República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 0823129-0 B1

(22) Data do Depósito: 27/10/2008

(45) Data de Concessão: 16/06/2020

(54) Título: METODO E SISTEMA PARA PERFILAGEM DE TRAFEGO DE COMUNICACÃO DE USUÁRIOS EM UMA REDE DE DADOS, E, REDE DE DADOS

(51) Int.Cl.: H04L 29/08.

(52) CPC: H04L 67/02; H04L 67/22; H04L 67/306.

(73) Titular(es): TELECOM ITALIA S.P.A..

(72) Inventor(es): MARIO ULLIO; EUGENIO MARIA MAFFIONE; ROBERTA MAGLIONE; ROBERTO PAGNIN.

(86) Pedido PCT: PCT EP2008064524 de 27/10/2008

(87) Publicação PCT: WO 2010/048980 de 06/05/2010

(85) Data do Início da Fase Nacional: 26/04/2011

(57) Resumo: "MÉTODO E SISTEMA PARA PERFILAGEM DE TRÁFEGO DE COMUNICAÇÃO DE USUÁRIOS EM UMA REDE DE DADOS, E, REDE DEDADOS" Um método de perfilagem de tráfego de comunicação de usuários em uma rede de dados (115), compreendendo: monitorar tráfego de comunicação originado por um usuário de um terminal de comunicação (105); atribuir ao usuário do terminal de comunicação um identificador de tráfego de usuário anônimo e único, onde o identificador de . tráfego de usuário é relacionado a um endereço de usuário atribuído ao terminal de comunicação na rede de dados, e onde o identificador de tráfego de usuário é adaptado para ser incluído no tráfego de comunicação em relação àquele usuário; comunicar o identificador de tráfego de usuário anônimo e único para o terminal do usuário e tendo o terminal de comunicação de usuário inclui o identificador de tráfego de usuário no tráfego de usuário, quando do recebimento de tráfego de comunicação incluindo o identificador de tráfego de usuário, obter um descritor do tráfego de comunicação útil recebido para descrever o tráfego detectado e pelo menos, temporariamente armazenar o descritor obtido; e perfilagem de usuário anônimo relacionado às atividades de comunicação do usuário com base nos descritores armazenados.

MÉTODO E SISTEMA PARA PERFILAGEM DE TRÁFEGO DE COMUNICAÇÃO DE USUÁRIOS EM UMA REDE DE DADOS, E, REDE DE DADOS

DESCRIÇÃO

Fundamentos da Invenção

Campo da Invenção

[001] A presente invenção se refere em geral ao campo das telecomunicações, mais particularmente às redes de dados. Especificamente, a presente invenção trata dos aspectos de monitoração de tráfego de dados, particularmente, embora não exclusivamente, em rede de dados de IP (Protocolo de Internet), para o propósito de perfilagem de usuários.

Discussão da técnica relacionada

[002] Perfilagem de tráfego de dados é útil de modo a ser capaz de oferecer serviços personalizados para usuários. Por exemplo, observando a rede de tráfego de dados correspondendo a um determinado usuário, um perfil dele pode ser criado, com base em que é possível enviar para o usuário anúncio personalizado, que pode ser incluída em estandartes das páginas da web exibidas através de um navegador da web, ou em janelas de pop-up; isto permite explorar as enormes potencialidades da internet navegando como um meio de anúncio extremamente potente.

[003] Através dos anos, provedores de conteúdo têm desenvolvido várias soluções para alcançar este objetivo, com base nas capacidades técnicas de tempo em tempo tornadas disponíveis pelos sistemas finais (clientes e servidores).

[004] Algumas soluções conhecidas são particularmente invasivas, conforme elas requerem a instalação de programas de aplicação específicos no terminal do usuário. Essas soluções têm tido pouco sucesso, principalmente devido a resistência dos usuários para instalar em seus softwares de terminal que podem ser considerados, embora não sejam, como

malware ou spyware.

[005] Outras soluções conhecidas exploram, para coletar informação útil para perfilagem de usuário, as interações do usuário com um ou mais servidores de provedores de conteúdo federado. Essas soluções são geralmente melhor aceitas pelos usuários, mas a quantidade de informação que elas podem fornecer é limitada, e somente a parte dos comportamentos do usuário pode ser acompanhado.

[006] Operadores de redes de telecomunicações (telecomunicação) e Provedores de Serviço de Conectividade de Internet (ISPs) estão em uma posição privilegiada comparada aos provedores de conteúdo, porque todos o tráfego de dados de um determinado usuário passa através deles.

[007] Recentemente, têm sido desenvolvidas técnicas que permitem a um operador de rede monitorar as atividades dos usuários em um nível de aplicação. Essas técnicas fazem uso de "Aparelhos de Internet " que analisam o tráfego passando por uma rede de telecomunicações e são capazes de produzir relatórios de estatísticas com análise detalhada no nível de aplicação, mesmo para cada usuário único. Todavia, essas técnicas não foram totalmente implantadas, em vista das restrições legais colocada nos operadores de telecomunicações, particularmente em conexão com questões de privacidade, que em muitos países proíbem um operador de redes de telecomunicações de associar aos usuários respectivos registros de suas atividades, como o tráfego de dados trocados. Por estas razões, este perfil do tráfego de dados do lado do operador não é frequentemente explorável.

[008] Um exemplo deste tipo de técnicas de perfilagem é dado em WO 2007/033097, que divulga métodos e sistemas de monitoração e controle de tráfego de comunicação que permitem controlar tráfego de comunicação sobre a internet com base na identidade de particulares usuários usando informação potencialmente volátil, tal como um endereço de IP dinamicamente atribuído. O sistema e método permitem a um controlador

personalizar serviços para os usuários sem a necessidade de o usuário fornece informação pessoal, tal como seu nome, endereço, e o similar, e sem a necessidade de ter programas de computador ou código instalado no computador do usuário. Um "aparelho de IP" necessita ser introduzido na rede, que monitora o tráfego ao nível de aplicação em relação à usuários únicos. Um módulo de análise de tráfego analisa o tráfego direcionado a partir dos clientes do usuário para os servidores da rede do ISP, e as respostas relacionadas. Em particular, a análise é feita nos protocolos (e.g., RADIUS, DHCP - Protocolo de Configuração de Hospedeiro Dinâmico) usada pelo ISP para autorizar o acesso do usuário à rede e para dinamicamente configurar o endereço de IP do terminal do usuário; com base na análise de protocolos, cada endereço de IP é associado com um cliente específico do ISP com base nas credenciais de acesso. O aparelho de IP é assim sendo capaz de estabelecer uma associação entre cada pacote de IP fluindo sobre a rede e um usuário específico, e assim sendo atualizar o perfil do usuário.

[009] US 5,948,061 divulga métodos e aparelhos para segmentar a entrega de anúncios sobre uma rede tal conforme as Estatísticas da Internet. são compiladas nas redes e usuários individuais e o uso das anúncios é acompanhado para permitir segmentação das anúncios de usuários individuais. Em resposta às solicitações de sítios afiliados, um servidor de anúncio transmite para as pessoas acessando a página de um sítio, um anúncio apropriado com base quando da perfilagem de usuários e redes. Um "Processo de Servidor de Anúncio" fornece serviços de perfilagem de usuário. Quando um usuário explorando um navegador acessa um "Sítio de Web Afiliado", a página de web endereçada contém uma referência para um banner de anúncio fornecido pelo Processo de Servidor de Anúncio. O banner de anúncio contém por sua vez um elo de comunicação para uma página de web de anúncio em um Sítio de Web do Anunciante, a ser exibida se e quando o usuário seleciona o banner de anúncio. Quando o navegador baixa o banner de anúncio, fornece

para a informação de Processo de Servidor de Anúncio incluindo o endereço de IP, um cookie (se o navegador está habilitado), o tipo e versão do navegador, o sistema operacional etc.; o Processos de Servidor de Anúncio analisa estes dados para perfil de usuário, e personaliza os banners de anuncio.

[0010] US 2008/0098220 divulga um método e sistema para monitorar usuários em uma ou mais rede de computadores, dissociar informação pessoalmente identificável a partir dos dados coletados, e armazená-las em um banco de dados tal que a privacidade dos usuários é protegida. O sistema inclui transações de monitoração em ambos um cliente e um servidor, coletar dados de transação de rede, e agregar os dados coletados no cliente e no servidor. O sistema recebe um identificador de usuário e o usa para criar um identificador anônimo. O identificador anônimo é então associado com uma ou mais transações de rede de computador do usuário. Os dados são armazenados por um dispositivo de coleta e então agregados a um servidor de banco de dados central através de uma rede de computador.

Sumário da Invenção

[0011] A Requerente acredita que soluções conhecidas para perfilagem dos usuários de redes de dados com base no tráfego que eles geram não são satisfatórias, por várias razões.

[0012] Em particular, a solução descrita em WO 2007/033097 não pode ser explorada em vários países porque contraria os regulamentos de privacidade existente, que proíbem a coleta de dados permitindo uma associação entre os dados pessoais do usuário e os dados que ele/ela troca.

[0013] A solução descrita em US 5,948,061 tem uma limitação na qual o Processo de Servidor de Anúncio é convocado somente pelo Sítio de Web Afiliado, assim sendo ele pode perfilar um usuário de modo limitado para seu acesso aos sítios de web afiliados, e não à qualquer web site. A informação obtida é assim sendo limitada, e a perfilagem do usuário é

bastante limitado.

[0014] A técnica divulgada in US 2008/0098220 é similar a outras soluções que extraem chaves anônimas a partir do tráfego de RADIUS e as explora para gerar dados relacionados à navegação de rede anônimos. O uso direto de dados de RADIUS pode trazer problemas de regulamento de privacidade para a implantação da solução em alguns países.

[0015] Um objetivo da presente invenção é fornecer uma solução melhorada para a perfilagem de usuários de redes de dados com base no tráfego de dados que eles geram, que não é afetado pelos problemas e limitações das soluções conhecidas na arte, particularmente em relação às questões de privacidade do usuário.

