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

(11) PI 0821370-4 B1

(22) Data do Depósito: 12/12/2008

(45) Data de Concessão: 24/09/2020

(54) Título: MÉTODO PARA CONFIGURAR ACLS NO DISPOSITIVO DE REDE BASEADO EM INFORMAÇÕES DE FLUXO

(51) Int.Cl.: H04L 12/26; H04L 29/06.

(52) CPC: H04L 43/18; H04L 63/101; H04L 63/1441.

(30) Prioridade Unionista: 18/12/2007 US 12/000,910.

(73) Titular(es): SOLARWINDS WORLDWIDE, LLC.

(72) Inventor(es): GREG NEWMAN.

(86) Pedido PCT: PCT US2008013694 de 12/12/2008

(87) Publicação PCT: WO 2009/082439 de 02/07/2009

(85) Data do Início da Fase Nacional: 18/06/2010

(57) Resumo: MÉTODO PARA CONFIGURAR ACLS NO DISPOSITIVO DE REDE BASEADO EM INFORMAÇÕES DE FLUXO As modalidades da presente invenção proporcionam um sistema e método para usar registros de fluxo de rede exportados a partir de roteadores de rede para proporcionar informações sobre o trafego que entra/sai do dispositivo. Os roteadores ou hubs de rede podem ser configurados para autorizar ou negar diversos tipos de tráfego de rede entre dois dispositivos de rede cujo tráfego transita através do roteador. O método apresentado descreve a criação e aplicação de lista de controle de acesso no roteador a partir das informações derivadas das informações de fluxo de rede exportadas pelo roteador de rede.

"MÉTODO PARA CONFIGURAR ACLS NO DISPOSITIVO DE REDE BASEADO EM INFORMAÇÕES DE FLUXO"

Campo da Invenção

A presente invenção refere-se ao uso de dados de fluxos de rede exportados a partir de roteadores de rede que proporcionam informações sobre o tráfego que entra/sai do dispositivo. Os roteadores de rede podem ser configurados para autorizar ou negar diversos tipos de tráfego de rede entre dois dispositivos de rede cujo tráfego transita através do roteador. O método apresentado descreve a criação e aplicação dinâmica de listas de controle de acesso no roteador a partir das informações derivadas das informações de fluxo de rede exportadas pelo roteador de rede.

Antecedentes da Invenção

Os dados de uso de rede são úteis para muitas funções de negócio importantes, tais como, cobrança de assinante, marketing & serviço de cliente, desenvolvimento de produto, gerenciamento de operações de rede, planejamento de capacidade de rede e sistemas e segurança. Os dados de uso de rede não incluem as informações reais trocadas em uma sessão de comunicações entre partes, porém, inclui, de preferência, inúmeros registros de detalhe de uso, conhecidos como "registros de fluxo" que contêm um ou mais tipos de metadados (isto é, "dados sobre dados"). Os protocolos de registros de fluxo de rede conhecidos incluem Netflow®, sFlow®, jFlow®, cFlow® ou Netstream®. Conforme usado no presente documento, um registro de fluxo é definido como uma pequena unidade de medição de uso de rede unidirecional por um fluxo de pacotes de IP que compartilham parâmetros de origem e destino comuns durante um intervalo de tempo.

Os tipos de metadados incluídos em cada registro de fluxo variam com base no tipo de serviço e rede envolvido e, em alguns casos, com base no dispositivo de rede particular que proporciona os registros de fluxo. Em geral, um registro de fluxo proporciona informações de uso detalhadas sobre um evento particular ou conexão de comunicações entre as partes, tais como, tempo inicial e

tempo de parada de conexão, origem (ou originador) dos dados que são transportados, o destino ou receptor dos dados, e a quantidade de dados transferida. Um registro de fluxo resume as informações de uso por períodos de tempo muito curtos (de milissegundos a segundos, ocasionalmente minutos). Dependendo do tipo de serviço e rede envolvido, um registro de fluxo também pode incluir informações sobre o protocolo de transferência, o tipo de dados transferido, o tipo de serviço (ToS) proporcionado, etc. Em redes de telefonia, os registros de fluxo que constituem as informações de uso são referidos como registros de detalhe de chamada (CDRs).

No monitoramento de rede, os registros de fluxo de rede são coletados, armazenados e analisador para produzirem resultados significativos. Os sistemas de análise de uso de rede processam estes registros de fluxo e geram relatórios ou arquivos de dados resumidos que suportam diversas funções de negócio. Os sistemas de análise de uso de rede proporcionam informações sobre como os serviços de rede estão sendo usados e por quem. Os sistemas de análise de uso de rede também podem ser usados para identificar (ou prever) problemas relacionados com a satisfação do cliente, tais como, aqueles causados pelo congestionamento de rede e abuso de segurança de rede. Em um exemplo, a utilização e o desempenho de rede, como uma função do comportamento de uso do assinante, podem ser monitorados para rastrear uma experiência do usuário, prever a capacidade de rede futura ou identificar o comportamento de uso indicativo de abuso de rede, fraude e roubo.

