas 106, e a entidade de rede 102C são cada um deles acoplados à rede 104. A entidade de rede 108C inclui o computador 118 e o dispositivo de interface de rede 120. O computador 118 é acoplado ao dispositivo de interface de rede 120.

Similarmente, a entidade de rede 102C inclui o computador 124 e o dispositivo de interface de rede 122. O computador 124 é acoplado ao dispositivo de interface de rede 122. Numa forma de realização, o sistema 100C contém uma *firewall* distribuída tal como descrito na Candidatura a Patente dos Estados Unidos com o Número de Série 09/578,314 e o Número de Publicação US 20030126468 com candidatura em 25 de Maio de 2000, intitulada: MÉTODO E SISTEMA DE *FIREWALL* DISTRIBUÍDA, em que os dispositivos de interface de rede 120 e 122 cada um deles inclui uma *firewall* embebida para autorizar pacotes de dados.

Noutra forma de realização da presente invenção, é providenciado um método para implementar uma política associativa. Nesta forma de realização, o método inclui fornecer uma política num servidor de políticas (a política tendo uma definição de serviço que contém primeiro e segundo componente relacional), fornecer primeira e segunda entidade de rede, acoplar operacionalmente a primeira e segunda entidade de rede ao servidor de políticas, associar dinamicamente a primeira entidade de rede com a segunda entidade de rede (em que tal associação inclui ligar o primeiro componente relacional da definição de serviço na política com a primeira entidade de rede, e ligar o segundo componente relacional da definição de serviço na política com a segunda entidade de rede), e aplicar a política na primeira e segunda entidade de rede.

Em algumas formas de realização, fornecer uma política num servidor de políticas inclui fornecer uma

política de segurança num servidor de políticas. Em algumas formas de realização, fornecer uma política num servidor de políticas inclui fornecer uma política com uma definição de serviço que inclui primeiro e segundo componente relacional, e em que a definição de serviço corresponde a um serviço de correio electrónico, um serviço de base de dados de vendas, um serviço de Sistema Básico de Entrada e Saída da Rede (NetBIOS), ou um serviço de *web*. Em algumas formas de realização, fornecer uma política num servidor de políticas inclui fornecer uma política com uma definição de serviço que inclui primeiro e segundo componente relacional, e em que cada primeiro e segundo componente relacional inclui um ou mais conjuntos de regras de filtragem de pacotes. Em algumas formas de realização, fornecer uma política num servidor de políticas inclui fornecer uma política com uma definição de serviço que inclui um componente relacional de cliente e um componente relacional de servidor, e em que fornecer primeira e segunda entidade de rede inclui fornecer um dispositivo servidor e um dispositivo cliente.

Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer primeira e segunda entidade de rede seleccionadas a partir de um grupo consistindo de dispositivos, utilizadores, e pacotes de software. Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer primeiro e segundo membro de um grupo privado virtual (VPG) (do inglês “VPG - Virtual Private Group”) ou

de um uma rede privada virtual (VPN) (do inglês "VPG - Virtual Private Network"). As VPG's são descritas na Candidatura a Patente em tramitação com o Número de Série 10/234,233, com o número de publicação US 20040044891. Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer um primeiro membro de uma primeira VPG e um segundo membro de uma segunda VPG. Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer primeira e segunda entidade de rede que estão associadas com um ou mais conjuntos de dispositivos. Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer primeira e segunda entidade com endereços do Protocolo Internet (IP) que são atribuídos de acordo com o Protocolo de Configuração Dinâmica de Nós (DHCP). Em algumas formas de realização, fornecer primeira e segunda entidade de rede inclui fornecer primeira e segunda entidade de rede em que cada uma delas inclui um dispositivo de interface de rede para gerir uma *firewall* embebida.

Em algumas formas de realização, acoplar operacionalmente a primeira e segunda entidade de rede ao servidor de políticas inclui enviar os endereços do Protocolo Internet (IP) da primeira e segunda entidade de rede ao servidor de políticas. Em algumas formas de realização, acoplar operacionalmente a primeira e a segunda entidade de rede ao servidor de políticas inclui associar um primeiro utilizador à primeira entidade de rede, o

primeiro utilizador sendo associado com uma primeira função, ligar um segundo utilizador com a segunda entidade de rede, o segundo utilizador sendo associado com uma segunda função, identificando um primeiro endereço do Protocolo Internet (IP) da primeira entidade de rede, identificando um segundo endereço IP da segunda entidade de rede, enviar a informação sobre a primeira função e o primeiro endereço IP ao servidor de políticas, e enviar a informação sobre a segunda função e o segundo endereço IP ao servidor de políticas.

Em algumas formas de realização, ligar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede inclui enviar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede. Em algumas formas de realização, ligar o segundo componente relacional da definição de serviço na política à segunda entidade de rede.

A FIG.2 ilustra um diagrama de blocos de um sistema cliente-servidor e servidor de políticas para implementar várias formas de realização da presente invenção. (Certas formas de realização, tal como será descrito adiante, também providenciam suporte não hierárquico (tal como cliente para cliente, ou servidor para servidor)). Na FIG.2, o sistema 200 inclui o dispositivo servidor 208, a rede 204, o servidor de políticas 206, e o dispositivo cliente 202. Numa forma de realização, a rede 204 é uma rede com fios. Numa forma de

realização, a rede 204 é uma rede sem fios. Numa forma de realização, a rede 204 é uma rede com base na Internet. Numa forma de realização, a rede 204 é uma Intranet. Numa forma de realização, cada dispositivo servidor 208 e dispositivo cliente 202 inclui NIC's. Numa forma de realização, cada dispositivo servidor 208 e dispositivo cliente 202 inclui componentes de software para implementar uma política associativa. O dispositivo servidor 208, o servidor de políticas 206, e o dispositivo cliente 202 são acoplados à rede 204. O dispositivo servidor 208 inclui a política do servidor 214, e o dispositivo cliente 202 inclui a política do cliente 208. O servidor de políticas 206 inclui o interface 210 (para acoplar o servidor de políticas 206 ao dispositivo servidor 208 e ao dispositivo cliente 202 através da rede 204), e a política principal 212. Numa forma de realização, a política principal 212 inclui um componente de cliente e um componente de servidor.

Quando o sistema 200 está operacional, o servidor de políticas 206 actua para obter informação do servidor sobre o dispositivo servidor 208, obter informação do cliente sobre o dispositivo cliente 202, criar a política do cliente 208 utilizando o componente de cliente da política principal 212 e da informação do servidor, criar a política do servidor 214 utilizando o componente de servidor da política principal 212 e da informação do cliente, enviar a política do cliente 208 ao dispositivo cliente 202, e enviar a política do servidor 214 ao dispositivo servidor 208.

Uma forma de realização aplica a política do cliente 208 no dispositivo cliente 202, e aplica a política do servidor 214 no dispositivo servidor 208. Outra forma de realização aplica apenas a política do servidor 214 no dispositivo servidor 208.

Noutra forma de realização da presente invenção, é providenciado um método implementado por computador num servidor de políticas. Nesta forma de realização, o método inclui fornecer uma política principal no servidor de políticas (a política principal tendo um primeiro componente e um segundo componente), associar o servidor de políticas a um primeiro dispositivo para obter informação sobre o primeiro dispositivo, associar o servidor de políticas a um segundo dispositivo para obter informação sobre o segundo dispositivo, criar uma primeira política no servidor de políticas utilizando o primeiro componente da política principal e a informação sobre o segundo dispositivo, criar uma segunda política no servidor de políticas utilizando o segundo componente da política principal e a informação sobre o primeiro dispositivo, enviar a primeira política ao primeiro dispositivo, e enviar a segunda política ao segundo dispositivo.

Em algumas formas de realização, associar o servidor de políticas a um primeiro dispositivo para obter informação sobre o primeiro dispositivo inclui ligar o servidor de políticas a um dispositivo cliente para obter

informação sobre o dispositivo cliente, e ligar o servidor de políticas a um segundo dispositivo para obter informação sobre o dispositivo cliente, e ligar o servidor de políticas a um segundo dispositivo para obter informação sobre o segundo dispositivo inclui ligar o servidor de políticas a um dispositivo servidor para obter informação sobre o dispositivo servidor.

Em algumas formas de realização, fornecer uma política principal no servidor de políticas inclui fornecer uma política de segurança principal no servidor de políticas.

Em algumas formas de realização, associar o servidor de políticas a um primeiro dispositivo para obter informação sobre o primeiro dispositivo inclui obter informação de endereçamento do Protocolo Internet (IP) sobre o primeiro dispositivo.

Em algumas formas de realização, associar o servidor de políticas a um segundo dispositivo para obter informação sobre o segundo dispositivo inclui obter informação de endereçamento do Protocolo Internet (IP) sobre o segundo dispositivo.

Em algumas formas de realização, a política principal inclui ainda um terceiro componente, e o método inclui ainda associar o servidor de políticas a um terceiro dispositivo para obter informação sobre o terceiro

dispositivo, criar uma primeira política no servidor de políticas utilizando o terceiro componente da política principal e a informação sobre o primeiro e o segundo dispositivo, e enviar a terceira política ao terceiro dispositivo, em que o primeiro, segundo, e terceiro dispositivo são dispositivos não hierárquicos.