[0016] De acordo com um aspecto da presente invenção, um método de perfilagem de tráfego de comunicação de usuários em uma rede de dados é fornecido, o método compreendendo:

- monitorar tráfego de comunicação originado por um usuário de um terminal de comunicação;

- atribuir ao usuário do terminal de comunicação um identificador de tráfego de usuário anônimo e único, onde o identificador de tráfego de usuária está relacionado a um endereço de usuário atribuído ao terminal de comunicação na rede de dados, onde o identificador de tráfego de usuário é adaptado para ser no tráfego de comunicação em relação àquele usuário;

- comunicar o identificador de tráfego de usuário anônimo e único para o terminal do usuário e tendo o terminal de comunicação de usuário incluir o identificador de tráfego de usuário no tráfego de usuário,

- quando recebimento de tráfego de comunicação incluindo o identificador de tráfego de usuário, obter um descritor do tráfego de comunicação útil recebido para descrever o tráfego detectado e pelo menos, temporariamente armazenar o descritor obtido; e

- perfilagem de usuário anônimo relacionado às atividades de comunicação do usuário com base nos descritores armazenados.

[0017] O identificador de tráfego de usuário pode compreender um cookie adaptado para ser incluído no tráfego de comunicação gerado pelo e endereçado ao terminal do usuário.

[0018] A atribuição mencionada do identificador de tráfego de usuário pode compreender:

- quando do recebimento de tráfego de comunicação originado pelo terminal do usuário, avaliar se o tráfego de comunicação recebido inclui o identificador de tráfego de usuário, e, no caso negativo, gerar um identificador de tráfego de usuário anônimo e único para ser atribuído ao endereço de rede do terminal do usuário.

[0019] Quando do recebimento de tráfego de comunicação originado pelo terminal de usuário não incluindo o identificador de tráfego de usuário anônimo e único, o terminal do usuário pode ser solicitado a re-enviar o tráfego de comunicação para uma função de atribuição de identificador de tráfego de usuário. A função de atribuição de identificador de tráfego de usuário pode então gerar o identificador de tráfego de usuário único e incluí-lo em uma resposta enviada para o terminal do usuário, a resposta mencionada enviada para o terminal do usuário solicitando ao terminal do usuário para re-enviar o tráfego de comunicação incluindo o identificador de tráfego de usuário.

[0020] A solicitação mencionada ao terminal do usuário para re-enviar o tráfego de comunicação to um função de atribuição de identificador de tráfego de usuário pode incluir enviar para o terminal do usuário uma mensagem de 303 SEE OTHER HTTP incluindo um URL da função de atribuição do identificador de tráfego de usuário, e incluindo um URL original contido no tráfego de comunicação recebido proveniente do terminal do usuário.

[0021] A resposta mencionada enviada pela função de atribuição de identificador de tráfego de usuário para o terminal do usuário pode incluir uma solicitação para o terminal do usuário para re-enviar o tráfego de comunicação com a indicação de tráfego do usuário para a função de atribuição de identificador de tráfego de usuário.

[0022] Quando do recebimento a partir do terminal do usuário da resposta mencionada incluindo o identificador de tráfego de usuário, uma monitoração do tráfego de comunicação do usuário pode ser iniciada, e uma resposta adicional pode ser enviada para o terminal do usuário solicitando ao terminal do usuário re-enviar o tráfego de comunicação para a destinação original.

[0023] O descritor mencionado pode compreender um ou mais de: informação relacionada aos pontos finais envolvidos na transação, e informação sobre o tempo que a transação ocorreu.

[0024] A monitoração mencionada do tráfego de comunicação originado pelo usuário do terminal de comunicação pode incluir analisar os pacotes do tráfego de comunicação originados pelo terminal de usuário.

[0025] A construção mencionada de um perfil de usuário pode incluir construir uma lista de páginas da web acessadas pelo usuário em uma sessão de navegação de web.

[0026] De acordo com um outro aspecto da presente invenção, um sistema é fornecido para perfilagem de tráfego de comunicação de usuários em um rede de dados, o sistema compreendendo:

- uma função de monitoração adaptada para:

- monitorar tráfego de comunicação originado pelo ou endereçado a um terminal de comunicação de um usuário;

- avaliar se o tráfego de comunicação do usuário mencionado está sendo monitorado com base em um endereço de usuário na rede de dados e na inclusão no tráfego de comunicação do identificador de tráfego de

usuário anônimo e único; e

- ou solicitar ao terminal do usuário para re-enviar o tráfego de comunicação para uma função de atribuição de identificador de tráfego de usuário no caso que o tráfego de comunicação recebido não inclui o identificador de tráfego de usuário, ou extrair um descritor do tráfego de comunicação e causar pelo menos, armazenamento temporário dele e deixar o tráfego de comunicação atingir a destinação pretendida no caso que o tráfego de comunicação recebido inclui o identificador de tráfego do usuário;

onde a função de atribuição de identificador de tráfego de usuário é adaptada para;

- gerar o identificador de tráfego de usuário único;

- enviar uma resposta para o terminal do usuário incluindo o identificador de tráfego de usuário, a resposta mencionada solicitando ao terminal do usuário para re-enviar o tráfego de comunicação para a destinação original incluindo o identificador de tráfego de usuário.

[0027] O identificador de tráfego de usuário mencionado pode compreender um cookie.

[0028] Para os propósitos da presente invenção, por "identificador de tráfego de usuário anônimo e único" é pretendido um identificador que é de modo unívoco atribuído ao usuário, particularmente a seu terminal de comunicação, e mesmo mais particularmente a um endereço de rede atribuído a ele, tal um identificador sendo anônimo tanto quanto pessoal, dados sensitivos sobre o usuário que podem impactar questões de privacidade (e.g., o nome do usuário, endereço, dados contratuais) são considerados, e que é adaptado para ser incluído em todo tráfego de comunicação originado pelo ou endereçado para o usuário, a fim de ser rastreável monitorando o tráfego de comunicação de rede.

[0029] Graças a solução de acordo com as modalidades da presente invenção, é assegurado que os dados de perfilagem de usuário coletados por

um operador de rede em relação ao tráfego de dados originados por um usuário permanece de modo intrínseco anônimo, e é garantido que uma associação de um identificador de usuário único atribuído ao usuário para coletar os dados de perfilagem de usuário com informação sensível possível, pessoa do usuário (como o nome, endereço, dados de nascimento do usuário, etc.) e dados contratuais são evitados. A solução de acordo com a presente invenção assim sendo condiz com questões e regulamentos de privacidade.

[0030] Uma outra vantagem da solução de acordo com modalidades da presente invenção é que ela permite um total, perfilagem completo do tráfego de dados gerado por um usuário, sem necessidade da instalação de software dedicado no terminal do usuário.

Descrição breve dos desenhos

[0031] Esses e outros recursos e vantagens da presente invenção serão melhor entendidos através da leitura, em conjunto com os desenho anexados listados aqui abaixo, da seguinte descrição detalhada de alguma modalidade exemplar e não limitante dela . Nos desenhos:

Figura 1, de forma esquemática, mostra um cenário exemplar do uso de uma solução de acordo com uma modalidade da presente invenção, e uma arquitetura exemplara dele;

Figura 2 mostra, de forma esquemática, mas em maior detalhe a estrutura funcional d em um momento dos componentes da Figura 1;

Figura 3 mostra, de forma esquemática, mas em maior detalhe a estrutura funcional de um outro dos componentes da Figura 1 ;

Figura 4 mostra, de forma esquemática, mas em maior detalhe a estrutura funcional de ainda um outro dos componentes da Figura 1 ;

Figura 5, de forma esquemática, representa a operação de uma máquina de estado que, em uma modalidade da presente invenção, é implementada no componente da Figura 2;

Figura 6, de forma esquemática, mostra uma seqüência de

operação de acordo com uma modalidade da presente invenção.

Descrição Detalhada das Modalidades da Invenção

[0032] Na discussão a seguir, uma solução de acordo com modalidades exemplares e não limitantes da presente invenção será apresentada e descrita em detalhe. Aqueles com habilidade na técnica vão, contudo, reconhecer que várias modificações para as modalidades descritas são possíveis, e que a presente invenção pode ser incorporada em maneiras diferentes.

[0033] Em particular, o cenário de uso aqui considerado à título de exemplo, e representado na figura 1, é aquele de um usuário que tem um terminal de processamento de dados do usuário 105 possibilitando ao usuário se comunicar através de uma rede de dados, particularmente uma rede de IP, e que, explorando os serviços de um provedor de serviço de conectividade de rede 110, por exemplo um ISP, pode se conectar (por exemplo usando um portão de passagem de acesso ou um modem de discagem) a uma rede de dados, como a Internet 115, e/ou a qualquer outra rede de dados, como por exemplo WANs (Redes de Área Ampla) abertas. O ISP pode ser ou pertencer a uma companhia de telecomunicações/telefone, por exemplo um operador de telecomunicações/telefonia virtual (i.e. uma companhia que fornece serviço de telefonia mas não tem sua própria alocação de freqüência licenciada do espectro de rádio, nem necessariamente tem toda a infra-estrutura requerida para fornecer serviço de terminal móvel de telefonia, e que re-vende pra os clientes, os serviços de telefonia trazidos de uma outra companhia de telecomunicações/telefonia).

[0034] No cenário exemplar aqui considerado, a solução de acordo com uma modalidade da presente invenção é explorada para monitorar o tráfego de Internet (IP) enviado pelo ISP 110 em relação à seus usuários assinantes. O tráfego de IP pode ser totalmente ou pelo menos, parcialmente gravado, por exemplo, para um período de tempo limitado, para facilitar o

tráfego de IP análise é direcionada para derivar informação sobre os hábitos/comportamento do usuário, e.g., suas atividades de navegação de web, e a informação derivada pode ser usada para perfilagem de usuário. O perfil de usuário pode então ser explorada para fornecer/oferecer os serviços personalizados de usuário, como enviar mensagens de anúncio relacionados ao usuário.

[0035] Um sistema de acordo com uma modalidade da presente invenção compreende um componente de monitoração 120, um componente de imposição de presença 125 e um componente de acompanhamento 130, que em operação cooperam cada um com o outro. Esses três componentes podem ser parte de um sistema único, co-localizado em uma mesma posição física, ou um ou mais deles pode ser distribuído em diferentes posições, dependendo nas necessidades/preferências do ISP 110. Um ou mais desses componentes podem mesmo ser possuídos por uma parte diferente a partir do ISP (isto é o cenário considerado na figura 1, onde o componente de imposição de presença 125 e um componente de acompanhamento 130 são representados como externo ao ISP 110).