Em segurança de computador, uma lista de controle de acesso (ACL) é uma lista de permissões anexada a um objeto. Mais especificamente, em sistema de rede, ACL refere-se a uma lista de regras que detalham as regras de filtragem de tráfego. As ACLs podem permitir ou negar o tráfego através de um dispositivo de rede. Apenas os roteadores e firewalls podem ter ACLs de rede. As listas de controle de acesso geralmente podem ser configuradas para controlar tanto o tráfego de entrada, como o de saída.

As ACLs são um modo de controlar o tráfego de rede através da

limitação do acesso de usuário e dispositivo para e a partir dos endereços e/ou portas indesejadas. As ACLs filtram o tráfego de rede ao controlar se os pacotes roteados são encaminhados ou bloqueados, tipicamente em uma interface de roteador, embora outros dispositivos possam filtrar pacotes. O roteador examina cada pacote para determinar se encaminha ou abandona o pacote, com base nos critérios especificados nas listas de acesso. Um critério de lista de controle de acesso pode ser o endereço de origem do tráfego ou do endereço de destino do tráfego, a porta ou protocolo alvo, ou alguma combinação destes. De maneira típica, os endereços de Protocolo de Internet (IP) servem como identificadores do dispositivo de origem em uma rede baseada em IP. As listas de controle de acesso permitem o acesso diferenciado com base neste identificador de IP na rede.

Embora as ACLs tenham funções úteis, o estabelecimento de ACLs pode ser trabalhoso. Em particular, atualmente as ACLs são programadas de maneira manual. Além disso, uma seleção de endereços IP para situar nas ACLs pode ser arbitrária e imprevisível.

Em particular, muitas redes de IP autônomas ou empresariais são grandes, complexas e dinâmicas, tornando as mesmas difíceis de gerenciar. As tarefas de gerenciamento de rede, tais como, monitoramento do tráfego em uma rede, análise do desempenho da rede ou reconfiguração da rede para desempenho aprimorado requerem informações sobre a rede. Entretanto, devido ao fato de as redes de IP grandes serem altamente dinâmicas, é difícil adquirir informações úteis para muitas tarefas de gerenciamento de rede. Considere que uma rede IP grande pode ter dezenas de milhares de nós e centenas de roteadores e portas. Uma rede corporativa grande pode ter 300.000 nós e 2.500 roteadores. Os roteadores, portas, comutadores e outros dispositivos de rede, algumas vezes, falham, ficam offline ou voltam a funcionar. Os links, muitas vezes, falha, voltam a funcionar ou reduzem o desempenho. Por exemplo, um link de microondas ou satélite pode experimentar a interferência que reduz sua largura de banda. Os protocolos, tais como, OSPF e BGP que são usados para rotear o tráfego em redes de IP grandes são dinâmicos e alteram as trajetórias de

roteamento em uma rede grande, à medida que as condições alteram na rede. Mesmo as redes relativamente estáveis podem levar um longo tempo para atingir um estado de convergência de roteamento. Através do projeto, o caminho de comunicação entre dois computadores em uma rede IP pode alterar mesmo durante o período de uma única conexão entre eles. Devido a estes fatores e outros discutidos abaixo, tem sido difícil para as ferramentas de gerenciamento de rede obter informações que ao longo do tempo representem uma imagem um tanto completa e precisa de uma rede.

A complexidade de rede torna o gerenciamento das redes dispendioso, à medida que este requer a intervenção manual de operadores humanos versados. A configuração e o gerenciamento de uma rede IP grande têm sido difíceis de automatizar. Este necessidade de supervisão humana próxima levou muitos operadores a adotarem uma política conservadora de preferência de estabilidade de rede através da reconfiguração frequente para otimizar o desempenho de rede. Deste modo, outro problema no campo de gerenciamento de rede consiste no fato de que as redes IP retêm configurações de rede sub-ótimas por mais tempo do que requerido, levando ao uso ineficiente de capacidade de largura de banda dispendiosa e latências de comunicação potencialmente mais altas do que, de outro modo, possíveis. As ferramentas para o gerenciamento e configuração automatizados não foram amplamente adotadas.

Embora existam ferramentas para o gerenciamento de rede, que incluem monitorar e manter as ACLS, as ferramentas são rudimentares e têm muitas falhas. A maioria das ferramentas de gerenciamento de rede simplesmente descobrem e sondam os dispositivos de rede ativos para gerar relatórios que contêm mapas, valores de contagem, médias, áreas de tráfego elevado, e assim por diante. As ferramentas atuais tendem a ignorar as dinâmicas globais de comportamento de rede, que se concentram em unificar de maneira potencialmente central os dados conflitantes localmente adotados a partir de dispositivos de rede individuais. As ferramentas atuais não tornam fácil para um operador realizar uma variedade de tarefas potencialmente úteis, tais como,

descobrir o caminho que um conjunto particular de tráfego faz através da rede, investigar o comportamento da rede em cenários 'whatif', monitorar a evolução da rede, à medida que falhas e recuperações ocorrem ou analisar o tráfego de rede, à medida que este se refere a aplicações ou serviços particulares, e assim por diante.