A FIG.3 ilustra um diagrama de blocos de um modelo de política associativa, de acordo com uma forma de realização da presente invenção. Na FIG.3, o modelo 300 inclui vários componentes. Numa forma de realização, as regras 302 estão incluídas no modelo 300. As regras 302 incluem uma especificação de filtragem de pacotes de baixo nível que identifica vários itens, tais como um intervalo de portos, uma direcção, e/ou um tuplo de um protocolo. Numa forma de realização, os conjuntos de regras 304 estão incluídos no modelo 300. Um conjunto de regras inclui um grupo para uma ou mais regras (tais como as regras 302) que representam uma aplicação em rede (e.g. Serviço de Nomes de Domínio, Telnet, etc.). Numa forma de realização, os conjuntos de regras 304 incluem um conjunto de regras com uma ou mais regras de filtragem de entrada e uma ou mais regras de filtragem de saída. Numa forma de realização, os serviços 306 estão incluídos no modelo 300. Numa forma de realização, uma definição de serviço inclui um ou mais conjuntos de regras (tais como os conjuntos de regras 304). Na forma de realização mostrada na FIG.3, os serviços 306 incluem definições de serviços com um componente de cliente e com um componente de servidor. Outras formas de

realização providenciam outros componentes relacionais na definição de serviço. O componente de cliente está associado com o dispositivo cliente 314 através da inclusão do componente de cliente na política do cliente 308. Numa forma de realização, o componente de cliente contém informação de endereçamento do Protocolo Internet (IP) sobre o dispositivo servidor 312. O componente de servidor está também associado com o dispositivo servidor 312 através da inclusão na política do servidor 310, que está associada com o dispositivo servidor 312. Numa forma de realização, o componente de servidor contém informação de endereçamento IP sobre o dispositivo cliente 314. Numa forma de realização, podem também ser definidos serviços não hierárquicos (e.g. NetMeeting). Numa forma de realização, uma definição de serviço define uma relação entre duas ou mais entidades (cliente, servidor, não hierárquica, etc.). Estas entidades (dispositivos, utilizadores, pacotes de software, etc.) não necessitam de ser especificadas na mesma altura em que a relação de serviço é definida. Podem ser associadas com o serviço mais tarde e as ligações serem resolvidas nessa altura.

Na FIG.3, uma política (tal como a política do cliente 308 ou a política do servidor 310) inclui um ou mais serviços (tais como os serviços 306). Quando uma entidade ou dispositivo (tal como um computador portátil) é associada com uma política, o endereço IP actual do dispositivo é processado utilizando a definição de serviço, e o endereço é incorporado na política que contém o serviço

associado (e.g. a outra metade do par cliente/servidor, ou a contraparte). Por exemplo, se um serviço Telnet é definido nos serviços 306, inclui um componente de cliente e um componente de servidor. O componente de cliente é incluído na política do cliente 308, enquanto o componente de servidor é incluído na política do servidor 310. Numa forma de realização, quando o dispositivo cliente arranca e recebe um endereço IP (e.g., através de DHCP), a informação de endereçamento IP do dispositivo cliente 314 é incorporada no componente de servidor da política do servidor 310 e aplicada no dispositivo servidor 312. Da mesma forma, a informação de endereçamento IP do dispositivo servidor 312 é incorporada no componente de cliente da política do cliente 308 e aplicada no dispositivo cliente 314.

Em operação, um sistema de política associativa implementando um modelo tal como o mostrado na FIG.3, é descrito em seguida. Primeiro, as regras 302 são escritas e combinadas para formar um conjunto de regras (a ser incluído nos conjuntos de regras 304). Os conjuntos de regras 304 são combinados para formar um serviço (a ser incluído nos serviços 306). Numa forma de realização, o nome de um grupo privado virtual (VPG) é associado ao serviço. Os serviços 306 são combinados para formar uma política num servidor de políticas. Os endereços IP do dispositivo cliente 314 e do dispositivo servidor 312 são determinados. Numa forma de realização, os endereços IP são determinados no arranque utilizando DHCP. A informação de

endereçamento IP é enviada ao servidor de políticas. Numa forma de realização, os utilizadores são associados com o dispositivo servidor 312 e com o dispositivo cliente 314, e tanto a informação sobre os utilizadores como a informação sobre o endereçamento IP é enviada ao servidor de políticas. Numa forma de realização, a informação sobre os utilizadores é autenticada e/ou autorizada utilizando um sistema tal como o Microsoft Active Directory ou o Safeword Premier Access (SPA). Nesta forma de realização, a utilização de um tal sistema de autenticação/autorização permite que a política atribuída a um dispositivo seja derivada a partir das autorizações associadas com um utilizador.

O servidor de políticas utiliza de seguida a informação sobre endereçamento IP (e a informação sobre utilizadores, numa forma de realização) para construir a política do cliente 308 e a política do servidor 310. A política do cliente 308 inclui a informação de endereçamento IP sobre o dispositivo servidor 312, e a política do servidor 310 inclui a informação de endereçamento IP do dispositivo cliente 314. Numa forma de realização, a política do cliente 308 e a política do servidor 310 incluem tabelas VPG para os dispositivos respectivos. A política do cliente 308 é enviada ao dispositivo cliente 314, e a política do servidor 310 é enviada ao dispositivo servidor 312.

Numa forma de realização da invenção, um sistema

de política associativa mais generalizado implementando um modelo associativo opera da forma descrita de seguida. Primeiro, ocorre a especificação da política. Isto envolve a especificação de serviços e as funções na associação. Estas relações podem ser cliente, servidor, não hierárquica ou de apenas um elemento. Uma entidade não hierárquica é um dispositivo ou sistema que actua como par para outro sistema (versus um cliente ou um servidor). Aplica uma definição de serviço não hierárquica que inclui os endereços IP dos pares com que está autorizada a comunicar. Uma entidade de elemento único é uma entidade na qual a entidade remota não forma parte do sistema de aplicação da política. As entidades que não participam no processo de resolução de endereços são, numa forma de realização, lidadas sob a relação de elemento único.

De seguida, ocorre a associação de entidades. Isto associa uma entidade a um dispositivo. Numa forma de realização, a entidade é associada a um conjunto de dispositivos. Numa forma de realização, a entidade é adicionalmente associada a uma função (e.g. de um utilizador, etc.). A entidade é então associada a uma política que pode residir num servidor de políticas.

Após a associação de entidades, ocorrem a resolução e a distribuição da política. Esta fase resolve a especificação da política (e.g. associa um endereço IP com uma entidade) e converte a representação humana da política numa política aplicável numa máquina.

Por fim, ocorre a aplicação da política. Esta fase implementa efectivamente a política/regras para as entidades na relação.

Numa forma de realização, os processos acima são repetidos em uma ou mais iterações. Por exemplo, se um segundo cliente se junta à rede, a informação do segundo cliente (e.g. o endereço IP) é adicionada à política do servidor.

Noutra forma de realização da presente invenção, é providenciado um método para gerir uma política associativa num servidor de políticas. Nesta forma de realização, o método inclui fornecer uma política com uma definição de serviço (em que a definição de serviço tem um ou mais conjuntos de regras cada um contendo um ou mais termos), especificar uma função associada com cada conjunto de regras, acoplando operacionalmente um ou mais dispositivos ao servidor de políticas, e após cada acoplamento, converter a política numa ou mais políticas de dispositivos através da inserção de informação sobre os dispositivos nos termos para cada conjunto de regras, e distribuir as políticas dos dispositivos aos dispositivos correspondentes.

Em algumas formas de realização, fornecer uma política com uma definição de serviço inclui fornecer uma política de segurança com uma definição de serviço. Em

algumas formas de realização, fornecer uma política com uma definição de serviço inclui fornecer uma política com uma definição de serviço, em que a definição de serviço tem um ou mais conjuntos de regras, e em que cada conjunto de regras inclui uma ou mais regras de filtragem de pacotes. Em algumas formas de realização, fornecer uma política com uma definição de serviço inclui fornecer uma política com uma definição de serviço, em que a definição de serviço tem um ou mais conjuntos de regras que contêm um ou mais termos de produtor ou consumidor.

Em algumas formas de realização, especificar uma função associada com cada conjunto de regras inclui especificar uma função seleccionada a partir de um grupo consistindo de uma função de cliente, uma função de servidor, uma função não hierárquica, e uma função de elemento único.

Em algumas formas de realização, acoplar operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente um ou mais dispositivos que são membros de um VPG ou de uma VPN ao servidor de políticas. Em algumas formas de realização, acoplar operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente o primeiro e o segundo dispositivo ao servidor de políticas, em que o primeiro dispositivo é um membro de um primeiro VPG, e em que o segundo dispositivo é um membro de um segundo VPG. Em algumas formas de realização, acoplar

operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente um ou mais dispositivos com endereços do Protocolo Internet (IP) ao servidor de políticas, e em que os endereços IP do dispositivo são atribuídos de acordo com DHCP. Em algumas formas de realização, acoplar operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente um ou mais dispositivos sem fios ao servidor de políticas.

Noutra forma de realização da presente invenção, é providenciado um método implementado por computador num cliente. Nesta forma de realização, o método inclui obter informação de arranque para o cliente, obter informação de funções para um utilizador no cliente, enviar a informação de arranque e a informação de funções para um servidor de políticas, obter uma política de segurança específica de um cliente a partir do servidor de políticas, e aplicar a política de segurança específica do cliente no cliente, em que a política de segurança específica do cliente inclui informação de segurança sobre um servidor que está associado com o cliente, e em que a informação de segurança é baseada em informação de arranque e informação de funções para o servidor.

Em algumas formas de realização, obter informação de arranque para o cliente inclui obter um endereço do Protocolo Internet (IP) do cliente. Em algumas formas de realização, obter um endereço IP do cliente inclui obter um endereço IP do cliente que foi atribuído utilizando DHCP.

Em algumas formas de realização, o método compreende ainda a autenticação da informação de funções para o utilizador no cliente.