[0036] As funções individuais e as interações entre os componentes 120, 125 e 130 são descritos em detalhes daqui em diante.

[0037] Como, de forma esquemática, representado na figura 2, o componente de monitoração 120 essencialmente compreende quatro funcionalidades: uma funcionalidade de inspeção profunda de pacote 205, incluindo uma funcionalidade de re-direção 215, uma funcionalidade de gerenciamento de acompanhamento 210, e uma funcionalidade de notificação de acompanhamento 220.

[0038] A funcionalidade de inspeção profunda de pacote 205 é adaptada para analisar profundamente tráfego de rede, particularmente pacotes de dados 230, para reconhecer protocolos de transmissão (pertencendo a um pré-determinado catalogo de protocolos de transmissão), e

para reconhecer padrões, dentro de um ou mais pacotes de dados, que correspondem a tais protocolos. Os pacotes de dados 230 são analisados não somente em relação a seus cabeçalhos, mas também em relação à seu corpo ou carga útil.

[0039] A funcionalidade de inspeção profunda de pacote 205 é assumida para ser capaz de analisar o tráfego e ser capaz de redirecionar (explorando a funcionalidade de redirecionamento 215) os pacotes de dados analisados para outras funcionalidades do componente de monitoração 120.

[0040] A funcionalidade de gerenciamento de acompanhamento 210 é adaptada para gerenciar o acompanhamento dos usuários em relação à suas atividades de comunicação na rede de dados, e.g. atividade de navegação na web; de acordo com uma modalidade da presente invenção, a funcionalidade de gerenciamento de acompanhamento 210 acompanha as atividades dos usuários explorando uma método de máquina de estado finito, cujos estados representam diferentes situações de monitoração de tráfego de rede, e onde as transições entre estados são acionados por eventos de tráfego como, por exemplo, o começo de um fluxo de tráfego, a existência de informação de presença relacionada ao usuário (discutido em detalhe na discussão a seguir), o decorrer de um tempo limite ou mudanças significativas no fluxo de tráfego.

[0041] A funcionalidade de gerenciamento de acompanhamento 210 faz uso de um banco de dados, por exemplo, na forma de uma tabela 235, que é mantida constantemente atualizada pela máquina de estado durante o processamento de eventos. Em uma modalidade da presente invenção, a tabela 235 compreende várias entradas, uma em relação à cada usuário cujas atividades estão para serem monitoradas. Em cada entrada, um campo de tabela 240 é fornecido, adaptado para armazenar um endereço IP correspondendo a um usuário que está conectado à rede; associada com o campo 240 é um campo 245 adaptado para armazenar uma informação de presença; associada com os campos 240 e 245 é um campo adicional 250

adaptado para armazenar uma indicação do estado de acompanhamento daquele usuário, i.e. de se aquele usuário está sendo acompanhado ou não (conforme descrito na discussão a seguir).

[0042] A funcionalidade de redirecionamento 215 é adaptada para re-direcionar, com base em regras específicas e pré-determinadas (que podem tomar a forma de parâmetros), mensagens específicas (recebidas como pacotes de dados 230) que forma identificados por uma funcionalidade de inspeção profunda de pacote 205, explorando as características do protocolo de transmissão considerado, ou para desviar um inteiro fluxo de tráfego de pacotes (tipicamente, um re-direcionamento é uma operação efetuada com base no reconhecimento de uma mensagem, ao passo que uma operação de desvio é efetuado com base no reconhecimento do fluxo de dados). Re-direcionamento de mensagens específicas pode, por exemplo, ser realizado, no caso do HTTP (Protocolo de Transferência de Hiper Texto), por meio da mensagem *303 SEE OTHER*, que permite um servidor de web/HTTP, quando do recebimento de um cliente (o navegador de web executando em um terminal do usuário) de uma solicitação de uma página de web ou de HTML (Linguagem de Marcação de Hiper Texto), re-direcionar o cliente em direção a um outro servidor de web (tendo um diferente URL – Localização de Recursos Uniforme). De acordo com uma modalidade da presente invenção, o re-direcionamento das mensagens específicas é feito para recompensar o componente de imposição de presença 125, dedicado à monitoração/acompanhamento do tráfego do usuário, conforme descrito na seguinte.

[0043] A funcionalidade de notificação de acompanhamento 220 é adaptado para emitir notificações considerando o reconhecimento de uma padrão pesquisado dentro de um pacote de dados recebido 230. As notificações podem ser emitidas ao componente de acompanhamento 130. Em uma modalidade da presente invenção, a funcionalidade de notificação de

acompanhamento 220 emite a notificação enviando um descritor da porção de tráfego de dados compreendendo o padrão reconhecido pela funcionalidade de inspeção profunda de pacote 205; o descritor pode incluir informação de presença relacionada ao usuário univocamente relacionada ao usuário a ser acompanhado, como discutido em sua estrutura, a fim de ser condizente com outros sistemas (como sistemas dedicados à monitoração/acompanhamento do tráfego de usuário e/ou a entrega de anúncio) e com restrições legais de privacidade que podem variar de país a país.

[0044] O componente de monitoração 120 pode tomar a forma de um aparelho de Internet, adaptado para ser inserido na rede de pacote de dados 110 da companhia de ISP/telecomunicações, por exemplo em um ponto da rede escolhido com base em uma negociação entre os requisitos de monitoração de tráfego e dimensionamento do sistema. Por exemplo, considerando a rede de um operador de telecomunicações de tamanho significativo, o componente de monitoração 120 pode estar localizado nos Pontos de Presença (PoP), no fluxo de descida em relação aos dispositivos de NAS (Serviço de Acesso de Rede) que controlam o acesso da rede.

[0045] Em uma modalidade da presente invenção, o componente de imposição de presença 125 compreende, como, de forma esquemática, representado na figura 3, uma funcionalidade de injeção 305 e uma funcionalidade de redirecionamento 310.

[0046] A funcionalidade de injeção 305 é adaptado para gerar e inserir, no tráfego de rede relacionado a um determinado usuário, informação relacionada àquele usuário a fim de marcar o tráfego de dados de usuários específicos em uma maneira que é univocamente relacionada a ele; em particular, a marcação de tráfego de dados é alcançada por meio de informação de presença relacionada ao usuário univocamente relacionada àquele usuário. A informação de presença relacionada ao usuário forma a entidade de agregação entre um aglomerado de tráfego de dados (um pacote

de dados 230) recebido a partir do componente de monitoração 120, ou a partir do terminal do usuário 105, e os aglomerados de tráfego de dados subseqüentemente acompanhado pelo componente de monitoração. A informação de presença relacionada ao usuário é usada como uma referência para acompanhar o tráfego de rede gerado por aquele usuário naquela sessão. A informação de presença relacionada ao usuário é anônima, porque não contém referencia para dados que podem conduzir a informação de pessoal do usuário (como o nome, dados de nascimento, endereço etc.).

[0047] De acordo com uma modalidade exemplar da presente invenção, considerando o caso de atividades de navegação da web, a informação de presença relacionada ao usuário pode compreender um cookie que o componente de imposição de presença 125 univocamente atribui a um determinado usuário. Como conhecido na técnica, cookies (também referido como cookies de HTTP, ou cookies de web), são parcelas de texto enviadas por um servidor de HTTP para um cliente de web (um navegador) e então enviado de volta não mudado pelo cliente cada vez que ele acessa aquele servidor. Um servidor de HTTP que recebe uma solicitação de um cliente (um navegador de web) pode inserir um cookie (set_cookie) na resposta enviada para o cliente, tal que, nas transações sucessivas com servidores do mesmo domínio do servidor que inseriu o cookie, o cliente inclui o cookie nas solicitações enviadas para tais outros servidores; o último, reconhecendo a presença do cookie na solicitação, será capaz de avaliar que o cliente considerado já apresentou a si mesmo para um dos servidores do domínio, e pode processar a informação. De acordo com uma modalidade da presente invenção, o componente de imposição de presença 125 atribui aos usuários cookies de informação de presença unívoca, e envia os cookies de informação de presença atribuídos para os navegadores de web dos usuários; os cookies de presença de texto são armazenados localmente no terminal do usuário 105, e o navegador de web do usuário inclui o cookie de informação de presença

nas subseqüentes solicitações, tal que o cookie de informação de presença pode ser reconhecido e processado pelo sistema de monitoração.

[0048] A funcionalidade de redirecionamento 310 é adaptada para re-direcionar as mensagens específicas em direção a sua destinação original (que meios, e.g. para HTTP, o URL solicitado original), ou em direção ao componente de imposição de presença 125 de modo a permitir o acompanhamento do tráfego de rede relacionado ao usuário.

[0049] Em uma modalidade da presente invenção, o componente de imposição de presença 125 compreende um software de aplicação instalado e executando em um servidor, por exemplo, considerando tráfego de HTTP, um servidor web executando uma aplicação de web pode ser usada.

[0050] De acordo com uma modalidade da presente invenção, o componente de acompanhamento 130 compreende, como, de forma esquemática, representado na figura 4, uma funcionalidade de armazenamento de notificação 405 adaptada para gerenciar o armazenamento de notificações recebido a partir do componente de monitoração 120, particularmente a partir de uma funcionalidade de notificação de acompanhamento 220. A funcionalidade de armazenamento 405 é projetada para armazenar as notificações em um arquivo estruturado 410, por exemplo um banco de dados relacional. Em particular, a funcionalidade de armazenamento de notificação 405 armazena no arquivo 410 a informação incluída no descrito de notificação que a funcionalidade de notificação de acompanhamento 220 do componente de monitoração 120 envia para o componente de acompanhamento 130 cada vez que o componente de monitoração 120 detecta pacotes de tráfego 230 em relação à um usuário cujas atividades estão sendo acompanhadas.

[0051] A informação de presença relacionada ao usuário incluída no descritor de notificação é explorada para agregar uma informação incluída na notificação recebida a partir do componente de monitoração 120 com dados já

armazenados no banco de dados 410, assegurando que os usuários são mantidos anônimos. A agregação, no banco de dados 410, de informação relacionado ao tráfego de rede gerado por um determinado usuário é útil para permitir processamento da informação sobre as atividades/comportamentos de usuário, em um ou mais intervalos de tempo, que pode ser configurável, a fim de perfilagem de usuário. Por exemplo, considerando a atividade de navegação de sítios de web, é possível definir a "seqüência de clique", i.e., a seqüência de "clique" feita pelo usuário, analisando a seqüência de sítios de web visitados; isto permite determinar os interesses do usuário. Com base no perfil de usuário assim sendo construído, o componente de acompanhamento 130, e/ou outro componentes (sistemas de mineração de dados, sistemas de inteligência de negócios), possivelmente externos ao sistema de monitoração da modalidade de invenção descrita, pode oferecer/propor serviços personalizados.

