



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

(21) **PI0707867-6 A2**

(22) Data de Depósito: 16/02/2007
(43) Data da Publicação: 10/05/2011
(RPI 2105)



(51) *Int.Cl.:*
G06F 17/30

(54) Título: **MÉTODO PARA DETERMINAR UM FLUXO DE DADOS, PROCESSADOR, E, MEIO LEGÍVEL POR COMPUTADOR**

(30) Prioridade Unionista: 01/11/2006 US 11/591802,
16/02/2006 US 60/773820

(73) Titular(es): Techguard Security Llc

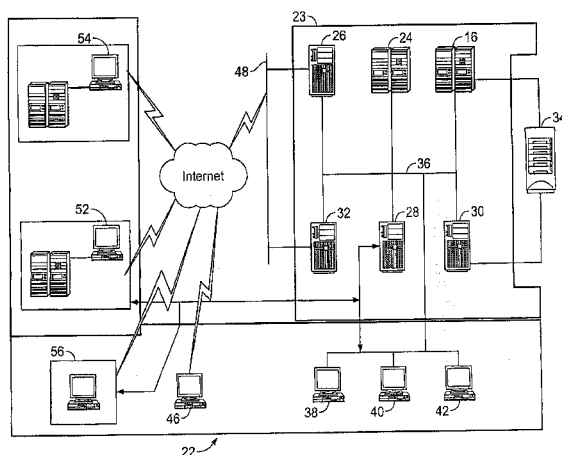
(72) Inventor(es): Brian Louis Cooper, David Edward Maestas

(74) Procurador(es): MOMSEN LEONARDOS & CIA

(86) Pedido Internacional: PCT US2007062313 de 16/02/2007

(87) Publicação Internacional: WO 2007/098405 de 30/08/2007

(57) Resumo: METODO PARA DETERMINAR UM FLUXO DE DADOS, PROCESSADOR, E, MEIO LEGÍVEL POR COMPUTADOR. Um método para determinar um fluxo de dados é descrito. O método inclui determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto e determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação. O método ainda inclui analisar, através de um processador, pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.



“MÉTODO PARA DETERMINAR UM FLUXO DE DADOS,
PROCESSADOR, E, MEIO LEGÍVEL POR COMPUTADOR”
FUNDAMENTOS DA INVENÇÃO

5 Esta invenção se relaciona de forma geral, à redes de
computador e mais particularmente à sistemas e métodos para determinar um
fluxo de dados.

Regras convencionais baseadas em barreiras de proteção de
segurança de computador são baseadas na variação dos conjuntos de regras
complexos, ou “ coleções de regra ”. Pacotes de dados que entram em tal uma
10 barreira de proteção são comparados com informação dentro, e regras de, uma
ou mais coleções de regra para determinar se aos pacotes de dados deve ser
permitido passar através da barreira de proteção. Coleção de regra são
estruturadas em torno de conceitos de comparações lógicas, tal como lógica
Boolean, e fluxo de regra seqüencial através de uma lista of regras. Conforme
15 coleções de regra se tornam mais complexas, elas requerem mais excesso de
sistema e processador. Conseqüentemente, organizações que usam barreiras
de proteção freqüentemente comprometem entre a complexidade da coleção
de regra e o desempenho de transmissão de dados requeridos percebido,
sacrificando alguma quantidade de segurança em favor de desempenho.

20 BREVE DESCRIÇÃO DA INVENÇÃO

Em um aspecto, um método para determinar um fluxo de
dados é descrito. O método inclui determinar se a um pacote incluindo um
primeiro número de pelo menos um bit dentro de um primeiro conjunto é
designado um valor de classificação com base no pelo menos um bit dentro
25 do primeiro conjunto, e determinar um resultado a ser aplicado ao pacote ao
determinar que ao pacote é designado ao valor de classificação. O método
ainda inclui analisar, através de um processador, pelo menos um bit de um
segundo número dentro de um segundo conjunto do pacote ao determinar que
ao pacote não pode ser designado ao valor de classificação com base no

primeiro número de pelo menos um bit do pacote.

Em um outro aspecto, um processador é descrito. O processador é configurado para determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto e determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação. O processador é ainda configurado para analisar pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.

Em ainda um outro aspecto, um meio legível por computador é descrito. O meio legível por computador é codificado dentro de um programa de computador configurado para determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto, determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação, e analisar pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.

Em ainda um aspecto, um método para determinar um fluxo de dados é descrito. O método inclui gerar uma interface de usuário gráfica incluindo um mapa, receber uma seleção de um ponto no mapa, exibir uma pluralidade de resultados ao receber a seleção do ponto, receber uma seleção de um dos resultados, e designar o um dos resultados do ponto.

BREVE DESCRIÇÃO DOS DESENHOS

Figura 1 é um diagrama de bloco de uma modalidade de um sistema para determinar um fluxo de dados.

Figura 2 é um diagrama detalhado de bloco de uma modalidade de um sistema para determinar um fluxo de dados.

Figura 3 é um diagrama de bloco de uma outra modalidade de um sistema para determinar um fluxo de dados.

5 Figura 4 é um diagrama de uma modalidade de um pacote de dados recebido através de um processador do sistema da Figura 3.

Figura 5 é a fluxograma de uma modalidade de um método para determinar um fluxo de dados.

Figura 6 é uma modalidade de uma interface de usuário gráfica (GUI) usada para criar uma pluralidade de tabelas.

10 DESCRIÇÃO DETEALHADA DA INVENÇÃO

Figura 1 é um diagrama de bloco de uma modalidade de um sistema 10 para determinar um fluxo de dados. Sistema 10 inclui um sistema de servidor 12 e uma pluralidade de dispositivos de usuário 14 conectado ao sistema de servidor 12. Conforme usado aqui, o termo servidor não é limitado para apenas aqueles circuitos integrados referido na técnica como um computador, mas de modo amplo se refere a um processador, a micro-controlador, a microcomputador, um controlador de lógica programável, um circuito integrado específico de aplicativo, qualquer outro circuito programável, e qualquer combinação de hardware e software, e esses termos são aqui usados de modo indiferente. Em uma modalidade, dispositivos de usuário 14 são computadores incluindo um navegador de web, e o sistema de servidor 12 é acessível para os dispositivos de usuário 14 através de uma rede, tal como, uma rede de área local (LAN) e uma rede de área ampla (WAN). A LAN pode incluir uma Intranet e a WAN pode incluir a Internet.

25 Dispositivos de usuário 14 são interconectados à rede através de muitas interfaces incluindo conexões de discagem, modem de cabo coaxial e linhas de rede de serviços digitais integrados de alta velocidade (ISDN). De forma alternativa, dispositivos de usuário 14 inclui um telefone baseado em

web ou outro equipamento possível de conectar baseado em web, que são capazes de se interconectar com a rede. O sistema de servidor 12 inclui um servidor de banco de dados 16 conectado a um banco de dados centralizado 18 que inclui um método para determinar um fluxo de dados.

5 Em uma modalidade, o banco de dados centralizado 18 é armazenada no banco de dados do servidor 16 e pode ser acessado por usuários em potencial em um dos dispositivos de usuário 14 se registrando no sistema de servidor 12 através de um dos dispositivos de usuário 14. Em uma modalidade, o banco de dados centralizado 18 é armazenado remotamente do
10 sistema de servidor 12.

 Figura 2 é um diagrama detalhado em bloco de uma modalidade de um sistema 22 para determinar um fluxo de dados. Sistema 22 inclui um sistema de servidor 23. O sistema de servidor 23 é um exemplo de sistema de servidor 12. O sistema de servidor 23 inclui um servidor de banco
15 de dados 16, um servidor de aplicativo 24, um servidor de web, um servidor de fax 28, um servidor de diretório 30, e um servidor de correio eletrônico 32. Uma unidade de armazenamento em disco 34, que é um único banco de dados, é acoplada ao servidor de banco de dados e ao servidor de diretório 30.

 Servidores 16, 24, 26, 28, 30, e 32 são acoplados em uma rede
20 de área local 36. De modo alternativo, a WAN poderia ser usada no lugar de LAN 36. Em adição, uma estação de trabalho do administrador do sistema 38, uma estação de trabalho de usuário 40, e uma estação de trabalho de supervisão 42 são acoplados à LAN 36. Cada estação de trabalho, 38, 40, e 42 é um computador pessoal tendo um navegador de web.

25 O sistema de servidor 23 é, de modo comunicativo, acoplado à várias estações de trabalho 52 e 54, que são operadas por individuais ou por empregados. Uma pessoa ou usuário operando estação de trabalho 52 pode ter acesso ao sistema de servidor 23. Estações de trabalho 52 e 54 são computadores pessoais tendo um navegador de web. Estação de trabalho 54

está localizada em uma localização remota. Sistema de servidor 23 é também de modo comunicativo, acoplado a uma estação de trabalho 46 através uma conexão ao provedor de serviço de Internet (ISP) 48.

5 Ainda mais, o servidor de fax 28 se comunica com estação de trabalho 52 e qualquer sistema de usuário localizado remotamente, incluindo uma estação de trabalho 56 através de um elo de comunicação de telefone. Cada estação de trabalho 38, 40, 42, 46, 52, 54, e 56 é um exemplo de dispositivo de usuário¹⁴. Da mesma forma o servidor de fax 28 se comunica com outras estações de trabalho 38, 40, e 42. O sistema de servidor 23
10 executa métodos, descritos aqui, para determinar um fluxo de dados.

A comunicação na modalidade exemplar é ilustrada como sendo efetuado através da Internet, Contudo, qualquer outra comunicação do tipo de rede de área ampla (WAN) pode ser utilizada em outras modalidades. Sistemas e métodos para determinar um fluxo de dados não são limitados de
15 serem praticados através da Internet. Em uma modalidade, métodos para determinar um fluxo de dados são armazenados em unidades de armazenamento em disco 34, que é um exemplo de um meio legível por computador, e são executados através de qualquer dos servidores 16, 24, 26, 28, 30, e 32. Outros exemplos de um meio legível por computador incluem,
20 um disco flexível, uma memória de somente leitura de disco compacto (CD-ROM), e um disco de vídeo digital (DVD).