A FIG.4 ilustra um diagrama de blocos de uma definição de serviços com componentes de cliente e de servidor, de acordo com uma forma de realização da presente invenção. A FIG.4 mostra o serviço 400, a política do cliente 404, a política do servidor 402, o cliente 406, e o servidor 408. O serviço 400 é um serviço de sistema de nomes de domínio (DNS) (do inglês "DNS - Domain Name System") de uma companhia. Inclui um componente de cliente e um componente de servidor. O componente de cliente contém um conjunto de regras de cliente DNS e um conjunto de regras de servidor DNS. O conjunto de regras de cliente DNS inclui um campo de produtor (com um termo para valor de produtor). Este campo é resolvido pelo servidor 408. Numa forma de realização, o endereço IP do servidor 408 é inserido como um valor no campo de produtor quando o servidor 408 é inicializado. O conjunto de regras de servidor DNS inclui um campo de consumidor (com um termo para campo de consumidor). Este campo é resolvido pelo cliente 406. Numa forma de realização, o endereço IP do cliente 406 é inserido como um valor no campo de consumidor quando o cliente 406 é inicializado. O componente de cliente do serviço 400 é utilizado para criar a política do cliente 404, que é então associada ao cliente 406. Similarmente, o componente de servidor do serviço 400 é

utilizado para criar a política do servidor 402, que é então associada ao servidor 408.

A FIG.5A e a FIG.5B ilustram diagramas de blocos de várias definições de serviços com componentes de cliente e de servidor, de acordo com certas formas de realização da presente invenção. A FIG.5A mostra uma definição 500 do serviço Protocolo de Transferência de Hipertexto (HTTP) (do inglês “HTTP - Hypertext Transfer Protocol”). A definição 500 do serviço HTTP serve como um exemplo de um serviço que pode ser definido num servidor de políticas numa forma de realização da presente invenção. A definição 500 do serviço HTTP inclui um componente de cliente (cliente HTTP) e um componente de servidor (servidor HTTP). O componente de cliente inclui um termo para um campo de produtor que deve ser resolvido por um servidor, e o componente de servidor inclui um termo para um campo de consumidor que deve ser resolvido por um cliente. O componente de cliente pode então ser utilizado pelo servidor de políticas, numa forma de realização, para criar uma política específica do cliente que é associada ao cliente, e o componente de servidor pode ser utilizado para criar uma política específica do servidor que é associada ao servidor. A definição 500 do serviço HTTP esconde os detalhes da informação de produtor e consumidor que é resolvida mais tarde pelo servidor e pelo cliente, respectivamente, quando se criam as políticas individuais. Isto permite que as definições de serviços sejam mais genéricas e independentes das topologias.

A FIG.5B mostra uma definição 502 do serviço de correio electrónico. A definição 502 do serviço de correio electrónico serve como outro exemplo de um serviço que pode ser definido num servidor de políticas numa forma de realização da presente invenção. A definição 502 do serviço de correio electrónico inclui um componente de cliente e um componente de servidor. O componente de cliente inclui um componente de cliente de Protocolo de Transferência de Correio Electrónico (SMTP) (do inglês "SMTP - Simple Mail Transfer Protocol") e um componente de cliente de Protocolo de Correio 3 (POP3) (do inglês "POP - Post Office Protocol"). Os componentes de cliente de SMTP e POP3 incluem cada um deles um termo para um campo de produtor que deve ser resolvido por um servidor. O componente de servidor inclui um componente de servidor de SMTP e um componente de servidor de POP3. Os componentes de servidor de SMTP e de POP3 incluem cada um deles um termo para um campo de consumidor que deve ser resolvido por um cliente. Numa forma de realização, um cliente de SMTP (associado ao componente de cliente de SMTP na definição 502 do serviço de correio electrónico) e um cliente de POP3 (associado ao componente de cliente de POP3) são membros de um VPG. Nesta forma de realização, o servidor de políticas enviaria chaves de encriptação para o VPG para o cliente de SMTP e para o cliente de POP3 para segurança adicional na comunicação.

A tabela seguinte mostra um exemplo de um conjunto de regras de cliente de HTTP com uma regra de transmissão para cliente de HTTP (Tx) e uma regra de recepção para cliente de HTTP (Rx).

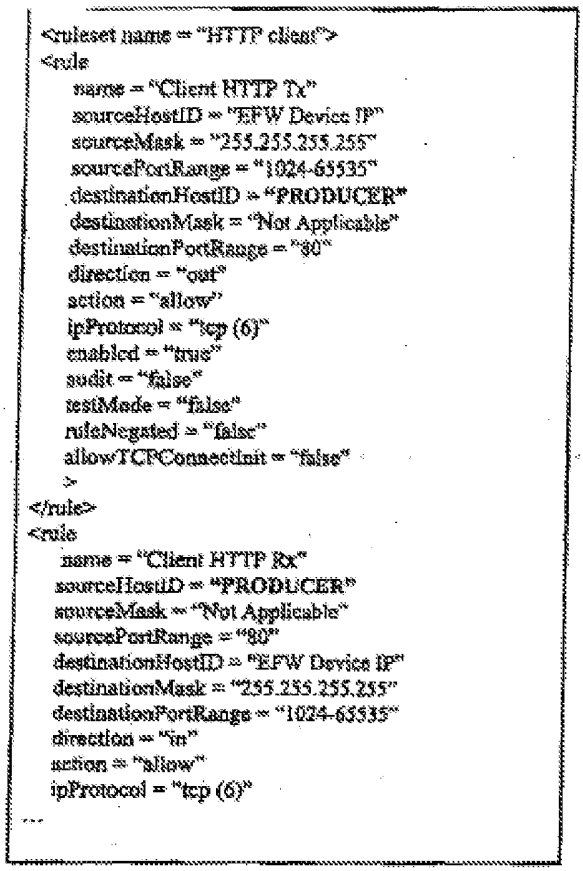


Tabela 1: Conjunto de Regras de Cliente de HTTP

Tal como pode ser visto na Tabela 1, a regra de transmissão para cliente de HTTP contém uma variável chamada "destinationHostID", e a regra de recepção para cliente de HTTP contém uma variável chamada "sourceHostID". Cada uma destas variáveis tem um valor de termo de "PRODUCER" ("PRODUTOR"). Este nome do termo é especificado

na altura da construção da política. Numa forma de realização, um servidor de políticas irá ser acoplado com uma entidade cliente e uma entidade servidor. Após o acoplamento, a entidade servidor irá enviar a sua informação de endereçamento IP ao servidor de políticas (numa forma de realização), e o servidor de políticas irá criar dinamicamente uma política específica do cliente, e inserir a informação de endereçamento IP do servidor no termo "PRODUCER" ("PRODUTOR") desta política. Então, o servidor de políticas irá enviar à entidade cliente uma cópia da política específica do cliente, que contém a informação de endereçamento IP específica do servidor.

Em varias formas de realização da invenção, vários conjuntos de regras diferentes (ou componentes de serviços) podem ser definidos para as definições de serviços nas políticas geridas por um servidor de políticas. A Tabela 1 mostra um exemplo de um conjunto de regras de cliente de HTTP. A Tabela 2 abaixo mostra exemplos disto e de muitos outros conjuntos de regras que podem ser definidos num serviço. A Tabela 2 é utilizada apenas para objectivos exemplificativos, e inclui uma lista não exclusiva de conjuntos de regras (ou componentes) que podem ser utilizados. Alguns dos conjuntos de regras listados podem requerer termos extra para além de "PRODUCER" ("PRODUTOR") e "CONSUMER" ("CONSUMIDOR").

HTTP client	Telnet client
HTTP server	Telnet server
HTTPS client	MSDS client
HTTPS server	MSDS server
Web proxy client	MSRPC client
Web proxy server	MSRPC server
IMAP client	DNS client
IMAP server	DNS server
Kerberos client	DHCP client
Kerberos server	DHCP server
NTP client	FTP client
NTP server	FTP server
POP3 client	NetBIOS client
POP3 server	NetBIOS server
SMTP client	X client
SMTP server	X server

Tabela 2: Conjuntos de Regras Exemplificativos

Noutras formas de realização, outros conjuntos de regras (para além dos conjuntos de cliente e servidor) estão incluídos nas definições de serviços.

A FIG.6 ilustra um diagrama de blocos da distribuição das especificações das políticas de um escritório corporativo para as filiais, de acordo com uma forma de realização da presente invenção. A FIG.6 mostra o escritório corporativo 600 e as filiais 602 e 604. No processo de distribuição das especificações das políticas,

várias políticas são escritas no escritório corporativo 600. No exemplo mostrado na FIG.6, foi escrita uma "POLÍTICA X" e uma "POLÍTICA Y". A "POLÍTICA X" inclui um serviço com um componente de cliente DNS (ou um conjunto de regras, numa forma de realização). A "POLÍTICA X" e a "POLÍTICA Y" são especificações de políticas genéricas, e não contêm nenhuns detalhes específicos de clientes ou de servidores que sejam dependentes da rede, ou topologia (tais como endereços IP, etc.). Estas políticas genéricas são então exportadas para as filiais 602 e 604. Nestas filiais, as políticas são atribuídas a vários conjuntos de dispositivos. Após a atribuição, os componentes de cliente e de servidor DNS são resolvidos por e associados aos dispositivos nos vários conjuntos de dispositivos. É apenas nessa altura que a informação dependente da rede, tal como os endereços IP dos dispositivos, é incluída nas políticas específicas utilizadas pelos dispositivos. O sistema de distribuição mostrado na FIG.6 permite que as políticas genéricas sejam criadas num escritório corporativo 600 e exportadas para as filiais 602 e 604. Desta forma, uma política de segurança consistente pode ser aplicada consistentemente em todas as filiais.