[0052] Em uma modalidade da presente invenção, o componente de acompanhamento 130 pode compreender um software de aplicação instalado e executando em um servidor.

[0053] A operação do sistema de acordo com a presente invenção é agora descrita. Tráfego bi-direcional de dados proveniente de/para o terminal do usuário 105 flui através do componente de monitoração 120. O componente de monitoração 120 ou deixa o tráfego de dados atingir a destinação pretendida (Internet 115, terminal do usuário 105), ou o re-direciona para o componente de imposição de presença 125 (por meios de uma funcionalidade de redirecionamento 215).

[0054] O componente de monitoração 120 gerencia o estado de tráfego de monitoração para cada endereço de IP acompanhado na tabela 235, que é mantido constantemente atualizado com base na fase de monitoração do tráfego gerado por aquele endereço de IP. No começo, a ausência de tráfego em relação àquele endereço de IP corresponde à ausência de qualquer entrada

na tabela 235 correspondendo a tal um endereço de IP. A funcionalidade de inspeção profunda de pacote 205 inspeciona o conteúdo dos pacotes de dados recebidos. A primeira vez que tráfego condizente com as regras de filtragem configuradas (regras que podem ser configuradas em uma funcionalidade de inspeção profunda de pacote 205 útil para reconhecer um fluxo de tráfego específico, e.g. para detectar mensagens de HTTP, e para conseqüentemente reagir, por exemplo redirecionando as mensagens) é detectado para aquele endereço de IP, a funcionalidade de gerenciamento de acompanhamento 210 do componente de monitoração 120 cria uma entrada na tabela 235 e coloca na entrada mais recentemente criada, o endereço de IP da entidade (o terminal do usuário 105) que originou o tráfego. A funcionalidade de gerenciamento de acompanhamento 210 também configura, no campo 250 da tabela 235 correspondendo à entrada recentemente criada, o estado de monitoração de corrente daquele usuário, por exemplo, de acordo com o que foi aqui descrito.

[0055] De acordo com uma modalidade da presente invenção, o gerenciamento de acompanhamento efetuado pelo componente de monitoração 120 em relação à cada usuário (visto como um endereço IP) é com base em um modelo de máquina de estado finito. Referindo à Figura 5, um diagrama de transição de estado para um usuário genérico é pictoricamente mostrado. Os estados e os eventos causando transições entre estados são aqui descritos mais tarde. Cada um dos diferentes estados corresponde a um diferente estado de monitoração configurado pela funcionalidade de gerenciamento de acompanhamento 210 no campo 250 da tabela 235.

[0056] O estado "Inativo" 505 é o estado padrão, i.e., o estado de um usuário cujo tráfego não é considerado, i.e. não monitorado pelo sistema de monitoração.

[0057] Quando, com base nas regras especificadas para a operação do componente de monitoração 120, o tráfego do usuário considerado (visto

como um endereço de IP) tem de ser monitorado, o estado de monitoração do usuário muda para o estado "Ativo" 510. As regras podem, por exemplo, especificar que, para o usuário considerado, a monitoração do tráfego relacionado a ele é para ser ativado em um base no tempo.

[0058] O estado "Ativo" 510 é o estado no qual o sistema de monitoração monitora o tráfego relacionado ao usuário considerado; quando o componente de monitoração 120 detecta tráfego de usuário condizendo com as regras de filtragem especificadas, o estado de monitoração de usuário muda para o estado "Capturado" 515, e o endereço de IP do usuário é colocado na tabela 235.

[0059] No estado "Capturado" 515, se o componente de monitoração 120 detecta que o tráfego de usuário não inclui a informação de presença relacionada ao usuário, o componente de monitoração 120 redireciona o tráfego relacionado ao usuário considerado em direção ao componente de imposição de presença 125; o componente de imposição de presença 125 atribui ao usuário a respectiva informação de presença relacionada ao usuário e a comunica para o terminal do usuário 105, que subseqüentemente inclui a informação de presença relacionada ao usuário em sua solicitação, como explicado na discussão a seguir. O estado de monitoração de usuário permanece "Capturado" até o componente de monitoração 120 detecta tráfego de usuário compreendendo a informação de presença relacionada ao usuário. Quando o componente de monitoração 120 detecta tráfego de usuário compreendendo a informação de presença relacionada ao usuário, o estado de monitoração de usuário muda para o estado "Acompanhado" 520; o componente de monitoração 120 armazena na tabela 235 a informação de presença relacionada ao usuário, em associação com o endereço de IP do usuário.

[0060] Quando no estado "Acompanhado" 520, sempre que o tráfego é detectado, a funcionalidade de notificação de acompanhamento 220 do

componente de monitoração 120 envia para o componente de acompanhamento 130 uma notificação incluindo um descritor. A notificação é recebida pelo componente de acompanhamento 130, que explora a informação de presença relacionada ao usuário incluído no descritor para agregar a informação incluída na notificação recebida com dados já armazenados no banco de dados 410. Os dados armazenados no banco de dados 410 são úteis para perfilagem de usuário.

[0061] A passagem a partir do estado "Acompanhado" 520 para o estado "Inativo" 505 pode acontecer de acordo com o que foi prescrito pelas regras especificada para a operação do componente de monitoração 120 (e.g., em uma base no tempo).

[0062] Essencialmente, durante sua operação normal a funcionalidade de inspeção profunda de pacote 205 do componente de monitoração 120 analisa o tráfego de rede relacionada aos protocolos selecionados e vindo dos endereços de IP gerenciado internamente ao ISP 110 (i.e., endereços de IP que o operador de telecomunicação atribui estática ou dinamicamente, para seus assinantes; assim sendo a monitoração, no exemplo considerado,, considera os assinantes do operador de telecomunicações considerados).

[0063] Quando a funcionalidade de inspeção profunda de pacote 205 do componente de monitoração 120 detecta, em um pacote de dados entrante, um padrão selecionado e configurado como um daqueles "a serem reconhecidos", a funcionalidade de gerenciamento de acompanhamento 210 do componente de monitoração 120 procura na tabela 235 e verifica (procurando o conteúdo do campo 250 da tabela 235) se o endereço de IP no pacote de dados enviado pelo emitente está ou não sob acompanhamento. No caso afirmativo, i.e. se a funcionalidade de gerenciamento de acompanhamento 210 do componente de monitoração 120 avalia que o endereço de IP considerado está já sendo acompanhado, o pacote de dados é deixado fluir em direção a sua destinação pretendida, e a funcionalidade de

notificação de acompanhamento 220 do componente de monitoração 120 envia um descritor de pacote de dados para o componente de acompanhamento 130, que armazena os dados contidos no descritor recebido no banco de dados 410. No caso negativo, i.e. se a funcionalidade de notificação de acompanhamento 220 do componente de monitoração 120 avalia que o endereço de IP considerado não está ainda sob acompanhamento, a funcionalidade de redirecionamento 215 do componente de monitoração 120 pergunta (o cliente executando) o terminal do usuário 105 para redirecionar o pacote de dados em direção ao componente de imposição de presença 125, a fim de causar o usuário para apresentá-lo ao componente de imposição de presença 125.

[0064] Quando o componente de imposição de presença 125 recebe os pacotes de dados redirecionados a ele pelo terminal do usuário 105, o componente de imposição de presença 125 atribui àquele usuário informação de presença unívoca relacionada ao usuário, e injeta, i.e. a insere em uma resposta enviada para o terminal do usuário 105.

[0065] O cliente executando o terminal do usuário 105 recebe a resposta enviada pelo componente de imposição de presença 125, que solicita ao terminal do usuário para redireciona seu tráfego em direção ao componente de imposição de presença 125, desta vez incluindo a informação de presença relacionada ao usuário atribuída e comunicada a ele pelo componente de imposição de presença 125. O tráfego de dados redirecionado a partir do terminal do usuário para o componente de imposição de presença 125 é visto pelo componente de monitoração 120, que pega a informação de presença relacionada ao usuário incluída no pacote de dados recebido e a coloca no campo 245 da tabela 235, a fim de começar o acompanhamento das atividades do usuário.

[0066] O componente de monitoração 120 também gera e notifica para o componente de acompanhamento 130 um descritor do pacote de dados

recebido.

[0067] O componente de imposição de presença 125 então envia para o terminal do usuário 105 uma nova solicitação de redirecionamento, perguntando ao terminal do usuário 105 para redirecionar a solicitação para a destinação original.

[0068] Subseqüentemente, cada vez que o componente de monitoração 120 detecta tráfego de dados gerado por aquele usuário que condiz com as regras de acompanhamento configuradas, o componente de monitoração 120 gera e envia para o componente de acompanhamento 130 uma notificação com um descritor. Usando os descritores incluídos nas notificações recebidas provenientes do componente de monitoração 120, o componente de acompanhamento 130 progressivamente povoa o banco de dados 410, onde a informação incluída nos descritores recebidos é agregada à informação já presente explorando a informação de presença relacionada ao usuário. Por exemplo, considerando a atividade de navegação na web, a agregação de informação no banco de dados 410 permite construir a "seqüência de clique" do usuário, i.e. a seqüência de sítio da web visitados pelo usuário (com base na seqüência de clique, o interesse do usuário pode por exemplo ser deduzido, enquanto mantendo o usuário anônimo).

[0069] O descritor incluído na notificação enviada pela funcionalidade de notificação de acompanhamento 220 do componente de monitoração 120 para o componente de acompanhamento 130 contém dados úteis para descrever o aglomerado de tráfego detectado; tais dados podem por exemplo se relacionar aos pontos finais (e.g., no contexto de navegação de Web/HTTP, o navegador de Web do usuário - o cliente - e o servidor de Web contatado) envolvido na transação, e para o tempo que a transação ocorreu. Por exemplo, como discutido no precedente, o acompanhamento da atividade de navegação na web do usuário pode prover para enviar descritores contendo, como a informação de presença relacionada ao usuário, o cookie de

informação de presença atribuído pelo componente de imposição de presença 125 ao usuário (e que, após ter sido recebido pelo navegador de usuário, será incluído no tráfego de HTTP relacionado àquele usuário), o endereço de IP do usuário, o hospedeiro de destinação, o URL completo, o agente do usuário (i.e., o navegador de web executando no terminal do usuário 105), marca de tempo da solicitação pelo usuário.