Figura 3 é um diagrama de bloco de uma modalidade de um sistema 100 para determinar um fluxo de dados. Sistema 100 inclui um processador 102, um dispositivo de memória 104, um dispositivo de entrada
25 106, e um dispositivo de saída 108. O processador 102 pode ser ou uma arquitetura de x86 operando um sistema de operação Linux™ ou uma arquitetura de x86_64 operando sistema de operação Linux™. A arquitetura de x86 é disponível da corporação Intel™ e a arquitetura de x86_64 é disponível da corporação Advanced Micro Dispositivos™ (AMD). Exemplos

de dispositivo de memória 104 incluem uma memória de acesso aleatório (RAM) e uma memória de somente leitura (ROM). Exemplos de dispositivo de entrada 106 incluem um mouse e um teclado. Exemplos de dispositivo de saída 108 incluem um tubo de raio catódico (CRT) e um mostrador de tela de cristal líquido (LCD). Conforme usado aqui, o termo processador não é limitado para apenas aqueles circuitos integrados referidos na técnica como um processador, mas de modo amplo se refere a um computador, a micro-controlador, a microcomputador, um controlador de lógica programável, um circuito integrado específico de aplicativo, e qualquer outro circuito programável.

O processador 102 executa os métodos para determinar um fluxo de dados. Em uma modalidade, o processador 102 é uma barreira de proteção que evita a comunicação de pacotes de dados entre duas redes, tal como Internet e uma Intranet, com base em uma política de segurança.

Figura 4 é um diagrama de uma modalidade de um pacote 150 de dados recebido pelo processador 102. O pacote 150 inclui uma versão 152, um endereço de rede de protocolo de Internet (IP), e dados 156. Exemplos de versão 152 incluem uma versão de IPv4 e uma versão de IPv6 de endereços de rede de IP rede. Exemplos do endereço de rede de IP 150 incluem ou um endereço de origem ou um endereço de destinação. O endereço de origem é um endereço de uma origem do emissor/remetente, tal como estação de trabalho 52, de pacote 150. O endereço de destinação inclui um endereço de um receptor ou um destino, tal como estação de trabalho 38 ou 40, de pacote 150. Em uma modalidade, pacote 150 também inclui um comprimento de cabeçalho de um cabeçalho de pacote 150, um tipo de serviço a ser fornecido para o pacote 150, um comprimento total de pacote 150, uma verificação de cabeçalho que é usada pelo o processador 102 para determinar se todos os bits do cabeçalho são válidos, um tempo de vida de pacote 150, uma pluralidade de sinalizações usada para determinar se

fragmenta o pacote 150, e um desvio de fragmentação é usado pelo o processador 102 para determinar se o pacote 150 é uma porção de datagrama de IP. Na modalidade, se o endereço de rede de IP do pacote 150 é o endereço de origem, pacote 150 ainda inclui o endereço de destinação e se IP rede endereço e rede de IP do pacote 150 é o endereço de destinação endereço, o pacote 150 inclui o endereço de origem.

Figura 5 é a fluxograma de uma modalidade de um método 200 para determinar um fluxo de dados. O processador 102 recebe 202 o pacote 150 e obtém 204 ou extrai N bits do pacote 150. O exemplo de N inclui 3, 4, 6, 8, ou 10. Um outro exemplo de N bits inclui menos do que 32 bits do Endereço de rede de IP do pacote 150. Ainda outro exemplo de N inclui menos do que 128 bits do endereço de rede de IP do pacote 150. Ainda outro exemplo de N bits inclui 2 bits de outros do que os 3bits mais significativos (MSBs) e 3 bits menos significativos (LSBs) de 8 MSBs do endereço de rede de IP do pacote 150. Outro exemplo de N inclui 2 LSBs de 8 MSBs do endereço de rede de IP do pacote 150. O processador 102 determina que o endereço de rede de IP do pacote 150 está localizado após um bit α e antes de um bit β do pacote 150 com base na versão 152 do pacote 150, e extrai N bits entre to bit α e o bit β do endereço de rede de IP do pacote 150. Como um outro exemplo, o processador 102 determina que os dados 156 estão localizados após um bit γ e antes de um bit η do pacote 150 com base na versão 152 do pacote 150 e extrai N bits dos dados 156 entre os bits γ e η . Como ainda um outro exemplo, o processador 102 determina que um endereço de porta está localizado após um bit σ e antes de um bit ω do pacote 150 com base na versão 152 do pacote 150 e extrai N bits entre os bits σ e ω bits do endereço de porta. Um exemplo do endereço de porta inclui um endereço de origem de porta, tal como um número de porta de um protocolo de controle de transmissão (TCP) ou de um protocolo de datagrama de usuário (UDP), de um aplicativo de computador de origem executado pela

origem, e o endereço de destinação de porta, tal como um número de porta de um TCP ou de um UDP, de um aplicativo de computador de destino executado pela destinação. Com um outro exemplo, o processador 102 extrai alguns de N bits do endereço de rede de IP do pacote 150 e o remanescente dos N bits do endereço de porta.

O processador 102 determina 206 se o pacote 150 pode ser classificado com base nos N bits do pacote 150. O processador 102 determina 206 se o pacote 150 pode ser classificado comparando N bits com uma tabela 1 fornecida, através do dispositivo de entrada 106, pelo usuário com o dispositivo de memória 104.

Número da linha	Intervalos Secundários	Valores de classificação	Resultados
1	R1 – R2	C1	S1
2	R3 – R4	C2	S2
3	R5 – R6		
4	R7 – R8		
5	R9 – R10		
6	R11 – R12		

Tabela I

Os intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11 - R12 dentro da tabela I formam um conjunto finito, tal como um conjunto de M bits do endereço de portas, um conjunto de M bits de dados de autorização, tal como nomes e senhas de usuário, um conjunto de M bits de endereços de rede de IP, e um conjunto de M bits de uma combinação de endereços de rede de IP e de endereço de portas. Exemplos dos valores de classificação C1 e C2 incluem um conjunto de códigos de país identificando uma pluralidade de países, um conjunto de códigos de região secundária identificando uma pluralidade de regiões secundárias, um conjunto de códigos de hacker de computador identificando uma pluralidade de hackers de computador, um conjunto de códigos de emissor de spam identificando uma pluralidade de emissores de spam de computador, um conjunto de códigos de vírus identificando uma pluralidade de vírus de computador, um conjunto de

códigos de Trojan identificando uma pluralidade de Trojans, um conjunto de códigos de worm identificando uma pluralidade de worms de computador, uma pluralidade de códigos de phishing identificando uma pluralidade de phishers, um conjunto de códigos de intrusos identificando uma pluralidade de intrusos que ganham acesso à uma rede de computador conectada ao o processador 102 através de uma porta de passagem, um conjunto de códigos de países da organização do tratado do Atlântico Norte (OTAN) identificando uma pluralidade de países da OTAN, um conjunto de códigos de corporação identificando uma pluralidade de corporações, um conjunto de códigos de agência de governo identificando uma pluralidade de agências de governo, um conjunto de códigos de provedor de serviço de Internet (ISP) identificando uma pluralidade de ISPs, um conjunto de código do setor industrial identificando uma pluralidade de setores industriais, e um conjunto de códigos do Departamento de Defesa (DoD) identificando uma pluralidade de DoDs. Por exemplo, C1 é um código de país para Canadá e C2 é um código de país para o Estados Unidos da América (U.S.A.). Exemplos dos setores da indústria incluem indústria de petróleo, uma indústria de aeroplanos, uma indústria de software de computador, e uma indústria de entretenimento e jogos.

Exemplos dos resultados ou procedimentos S1 e S2 incluem uma aceitação ou negação do pacote 150 pelo processador 102. Outro exemplo dos resultados S1 e S2 incluem designar uma prioridade ou não designar uma prioridade para o pacote 150. Ainda outros exemplos dos resultados inclui, designar uma Qualidade de Serviço (QoS) para o pacote 150. Exemplo de QoS inclui que o pacote 150 não é descartado ao alcançar o destino. Outro exemplo de QoS inclui que o pacote 150 não é atrasado ao alcançar ao destino.. A aceitação do pacote 150 pelo o processador 102 inclui permissão do pacote 150 de passar através da barreira de proteção de uma rede de computador para uma outra rede de computador ao alcançar a

destinação. Um exemplo da negação do pacote 150 pelo o processador 102 inclui enviar, pelo processador 102, o pacote 150 para aplicar um dos procedimentos para uma condição que salvaguarda o sistema 100 de armadilha ou de um agressor, tal como a emissor de spam de um hacker de computador, para determinar a característica do agressor e representar a característica do agressor para uma Agência de Imposição da Lei. Um exemplo da negação do pacote 150 inclui eliminar o pacote 150 para prevenir o pacote 150 de ainda prosseguir através de uma rede. Ainda um outro exemplo da negação do pacote 150 pelo o processador 102 inclui não permitir ao pacote 150 passar através da barreira de proteção para alcançar o destino. Como ainda um outro exemplo, a negação do pacote 150 pelo o processador 102 inclui manobrar, através do processador 102, o pacote 150 para um outro o processador 102 para efetuar pelo menos um de uma indagação “ Quem é ”, uma procura do Registro Americano de Números Internacionais (ARIN) do pacote 150, e traçar uma rota do pacote 150 dentro de uma rede de computador para determinar o agressor que enviou o pacote 150. Ao determinar o agressor, o processador 102 relata o agressor para a Agência de Imposição da Lei.