Certas formas de realização da presente invenção são ligadas a grupos privados virtuais (VPG's). Isto cria túneis criptograficamente protegidos entre dispositivos com base nas associações definidas por um administrador.

Em várias formas de realização, um sistema

implementando um modelo de política associativa reduz os erros e o esforço permitindo ao administrador identificar serviços (e.g. FTP) e de seguida construir políticas como colecções de serviços. Quando estes serviços são então associados a dispositivos, o servidor de políticas resolve os endereços IP automaticamente e providencia uma política actualizada aos dispositivos geridos. Existem muitos benefícios e vantagens numa tal aproximação quando comparada com outras aproximações tradicionais. Alguns destes benefícios e vantagens são descritas abaixo.

Servidor(es) Adicional(ais) Adicionado(s)

Os modelos de política de elemento único tradicionais requerem tipicamente que os administradores especifiquem explicitamente o nome DNS ou endereço IP dos servidores de modo a que as regras de filtragem possam ser instanciadas na *firewall* do cliente ou em dispositivos intermédios (tais como encaminhadores). Em tais modelos tradicionais, se uma organização adicionar mais um servidor (para balanceamento de carga, tolerância a faltas, etc.), o administrador deve actualizar as políticas existentes para adicionar o endereço IP ou nome DNS do servidor em todas as políticas cliente/encaminhador. Em algumas formas de realização da presente invenção utilizando uma política associativa, porém, o administrador simplesmente associa o novo servidor com o conjunto de dispositivos servidores e todas as políticas cliente são automaticamente actualizadas sem se modificar uma única política.

Reposicionamento do(s) Servidor(es) Existente(s)

Geralmente, os servidores são nós estacionários e estáveis. Contudo, ocasionalmente um servidor necessita de ser reposicionado devido a uma alteração na rede (e.g. adicionar um encaminhador) ou devido a uma alteração organizacional. Tipicamente, quando isto ocorre, as políticas de segurança devem ser actualizadas (num sistema tradicional) para permitir que todos os clientes acedam ao novo endereço IP. Todavia, em certas formas de realização da presente invenção, os mecanismos da política associativa aprendem o endereço IP de um servidor cada vez que ele arranca, e o endereço é escrito nas políticas dos clientes autorizados a aceder ao servidor.

Outra consideração é a utilização do DHCP. O DHCP é utilizador para atribuir endereços IP a estações de trabalho. Isto pode simplificar a administração de endereços IP para os administradores de redes, mas também cria problemas para as políticas de segurança baseadas em endereços IP. Por exemplo, assuma-se que um utilizador/estação de trabalho tem acesso autorizado a um servidor de bases de dados enquanto um segundo utilizador/estação de trabalho não tem. A política de segurança do servidor de bases de dados poderia incluir o endereço IP da estação de trabalho do utilizador autorizado. Porém, se o endereço do utilizador/estação de trabalho se alterar devido à utilização do DHCP, a política

da base de dados já não é válida. Devido à dificuldade de gerir políticas baseadas em endereços IP neste ambiente dinâmico, muitos administradores de segurança desistiram no passado e não tentam aplicar limites no endereçamento IP. Certas formas de realização da presente invenção, porém, utilizam um modelo de política associativa e mecanismos de suporte para endereçar este problema aprendendo o endereço IP do utilizador/estação de trabalho cada vez que arranca. Este endereço é então carregado na política da base de dados. Isto providencia um nível máximo de segurança sem o custo de manter manualmente os endereços.

Especificação de Política Independente da Rede

Frequentemente, uma organização possui peritos em *firewalls* e especificação de políticas num escritório corporativo enquanto muitos dos administradores em locais mais pequenos possuem menos formação e experiência. Existe a necessidade de um mecanismo que permita aos administradores centrais altamente especializados escrever políticas portáteis que possam ser importadas e utilizadas por administradores menos especializados. O esquema associativo de especificação de políticas de várias formas de realização da presente invenção permite que uma política seja escrita independentemente dos nomes das máquinas, endereços IP ou da topologia de rede remota. O administrador importando uma política associativa construída externamente apenas necessita de associar máquinas com as suas funções/conjuntos de dispositivos

(numa forma de realização). O administrador que importa não necessita de especificar protocolos, números de portos, endereços IP ou a informação sobre dispositivos intermédios tais como encaminhadores.

Filiação dinâmica para serviços não hierárquicos

Um administrador pode necessitar de definir um serviço de rede não hierárquico (e.g. Microsoft NetMeeting) cujos membros mudam frequentemente. A aproximação tradicional para construir uma política identifica explicitamente, para o propósito de especificar as comunicações permitidas, os membros actuais através dos seus endereços IP. As políticas resultantes são propensas a erros e onerosas de manter, porque os endereços IP mudam constantemente. O esquema associativo de especificação de políticas de várias formas de realização da presente invenção, porém, permite ao administrador adicionar e cancelar membros meramente adicionando ou removendo o serviço das políticas dos membros. As políticas não requerem endereços IP explícitos (no interface de gestão) para identificar clientes actuais do serviço. Assim a própria política não muda como a filiação.

Portos efémeros

Muitas aplicações (e.g. Microsoft NetMeeting) não utilizam um único porto universalmente conhecido. Em vez disso, escolhem portos aleatoriamente. Isto torna

extremamente difícil escrever filtros de pacotes eficazes. Uma aproximação tradicional a este problema tem sido a utilização de inspecção de pacotes com manutenção do estado. Todavia, isto apenas garante que uma sessão siga adequadamente a máquina de estados do protocolo. Não determina se a comunicação com o endereço remoto está de facto autorizada. A aproximação de política associativa de certas formas de realização da presente invenção permite que o dispositivo que aplica a política determine efectivamente se as comunicações com a entidade remota no intervalo de portos estão autorizadas. Quando a política associativa é combinada com tecnologia VPG ou VPN (em algumas formas de realização), também evita a manipulação do endereço remoto.

Embora formas de realização específicas tenham sido aqui ilustradas e descritas, deverá ser apreciado por aqueles com especialização normal na técnica que qualquer disposição que seja calculada para atingir o mesmo propósito pode ser substituída para a forma de realização específica mostrada. Esta aplicação está pensada para cobrir quaisquer adaptações ou variações das formas de realização descritas da presente invenção.

A presente invenção pode ser implementada através de software ou através de equipamento computacional programável. Isto inclui qualquer computador, incluindo PDA's (assistentes pessoais digitais), telefones móveis, etc. Deste modo a presente invenção abrange um suporte

portador transportando código legível por computador para configurar um computador ou um número de computadores como equipamentos da invenção. O suporte portador pode compreender um suporte transiente, e.g. um sinal eléctrico, óptico, microondas, RF, electromagnético, acústico ou magnético (e.g. um sinal TCP/IP sobre uma rede IP tal como a Internet), ou um suporte portador tal como uma disquete, CD-ROM, disco rígido, ou um dispositivo de memória programável.

Lisboa, 28 de Dezembro de 2006

REIVINDICAÇÕES

1. Um método para implementar uma política associativa, o método compreendendo:

fornecer uma política num servidor de políticas (106), a política tendo uma definição de serviço que contém primeiro e segundo componente relacional e em que cada componente relacional tem um ou mais conjuntos de regras (304) que contêm cada um deles um ou mais termos;

especificar uma função associada com cada conjunto de regras (304);

fornecer primeira e segunda entidade de rede (108A, 102A);

acoplar operacionalmente a primeira e a segunda entidade de rede (108A, 102A) ao servidor de políticas (106);

associar dinamicamente a primeira entidade de rede (108A) com a segunda entidade de rede (102A), em que tal associação inclui:

associar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede (108A), e

associar o segundo componente relacional da definição de serviço na política à segunda entidade de rede (102A); e

aplicar a política na primeira e segunda entidade de rede (108A, 102A).

2. O método da reivindicação 1, em que fornecer uma política num servidor de políticas (106) inclui fornecer uma política de segurança num servidor de políticas.

3. O método da reivindicação 1, em que a definição de serviço corresponde a um serviço de correio electrónico, um serviço de vendas, um serviço básico de entradas/saídas de rede, ou um serviço *web*.

4. O método da reivindicação 1, em que os conjuntos de regras incluem um ou mais conjuntos de regras de filtragem de pacotes.

5. O método da reivindicação 1, em que fornecer uma política com uma definição de serviço que contém primeiro e segundo componente relacional inclui fornecer uma política com uma definição de serviço que inclui um componente relacional de cliente e um componente relacional de servidor, e em que fornecer primeira e segunda entidade de rede inclui fornecer um dispositivo servidor (208) e um dispositivo cliente (202).

6. O método da reivindicação 1, em que fornecer primeira e segunda entidade de rede (108A, 102A) inclui fornecer primeira e segunda entidade de rede seleccionadas a partir de um grupo consistindo de dispositivos, utilizadores, e pacotes de software.

7. O método da reivindicação 1, em que fornecer primeira e segunda entidade de rede (108A, 102A) inclui fornecer primeiro e segundo membro de um grupo privado virtual ou de uma rede privada virtual.

8. O método da reivindicação 1, em que fornecer primeira e segunda entidade de rede (108A, 102A) inclui fornecer um primeiro membro de um primeiro grupo privado virtual e um segundo membro de um segundo grupo privado virtual.

9. O método da reivindicação 1, em que fornecer primeira e segunda entidade de rede (108A, 102A) inclui fornecer primeira e segunda entidade de rede que estão associadas com um ou mais conjuntos de dispositivos.