[0070] Na discussão a seguir, um cenário de aplicação exemplar de uma modalidade da presente invenção será descrito, relacionando ao acompanhamento de atividade de navegação na web feita pelos usuários conectados à Internet através de pontos de acesso de um ISP genérico (como o ISP 110). Os usuários podem explorar, como terminais de usuário 105, qualquer tipo de terminal de processamento/comunicação de dados, como computadores pessoais, PDAs (Assistentes Digitais Pessoais), telefones inteligentes, capaz de conectar à Internet ou diretamente ou através de outras, redes interconectadas (como por exemplo uma rede de telefonia de terminal móvel). O terminal do usuário 105 pode ser conectado à rede de ISP 110 através de conexão ou com fio ou sem fio. Quando o usuário considerado acessa sítios da web, ele/ela gera tráfico de rede. O propósito do acompanhamento das atividades de usuário pode por exemplo ser aquele de acompanhar, de forma em anonimato, os sítios de web visitado pelos usuários, a fim de derivar uma "seqüência de clique", i.e. a seqüência de sítios de web visitados (em um período de tempo de observação). O sistema tem uma arquitetura distribuída, e o componente de monitoração 120 pode estar localizado em um ponto da rede de ISP 110 caracterizado por um alto grau de agregação de tráfego a fim de alcançar uma boa negociação entre quantidade de tráfego gerenciado, recursos explorados e dimensionamento do sistema de monitoração. Geralmente, a rede de um ISP é caracterizada por um grau crescente de agregação de tráfego enquanto se movendo a partir da periferia dela (a rede de acesso) em direção ao núcleo de rede (estrutura de rede): o

componente de monitoração 120 pode ser localizado em um ponto da rede de ISP 110 que está relativamente perto da rede núcleo. O componente de monitoração 120 é configurado para monitorar tráfego de web (i.e., tráfego com base no HTTP) gerado por um conjunto de endereço de IP, a monitoração pode ser ativada/desativada em uma base no tempo (por exemplo, através de um gerenciador de política).

[0071] Figura 6, de forma esquemática, mostra as interações entre os componentes durante sua operação normal.

[0072] Quando o componente de monitoração 120 detecta tráfego de web, tipicamente uma solicitação de página de web tomando a forma de uma mensagem de HTTP GET (interação 1) em relação à um URL específico vindo do terminal do usuário 105, o componente de monitoração 120 verifica na tabela 235 se o endereço de IP daquele usuário está presente, e o tráfego daquele usuário já está sob monitoração (interação 2) (i.e., o estado de monitoração de usuário é "Ativo", "Capturado" ou "Acompanhado"). Assumindo, conforme mostrado na figura 6, que o componente de monitoração 120 não acha o endereço de IP do usuário na tabela 235 (i.e., o estado de monitoração de usuário está "Inativo"), mas as regras governando o comportamento do componente de monitoração 120 prescreve que o tráfego é para ser monitorado, o componente de monitoração 120 pergunta ao terminal do usuário 105 para apresentar a si próprio para o componente de imposição de presença 125 (interação 3); por exemplo, o componente de monitoração 120 pode para este propósito enviar para o terminal do usuário 105 a mensagem de 303 SEE OTHER HTTP com o cabeçalho "Localização" configurado para o valor do URL do componente de imposição de presença 125; o URL original que foi incluído na mensagem de HTTP GET recebida proveniente do terminal do usuário 105 é colocado na mensagem de 303 SEE OTHER HTTP como um ou mais parâmetros, onde permanece até que o sistema subseqüentemente solicita ao terminal do usuário 105 para re-emitir a

solicitação de interação com aquele URL original. O componente de monitoração 120 também adiciona para a tabela 235 o endereço de IP do usuário, extraído a partir da mensagem de HTTP GET original (o estado de monitoração de usuário, inicialmente "Inativo", passa para o estado "Ativo"). Se em vez disso o usuário já está no estado "Acompanhado" (i.e., o endereço de IP do usuário e a informação de presença relacionada ao usuário já estão presentes na tabela 235), o componente de monitoração 120 deixa o fluxo de tráfego em direção a destinação pretendida (e envia uma notificação para o componente de acompanhamento 130).

[0073] Quando do recebimento da mensagem de 303 SEE OTHER HTTP proveniente do componente de monitoração 120, o terminal do usuário 105 emite uma mensagem de HTTP GET endereçada ao componente de imposição de presença 125 (interação 4). A nova mensagem de HTTP GET enviada pelo terminal do usuário 105 também inclui, como um ou mais parâmetros, o URL que foi incluído na solicitação de página de web original.

[0074] Monitorar o tráfego de HTTP relacionado ao endereço de IP do usuário, o componente de monitoração 120 verifica se a mensagem de HTTP GET enviada pelo terminal do usuário 105 para o componente de imposição de presença 125 contém a informação de presença relacionada ao usuário (i.e., no exemplo considerado, o cookie de informação de presença) (interação 5). Já que neste momento ao terminal do usuário 105 ainda não foi atribuído e comunicado o cookie de informação de presença (o cookie de informação de presença pode estar ausente no terminal do usuário 105 na ativação do sistema de monitoração, ou após uma eliminação de um cookie anteriormente comunicado forçado pelo usuário), o último não está incluído na mensagem de HTTP GET endereçada ao componente de imposição de presença 125. O componente de monitoração 120 assim sendo deixa o fluxo de mensagem de HTTP GET para o componente de imposição de presença 125 (interação 6).

[0075] Quando do recebimento da mensagem de HTTP GET proveniente do terminal do usuário 105, o componente de imposição de presença 125 verifica para a presença de um cookie de informação de presença oficial para seu domínio. Um cookie de informação de presença (constituindo a informação de presença relacionada ao usuário) oficial para o domínio do componente de imposição de presença 125 é, no protocolo de HTTP, um cookie oficial para um domínio somente, sendo o domínio aquele ao qual o servidor de HTTP que primeiramente liberou o cookie pertence; nesta modalidade da invenção, já que o cookie de informação de presença está liberado pelo componente de imposição de presença 125, o cookie é oficial para o domínio ao qual o componente de imposição de presença 125 pertence. No caso de tal um cookie de informação de presença não é incluída na mensagem de HTTP GET recebida, o componente de imposição de presença 125 responde para o terminal do usuário 105 com uma mensagem de 303 SEE OTHER HTTP, inserindo nele um novo cookie de informação de presença para aquele usuário (interação 7), e configurar em uma mensagem o cabeçalho "Localização" igual ao URL do componente de imposição de presença 125. Em outras palavras, já que o navegador de web executando o terminal do usuário 105 não tem localmente o cookie de informação de presença e não pode incluí-lo nas solicitações que ele emite, o componente de imposição de presença 125 força uma re-direção em sua própria direção, tal que o componente de monitoração 120 pode acompanhar a interação, capturar o cookie de informação de presença e configura o começo da fase de acompanhamento.

[0076] Quando do recebimento da mensagem de 303 SEE OTHER HTTP a partir do componente de imposição de presença 125 incluindo o cookie de informação de presença, o navegador de web executando no terminal do usuário 105 localmente armazena o cookie de informação de presença incluído na mensagem recebida, e emite uma nova solicitação de

página de web (mensagem de HTTP GET), endereçando-a ao URL presente no cabeçalho "Localização" da mensagem (interação 8), i.e. para o componente de imposição de presença 125.

[0077] A nova mensagem de HTTP GET enviada pelo terminal do usuário 105, endereçado ao componente de imposição de presença 125 e esta vez incluindo o cookie de informação de presença, é acompanhado pelo componente de monitoração 120 (interação 9), que procura pelo cookie de informação de presença na mensagem de HTTP GET. Achando o cookie, o componente de monitoração 120 o extrai a partir de uma mensagem e o armazena na tabela 235 em associação com o endereço de IP do usuário, e ainda muda o estado do usuário para "Acompanhado". O componente de monitoração 120 então gera e envia para o componente de acompanhamento 130 uma notificação "iniciar acompanhamento" incluindo um descritor do URL do componente de imposição de presença 125 (interação 10). O componente de acompanhamento 130 armazena o descritor recebido no banco de dados 410. O componente de monitoração 120 então deixa o fluxo de solicitação de página da web em direção a sua destinação que é o componente de imposição de presença 125 (interação 11).

[0078] O componente de imposição de presença 125 recebe a mensagem de GET HTTP e responde com uma mensagem de 303 SEE OTHER HTTP adicional (interação 12), com o cabeçalho de "Localização" configurado igual ao URL originalmente solicitado, e assim sendo acionando um solicitação de página de web emitido pelo terminal do usuário 105 para o URL originalmente solicitado URL (interação 13); esta nova solicitação é acompanhada pelo componente de monitoração 120 na maneira descrita acima (interações14 e 15), e o componente de monitoração 120 deixa a solicitação fluir em direção sua destinação original (interação 16).

[0079] Subseqüente solicitações de página (mensagens de HTTP GET) a partir do terminal do usuário 105 inclui o cookie de informação de

presença, e são monitoradas de modo transparente pelo componente de monitoração 120, que gera e notifica os descritores relacionadas ao componente de acompanhamento 130; o componente de acompanhamento 130 agrega os descritores recebidos no banco de dados 410 com base na informação de presença relacionada ao usuário (cookie de informação de presença) anteriormente armazenada, e por meio disso, criar uma seqüência de clique do usuário, por exemplo para um pré-determinado, fixo ou tempo de observação configurável. O componente de monitoração 120 ainda deixa as solicitações de página de web a partir do terminal do usuário 105 fluir em direção a sua destinação.

[0080] Preferencialmente, de modo a aumentar o nível de privacidade, o componente de acompanhamento 130 descarta o valor do endereço de IP do usuário a partir do descritor recebido a partir do componente de monitoração 120 (somente a formação de presença relacionada ao usuário é explorado para identificar aquele usuário). Isto melhora o nível de anonimato da informação armazenada, porque não há elo de comunicação entre eles e o usuário. Neste respeito, é observado que endereços de IP são usualmente atribuídos aos usuários dinamicamente, i.e. eles tipicamente mudam de sessão para sessão, mas também no caso de uma atribuição de IP estático, o endereço de IP sozinho não inequivocamente identifica um sujeito único, ao menos que o endereço de IP é correlacionado a outra informação de pessoal do usuário.