O processador 102 compara N bits do pacote 150 com M Bits de cada um dos intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11 - R12 da tabela I para determinar se um dos intervalos secundários tem M bits que coincidem com N bits. É notado que M é igual à N. Ao determinar que um dos intervalos secundários, tal como R1 - R2, tem M bits que coincidem com N bits, o processador 102 designa um dos valores de classificação correspondentes, tal como C1, para o pacote 150. Como um exemplo, ao determinar que N bits coincide com M bits do intervalo secundário R3 - R4, o processador 102 designa o valor de classificação C2 para o pacote 150. Se o processador 102 determina que um dos valores de

classificação dentro da tabela I existe correspondendo a um dos intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11 - R12, da tabela I, tendo M bits que coincidem com os N bits, o processador 102 determina que o pacote 150 está classificado. Por outro lado, se o processador 102 determina que um dos valores de classificação, dentro da tabela I, correspondendo a um dos intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11 - R12, da tabela I, tendo M bits que coincidem com os N bits não existem, o processador 102 determina que o pacote 150 não pode ser classificado. Por exemplo, ao comparar M e N bits, o processador 102 determina que os N bits do pacote 150 coincidem com M bits dentro do intervalo secundário R5 - R6 que não correspondem a um dos valores de classificação C1 e C2. No exemplo, ao determinar, através do processador 102, que os N bits não correspondem a um dos valores de classificação C1 e C2, o processador 102 determina que o pacote 150 não pode ser classificado.

Ao determinar que o pacote 150 está classificado, o processador 102 ou fornece 208 um procedimento ou um dos resultados S1 e S2 correspondendo a um dos valores de classificação ou envia o pacote 150 para um processador 102, tal como um incluído dentro da estação de trabalho 52, que aplica um dos resultados para o pacote 150. Como um exemplo, ao determinar que o pacote 150 está classificado sob o valor de classificação C1, o processador 102 aplica o resultado S1 para o pacote 150. Como um outro exemplo, ao determinar através do processador 102 que o pacote 150 tem o valor de classificação C2, o processador 102 envia o pacote 150 para um outro processador, tal como um incluído dentro da estação de trabalho 54, que aplica o resultado S2 para o pacote 150. Ao determinar que o pacote 150 está classificado, o processador 102 não examine bits do pacote 150 outros do que N bits.

A tabela II, fornecida abaixo, é um exemplo da tabela I.

Número de linha	Intervalos secundários de endereço de rede de IP	Códigos de País	Países	Resultados
1	0	148	Reservado	Aceitar
2	1 – 2	199	Não designado	Negar
3	3 – 4	189	Estados Unidos	Aceitar
4	5 – 9	199	Não designado	Negar
5	10 – 22	148/189	Reservado, Estados Unidos	Aceitar
6	23	199	Não designado	Negar
7	24			
8	25	188	Reino Unido	Aceitar
9	...	...	..	..
10	43	88	Japão	Aceitar
11	...	...	...	...
12	47	36	Canadá	Aceitar
13	...	...	...	...
14	53	66	Alemanha	Negar
15	54 – 56	189	Estados Unidos	Aceitar
16	57	61	França	Negar
17	...	...	...	...
18	80 – 88			
19	89 – 124	199	Não designado	Negar
20	...	...	...	...
21	216 – 223			
22	224 - 255	148	Reservado	Aceitar

Tabela II

Os intervalos secundários de endereço de rede de IP da tabela II são um exemplo dos intervalos secundários da tabela I, códigos de país da tabela II são um exemplo dos valores de classificação da tabela I, e resultados da tabela II são um exemplo dos resultados da tabela I. Por exemplo, cada intervalo secundário de endereço de rede de IP, tal como 54 ou 57, são MSBs de um endereço de rede de IP dentro do conjunto finito.

O processador 102 compara N bits do pacote 150 com cada um dos intervalos secundários de endereço de rede de IP da tabela II e determina um dos intervalos secundários de endereço de rede de IP tendo M bits que coincidem com os N bits. Por exemplo, ao determinar que os endereços de rede 47.0.0.0 - 47.255.255.255 da tabela II coincide com N bits do pacote 150, o processador 102 designa um código de país 36 da tabela II para o pacote 150 e determina que o pacote 150 é enviado do Canadá. Ao determinar

que o pacote 150 é enviado do Canadá, o processador 102 determina aceitar o pacote 150 com base na tabela II. Como um outro exemplo, ao determinar através do processador 102 que M bits do intervalo secundário de rede de IP 23 da tabela II coincidem com N bits do pacote 150, o processador 102 designa um código de país 199 da tabela II para o pacote 150 e determina que o pacote 150 é enviado de uma região não designada. Ao determinar que o pacote 150 é enviado de uma região não designada, o processador 102 determina negar o pacote 150 como mostrado na tabela II. Como ainda um outro exemplo, ao determinar através do processador 102 que M bits do intervalo secundário de rede de IP 227 de uma pluralidade de Endereços de rede de IP 224.0.0.0 - 255.255.255.255 da tabela II coincide com N bits do pacote 150, o processador 102 designa um código de país 148 da tabela II para o pacote 150 e determina que o pacote 150 é enviado de uma região reservada. Ao determinar que o pacote 150 é enviado de uma região reservada, o processador 102 determina aceitar pacote 150 com base na tabela II. Como ainda um outro exemplo, ao determinar através do processador 102 que M bits do intervalo secundário de endereço de rede de IP 216 - 223 coincide com N bits do pacote 150, o processador 102 determina que o pacote 150 não pode ser classificado com base em um valor de classificação.

A tabela III, fornecida abaixo, é um outro exemplo da tabela I.

Intervalos secundários de endereço de rede de IP	Resultados
0 -127	Permitir
128 – 160	Negar
161 – 163	Permitir
164 – 167	Negar
168 – 191	Permitir
192 – 207	Negar
208 - 255	Permitir

Tabela III

Os intervalos secundários de endereço de rede de IP da tabela III são 8 MSBs, que são um exemplo de M bits, dos intervalos secundários de endereço de rede de IP, dentro do conjunto finito, da tabela I. Mais ainda,

resultados da tabela III são um exemplo dos resultados da tabela I

O processador 102 recebe N bits do pacote 150, compara os N bits com M bits de cada um dos intervalos secundários de endereço de rede de IP da tabela III para determinar um dos intervalos secundários de endereço de rede de IP tendo M bits que coincidem com o N bits. Ao determinar que N bits do pacote 150 coincidem com M bits dentro de qualquer dos IP intervalos secundários de endereço de rede de IP 0 -127, 161 -163, 168 -191, e 208 -255, o processador 102 determina que o pacote 150 é permitido passar através da barreira de proteção. Por outro lado, ao determinar que N bits do pacote 150 coincidem com M bits dentro de qualquer dos intervalos secundários de endereço de rede de IP 128 -160, 164 -167, e 192 - 207, o processador 102 determina negar passagem do pacote 150 através da barreira de proteção.

A tabela IV, mostrada abaixo, é ainda um outro exemplo da tabela I.

intervalos secundários de endereço de rede de IP	intervalos secundários de endereço de rede de IP de MSBs	Resultados
0 -127	0	Permitir
128 - 255	1	

Tabela IV

Os intervalos secundários de endereço de rede de IP da tabela IV são um exemplo dos intervalos secundários da tabela I e os resultados da tabela IV são um exemplo dos resultados da tabela I.

O processador 102 compara um MSB, que é um exemplo de N, do endereço de rede de IP do pacote 150 com um MSB, que é um exemplo de M, de cada um dos intervalos secundários de endereço de rede de IP da tabela IV para determinar se o MSB do pacote 150 coincide com ou bit 1 ou bit 0. Ao determinar que MSB do endereço de rede de IP do pacote 150 coincide com bit 0, que é um MSB do intervalo secundário de endereço de rede de IP 0-127 da tabela IV, o processador 102 determina, com base nos resultados da tabela IV, permitir passagem do pacote 150 através da barreira de proteção. Por outro lado, ao determinar que MSB do endereço de rede de

IP do pacote 150 coincide com bit 1, que é um MSB do intervalo secundário de endereço de rede de IP 128 - 255 da tabela IV, o processador 102 determina, com base nos resultados da tabela IV, que o pacote 150 não pode ser classificado e não fornece um resultado para o pacote 150.

5 Ao determinar que o pacote 150 não pode ser classificado com base nos N bits do pacote 150, o processador 102 obtém 210 G bits outros do que N bits do pacote 150. Ao determinar que o pacote 150 não pode ser classificado comparando N bits com M bits dos intervalos secundários da tabela 1, o processador 102 obtém G bits do pacote 150. Como um exemplo, o
10 processador 102 determina que o pacote 150 é um pacote 150 de IPv4 e sequencialmente extrai 7 bits seguintes ao MSB do endereço de rede de IP do pacote 150, onde o MSB é Nth bit do endereço de rede de IP do pacote 150. Como ainda um outro exemplo, o processador 102 determina que o pacote 150 é um pacote de IPv4 150 e extrai 3 MSBs de 8 MSBs do endereço de rede
15 de IP do pacote 150, onde 2 bits outros do que os 3 MSBs e 3 LSBs do endereço de rede de IP são N bits do endereço de rede de IP do pacote 150. Como ainda um outro exemplo, o processador 102 determina que o pacote 150 é um pacote de IPv6 150 e extrai 4 LSBs dos 16 MSBs do endereço de rede de IP do pacote 150, onde 12 MSBs são N bits do endereço de rede de IP
20 do pacote 150. Um exemplo de G inclui bits outros do que N bits de 8 MSBs do endereço de rede de IP do pacote 150. Um outro exemplo de G inclui consecutivamente 15 bits seguintes a um MSB dos 16 MSBs do endereço de rede de IP do pacote 150, onde o MSB é o Nth bit do endereço de rede de IP do pacote 150.