10. O método da reivindicação 1, em que fornecer primeira e segunda entidade de rede (108A, 102A) inclui fornecer primeira e segunda entidade de rede com endereços do Protocolo Internet que são atribuídos de acordo com o Protocolo de Configuração Dinâmica de Nós.

11. O método da reivindicação 1, em que fornecer

primeira e segunda entidade de rede (108A, 102A) inclui fornecer primeira e segunda entidade de rede em que cada uma delas inclui um dispositivo de interface de rede para gerir uma *firewall* embebida.

12. O método da reivindicação 1, em que acoplar operacionalmente a primeira e segunda entidade de rede (108A, 102A) ao servidor de políticas inclui enviar os endereços do Protocolo Internet da primeira e segunda entidade de rede ao servidor de políticas (106).

13. O método da reivindicação 1, em que acoplar operacionalmente a primeira e segunda entidade de rede (108A, 102A) ao servidor de políticas inclui:

associar um primeiro utilizador com a primeira entidade de rede (108A), o primeiro utilizador sendo associado com uma primeira função;

associar um segundo utilizador com a segunda entidade de rede (102A), o segundo utilizador sendo associado com uma segunda função;

identificar um primeiro endereço do Protocolo Internet da primeira entidade de rede (108A);

identificar um segundo endereço do Protocolo Internet da segunda entidade de rede (102A);

enviar a primeira função e a primeira informação de endereçamento do Protocolo Internet da segunda entidade de rede ao servidor de políticas (106); e

enviar a segunda função e a segunda informação de endereçamento do Protocolo Internet da segunda entidade de rede ao servidor de políticas;

14. O método da reivindicação 1, em que associar o primeiro componente relacional da definição de serviço na política à primeira entidade de rede (108A) inclui enviar o primeiro componente relacional da definição de serviço na política para a primeira entidade de rede.

15. O método da reivindicação 1, em que associar o segundo componente relacional da definição de serviço na política à segunda entidade de rede (102A) inclui enviar o segundo componente relacional da definição de serviço na política para a segunda entidade de rede.

16. O método da reivindicação 1, incluindo ainda a gestão de uma política associativa num servidor de políticas (106), a gestão compreendendo:

acoplar operacionalmente um ou mais dispositivos ao servidor de políticas; e após tal acoplamento,

converter a política numa ou mais políticas de dispositivos inserindo informação sobre dispositivos nos termos para cada conjunto de regras, e

distribuindo as políticas de dispositivos aos dispositivos correspondentes.

17. O método da reivindicação 16, em que a gestão inclui fornecer uma política de segurança com uma definição de serviço.

18. O método da reivindicação 16, em que a gestão inclui fornecer um ou mais conjuntos de regras em que cada um deles contém um ou mais termos de produtor ou de consumidor.

19. O método da reivindicação 16, em que a gestão inclui especificar uma função seleccionada a partir de um grupo consistindo de uma função cliente, uma função servidor, uma função não hierárquica, e uma função de elemento único.

20. O método da reivindicação 16, em que acoplar operacionalmente um ou mais dispositivos ao servidor de políticas (106) inclui acoplar operacionalmente um ou mais dispositivos que são membros de um grupo privado virtual ou de uma rede privada virtual ao servidor de políticas.

21. O método da reivindicação 16, em que acoplar operacionalmente um ou mais dispositivos ao servidor de políticas (106) inclui acoplar operacionalmente primeiro e segundo dispositivo ao servidor de políticas, em que o primeiro dispositivo é um membro de um primeiro grupo

privado virtual, e em que o segundo dispositivo é um membro de um segundo grupo privado virtual.

22. O método da reivindicação 16, em que acoplar operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente um ou mais dispositivos com endereços do Protocolo Internet ao servidor de políticas, e em que os endereços IP do dispositivo são atribuídos de acordo com o Protocolo de Configuração Dinâmica de Nós.

23. O método da reivindicação 16, em que acoplar operacionalmente um ou mais dispositivos ao servidor de políticas inclui acoplar operacionalmente um ou mais dispositivos sem fios ao servidor de políticas.

24. Um sistema, compreendendo:

uma rede (104);

uma primeira entidade de rede (108A) acoplada à rede;

uma segunda entidade de rede (102A) acoplada à rede; e

um servidor de políticas (106) acoplado à rede, o servidor de políticas (106) tendo uma política de segurança que inclui um primeiro conjunto de regras e um segundo

conjunto de regras, e cada um dos conjuntos de regras tendo um ou mais termos,

em que o servidor de políticas (106) é operável para:

converter a política de segurança numa política de primeira entidade de rede inserindo informação sobre a entidade para a segunda entidade de rede nos termos do primeiro conjunto de regras;

converter a política de segurança numa política de segunda entidade de rede inserindo informação sobre a entidade para a primeira entidade de rede nos termos do segundo conjunto de regras;

enviar a política de primeira entidade à primeira entidade de rede (108A); e

enviar a política de segunda entidade à segunda entidade de rede (102A).

25. O sistema da reivindicação 24, em que a primeira entidade de rede (108C) inclui um primeiro computador (118) e um primeiro dispositivo de interface de rede (120), e em que a segunda entidade de rede (102C) inclui um segundo computador (124) e um segundo dispositivo de interface de rede (122).

26. O sistema da reivindicação 25, em que o primeiro e o segundo dispositivo de interface de rede incluem cada um deles uma *firewall* embebida para autorizar pacotes de dados.

27. O sistema da reivindicação 24, em que a primeira entidade de rede (108B) inclui um primeiro computador (110) com um primeiro componente de software (112), e em que a segunda entidade de rede (102B) inclui um segundo computador (114) com um segundo componente de software (116).

28. O sistema da reivindicação 24, em que o servidor de políticas compreende ainda:

uma política de segurança principal (212) com um componente de cliente e um componente de servidor; e

um interface (210) para acoplar o servidor de políticas com um dispositivo servidor (208) e um dispositivo cliente (202).

29. O sistema da reivindicação 28, em que o servidor de políticas é ainda operável para:

obter informação do servidor sobre o dispositivo servidor (208);

obter informação do cliente sobre o dispositivo cliente (202);

criar uma política do cliente utilizando o componente de cliente da política de segurança principal e a informação do servidor;

criar uma política do servidor utilizando o componente de servidor da política de segurança principal e a informação do cliente;

enviar a política do cliente ao dispositivo cliente (202); e

enviar a política do servidor ao dispositivo servidor (208).