Conforme descrito acima, houve tentativas de medir o tráfego de rede em computadores de usuário individual, porém, os dados de tráfego de hospedeiro eram limitados no escopo e geralmente não puderam revelar as informações relacionadas ao fluxo de tráfego ao longo de caminhos particulares em uma rede IP. A medição de rede hospedeira ou de sistema final não proporciona informações úteis sobre a topologia de rede. Existem também ferramentas que agregam os dados de tráfego IP em dispositivos de rede, tais como, roteadores e comutadores, por exemplo, NetFlow®, disponível junto a Cisco Sistemas. Entretanto, estas abordagens se provaram inadequadas por inúmeros motivos, tais como, tráfego opaco (por exemplo, criptografado, tunelado), padrões de comunicação de aplicação complexa, artefatos de amostragem, carga nos roteadores introduzidos por monitoramento, e outros.

Além disso, as técnicas conhecidas para identificar vírus são limitadas. As técnicas conhecidas geralmente procuram efeitos secundários do vírus, tais como, monitorar o uso de recurso de rede e identificar aplicativos que solicitam uma grande quantidade anormal dos recursos de rede. Entretanto, pode ser difícil diferenciar entre os vírus e os aplicativos legítimos que requerem uma grande quantidade de recursos de rede. Também, os vírus estão se tornando mais inteligentes para evitar a detecção. Por exemplo, um vírus pode ficar inativo em um sistema por algum tempo, aguardando um sinal para iniciar. Por exemplo, a os mal intencionados podem ficar inativos até o dado confidencial ser adquirido. Deste modo, enquanto o vírus está aguardando para agir, pode ser difícil detectá-lo porque o mesmo produz efeitos colaterais mínimos.

Sumário da Invenção

Em resposta a estas e outras necessidades, as modalidades da

presente invenção proporcionam um sistema e método para usar registros de fluxo de rede exportados a partir de roteadores de rede que proporcionam informações sobre o tráfego que entra/sai do dispositivo. Os roteadores de rede podem ser configurados para autorizar ou negar diversos tipos de tráfego de rede entre dois dispositivos de rede cujo tráfego transita através do roteador. O método apresentado descreve a criação e aplicação de listas de controle de acesso no roteador a partir das informações derivadas das informações de fluxo de rede exportadas pelo roteador de rede.

Um sistema proporciona o controle dinâmico de uma rede, o sistema que inclui: um armazenamento de registro de fluxo configurado para receber os registros de fluxo da rede e agregar os registros de fluxo; uma ferramenta de análise de dados configurada para receber os registros de fluxo agregados e analisar os registros de fluxo agregados, de acordo com os critérios predefinidos para identificar um ou mais endereços e portas de rede, e um dispositivo de rede configurado para receber os endereços de rede identificados e adicionar os endereços e portas de rede identificados a uma lista de controle de acesso. De maneira opcional, o sistema inclui adicionalmente o armazenamento de lista de controle de acesso opcionalmente configurado para armazenar os endereços e portas de rede identificados e proporcionar os endereços de rede identificados para o dispositivo de rede. De maneira opcional, cada um dos registros de fluxo inclui um endereço de origem e os registros de fluxo são agregados de acordo com os endereços de origem. De outro modo, os registros de fluxo incluem o tamanho de byte transmitido em cada fluxo associado, e sendo que o critério predefinido inclui o número total de bytes transmitido no fluxo associado a cada um dos endereços de origem. De maneira opcional, um dispositivo de entrada de dados recebe a entrada de um usuário para definir o critério predefinido.

Os componentes na rede podem ser monitorados ao receber os registros de fluxo dos componentes sobre o tráfego em uma rede. O dado que define o critério de controle de acesso é recebido, de maneira opcional, e os registros de fluxo são analisados usando o critério de controle de acesso. Os

endereços de rede alvo e de origem ou faixas e/ou portas alvo e de origem satisfazem o critério de controle de acesso e são identificadas e apresentadas para o usuário. O usuário pode rever os endereços ou faixas identificados e/ou portas, então, optar encaminhar os mesmos para um dos componentes de rede. Se enviado, o componente adiciona o endereço e/ou porta de rede identificado a uma lista de controle de acesso associada, em que a lista de controle de acesso evita que o tráfego alcance o endereço e/ou porta de rede identificado. De maneira opcional, os períodos de tempo para cada lista de controle de acesso podem ser ajustados para permitir a remoção das entradas de ACL automaticamente lançadas.