25 O processador 102 determina 206 se o pacote 150 pode ser classificado com base nos G bits do pacote 150. O processador 102 aplica a tabela V, mostrada abaixo, armazenada no dispositivo de memória 104 pelo usuário para determinar se o pacote 150 pode ser classificado com base nos G bits do pacote 150.

Intervalos secundários	Valores de classificação	Resultados
SR1 – SR2	C3	S3
SR3 – SR4	C4	S4
SR5 – SR6		
SR7 – SR8		

Tabela V

Os intervalos secundários SR1 - SR2, SR3 - SR4, SR5 - SR6, e SR7 - SR8 dentro da tabela V formam um conjunto finito, tal como um conjunto de G bits de endereço de portas, um conjunto de G bits de dados de autorização, um conjunto de G bits de endereços de rede de IP, e um conjunto de G bits de uma combinação de endereços de rede de IP e endereços de portas. Exemplo dos valores de classificação C3 e C4 incluem um conjunto de códigos de país identificando uma pluralidade de países, um conjunto de códigos de região secundária identificando uma pluralidade de regiões secundárias, um conjunto de códigos de hacker de computador identificando uma pluralidade de hackers de computador, um conjunto de códigos de emissor de spam identificando uma pluralidade de emissores de spam de computador, um conjunto de códigos de vírus identificando uma pluralidade de vírus de computador, um conjunto de códigos de Trojan identificando uma pluralidade de Trojans, um conjunto de códigos de worm identificando uma pluralidade de worms de computador, uma pluralidade de códigos de phishing identificando uma pluralidade de phishers, um conjunto de códigos de intruso identificando uma pluralidade de intrusos que ganham acesso a uma rede de computador conectada ao processador 102 através de uma porta de passagem, um conjunto de códigos de países da OTAN identificando uma pluralidade de países da OTAN, um conjunto de códigos de corporação identificando uma pluralidade de corporações, um conjunto de códigos de agência de governo identificando uma pluralidade de agências de governo, um conjunto de códigos de ISP identificando uma pluralidade de ISPs, um conjunto de código do setor industrial identificando uma pluralidade de setores industriais, e um conjunto de códigos do DoD identificando uma pluralidade de DoDs.

Exemplos dos resultados S3 e S4 incluem uma aceitação ou negação do pacote 150 pelo processador 102. Outros exemplos dos resultados S3 e S4 incluem designar uma prioridade ou não designar uma prioridade para o pacote 150. É notado que G é igual à H.

5 Ao determinar que um dos intervalos secundários SR1 - SR2, SR3 - SR4, SR5 - SR6, e SR7 - SR8 da tabela V tem H bits que coincidem com G bits do pacote 150, o processador 102 designa um dos classificação valores correspondentes, tal como C3 e C4, para o pacote 150. Como um exemplo, ao determinar que G bits coincidem com H bits dos intervalos secundários SR3 - SR4, o processador 102 designa o valor de classificação C4 para o pacote 150. Se o processador 102 determina que um dos valores de classificação dentro da tabela V existe correspondendo a um dos intervalos secundários, da tabela V, tendo H bits que coincidem com G bits do pacote 150, o processador 102 determina que o pacote 150 está classificado. Por 10 outro lado, se o processador 102 determina que um dos valores de classificação dentro tabela V não existe correspondendo a um dos intervalos secundários, dentro tabela V, tendo H bits que coincidem com ao comparar, através do processador 102, G bits do pacote 150 com os intervalos secundários da tabela V, o processador 102 determina que G bits coincidem 15 com H bits dentro do intervalo secundário SR5 - SR6 que não correspondem a um dos valores de classificação C3 e C4. No exemplo, ao determinar pelo processador 102 que G bits do pacote 150 não correspondem a um dos valores de classificação C3 e C4, o processador 102 determina que o pacote 150 não pode ser classificado.

25 Ao determinar que o pacote 150 está classificado, o processador 102 ou fornece 208 um procedimento ou um dos resultados S3 e S4 correspondendo a um dos valores de classificação da tabela V ou envia o pacote 150 para um outro processador 102, tal como um incluído dentro da estação de trabalho 54, que fornece 208 um dos resultados S3 e S4 para o

pacote 150. Como um exemplo, ao determinar que o pacote 150 está classificado como tendo o valor de classificação C3, o processador 102 aplica o resultado S3 para o pacote 150. Como um outro exemplo, ao determinar através do processador 102 que o pacote 150 tem o valor de classificação C2, o processador 102 envia o pacote 150 para um outro processador 102 que aplica o resultado S2 para o pacote 150. Ao determinar que o pacote 150 está classificado, o processador 102 não extrai bits do pacote 150 outros do que os G e N bits para determinar se o pacote 150 pode ser classificado.

A tabela VI, mostrada abaixo, é um exemplo da tabela V.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
128 – 160	00	Negar
1261 – 2078	01 – 10	
168 - 255	11	Permitir

Tabela VI

Bits dos intervalos secundários de endereço de rede de IP da tabela VI são um exemplo dos H bits dos intervalos secundários da tabela V. Por exemplo, dois, que é um exemplo de H, bits 00 são segundo e terceiro MSBs de 128 dentro do intervalo secundário de endereço de rede de IP 128 - 160 da tabela VI. Como um outro exemplo, bits 01 dentro tabela VI são segundo e terceiro MSBs de 161 dentro do intervalo secundário de endereço de rede de IP 161 - 207 da tabela VI. Resultados da tabela VI são um exemplo de resultados da tabela V.

O processador 102 recebe G bits do pacote 150, compara os G bits com H bits para determinar se o pacote 150 pode ser classificado. Por exemplo, ao receber G bits, o processador 102 determina que G bits coincidem com 01 e determina que o pacote 150 não pode ser classificado e não fornece um resultado com base na tabela VI. Por outro lado, o processador 102 recebe G bits do pacote 150, compara os G bits com bits 00 para determinar que G bits são 00 e negar passagem do pacote 150 através da barreira de proteção com base na tabela VI. Mais ainda, o processador 102

recebe G bits do pacote 150 compara os G bits com bits 11 dentro tabela VI para determinar que G bits são 11 e para determinar permitir passagem do pacote 150 através da barreira de proteção como mostrado in tabela VI.

5 Ao determinar que o pacote 150 não pode ser classificado com base nos G e N bits do pacote 150, o processador 102 determina se o pacote 150 pode ser classificado através da análise de A bits do pacote 150 outros do que os G e N bits. A tabela VII é mostrada abaixo.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
192 – 207	0	Negar
208 - 223	1	Permitir

Tabela VII

O processador 102 recebe A bits, tal como o 5th LSB de 8
 10 MSBs do endereço de rede de IP do pacote 150, compara os A bits com B bits, tal como o 5th LSB de 8 MSBs de cada endereço de rede de IP com os intervalos secundários de endereço de rede de IP da tabela VII, para determinar se o pacote 150 pode ser classificado. Por exemplo, ao receber A bits do pacote 150, o processador 102 determina que os A bits coincidem com
 15 0, que é o 5th LSB de 8MSBs do intervalo secundário 193 de um endereço de rede de IP 193.0.0.0, determina que o pacote 150 pode ser classificado, e nega passagem do pacote 150 através da barreira de proteção com base na tabela VII. Como um outro exemplo, ao receber A bits do pacote 150, o processador 102 determina que os A bits coincidem com bit 1, que é o 5th LSB de 8MSBs
 20 do intervalo secundário de endereço de rede de IP 210 de um endereço de rede de IP rede 210.1.1.1, determina que o pacote 150 pode ser classificado, e permite passagem do pacote 150 através da barreira de proteção com base na tabela VII. É notado que A é igual à B.

A tabela VIII, mostrada abaixo, é um exemplo da tabela V.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
160 - 168	0	
191	1	Permitir

Tabela VIII

Os intervalos secundários de endereço de rede de IP da tabela VIII são um outro exemplo dos intervalos secundários da tabela V. Bits dos intervalos secundários de endereço de rede de IP da tabela VI são um outro exemplo dos H bits dos intervalos secundários da tabela V. Por exemplo, bit 0 é o 5th LSB de cada dos 8 MSBs 160 - 168 de uma pluralidade de endereços de rede de IP com MSBs variando de e incluindo 160 à 168, e 160 -168 é um exemplo do intervalo secundário SR5 - SR6. Como um outro exemplo, bit 1 é o 5th LSB de 8 MSBs 191 de uma pluralidade de endereços de rede de IP com MSB 191, e 191 é o intervalo secundário de endereço de rede de IP SR1 - SR2.

O processador 102 recebe G bits do pacote 150, compara os G bits com H bits da tabela VIII para determinar se o pacote 150 pode ser classificado. Por exemplo, ao receber G bits do pacote 150, o processador 102 determina que os G bits coincidem com 0 dos intervalos secundários de endereço de rede de IP 160 -168 da tabela VIII, determina que os G bits não podem ser classificados, e não fornece um resultado para o pacote 150. Como um outro exemplo, ao receber G bits do pacote 150, o processador 102 determina que os G bits coincidem com 1 do intervalo secundário de endereço de rede de IP 191 para determinar que o pacote 150 pode ser classificado para permitir ao pacote 150 passar através da barreira de proteção.

Ao determinar que o pacote 150 não pode ser classificado com base na comparação de G bits do pacote 150 com H bits, o processador 102 determina se o pacote 150 pode ser classificado com base na comparação de A bits do pacote 150 com B bits. A tabela IX é mostrada abaixo.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
160 - 167	0	
168	1	Permitir

Tabela IX

O processador 102 recebe A bits do pacote 150, compara os A bits com B bits, tal como 4th LSB de cada dos 8 MSBs 160 -167 de uma pluralidade de endereços de rede de IP160.0.0.0 - 167.255.255.255, para determinar se o pacote 150 pode ser classificado. Por exemplo, ao receber A bits do pacote 150, o processador 102 determina que A bit coincide com bit 0, que é o 4th LSB de cada 8 dos MSBs 160 - 167, determina que o pacote 150 não pode ser classificado e não pode ser fornecido um resultado. Como um outro exemplo, ao receber A bit do pacote 150, o processador 102 determina que o A bit coincidem com bit 1, que é o 4th LSB dos 8 MSBs 168 de uma pluralidade de endereços de rede de IP168.0.0.0 — 168.255.255.255, determina que o pacote 150 pode ser classificado, e permite passagem do pacote 150 através da barreira de proteção.