Lisboa, 28 de Dezembro de 2006

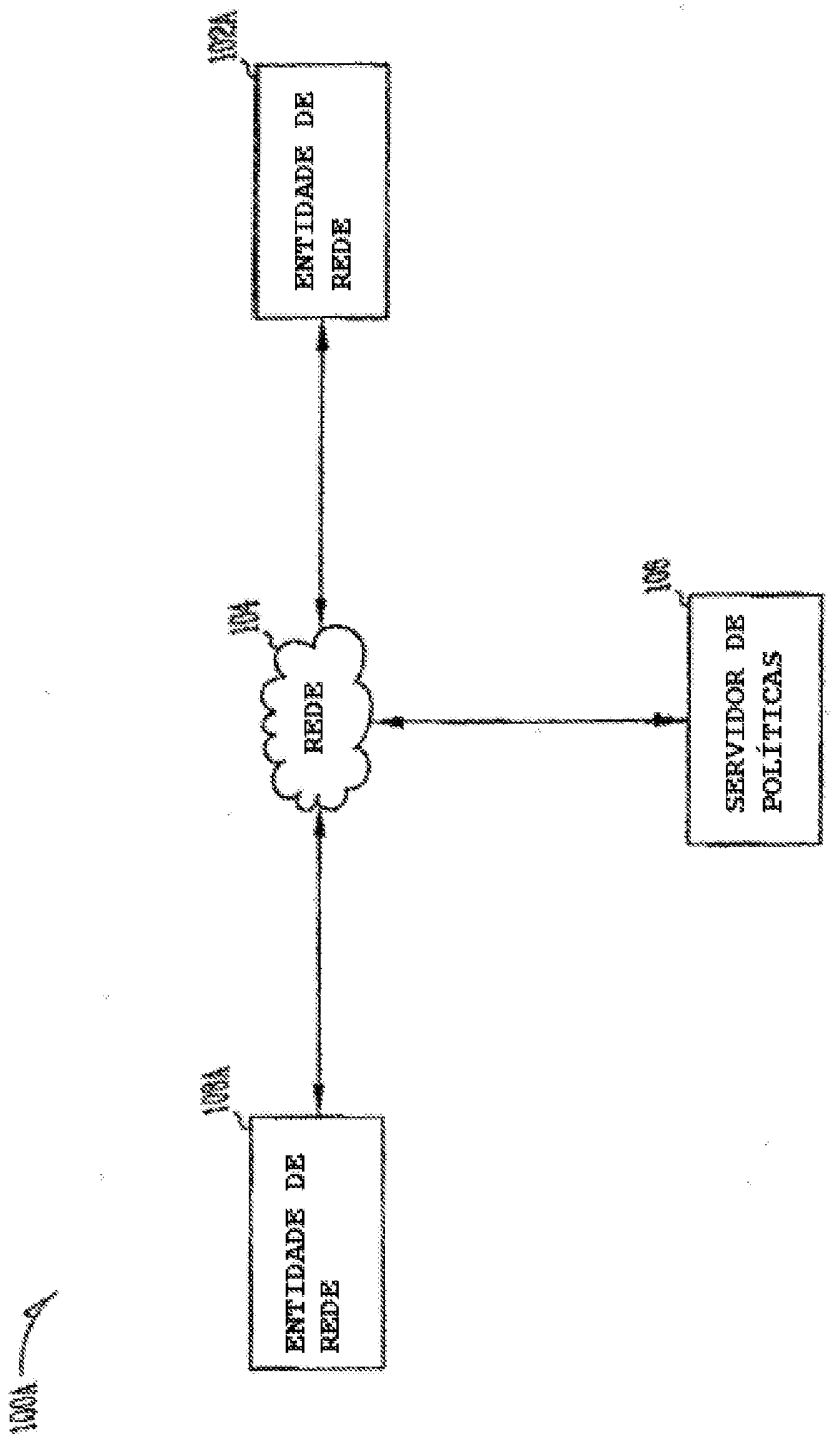

100A
102A
ENTIDADE DE REDE
104
REDE
106
SERVIDOR DE POLÍTICAS
108A
ENTIDADE DE REDE

Fig.1A

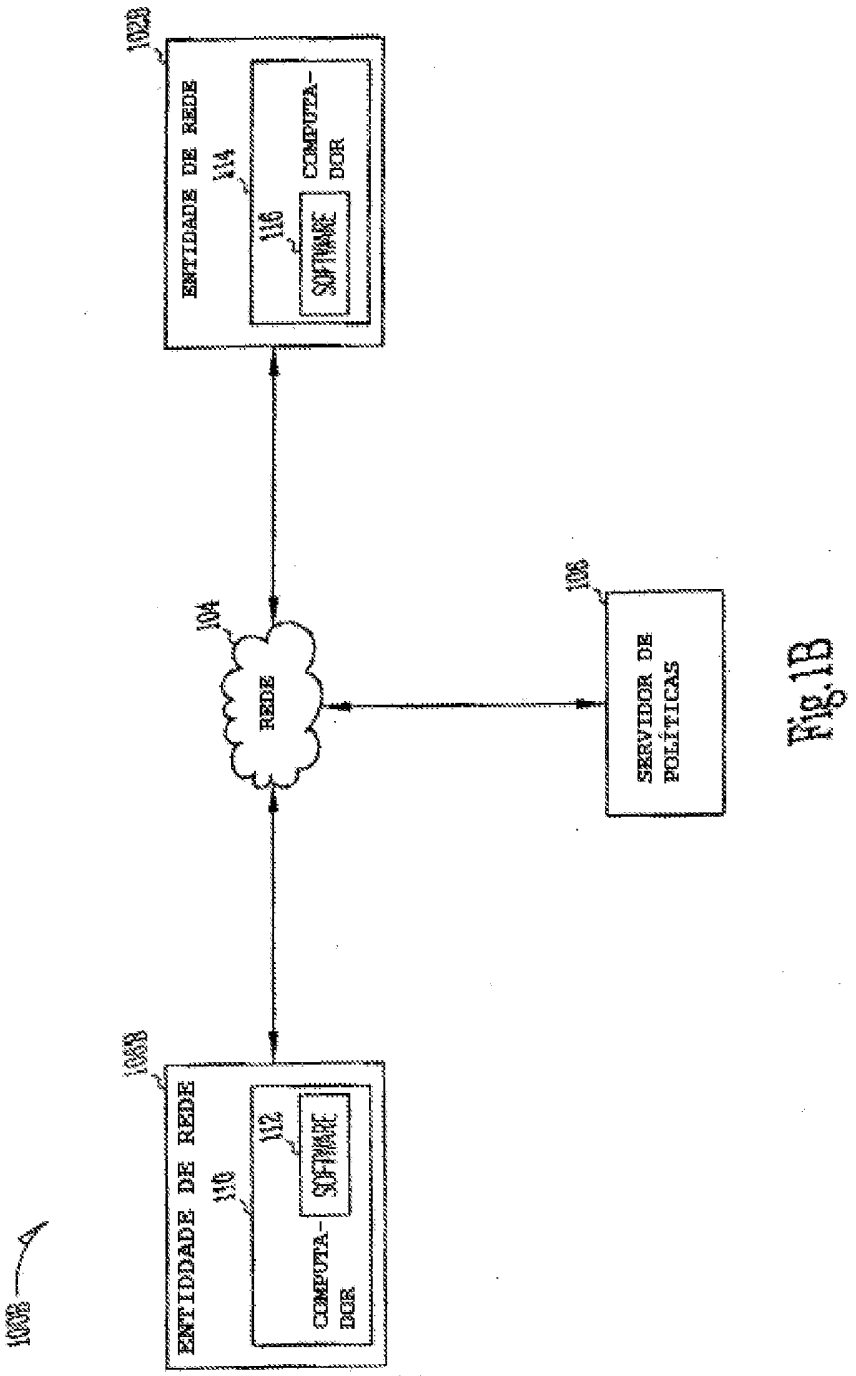

100A
ENTIDADE DE REDE
110
COMPUTA-DOR
112
SOFTWARE
100B
ENTIDADE DE REDE
114
COMPUTA-DOR
116
SOFTWARE
100C
REDE
104
SERVIDOR DE POLÍTICAS
106

Fig.1B

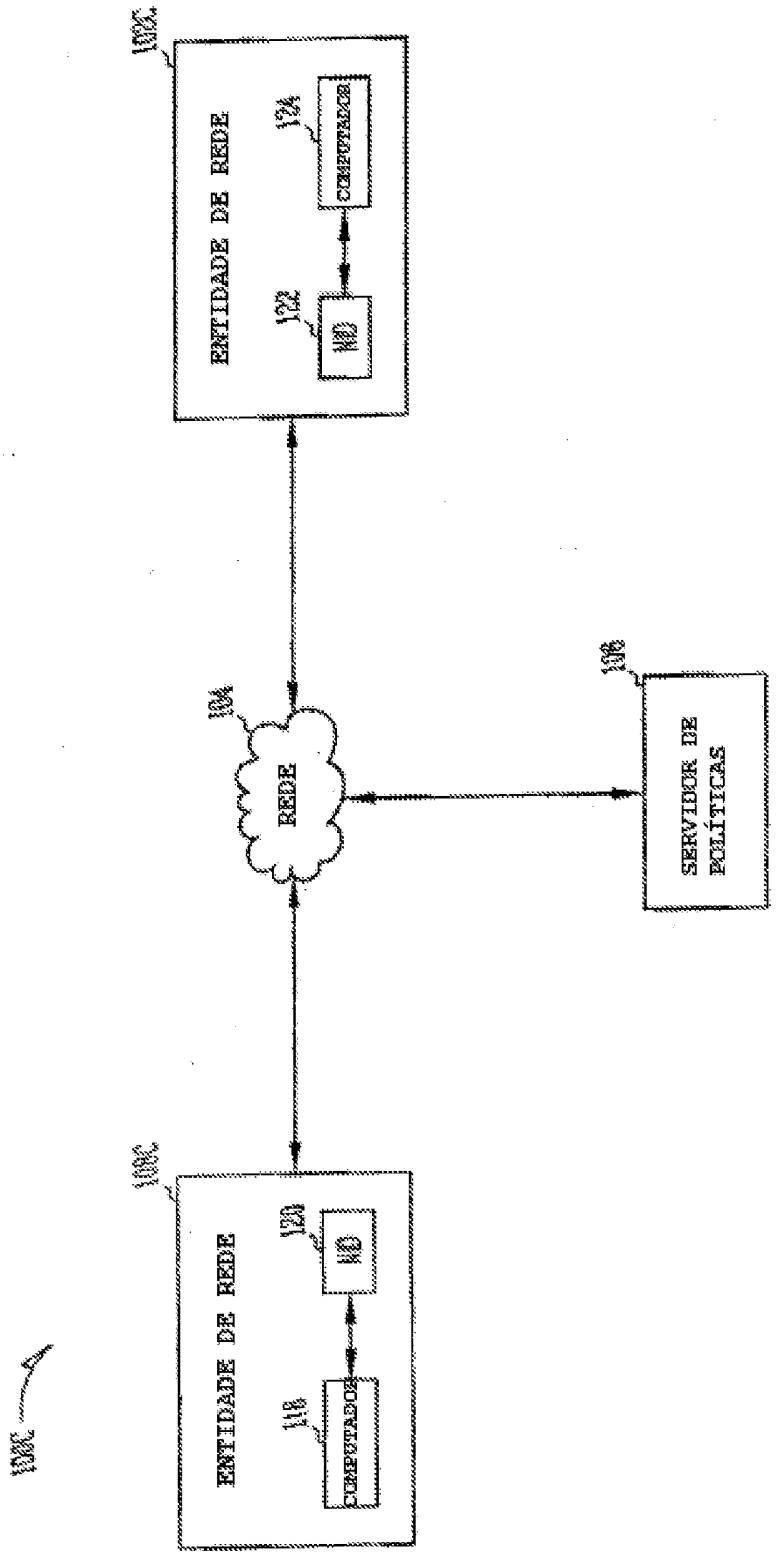

100C
ENTIDADE DE REDE
118
COMPUTADOR
120
ND
108C
REDE
104
SERVIDOR DE POLÍTICAS
106
ENTIDADE DE REDE
122
ND
124
COMPUTADOR
102C
ND=DISPOSITIVO DE INTERFACE DE REDE