[0081] No cenário de aplicação exemplar descrito acima, todas as interações entre os diferentes componentes (terminal do usuário, componente de monitoração, componente de imposição de presença, componente de acompanhamento) são condizente com o HTTP, incluído o gerenciamento do cookie de presença.

[0082] A sessão de acompanhamento pode corresponder a um período de tempo de observação (tempo de acompanhamento), configurável no componente de monitoração e no componente de acompanhamento, durante

que o tráfego de HTTP de um usuário conectado à rede de ISP é acompanhado. O tempo de acompanhamento pode ser igual à ou maior do que um tempo limite decorrido que é assumido que o usuário acabou de gerar tráfico. O decorrer do tempo limite causa a remoção da entrada com o endereço de IP do usuário a partir da tabela 235 do componente de monitoração 120.

[0083] Deve um histórico das seqüências de clique diferentes de um determinado usuário ser armazenado em vez de ser eliminado após a respectiva sessão de acompanhamento, o cookie de informação de presença forma o elo de comunicação entre os dados inerentes às seqüência de clique diferentes daquele usuário. Esta possibilidade de agregar múltiplos dados permite uma perfilagem mais eficiente e refinado dos usuários. Também, diferentes usuários, embora compartilhando um mesmo endereço de IP, são discriminados com base na informação de presença relacionada ao usuário.

[0084] A solução de acordo com a presente invenção, particularmente o componente de monitoração 120, o componente de imposição de presença 125 e o componente de acompanhamento 130, podem ser implementados em software, em hardware ou parcialmente em software e parcialmente in hardware.

[0085] A solução de acordo com a presente invenção é útil para coletar informação de tráfego de dados de rede gerado por um usuário para o propósito de estabelecer um perfil de usuário, por exemplo, mas não de modo limitado, para enviar ao usuário anúncio adequado e/ou sugestões de compra/aluguel.

[0086] A localização dentro da rede do operador de telecomunicação do sistema de monitoração de acordo com a presente invenção, ou na forma de uma única entidade, com todos os seus componentes co-localizados em um mesmo ponto, ou na forma distribuída, pode variar dependendo de vários fatores, tal como a arquitetura da rede de ISP, o número de usuários a ser

monitorado e acompanhado, um dimensionamento e confiabilidade do sistema de monitoração.

[0087] Graças a sua flexibilidade, a solução de acordo com a presente invenção pode ser aplicada a qualquer tipo de sistemas de comunicações baseados em computador, como a Internet e redes de telefonia de terminais móveis com fio ou sem fio; a solução da presente invenção permite a monitoração e acompanhamento de tráfego de dados gerado pela maioria dos aparelhos de usuário diferentes, como computadores, PDAs, telefones inteligentes, e em geral por qualquer terminal que possa ser conectado a uma rede que esteja interconectada a uma rede de IP, como a internet, sendo atribuído um endereço de IP.

[0088] A solução de acordo com a presente invenção também permite discriminar dentre vários usuários que geram tráfego de diferentes terminais enquanto apresentando eles mesmos com um endereço de IP único (alguma coisa típica no caso de diferentes terminais conectados para um modem xDSL); isto é tornado possível pela injeção no tráfego de dados de informação de presença relacionada ao usuário, que permite discriminar dentre diferentes usuários enquanto ao mesmo tempo preservando o anonimato dos usuários.

REIVINDICAÇÕES

1. Método para perfilagem de tráfego de comunicação de usuários em uma rede de dados (115), caracterizado pelo fato de compreender:

- monitorar tráfego de comunicação originado por um usuário de um terminal de comunicação (105) conectado à rede de dados explorando os serviços de um provedor de serviço de conectividade de rede (110), o tráfego de comunicação do usuário sendo monitorado com base em um endereço de usuário atribuído ao terminal de comunicação do usuário na rede de dados, em que monitorar compreende criar uma entrada em uma tabela com relação ao usuário e armazenar na entrada de tabela o endereço do usuário na rede de dados;

- atribuir ao usuário do terminal de comunicação um identificador de tráfego de usuário anônimo e único, onde o identificador de tráfego de usuário é relacionado a um endereço de usuário atribuído ao terminal de comunicação na rede de dados, e onde o identificador de tráfego de usuário é adaptado para ser incluído no tráfego de comunicação em relação àquele usuário;

- comunicar o identificador de tráfego de usuário anônimo e único para o terminal do usuário e tendo o terminal de comunicação de usuário inclui o identificador de tráfego de usuário no tráfego de usuário,

- manter na tabela de entrada uma indicação de um estado de acompanhamento do usuário, refletindo o estado de acompanhamento do usuário, em associação com o endereço do usuário e o identificador de tráfego do usuário e, quando do recebimento de tráfego de comunicação incluindo o identificador de tráfego de usuário, mudar o estado de acompanhamento do usuário para um estado acompanhado, extrair um descritor do tráfego de comunicação recebido, o descritor incluindo o identificador de tráfego de usuário e sendo útil para descrever o tráfego identificado, e pelo menos

temporariamente armazenar o descritor obtido;

- construir um perfil de usuário anônimo relacionado às atividades de comunicação do usuário com base nos descritores armazenados;

em que a etapa de atribuir o identificador de tráfego de usuário compreende:

- tendo um provedor de serviço de conectividade de rede, quando do recebimento de tráfego de comunicação originado pelo terminal de usuário, avaliar se o tráfego de comunicação recebido inclui o identificador de tráfego de usuário anônimo e único, e caso contrário:

- solicitar ao terminal do usuário para reenviar o tráfego de comunicação para uma função de atribuição de identificador de tráfego de usuário (125) para gerar o identificador de tráfego de usuário anônimo e único para ser atribuído ao endereço de rede do terminal de usuário;

- tendo a função de atribuição de identificador de tráfego de usuário (125), gerar o identificador de tráfego de usuário anônimo e único e incluí-lo em uma resposta enviada para o terminal do usuário, a resposta enviada para o terminal do usuário solicitando ao terminal do usuário para reenviar o tráfego de comunicação incluindo o identificador de tráfego de usuário, em que a resposta enviada pela a função de atribuição de identificador de tráfego de usuário (125) ao terminal usuário inclui uma solicitação para o terminal usuário reenviar o tráfego de comunicação com o identificador de tráfego do usuário para a função de atribuição de identificador de tráfego de usuário,

- quando do recebimento a partir do terminal de usuário do tráfego de comunicação incluindo o identificador de tráfego de usuário, enviar para o terminal de usuário uma resposta adicional solicitando que o terminal de usuário reenvie o tráfego de comunicação para o destino original.

2. Método de acordo com a reivindicação 1, caracterizado pelo fato de que o identificador de tráfego de usuário compreende um cookie

adaptado para ser incluído no tráfego de comunicação gerado pelo e endereçado para o terminal do usuário.

3. Método de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que a solicitação ao terminal do usuário para re-enviar o tráfego de comunicação para uma função de atribuição de identificador de tráfego de usuário inclui:

- enviar para o terminal do usuário a mensagem de *303 SEE OTHER* HTTP incluindo um URL da função de atribuição do identificador de tráfego de usuário, e incluir um URL original contido no tráfego de comunicação recebido do terminal do usuário.

4. Método de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pelo fato de que o descritor compreende um ou mais de: informação relacionada aos pontos finais envolvidos na transação, e informação sobre o tempo em que a transação ocorreu.

5. Método de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que o tráfego de comunicação monitorado originado pelo usuário do terminal de comunicação inclui analisar os pacotes de tráfego de comunicação originados pelo terminal de usuário.

6. Método de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que a construção de um perfil de usuário inclui construir uma lista de páginas da web acessadas pelo usuário em uma sessão de navegação de web.

7. Sistema para perfilagem de tráfego de comunicação de usuários de terminais de comunicação (105) em uma rede de dados (115), caracterizado pelo fato de compreender:

- uma função de monitoração (120) residindo em um provedor de serviço de conectividade de rede (110) que provê serviços de conectividade dos terminais de usuário para redes de dados, em que a função

de monitoração é adaptada para :

- monitorar tráfego de comunicação originado por ou endereçado para um terminal de comunicação (105) de um usuário;

- avaliar se o tráfego de comunicação do usuário está sendo monitorado com base em um endereço de usuário na rede de dados e na inclusão no tráfego de comunicação do identificador de tráfego de usuário anônimo e único;

- criar uma entrada em uma tabela com relação ao usuário e armazenar na entrada de tabela o endereço do usuário na rede de dados;

- armazenar o identificador de tráfego de usuário único na entrada da tabela em associação com o endereço de usuário;

- solicitar ao terminal do usuário para reenviar o tráfego de comunicação para uma função de atribuição de identificador de tráfego de usuário (125) no caso de o tráfego de comunicação recebido não incluir o identificador de tráfego de usuário, e extrair um descritor do tráfego de comunicação, o descritor incluindo o identificador de tráfego de usuário e sendo útil para descrever o tráfego detectado, e fazendo pelo menos temporariamente o armazenamento do mesmo e permitindo que o tráfego de comunicação alcance o destino desejado caso o tráfego de comunicação recebido inclua o identificador de tráfego de usuário;

em que o sistema compreende ainda a função de identificador de tráfego de usuário (125) que é adaptada para:

- gerar o identificador de tráfego de usuário único;

- enviar uma resposta para o terminal do usuário incluindo o identificador de tráfego de usuário, a resposta enviada ao terminal de usuário solicitando ao terminal do usuário para re-enviar o tráfego de comunicação incluindo o identificador de tráfego de usuário, em que a resposta enviada para a função de atribuição de identificador de tráfego de usuário (125) para o terminal de usuário inclui uma solicitação para o terminal

de usuário reenviar o tráfego de comunicação com o identificador de tráfego de usuário para a função de atribuição de identificador de tráfego de usuário,

- quando do recebimento a partir do terminal de usuário do tráfego de comunicação incluindo o identificador de tráfego de usuário, enviar para o terminal de usuário uma resposta adicional solicitando o terminal de usuário a reenviar o tráfego de comunicação para o destino original incluindo o identificador de tráfego de usuário,

em que a função de monitoração é ainda adaptada para manter na tabela de entrada uma indicação de um estado de acompanhamento do usuário, refletindo o estado de acompanhamento do usuário, em associação com o endereço de usuário e o identificador de tráfego de usuário e muda o estado de acompanhamento do usuário para um estado acompanhado quando do recebimento de tráfego de comunicação incluindo o identificador de tráfego de usuário.