Ao determinar que o pacote 150 não pode ser classificado com base nos N, G, e A bits do pacote 150, o processador 102 obtém C bits do pacote 150 e determina se o pacote 150 pode ser classificado com base nos C bits. A tabela X é mostrada abaixo.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
160 -163	0	
164 - 167	1	Negar

Tabela X

Como exemplo de C bits do pacote 150 inclui 3rd LSB dos 8 MSBs do endereço de rede de IP do pacote 150 isto é um pacote de IPv4 150. Um outro exemplo de C bits do pacote 150 inclui 4th LSB do endereço de rede de IP do pacote 150 que é um pacote de IPv6 150.

O processador 102 recebe C bits do pacote 150, compara os C bits com D bits, tal como o 3rd LSB de cada dos 8MSBs de uma pluralidade de endereços de rede de IP160.0.0.0 - 163.255.255.255, para determinar se o pacote 150 pode ser classificado. Por exemplo, o processador 102 compara C bits do pacote 150 com o bit 0, que é a 3rd LSB de cada dos 8 MSBs 160 -163

para determinar que o pacote 150 não pode ser classificado e não fornece um resultado para o pacote 150. Como um outro exemplo, o processador 102 compara C bits do pacote 150 com o bit 1, que é o 3rd LSB de cada dos 8 MSBs 164 -167 de uma pluralidade de endereços de rede de IP 164.0.0.0 - 167.255.255.255, para determinar que o pacote 150 pode ser classificado e negar passagem do pacote 150 através do barreira de proteção. É notado que C é igual à D.

Ao determinar que o pacote 150 não pode ser classificado com base nos N, G, A, e C bits do pacote 150, o processador 102 obtém E bits do pacote 150 e determina se o pacote 150 pode ser classificado com base nos E bits. A tabela XI é mostrada abaixo.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
160 -161	0	
163	1	Permitir

Tabela XI

Um exemplo de E bits do pacote 150 inclui o 2nd LSB dos 8 MSBs do endereço de rede de IP do pacote 150 que é um pacote de IPv4. Um outro exemplo de E bits do pacote 150 inclui o 5th LSB dos 8 MSBs do endereço de rede de IP do pacote 150 que é um pacote de IPv6.

O processador 102 recebe E bits do pacote 150, compara os E bits com F bits, tal como o 2nd LSB de cada dos intervalos secundários de endereço de rede de IP da tabela XI, para determinar se o pacote 150 pode ser classificado. Por exemplo, o processador 102 compara E bits do pacote 150 com bit 0, que é o 2nd LSB de cada dos 8 MSBs 160 - 161 de uma pluralidade de endereços de rede de IP 160.0.0.0-161.255.255.255 para determinar que o pacote 150 não pode ser classificado. Como um outro exemplo, o processador 102 recebe E bits do pacote 150, compara os E bits com bit 1, que é o 2nd LSB dos 8 MSBs 163 de uma pluralidade de endereços de rede de IP 163.0.0.0-163.255.255.255 para determinar que o pacote 150 pode ser classificado e para permitir passagem do pacote 150 através da barreira de proteção. É

notado que E é igual à F.

Ao determinar que o pacote 150 não pode ser classificado com base nos N, G, A, C, e E bits do pacote 150, o processador 102 obtém I bits outros do que os N, G, A, C, e E bits do pacote 150 para determinar se o pacote 150 pode ser classificado com base nos I bits. A tabela XII é mostrada abaixo.

intervalos secundários de endereço de rede de IP	Bits dos intervalos secundários de endereço de rede de IP	Resultados
160	0	Negar
161	1	Permitir

Tabela XII

Um exemplo de I bits do pacote 150 inclui o LSB dos 8 MSBs do endereço de rede de IP do pacote 150 que é um pacote de IPv4. Um outro exemplo de I bits do pacote 150 inclui o LSB dos 16 MSBs do endereço de rede de IP do pacote 150 que é um pacote de IPv6.

O processador 102 recebe I bits do pacote 150, compara os I bits com J bits, tal como o LSB de cada dos intervalos secundários de endereço de rede de IP da tabela XII, para determinar se o pacote 150 pode ser classificado. Por exemplo, o processador 102 compara I bit do pacote 150 com bit 0, que é o LSB do 160 de uma pluralidade de endereços de rede de IP 160.0.0.0 - 160.255.255.255 para determinar que o pacote 150 pode ser classificado e negar passagem do pacote 150 através da barreira de proteção. Como um outro exemplo, ao receber I bit do pacote 150, o processador 102 compara to I bit com bit 1, que é o LSB do 161 de uma pluralidade de endereços de rede de IP 161.0.0.0 - 161.255.255.255, para determinar que o pacote 150 pode ser classificado e para permitir passagem do pacote 150 através da barreira de proteção. Conseqüentemente, o processador 102 continua a comparar bits adicionais do pacote 150 com uma pluralidade de tabelas, tal como tabela V - XII, até o pacote 150 poder ser classificado. É notado que I é igual à J.

Figura 6 é uma modalidade de uma interface de usuário gráfica

(GUI) 250 usada para criar qualquer das tabelas I - XII. O processador 102
 5 exibe, no dispositivo de saída 108, a GUI 250 para o usuário. A GUI 250
 inclui um mapa 252 do mundo. O processador 102 associa ou se conecta a
 uma pluralidade de pontos 254, 256, e 258, no mapa 252, com um dos
 intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11 -
 R12. Por exemplo, o processador 102 associa o ponto 254 com o intervalo
 secundário R1 - R2 da tabela I e associa ao ponto 256 o intervalo secundário
 de endereço de rede R5 - R6 da tabela I. Como um outro exemplo, o
 10 processador 102 associa o ponto 254 com um endereço de porta de uma porta
 de um computador localizado dentro dos U.S.A. e associa ponto 256 dentro
 de um endereço de porta de uma porta de um computador localizado dentro
 do Canadá.

Quando o usuário seleciona, através do dispositivo de entrada
 106, um ponto no mapa 252, o processador 102 exibe uma pluralidade de
 15 resultados para o usuário. Por exemplo, quando o usuário seleciona ponto
 254, o processador 102 exibe uma pluralidade de opções incluindo uma
 permissão do pacote 150, tendo N bits que coincidem com M bits de um dos
 intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R11-
 R12 de um endereço de rede de IP de um computador localizado no ponto
 20 254, através da barreira de proteção, uma negação do pacote 150, fornecendo
 uma prioridade para o pacote 150, e não fornecendo a prioridade para o
 pacote 150. Quando o usuário seleciona uma das opções, o processador 102
 associa a uma das opções com um ponto no mapa 252. Por exemplo, quando o
 usuário seleciona a permissão do pacote 150, tendo N bits que coincidem com
 25 M bits de um dos intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8,
 R9 - R10, e R1 - R12, associada com o ponto 254 através da barreira de
 proteção, o processador 102 armazena, dentro do dispositivo de memória 104,
 que o pacote 150, tendo N bits que coincidem com M bits de um dos
 intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R1 -

R12, é para ser permitido através da barreira de proteção. Como um outro exemplo, quando o usuário seleciona fornecer uma prioridade para o pacote 150, tendo N bits que coincidem com M bits de um dos intervalos secundários R1 - R2, R3 - R4, R5 - R6, R7 - R8, R9 - R10, e R1 - R12, associada com o ponto 258, o processador 102 armazena, no dispositivo de memória 104, que ao pacote 150 tendo o um dos intervalos secundários é para ser fornecido a prioridade.

Em uma modalidade, o processador 102 associa uma pluralidade de pontos dentro de uma região, tal como um país, uma cidade, um estado, uma corporação, e uma rede de computador, no mapa 252 com um dos resultados S1 e S2 quando o usuário seleciona uma vez, tal como clicando um mouse uma vez, qualquer um dos pontos e seleciona o um dos resultados. Por exemplo, quando o usuário clica uma vez no ponto 254 dentro dos U.S. A. e seleciona permissão do pacote 150, o processador 102 associa todos os pontos dentro U.S.A. no mapa 252 com a permissão do pacote 150 recebido do U.S.A. pelo processador 102. Na modalidade, o processador 102 associa pelo menos um ponto com uma região secundária, tal como uma cidade, uma agência governamental, um ISP, uma corporação, um DoD, um computador, uma porta, localizada dentro da região com um dos resultados S1 e S2 quando o usuário seleciona para a número, tal como duas vezes, um do pelo menos um ponto e seleciona o um dos resultados. Por exemplo, quando o usuário clica duas vezes no ponto 254 representando uma cidade dentro do U.S.A. e seleciona nenhuma prioridade clicando duas vezes no ponto 254, o processador 102 associa o pacote 150 recebido da cidade para não ter prioridade. Como um outro exemplo, quando o usuário clica duas vezes no ponto 258 representando uma rede de computador dentro do Canadá e seleciona negação da passagem do pacote 150 clicando duas vezes no ponto 258, o processador 102 associa o ponto 258 com a negação, através da barreira de proteção, da passagem do pacote 150 recebido da rede de

computador.