Deste modo, as ACLs são regras de filtragem de tráfego aplicadas em um roteador ou firewall. Existem dois tipos de ACLs, ACLs padrão que bloqueiam ou permitem o tráfego apenas por Endereço IP de Origem e as ACLs estendidas que bloqueiam através do Endereço IP de Destino e Porta de Origem e Destino. Consequentemente, as modalidades do presente pedido incluem o armazenamento dos endereços ou portas identificados.

Em um sistema para controlar dinamicamente o tráfego de rede, o sistema inclui uma fluxo que gera o dispositivo configurado para acessar um sistema de armazenamento para proporcionar os registros de fluxo; um sistema de armazenamento de registro de fluxo configurado para receber e armazenar os registros de fluxo; e um dispositivo de análise de dados configurado para acessar o sistema de armazenamento e avaliar os registros de fluxo armazenados de acordo com o critério predefinido. Se aqueles registros de fluxo satisfizerem o critério predefinido, aquele endereço/porta pode ser encaminhado para um usuário rever e aprovar e ser adicionado na ACL. Para auxiliar o usuário, o dado de registro de fluxo associado ao endereço/porta identificado também pode ser exibido para o usuário.

Em outra modalidade, as técnicas descritas no presente documento descrevem um método para avaliar endereço/portas em uma ACL. Em particular, os registros de fluxo associados a um endereço/portas na ACL podem ser

avaliados de acordo com um critério predefinido. Se aqueles registros de fluxo satisfizerem o critério predefinido, o endereço/porta pode ser encaminhado para um usuário para que a revisão e aprovação sejam renovadas na ACL. De outro modo, se aqueles registros de fluxo falham ao satisfazer o critério predefinido, e o endereço/porta pode ser encaminhado para um usuário para que a revisão e aprovação sejam removidas da ACL.

Breve Descrição dos Desenhos

Os objetivos, características e vantagens acima e outros de certas modalidades exemplificativas da presente invenção serão mais aparentes a partir da seguinte descrição detalhada tomada em conjunto com os desenhos em anexo em que:

A Figura 1A mostra uma rede exemplificativa, de acordo com as modalidades da rede da presente invenção;

A Figura 1B (técnica anterior) mostra um sistema de análise de registros de fluxo exemplificativo;

A Figura 2 (técnica anterior) mostra um registro de fluxo exemplificativo conhecido;

A Figura 3 mostra uma tabela exemplificativa conhecida para armazenar os registros de fluxo, de acordo com as modalidades da presente invenção;

A Figura 4 mostra uma tabela exemplificativa para armazenar os registros de fluxo agregados, de acordo com as modalidades da presente invenção;

A Figura 5 mostra um sistema para criar ACLs usando o dado de fluxo, de acordo com as modalidades da presente invenção;

A Figura 6 é um fluxograma de serviço que explica as comunicações entre um nó de rede, um sistema de controle de acesso, e um sistema de armazenamento de registro de fluxo, de acordo com as modalidades da presente invenção; e

A Figura 7 é um fluxograma que mostra as etapas em um método

para criar ACLs usando registros de fluxo, de acordo com as modalidades da presente invenção.

Descrição Detalhada das Modalidades Preferidas

Uma rede 100, de acordo com modalidades da presente invenção, é mostrada na Figura 1A, em que um diagrama de bloco que ilustra uma vista de rede da presente invenção, de acordo com uma modalidade é mostrado. Conforme ilustrado, dispositivos de cliente 108a-108n são acoplados aos servidores 110a-110n através da malha de rede 112, que inclui inúmeros dispositivos de roteamento 106a-106n acoplados uns aos outros formando uma pluralidade de links de rede. Os dispositivos de cliente 108a-108n, através dos dispositivos de roteamento 106a-106n ou, mais especificamente, através dos links de rede formados por dispositivos de roteamento 106a-106n, acessa, seletivamente os servidores 110a-110n para serviços. Infelizmente, conforme aqueles versados na técnica irão avaliar, os mesmos links de rede que tornam os servidores 110a-110n prontamente acessíveis aos dispositivos de cliente 108a-108n também tornam os mesmos vulneráveis a abuso ou uso impróprio por um ou mais dispositivos de cliente 108a-108n. Por exemplo, um ou mais dispositivos de cliente 108a-108n podem individualmente ou em combinação desenvolver um ataque, tal como, negação de ataque de serviço ou, de outro modo, punir um ou mais servidores 110a-110n, dispositivos de roteamento 106a-106b e/ou links interconectados aos elementos. De acordo com a presente invenção, o diretor 102, complementado por inúmeros sensores 104a-104n, é empregado para detectar e evitar tal abuso ou uso impróprio dos links de rede, que será descrito mais completamente abaixo. Na modalidade ilustrada, os sensores 104a-104n são dispostos em locais distribuídos. Nas modalidades alternativas, alguns ou todos os sensores 104a-104n podem ser integralmente dispostos com os dispositivos de roteamento 106a-106b.