Fig.1C

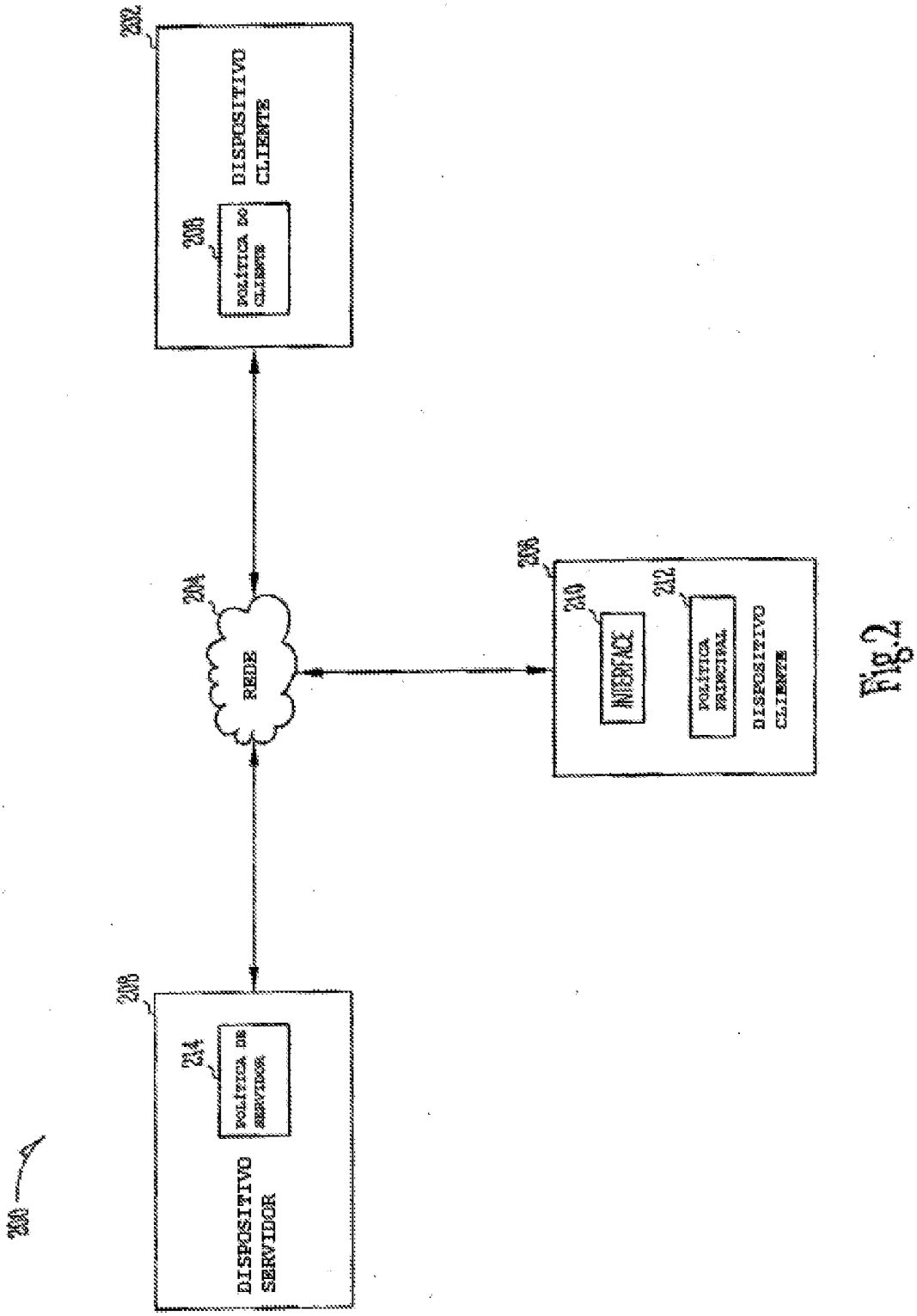

200
202
DISPOSITIVO CLIENTE
208
POLÍTICA DE CLIENTE
204
REDE
206
210
INTERFACE
212
POLÍTICA PRINCIPAL
DISPOSITIVO CLIENTE
216
DISPOSITIVO SERVIDOR
214
POLÍTICA DE SERVIDOR

Fig.2

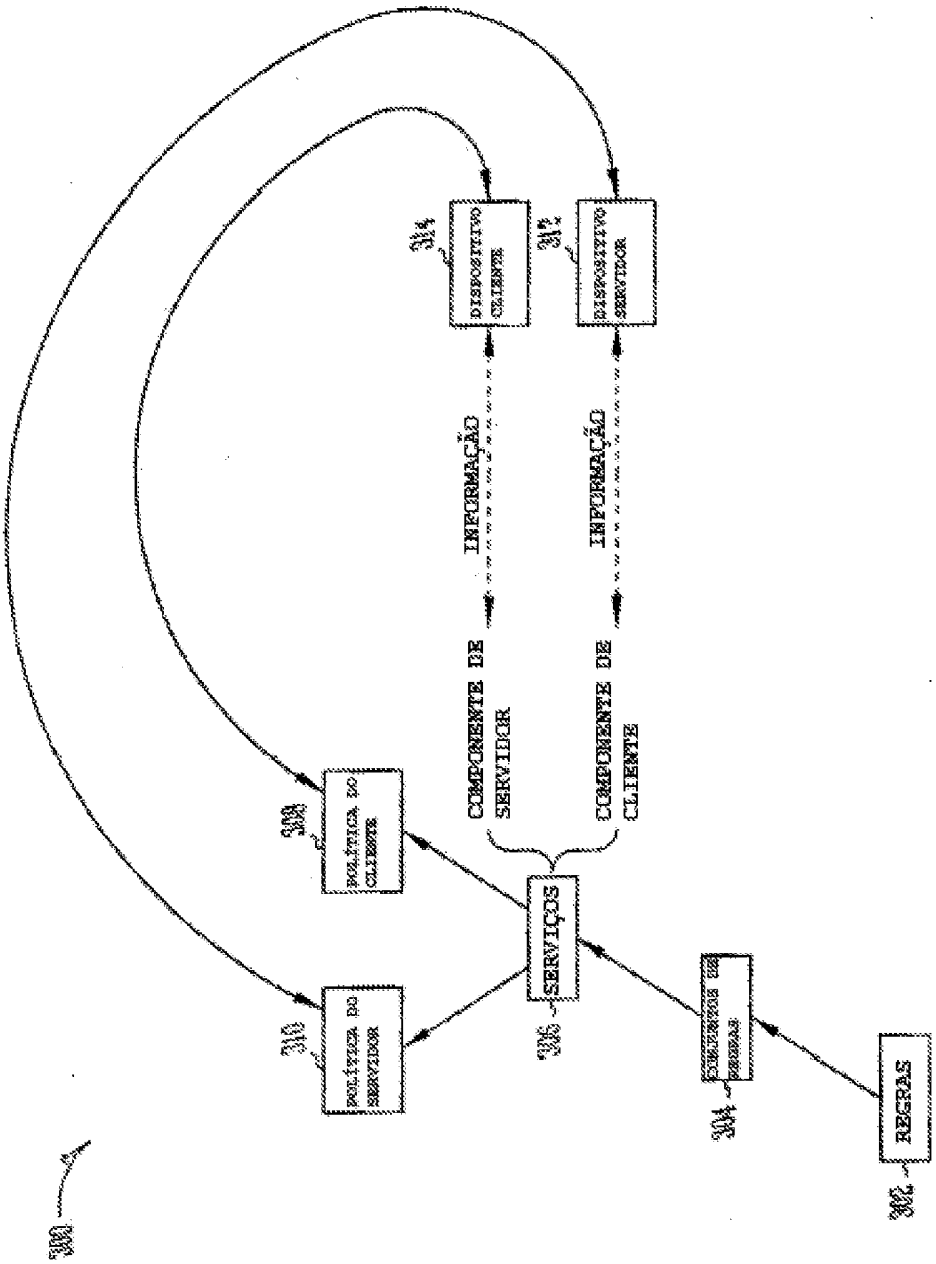

300
302
304
306
308
310
312
314
REGRAS
SERVIÇOS
POLÍTICA DO CLIENTE
POLÍTICA DO SERVIDOR
COMPONENTE DE SERVIDOR
COMPONENTE DE CLIENTE
INFORMAÇÃO
INFORMAÇÃO
DISPOSITIVO CLIENTE
DISPOSITIVO SERVIDOR