8. Sistema de acordo com a reivindicação 7, caracterizado pelo fato de que o identificador de tráfego de usuário compreende um cookie.

9. Rede de dados caracterizada pelo fato de incluir um sistema de monitoração como definido na reivindicação 7 ou 8.

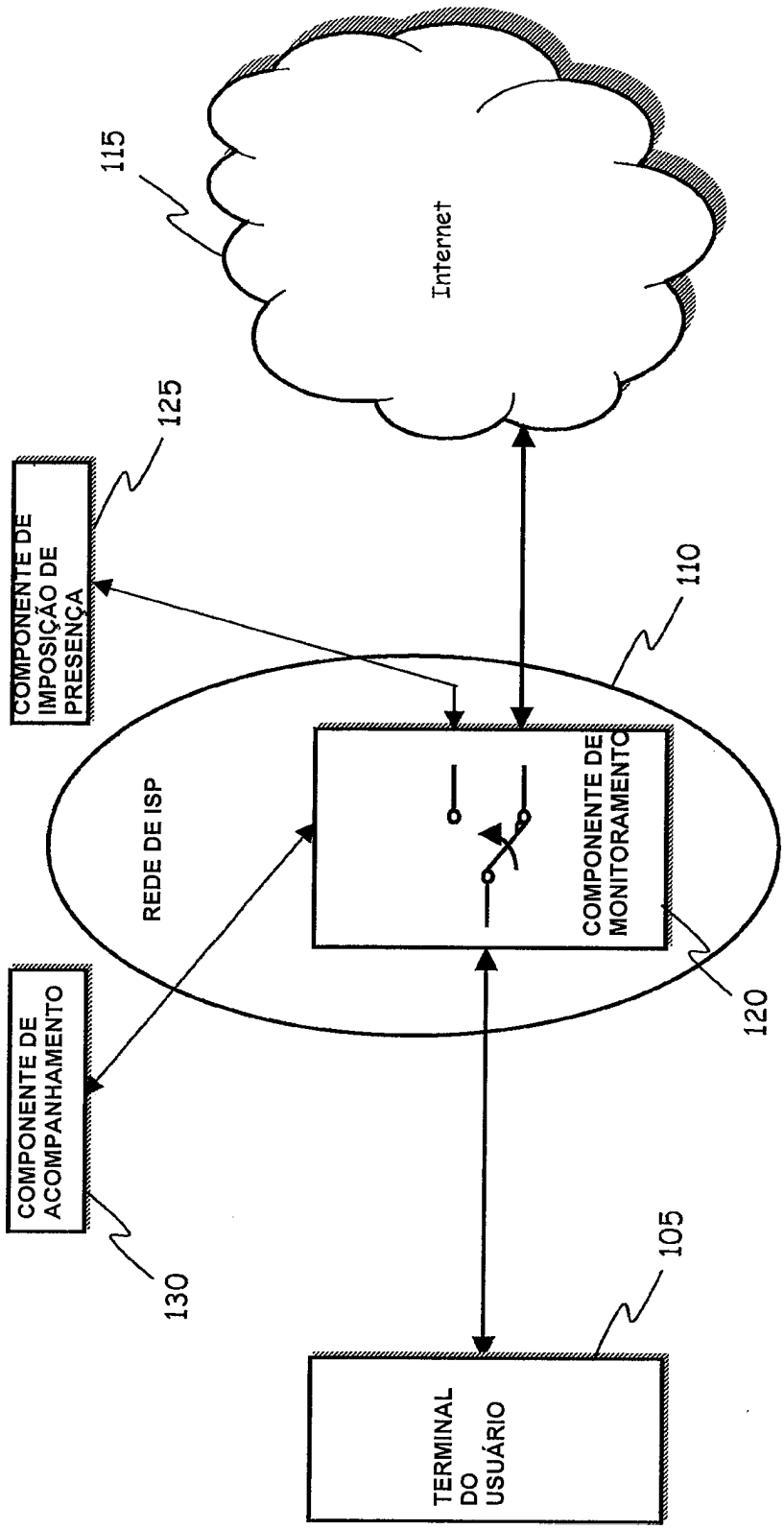
115
Internet
125
COMPONENTE DE IMPOSIÇÃO DE PRESENÇA
110
REDE DE ISP
COMPONENTE DE MONITORAMENTO
120
COMPONENTE DE ACOMPANHAMENTO
130
105
TERMINAL DO USUÁRIO

FIG. 1

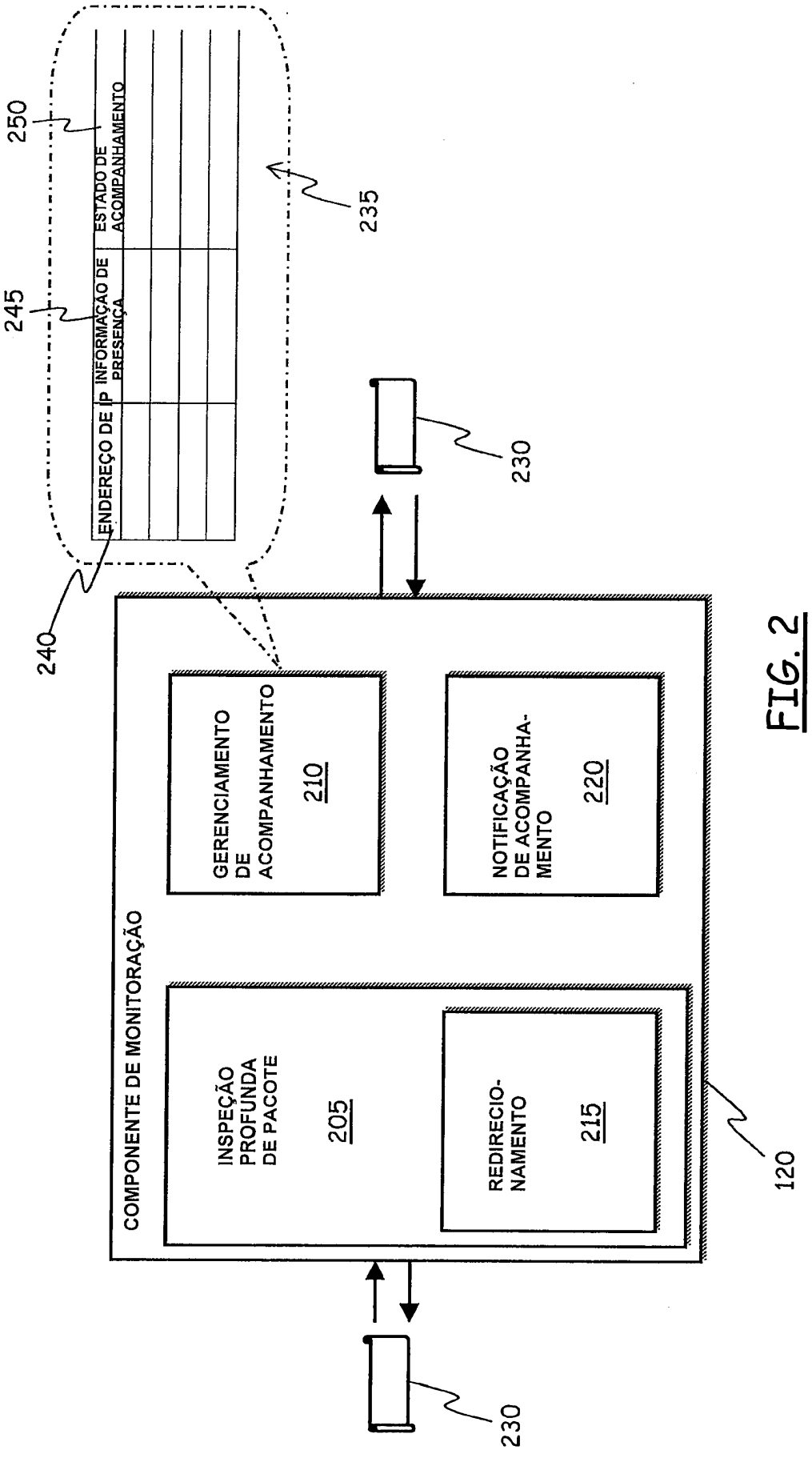
250
245
235
240
230
230
ENDEREÇO DE IP
INFORMAÇÃO DE PRESENÇA
ESTADO DE ACOMPANHAMENTO
COMPONENTE DE MONITORAÇÃO
GERENCIAMENTO DE ACOMPANHAMENTO
210
NOTIFICAÇÃO DE ACOMPANHA-MENTO
220
INSPEÇÃO PROFUNDA DE PACOTE
205
REDIRECIO-NAMENTO
215
120

FIG. 2

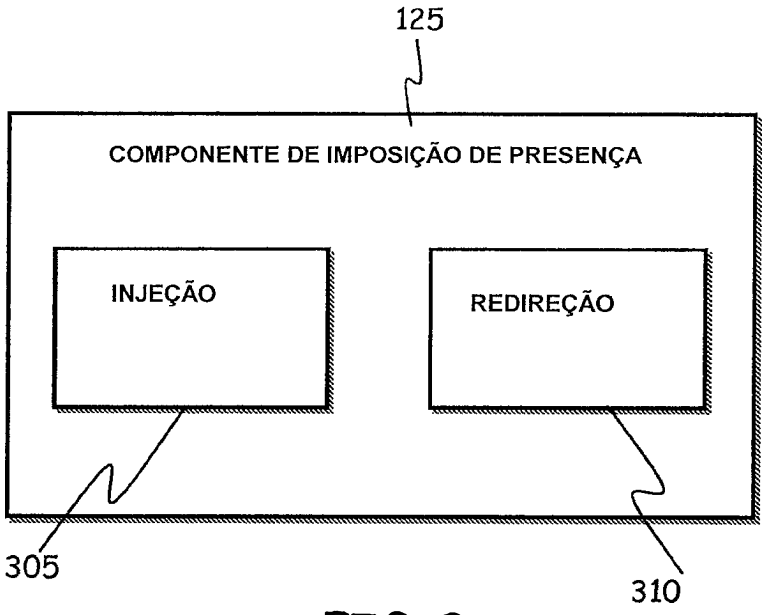
125
COMPONENTE DE IMPOSIÇÃO DE PRESENÇA
INJEÇÃO
REDIREÇÃO
305
310