A rede 112 representa uma ampla faixa de redes privadas, assim como, públicas ou redes interconectadas, tal como, uma rede corporativa de uma corporação multinacional ou a Internet. Os nós de rede, tais como, os clientes

108a-108n e o servidor 110a-110n representam uma ampla faixa destes elementos conhecidos na técnica, que incluem máquinas de usuário individual, sites de comércio eletrônico, e similares. Conforme anteriormente aludido, os dispositivos de roteamento 106a-106n representam uma ampla faixa de equipamentos de tráfego de rede, que incluem, porém, não se limitam a roteadores, comutadores, portas, hubs convencionais, e similares.

Para facilidade de entendimento, apenas um diretor 102 e um pequeno número de cada um dos nós de rede, clientes 108a-108n e servidores 110a-110n, dispositivos de roteamento 106a-106n e sensores 104a-104n são incluídos na ilustração, a partir da seguinte descrição, aqueles versados na técnica irão avaliar que a presente invenção pode ser praticada com mais de um diretor 102, assim como, mais ou menos nós de rede, dispositivos de roteamento 106a-106n e sensores 104a-104n. Em particular, a presente invenção também pode ser praticada com um ou mais diretores 102. Quando mais de um diretor 102 é empregado, cada diretor 102 pode ser responsável por um subconjunto de sensores 104a-104n, e os diretores 102 podem se referir uns aos outros em uma relação mestre/escrava, com um dos diretores 102 servindo como o "mestre" (e os outros como "escravos"), ou similares uns aos outros ou organizados em uma hierarquia para descarga coletiva das responsabilidades descritas abaixo.

A operação do diretor 102 é descrita em maiores detalhes abaixo, e o diretor 102 inclui um sistema de conexão de dados de fluxo e um dispositivo de controle de acesso, conforme descrito em maiores detalhes abaixo.

Conforme mostrado na Figura 1B, um sistema de análise de uso de rede conhecido 111 inclui um servidor de sistema de coleta de dados 130 e um sistema de armazenamento de dados 140, em uma modalidade. O servidor de sistema de coleta de dados 130, também chamado de ouvinte, é um servidor central que coleta os datagramas de fluxo 190 a partir de todos os agentes de rede 120 para armazenamento e análise. O servidor de sistema de coleta de dados 130 recebe os registros de fluxo 190 a partir do dispositivo de geração de registro de fluxo 120, que consiste em um dispositivo de rede que é parte de uma rede IP 114.

Em uma modalidade, a rede 114 inclui a Internet 115.

Em geral, os dispositivos de geração de registro de fluxo 120 podem incluir substancialmente qualquer dispositivo de rede capaz de manusear o tráfego de rede bruto em "velocidades de linha" e gerar registros de fluxo a partir daquele tráfego. Os dispositivos de geração de registro de fluxo exemplificativos 120 incluem roteadores, comutadores e portas e, em alguns casos, podem incluir provas de servidores, sistemas e rede de aplicativo. Na maioria dos casos, os registros de registro de fluxo pequenos gerados pelos dispositivos de geração de registro de fluxo 120 são exportados como um fluxo de registros de fluxo 190 para o servidor de sistema de coleta de dados 130.

Diversos protocolos de rede executam no equipamento de rede para coletar informações de tráfego de protocolo de rede e internet. Tipicamente, diversos agentes de rede 120, tais como, roteadores, têm a característica de fluxo capacitada para gerar os registros de fluxo. Os registros de fluxo 190 são tipicamente exportados a partir do agente de rede 120 nos pacotes de Protocolo de Datagrama de Usuário (UDP) ou Protocolo de Transmissão de Controle de Fluxo (SCTP) e coletados usando um coletor de fluxo. Para mais informações, por favor, consulte o padrão de Força Tarefa de Engenharia de Internet (IETF) para Internet Protocol Flow Information eXport (IPFIX) em http://www.ietf.org/html.charters/ipfix-charter.html.

Conforme descrito acima, os registros de fluxo 190 geralmente são enviados pelos agentes de rede 120 através de um DP ou SCTP, e por questões de eficiência, os agentes de rede 120 não armazenam os registros de fluxo uma vez que eles são exportados. Com um fluxo de UDP, se o registro de fluxo 190 for abandonado devido ao congestionamento de rede, entre o agente de rede 120 e o servidor de coleta de dados 130, o mesmo pode ser perdido para sempre porque não existe maneira de o agente de rede 120 reenviar o registro de fluxo 190. Também, pode-se permitir o fluxo em uma base por interface para evitar a sobrecarga desnecessária do processador do roteador. Deste modo, os registros de fluxos 190 geralmente são baseados na entrada de pacotes nas interfaces em

que são capacitados para evitar a contagem dupla e economizar o trabalho do agente de rede 120. Também, o agente de rede 120 pode exportar os registros de fluxo para pacotes abandonados.