Fig.3

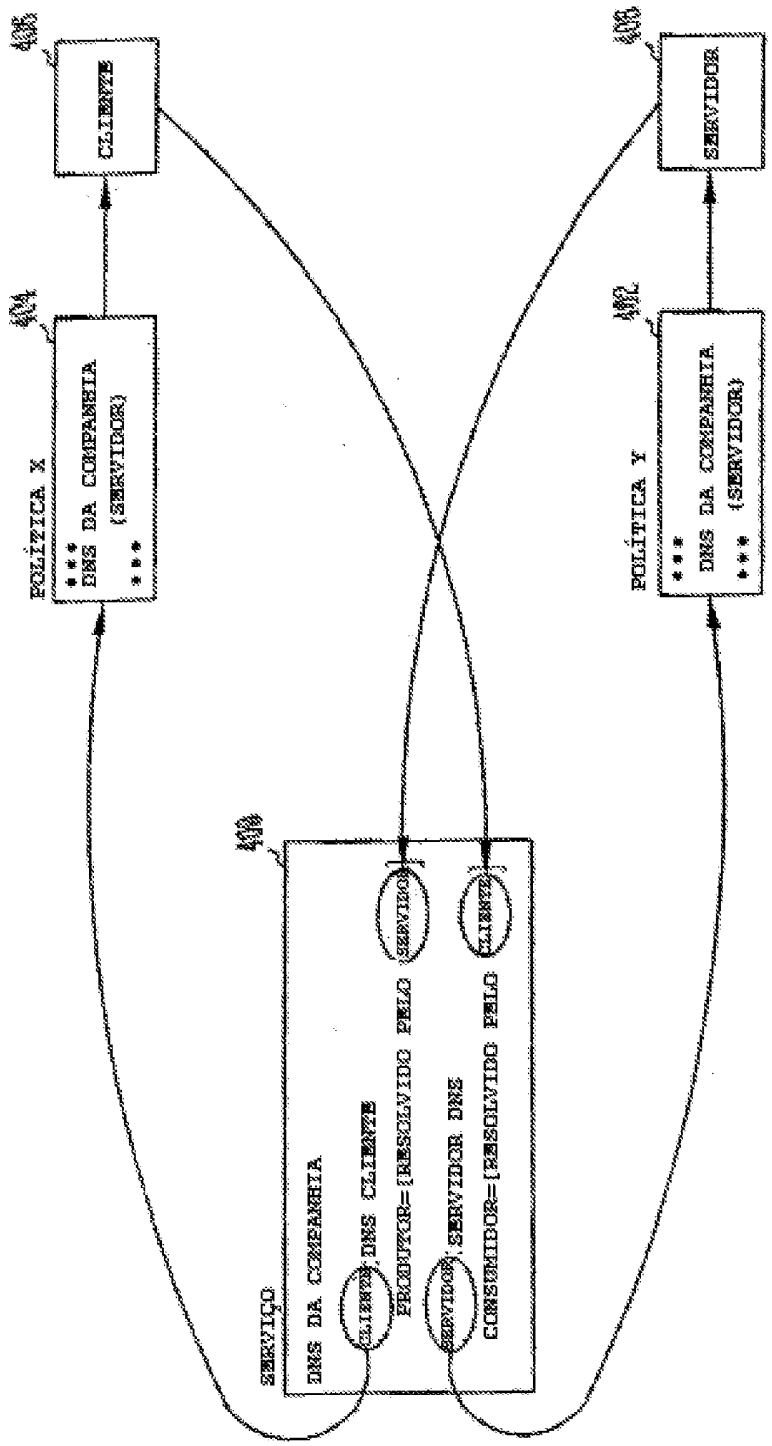

406
CLIENTE
404
POLÍTICA X
DNS DA COMPANHIA
(SERVIDOR)
406
SERVIDOR
402
POLÍTICA Y
DNS DA COMPANHIA
(SERVIDOR)
408
SERVIÇO
DNS DA COMPANHIA
DNS CLIENTE
SERVIDOR DNS
SERVIDOR
CLIENTE

Fig. 4

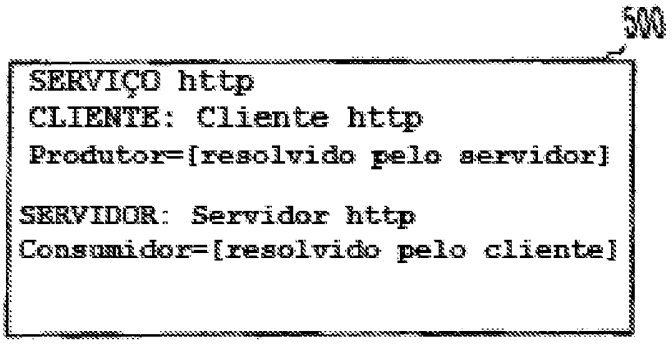

500
SERVIÇO http
CLIENTE: Cliente http
Produtor=[resolvido pelo servidor]
SERVIDOR: Servidor http
Consumidor=[resolvido pelo cliente]

Fig.5A

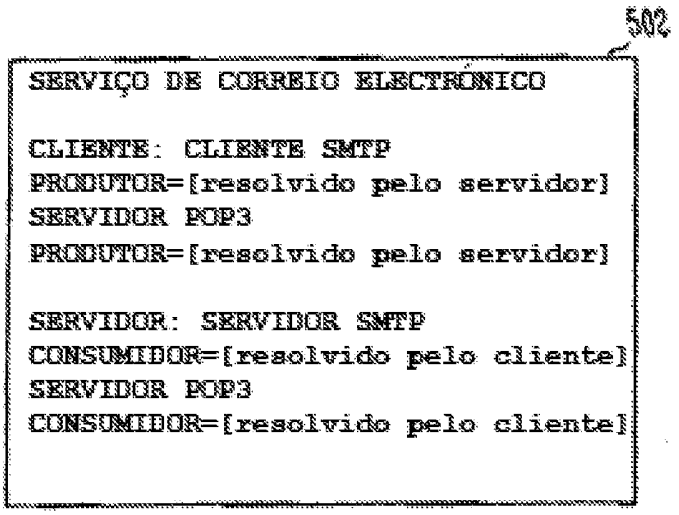

502
SERVIÇO DE CORREIO ELECTRÓNICO
CLIENTE: CLIENTE SMTP
PRODUTOR=[resolvido pelo servidor]
SERVIDOR POP3
PRODUTOR=[resolvido pelo servidor]
SERVIDOR: SERVIDOR SMTP
CONSUMIDOR=[resolvido pelo cliente]
SERVIDOR POP3
CONSUMIDOR=[resolvido pelo cliente]

Fig.5B

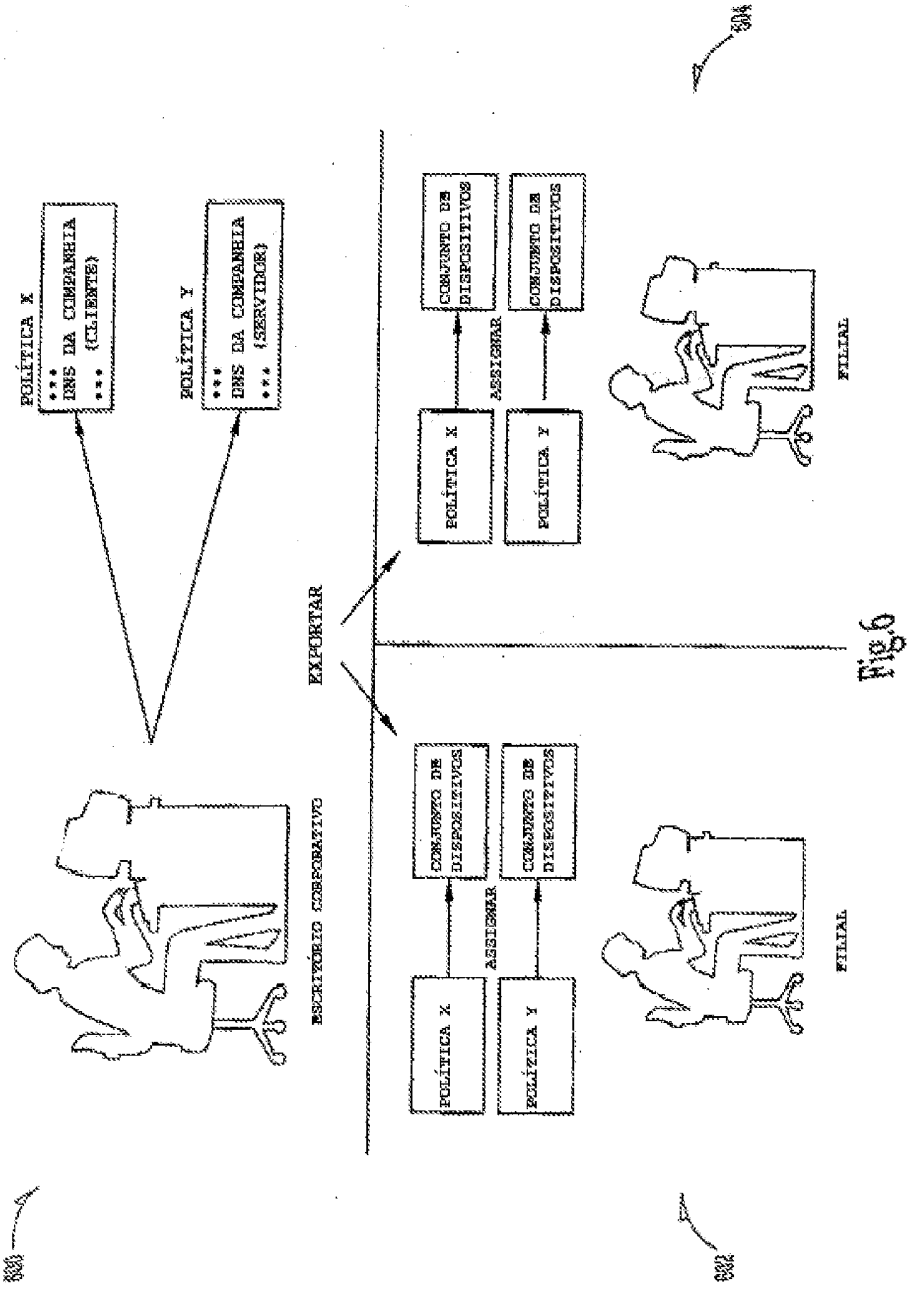

POLÍTICA X
*** DNS DA COMPANHIA
*** (CLIENTE)
POLÍTICA Y
*** DNS DA COMPANHIA
*** (SERVIDOR)
EXPORTAR
ESCRITÓRIO CORPORATIVO
FILIAL
FILIAL
POLÍTICA X
POLÍTICA Y
ASSINAR
CONJUNTO DE DISPOSITIVOS
CONJUNTO DE DISPOSITIVOS
POLÍTICA X
POLÍTICA Y
ASSINAR
CONJUNTO DE DISPOSITIVOS
CONJUNTO DE DISPOSITIVOS
602
604
606

Fig.6