FIG. 3

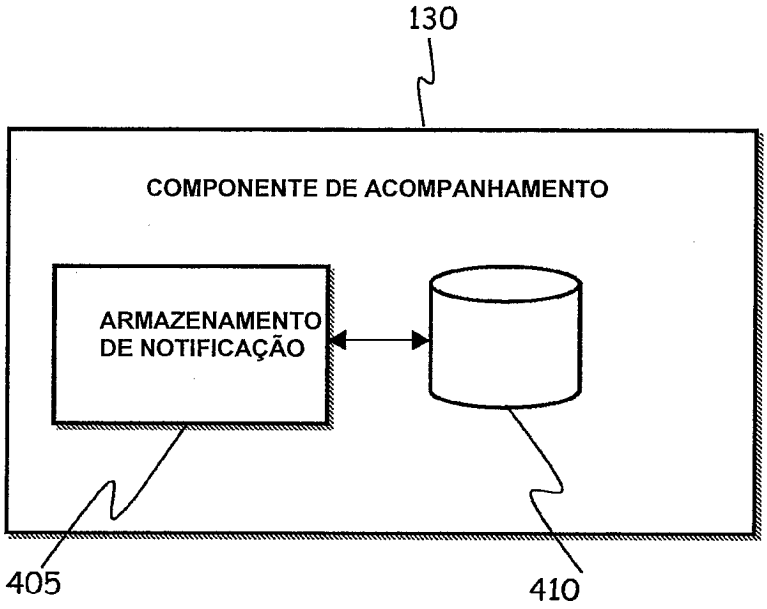
130
COMPONENTE DE ACOMPANHAMENTO
ARMAZENAMENTO
DE NOTIFICAÇÃO
405
410

FIG. 4

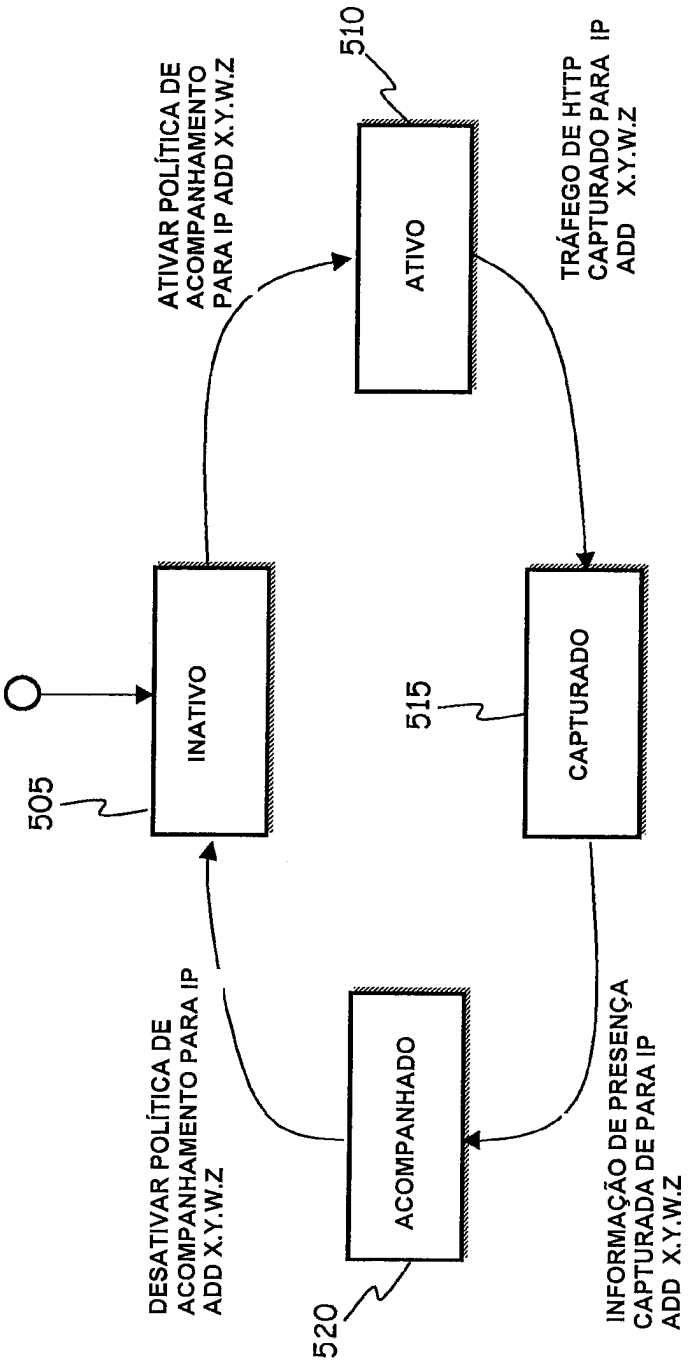
INATIVO
505
ATIVO
510
CAPTURADO
515
ACOMPANHADO
520
ATIVAR POLÍTICA DE ACOMPANHAMENTO PARA IP ADD X.Y.W.Z
TRÁFEGO DE HTTP CAPTURADO PARA IP ADD X.Y.W.Z
DESATIVAR POLÍTICA DE ACOMPANHAMENTO PARA IP ADD X.Y.W.Z
INFORMAÇÃO DE PRESENÇA CAPTURADA DE PARA IP ADD X.Y.W.Z

FIG. 5

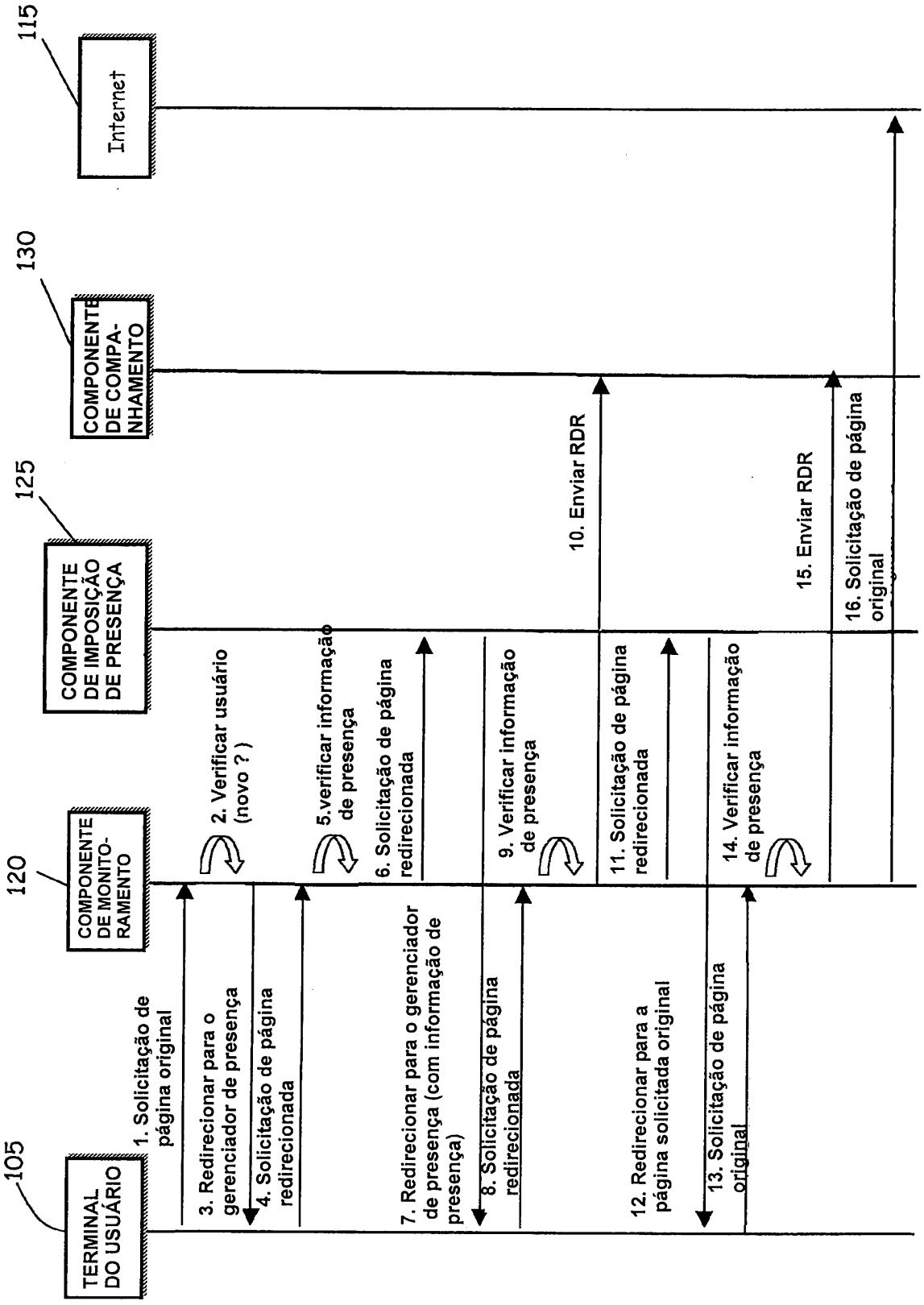
105
TERMINAL DO USUÁRIO
120
COMPONENTE DE MONITO-RAMENTO
125
COMPONENTE DE IMPOSIÇÃO DE PRESENÇA
130
COMPONENTE DE COMPA-NHAMENTO
115
Internet
1. Solicitação de página original
2. Verificar usuário (novo ?)
3. Redirecionar para o gerenciador de presença
4. Solicitação de página redirecionada
5.verificar informação de presença
6. Solicitação de página redirecionada
7. Redirecionar para o gerenciador de presença (com informação de presença)
8. Solicitação de página redirecionada
9. Verificar informação de presença
10. Enviar RDR
11. Solicitação de página redirecionada
12. Redirecionar para a página solicitada original
13. Solicitação de página original
14. Verificar informação de presença
15. Enviar RDR
16. Solicitação de página original

FIG. 6