Os fluxos de rede foram definidos de muitas maneiras. Em uma implementação, um fluxo inclui um quíntuplo: uma sequência unidirecional de pacotes para definir endereço IP de Origem, endereço IP de Destino, porta TCP de Origem, porta TCP de Destino e protocolo IP. Tipicamente, o agente de rede 120 irá emitir um registro de fluxo quando o mesmo determina que o fluxo foi terminado. O agente de rede 120 efetua isto através do "envelhecimento de fluxo", onde o agente de rede 120 reinicia um contador de envelhecimento quando o agente de rede 120 observa o novo tráfego para um fluxo existente. Também, a terminação de sessão TCP em um fluxo TCP faz com que o agente de rede 120 termine o fluxo. O agente de rede 120 também pode ser configurado para emitir um registro de fluxo em um intervalo fixo mesmo se o fluxo ainda estiver em andamento. Alternativamente, um administrador pode definir as propriedades de fluxo no agente de rede 120.

Um registro de fluxo 190 pode conter uma ampla variedade de informações sobre o tráfego em um determinado fluxo. Um registro de fluxo exemplificativo 200 contém os seguintes valores, conforme definido na Figura 2. Em particular, os registros de fluxo típicos 200 podem incluir um número de versão 210 para identificar o tipo de fluxo que é usado. Um número de sequência 220 identifica o registro de fluxo.

Referindo-se à Figura 2, os índices de protocolo de gerenciamento de rede de interface de entrada e saída simples (SNMP) 230 podem ser usados para identificar dinamicamente os dispositivos de rede através de SNMP. O SNMP é usado pelos sistemas de gerenciamento de rede para monitorar os dispositivos conectados à rede para condições que garantam a atenção administrativa, e consiste em um conjunto de padrões para gerenciamento de rede, incluindo um protocolo de Camada de Aplicativo, um esquema de banco de dados e um conjunto de objetos de dados. O SNMP expõe os dados de gerenciamento sob a

forma de variáveis nos sistemas gerenciados, que descrevem a configuração de sistema. Estas variáveis, então, podem ser consultadas (e, algumas vezes, ajustadas) através dos aplicativos de gerenciamento. Os dispositivos modulares podem renumerar seus índices SNMP quando o hardware designado for adicionado ou removido. Os valores de índice são tipicamente atribuídos ao tempo de inicialização e permanecem fixos até a próxima reinicialização.

Referindo-se à Figura 2, cada um dos registros de fluxo 200 inclui de maneira tipicamente adicional informações sobre a transmissão de dados, incluindo um carimbo de data/hora dos tempos de início e término 240. Outras informações sobre a transmissão de dados incluem informações sobre o número de bytes e/ou pacotes em um fluxo 250. As condicionais da transferência de dados também podem ser incluídas no registro de fluxo 200, tais como, dados de cabeçalho 260 que descrevem os endereços de origem e destino, os números de porta de endereços de origem e destino, protocolo de transmissão e o tipo de serviço (ToS). Para o Protocolo de Controle de Transmissão (TCP), o registro de fluxo 200 pode indicar adicionalmente a união de todos os sinalizadores TCP durante o fluxo. Conforme bem conhecida a partir do TCP, uma transmissão de dados envolve uma série de confirmações de comunicações, por exemplo, através de pares de sinalizadores de confirmações (ACKs). Um desequilíbrio dos sinalizadores TCP sugere uma falha de mensagem, em que uma mensagem foi enviada e nunca recebida.

A falta de confiabilidade no mecanismo de transporte UDP não afeta de maneira significativa a precisão das medições obtidas a partir de um fluxo amostrado. Por exemplo, se as amostras de fluxo forem perdidas, então, novos valores serão enviados quando o próximo intervalo de sondagem tiver passado. Deste modo, a perda de amostras de fluxo de pacote consiste em uma ligeira redução na taxa de amostragem efetiva. Quando a amostragem é usada, a carga útil de UDP contém o datagrama de fluxo amostrado. Deste modo, em vez de incluir todo o registro de fluxo 190 cada datagrama, por sua vez, proporciona informações, tal como, a versão de fluxo, seu endereço IP do agente de origem,

um número de sequência, quantas amostras o mesmo contém e as amostras de fluxo.

Referindo-se à Figura 1B, o servidor de sistema de coleta de dados 130 recebe os registros de fluxo contínuo 190 a partir do dispositivo de geração de registro de fluxo 120 através de um link de comunicação 170. Em uma modalidade, o dispositivo de geração de registro de fluxo 120 pode ser incluído na rede 114. Em outra modalidade, o dispositivo de geração de registro de fluxo 120 pode ser implementado em um local fisicamente separado, através da funcionalidade acoplada à rede 114. Embora mostrado na Figura 1 separado do servidor de sistema de coleta de dados 130, o dispositivo de geração de registro de fluxo 120 pode ser uma parte do servidor de sistema de análise de dados 130, em outra modalidade.