É notado que em uma modalidade, o método das Figuras 5 e 6, e tabelas I - XII é uma máquina de estado finito (FSM) implementada dentro de um conjunto de portas lógicas e registros de deslocamento para implementar a barreira de proteção. Em uma outra modalidade, em vez de designar uma prioridade, ao pacote 150 é designado um alta prioridade e em vez de não designar prioridade, ao pacote 150 é designado um baixa prioridade mais baixa do que a alta prioridade. É notado que os métodos ilustrados através das Figures 5 e 6, e tabelas I - XII são implementados em ou um hardware mini, micro, ou de mainframe. Em ainda outra modalidade, os métodos ilustrados pelas Figures 5 e 6, e tabelas I - XII são implementados dentro de um arranjo de porta programável por campo (FPGA). Os sistemas e métodos aqui descritos para determinar um fluxo de dados fornecem uma estrutura transversal baseado em árvore que permite uma execução exponencial de uma pluralidade de regras ou listas de controle de acesso (ACLs). Por exemplo, o processador 102 atinge um resultado comparando 8 MSBs do endereço de IP do pacote 150 com ou intervalo secundário de endereço de IP 3 - 4 de uma pluralidade de endereços de IP de 3.0.0.0 - 4.255.255.255 na linha 4 da tabela II ou intervalo secundário de endereço de rede de IP 5 - 9 de uma pluralidade de endereços de IP de 5.0.0.0 - 9.255.255.255 na linha 4 da tabela II como oposto para comparar todos os bits do pacote 150 com os endereços de IP de 3.0.0.0 - 4.255.255.255 e 5.0.0.0 - 9.255.255.255. Como um outro exemplo, o processador 102 fornece um resultado exponencialmente mais rápido do que o fornecido para comparar todos os bits do pacote 150 com um conjunto de bits. No exemplo, o processador 102 fornece um resultado exponencialmente mais rápido comparando o 2nd e 3rd MSBs dos 8 MSBs do endereço de IP do pacote 150 com 2nd e 3rd MSBs de 8 MSBs 128 -160, dentro da tabela VI, dos endereços de IP 128.0.0.0- 160.255.255.255. Os métodos e sistemas para determinar um

fluxo de dados aqui descritos não necessitam executar uma operação de ponto de flutuação e por conseguinte pode rodar dentro de uma espaço de Kernel.

Sistemas e métodos descritos aqui alcançam uma isolação entre duas redes conectadas através da barreira de proteção através da negação do pacote 150 de uma região, tal como um país, ou alternativamente da região secundária. Mais ainda, sistemas e métodos aqui descritos permitem a passagem do pacote 150 através da barreira de proteção ao determinar que o pacote 150 é recebido a partir de um aliado de um país no qual a barreira de proteção está localizada. Adicionalmente, os sistemas e métodos descritos aqui são usados para negar o pacote 150 recebido de uma entidade outra do que uma pluralidade de organizações dentro de um grupo.

Sistemas e métodos aqui descritos são executados reduzindo incidências de correios eletrônicos não solicitados ou spam para melhorar o desempenho de transmissão da Internet. Por exemplo, o processador 102 determina com base nos N bits do pacote 150 e tabela II se o pacote 150 está classificado dentro um código de país 66 da Alemanha. Ao determinar que o pacote 150 tem um valor de classificação de 66, o processador 102 determina negar o pacote 150 que pode incluir spam proveniente da Alemanha e aumenta o desempenho de transmissão da Internet reduzindo a passagem de spam através da barreira de proteção para uma rede. Como um outro exemplo, o processador 102 determina com base nos N bits do pacote 150 que o pacote 150 é designado um código de país outro do que 189. Ao determinar que ao pacote 150 é designado um código de país outro do que 189, o processador 102 nega a passagem do pacote 150 através da barreira de proteção e a negação reduz a recepção, através de uma rede acoplada para a barreira de proteção, de spam proveniente de países outros do que U.S.A. Mais ainda, no exemplo, reduzindo a recepção de spam proveniente do U. S. A., o processador 102 torna, de forma significativa, mais fácil monitorar emissores de spam dentro do U.S.A. No exemplo, o processador 102 aplica os métodos

para determinar um fluxo de dados para processar o pacote 150, enviado proveniente do U.S A., de forma significativa, tal como dez vezes, mais rápido do que a velocidade de comunicação de 9.6 Gigabits por segundo (Gbps) de uma portadora óptica 192 (OC-192). Os métodos aqui descritos são

5 usados para diminuir um ampla variedade de ameaças de segurança de rede de comunicação por computador, tal como, vírus de computador enviado por agressores. Os métodos fornecem, características de escalonamento, adaptabilidade, e desempenho usadas para adaptar a cada um de escopo envolvendo os problemas de segurança. Os métodos aqui descritos podem ser

10 implementados dentro de inúmeros produtos de segurança, tal como dispositivos de shunt de dados, sistemas de simulação de redes, sistemas de análises biométricas, sistemas de análise de anomalias biométricas, sistemas de projetos de arquitetura de segurança, centros de operação de rede, redes privadas virtuais (VPNs), e sistemas de gerenciamento de informação de

15 segurança..

Enquanto a invenção foi descrita em termos de várias modalidades específicas, aqueles qualificados na técnica irão reconhecer que uma invenção pode ser praticada com modificação dentro do espírito e escopo das reivindicações.

REIVINDICAÇÕES

1. Método para determinar um fluxo de dados, caracterizado pelo fato de compreender:

- determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto, é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto;
- determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação; e
- analisar, através de um processador, pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o pelo menos um bit dentro do primeiro conjunto é outro do que o pelo menos um bit dentro do segundo conjunto.

3. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o pelo menos um bit dentro do segundo conjunto seqüencialmente segue o pelo menos um bit dentro do primeiro conjunto.

4. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o pelo menos um bit dentro do primeiro conjunto seqüencialmente segue o pelo menos um bit dentro do segundo conjunto.

5. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação se ao pacote é designado ao valor de classificação compreende determinar se o pelo menos um bit dentro do primeiro conjunto coincide com pelo menos um bit dentro de um terceiro conjunto.

6. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação do resultado a ser aplicado ao pacote compreende determinar que o pacote é um dos a serem aceitos, negados, e

designados uma prioridade, ao determinar que ao pacote é designado ao valor de classificação.

5 7. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o valor de classificação compreende um de um código identificando um país, um código identificando uma região secundária, um código identificando um hacker de computador, um código identificando um emissor de spam de computador, um código identificando um vírus de computador, um código identificando um Trojan, um código identificando um worm de computador, um código identificando um phisher, um código
10 identificando um intruso, um código identificando um país da organização de tratado do Atlântico Norte, um código identificando uma corporação, um código identificando uma agência governamental, um código identificando um provedor de serviço de Internet, um código identificando um setor industrial, e um código identificando um Departamento de Defesa.

15 8. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação se ao pacote é designado ao valor de classificação compreende determinar se o pelo menos um bit dentro do primeiro conjunto coincide com pelo menos um bit dentro de um terceiro conjunto, e em que mencionada análise do pelo menos um bit do segundo
20 número compreende determinar se o pelo menos um bit dentro do segundo conjunto coincide com pelo menos um bit dentro de um quarto conjunto.

25 9. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação se ao pacote é designado ao valor de classificação compreende determinar se o pelo menos um bit dentro do primeiro conjunto coincide com pelo menos um bit dentro de um terceiro conjunto, e em que mencionada análise do pelo menos um bit do segundo número compreende determinar se o pelo menos um bit dentro do segundo conjunto coincide com pelo menos um bit dentro de um quarto conjunto, método mencionado ainda compreendendo determinar um resultado a ser

aplicado ao pacote ao determinar que o pelo menos um bit dentro do segundo conjunto coincide com o pelo menos um bit dentro do quarto conjunto.

10. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação se ao pacote é designado ao valor de classificação compreende determinar se o pelo menos um bit dentro do primeiro conjunto coincide com pelo menos um bit dentro de um terceiro conjunto, método mencionado ainda compreendendo determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado um valor de classificação com base na comparação do pelo menos um bit dentro do segundo conjunto com o pelo menos um bit dentro do terceiro conjunto.

11. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o pelo menos um bit dentro do primeiro conjunto inclui pelo menos um bit de um endereço de protocolo de Internet do pacote.

12. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o processador compreende uma barreira de proteção.

13. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o valor de classificação é incluído dentro de um intervalo finito dos valores de classificação.

14. Método de acordo com a reivindicação 1, caracterizado pelo fato de que mencionada determinação se ao pacote é designado ao valor de classificação compreende determinar se o pelo menos um bit dentro do primeiro conjunto coincide com pelo menos um bit dentro de um terceiro conjunto, em que o pelo menos um bit do terceiro conjunto é localizado dentro de um intervalo finito de um de um conjunto de endereços de porta, um conjunto de dados de autorização, um conjunto de endereços de rede de protocolo de Internet (IP), e um conjunto de uma combinação dos endereços de rede de IP e dos endereços de porta.

15. Processador, caracterizado pelo fato de ser configurado para:

- determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto;

- determine um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação; e

- analisar pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.

10 16. Processador de acordo com a reivindicação 15, caracterizado pelo fato de que o pelo menos um bit dentro do primeiro conjunto é outro do que o pelo menos um bit dentro do segundo conjunto.

15 17. Processador de acordo com a reivindicação 15, caracterizado pelo fato de que o pelo menos um bit dentro do segundo conjunto seqüencialmente segue o pelo menos um bit dentro do primeiro conjunto.

18. Meio legível por computador, caracterizado pelo fato de ser codificado dentro de um programa de computador configurado para:

- determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto;

- determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação; e

- analisar pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.

19. Meio legível por computador de acordo com a reivindicação 18, caracterizado pelo fato de que o pelo menos um bit dentro

do primeiro conjunto é outro do que o pelo menos um bit dentro do segundo conjunto.

5 20. Meio legível por computador de acordo com a reivindicação 18, caracterizado pelo fato de que o pelo menos um bit dentro do segundo conjunto seqüencialmente segue o pelo menos um bit dentro do primeiro conjunto.