Um servidor de sistema de análise de dados 150 acessa e usa os registros de fluxo 190 para realizar a análise estatística de isso de rede predeterminada. Em geral, o servidor de sistema de análise de dados 150 implementa diversos modelos estatísticos que são definidos para solucionar um ou mais problemas relacionados ao uso de rede, tais como, congestionamento de rede, abuso de segurança de rede, fraude e roubo, entre outros. O servidor de sistema de análise de dados 150 usa os registros de fluxo 190 e os modelos estatísticos para gerar um resultado estatístico, que também pode ser subsequentemente armazenado em um sistema de armazenamento de dados 140. As modalidades exemplificativas para armazenar o resultado estatístico serão descritas em mais detalhes abaixo. Analisando-se os dados de fluxo, o servidor de sistema de análise de dados 150 pode construir uma imagem do fluxo de tráfego e do volume de tráfego em uma rede. O requerente do sistema de análise de dados 150 é descrito em maiores detalhes abaixo.

Em um aspecto, o servidor de sistema de análise de dados 150 pode ser responsivo a uma interface de usuário 160 para análise interativa dos registros de fluxo 190. A interface de usuário 160 pode compreender substancialmente qualquer dispositivo de entrada/saída conhecido na técnica, tais como, um teclado,

um mouse, um dispositivo sensível ao toque, uma tela de exibição, etc. Em um exemplo, uma exibição gráfica dos resultados estatísticos pode ser emitida em uma tela de exibição na interface de usuário 160.

Em uma modalidade, o servidor de sistema de análise de dados 150 compreende um programa de software de computador que é executável em um ou mais computadores ou servidores para analisar os dados de uso de rede, de acordo com diversas modalidades da invenção. Embora o sistema de armazenamento de dados 140 seja mostrado externo ao servidor de sistema de coleta de dados 130 e/ou ao servidor de sistema de análise de dados 150, o sistema de armazenamento de dados 140 pode ser alternativamente disposto em cada um dos servidores 130 e 150. O sistema de armazenamento de dados 140 pode compreender substancialmente qualquer memória volátil (por exemplo, RAM) e/ou memória não volátil (por exemplo, uma unidade de disco rígido ou outro dispositivo de armazenamento persistente) conhecida na técnica.

Referindo-se à Figura 3, uma tabela exemplificativa 300 para armazenar múltiplos registros de fluxo 200 em um dispositivo de armazenamento 140 é apresentada. Em particular, a tabela mostrada 300 inclui uma coluna que atribui um identificador de registro de fluxo 310 para cada um dos n registros de fluxo recebidos 200. A tabela 300 também inclui uma coluna que contém um endereço IP de origem 320 para cada um dos registros de fluxo recebidos 200, uma coluna que contém um carimbo de data/hora 330 para cada um dos registros de fluxo recebidos 200, e uma coluna que contém um tamanho de byte 340 nos fluxos associados aos registros de fluxo recebidos 200.

No exemplo da Figura 3, a tabela de fluxo exemplificativa 300 inclui sete registros de fluxo que descrevem sete fluxos, conforme indicado pelo identificador de registro de fluxo 310. Neste exemplo particular, os sete fluxos originados em 3 endereços de origem exclusivos 320. Por exemplo, todos os registros de fluxo 1, 2, 4 e 7 se originaram a partir das mesmas origens. Embora não mostrada, a tabela de fluxo exemplificativa 300 pode incluir, de maneira similar, outros aspectos do registro de fluxo 200, conforme descrito acima na

Figura 2, tal como, um local de destino, QoS, protocolo de transmissão, etc. Referindo-se à tabela de fluxo exemplificativa 300 na Figura 3, um valor de carimbo de data/hora 330 indica um tempo associado a cada um dos valores de tamanhos de fluxos e bytes 340 que indica o tamanho de cada um dos fluxos associados aos registros de fluxo listados 1-7 identificados na coluna 310.

Referindo-se agora à Figura 4, os dados na tabela de dados de fluxo exemplificativa 300 são agregados à tabela de fluxo agregado 400 de acordo com o endereço IP de origem 420. Tipicamente, a agregação é feita através de um ou mais períodos de tempo predefinidos. Por exemplo, a tabela de fluxo agregado exemplificativa 400 inclui uma coluna com o número agregado de registros de fluxo 410 associado a cada um dos endereços IP 420 na tabela 300. A tabela de fluxo agregado 400 indica adicionalmente o tamanho de byte total dos fluxos para cada um dos endereços IP origem 420 na tabela 300. As aplicações da Tabela de fluxo agregado 400 são descritas abaixo. Como na tabela de registro de fluxo 300, deve-se avaliar que os registros de fluxo 190 podem ser agregados conforme desejado, por exemplo, de acordo com um ou mais das categorias de registros de fluxo descritas no registro de fluxo exemplificativo 200 na Figura 2.