 21. Método para determinar um fluxo de dados, caracterizado pelo fato de compreender :

- 10 - gerar uma interface de usuário gráfica incluindo um mapa;
 - receber uma seleção de um ponto no mapa;
 - exibir uma pluralidade de resultados ao receber a seleção do ponto;
 - receber uma seleção de um dos resultados; e
 - designar o um dos resultados do ponto.

15 22. Método de acordo com a reivindicação 21, caracterizado pelo fato de que mencionada designação do um dos resultados do ponto compreende aplicar o um dos resultados a um pacote recebido de uma localização física representada através do ponto.

20 23. Método de acordo com a reivindicação 21, caracterizado pelo fato de ainda compreender exibir o mapa do mundo.

 24. Método de acordo com a reivindicação 21, caracterizado pelo fato de que o um dos resultados inclui negar passagem de um pacote através de uma barreira de proteção, permitir passagem do pacote através da barreira de proteção, e designar uma prioridade ao pacote.

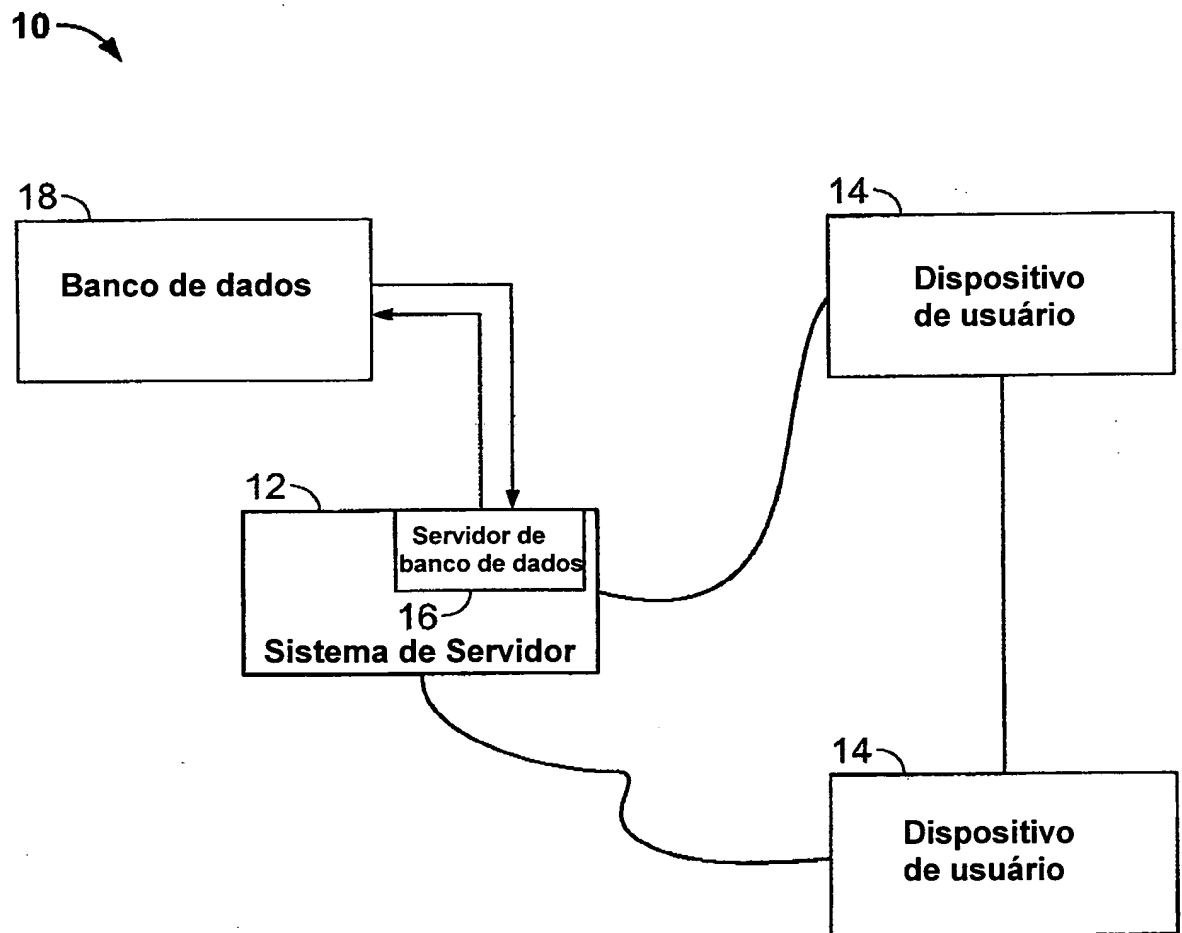


FIG. 1

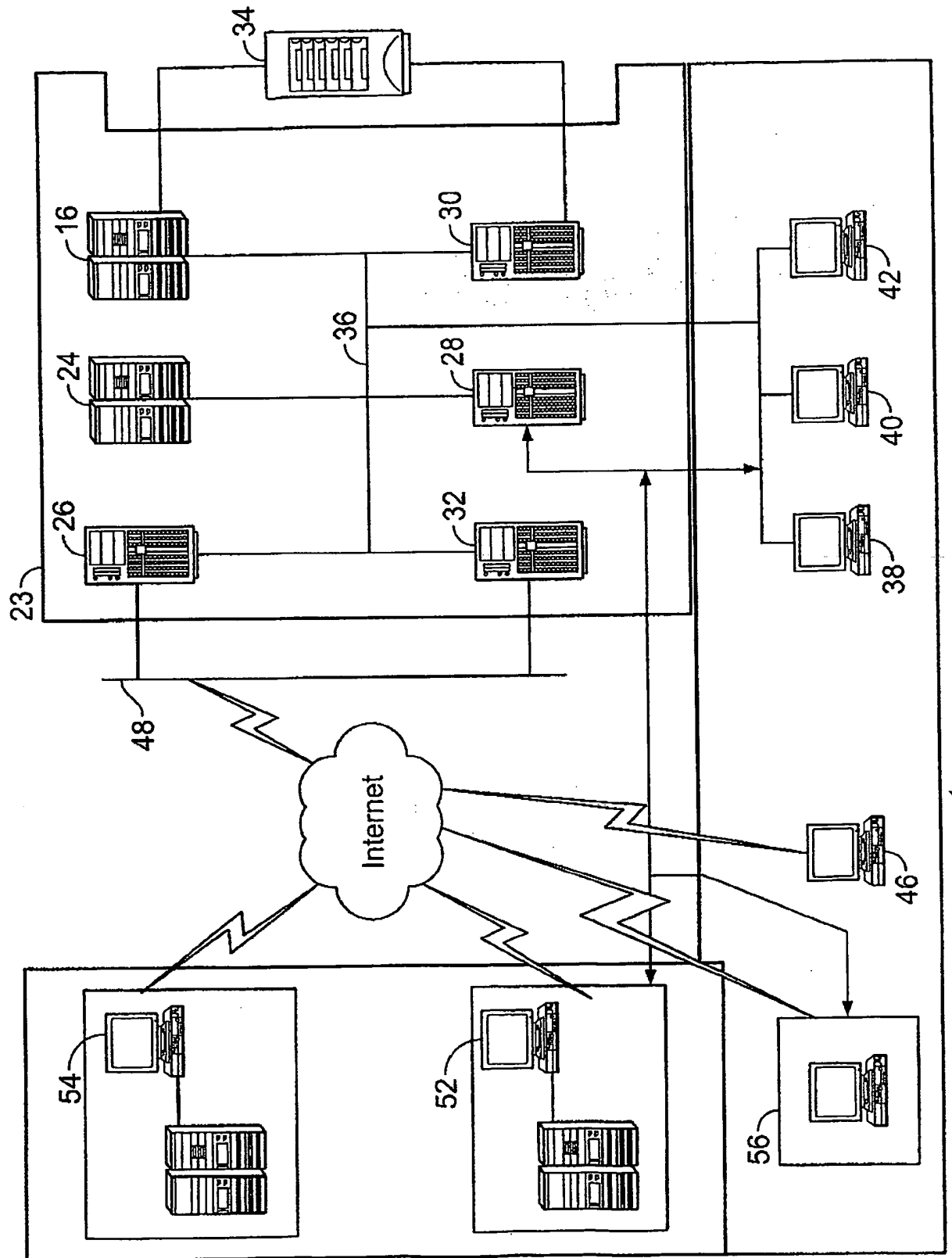


FIG. 2

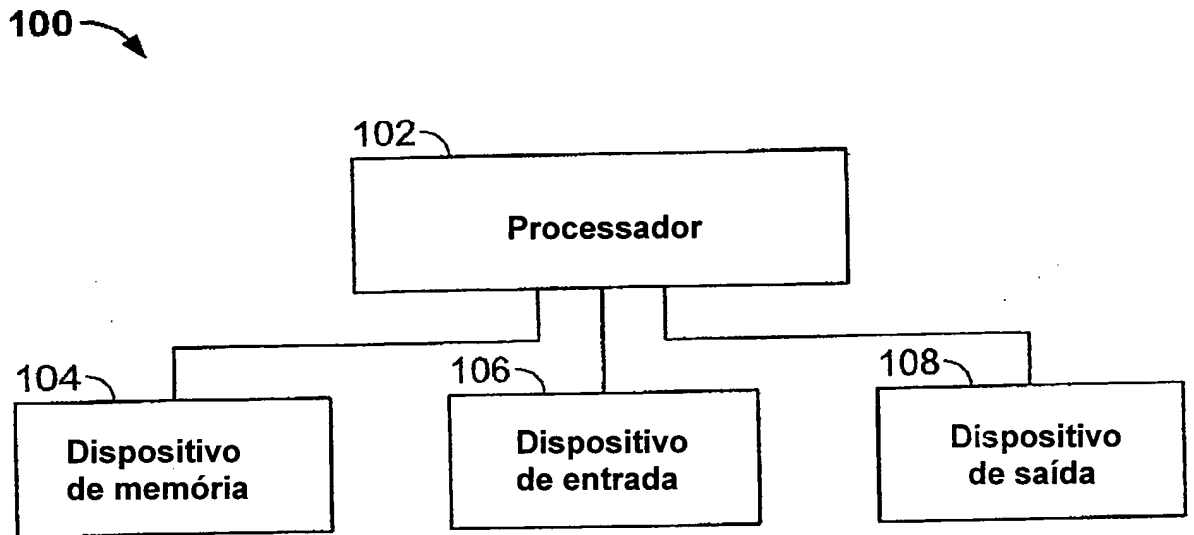


FIG. 3

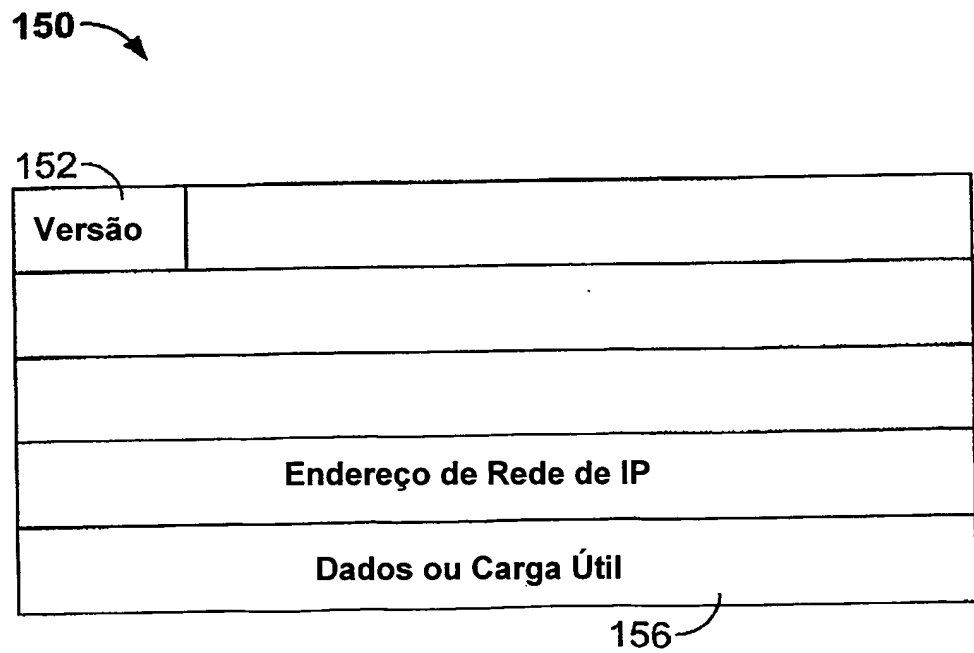


FIG. 4

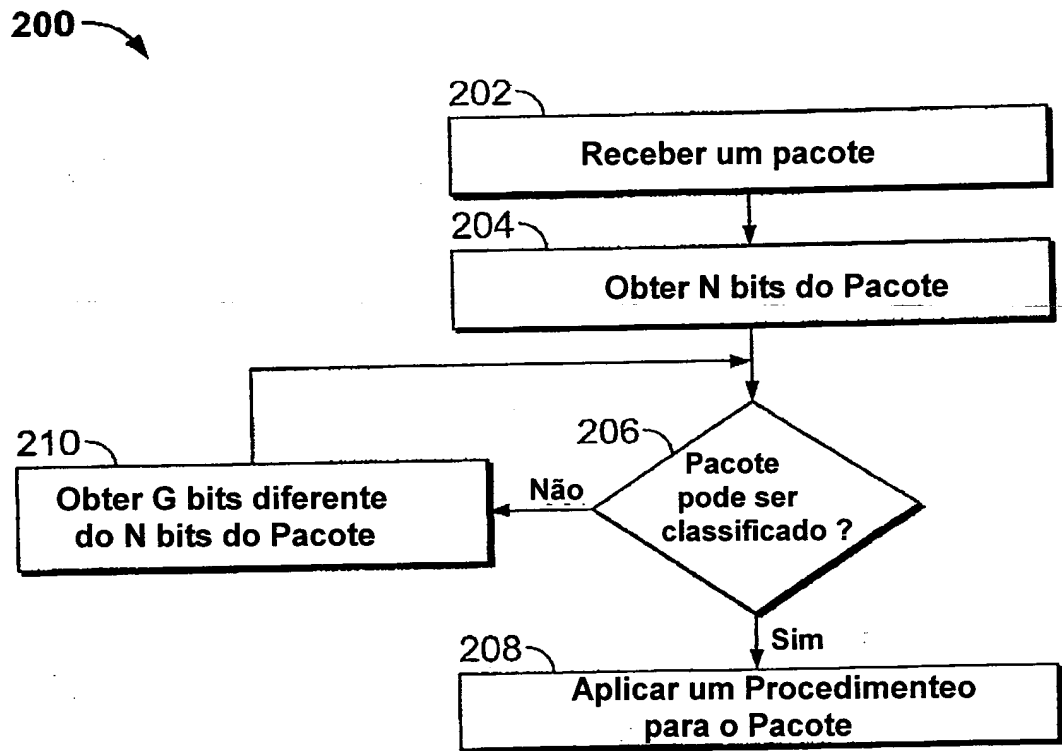


FIG. 5

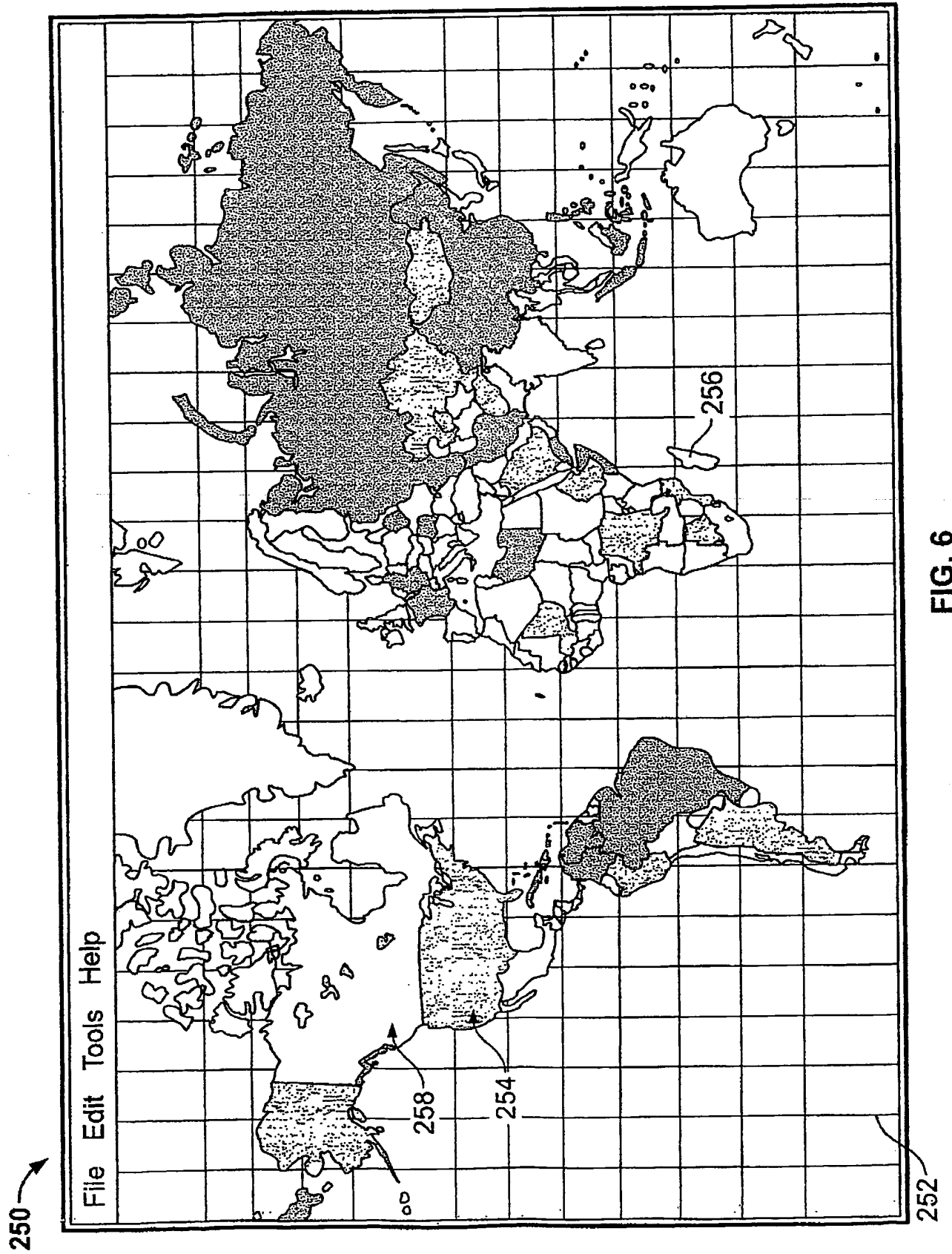


FIG. 6

RESUMO

“MÉTODO PARA DETERMINAR UM FLUXO DE DADOS, PROCESSADOR, E, MEIO LEGÍVEL POR COMPUTADOR”

- Um método para determinar um fluxo de dados é descrito. O
- 5 método inclui determinar se a um pacote incluindo um primeiro número de pelo menos um bit dentro de um primeiro conjunto é designado um valor de classificação com base no pelo menos um bit dentro do primeiro conjunto e determinar um resultado a ser aplicado ao pacote ao determinar que ao pacote é designado ao valor de classificação. O método ainda inclui analisar, através
- 10 de um processador, pelo menos um bit de um segundo número dentro de um segundo conjunto do pacote ao determinar que ao pacote não pode ser designado ao valor de classificação com base no primeiro número de pelo menos um bit do pacote.