Referindo-se agora à Figura 7, um método de controle de acesso 700 de acordo com modalidades da presente invenção é descrito agora. Na etapa 710, o tráfego nos componentes de rede é monitorado, de acordo com as técnicas conhecidas, conforme descrito acima, e os registros de fluxo são coletados na etapa 720. Tipicamente, as etapas 710 e 720 podem ser realizadas usando as funcionalidades já incluídas na maioria dos componentes de rede, tais como, roteadores, hubs, servidores, etc, e podem ser usados para coletar e armazenar um registro de fluxo, tal como, a tabela de registro de fluxo exemplificativa 300. Os registros de fluxo coletados da etapa 720 são analisados na etapa 730. Por exemplo, os registros de fluxo podem ser agregados, tal como, a formação de uma tabela de registro de fluxo agregada 400 descrita acima.

Continuando com o método de controle de acesso 700, as condições de controle de acesso são definidas na etapa 740. As condições de controle de

acesso predefinidas padrão podem ser usadas para avalia os registros de fluxo. Por exemplo, o endereço ou as portas associadas a uma certa porcentagem ou quantidade de tráfego podem ser identificadas. Por exemplo, o acesso pode ser limitado para os endereços IP de origem 420 com base na maioria das transações 410, tempos de 330, ou na maior quantidade de dados transferidos 430. Estes critérios podem ser objetivos, tal como, estabelecendo um limite máximo para certos critérios ou subjetivos com base em rankings dos critérios através da porta e/ou endereço IP de origem ou alvo com o maior número de ou os mais frequentes consumidores de recursos de rede (ou outros critérios). De maneira opcional, os critérios podem ser fornecidos por um usuário.

A porta e/ou endereço IP de origem ou alvo que satisfaz estes critérios pode ser identificada na etapa 750 com o uso de lógica simples. Na etapa 760, os identificadores da porta e/ou endereço IP de origem ou alvo identificada podem ser apresentados para um usuário. Estes endereços IP de origem (ou outros identificadores de dispositivo) para os dispositivos de rede identificados podem, então, ser colocados em ACL na etapa 770 para solicitar dispositivos de rede para ignorar ou, de outro modo, recusar a transmissão de tráfego associada à portas/endereços identificados, se aprovada por um usuário.

Referindo-se agora à Figura 5, um sistema de controle de acesso 500 de acordo com modalidades da presente invenção é apresentado agora. Conforme descrito acima, um sistema de armazenamento de dados de fluxo 140 pode receber os registros de fluxo brutos 190. O sistema de armazenamento de dados de fluxo 140 pode agregar os registros de fluxo 190, conforme descrito acima, em várias maneiras conhecidas para realizar os objetivos do sistema ou os registros de fluxo podem ser armazenados em uma forma bruta. Os registros de fluxo podem ser acessados e avaliados pela ferramenta de análise de dados 150 de acordo com os critérios recebidos e/ou definidos através da interface de usuário 160 para definir os endereços/portas de rede a serem adicionados a ACLs. Do mesmo modo, deve ser observado que as portas/endereços que não satisfazem o critério predefinido ao longo do período de tempo também podem ser

automaticamente identificadas e sugeridas para o usuário para remoção das ACLs. Tipicamente, qualquer endereço nos registros ou endereços de fluxo na ACL identificado dinamicamente de acordo com o critério predefinido é encaminhado à interface de usuário a ser revisada por um administrador. O administrador pode, então, aprovar a adição/remoção da porta/endereço identificada da ACL.

As ACLs 590 são armazenadas em um dispositivo de rede 520 ou, de maneira opcional, podem ser armazenadas em um sistema de armazenamento de ACL 530 e encaminhadas para qualquer dispositivo de rede 520 que recebe tráfego através de LANs 510 ou da Internet 115. O dispositivo de rede 520 tipicamente recusa o encaminhamento de qualquer tráfego associado a um dispositivo identificado na ACL no dispositivo 520 ou no armazenamento de ACL opcional 530. Ou seja, o tráfego destinado e/ou que se origina a partir de um endereço na ACL chega no dispositivo 520 e não é encaminhado através das redes 510, 115. Quando as comunicações de tráfego atingem o tempo limite, a comunicação é removida do armazenamento e nunca alcança um destino indicado.

Referindo-se agora ao fluxograma de serviço 600 na Figura 6, um nó de rede 610 pode encaminhar relatórios de fluxo 650 que descrevem o tráfego de rede para um sistema de monitoramento de rede 620. Conforme descrito acima, o sistema de monitoramento de rede 620 pode coletar e armazenar os registros de fluxo 650. Os registros de fluxo armazenados 660 podem ser acessados por um sistema de controle de acesso 630 que avalia os registros de fluxo armazenados 660 de acordo com critério predefinido para identificar automaticamente os endereços/portas de rede. Os endereços identificados são encaminhados para uma interface de usuário 640 para serem revisados. Se o endereço/porta identificado for aceito pelo usuário, o endereço/porta pode ser enviado para o nó de rede 610 como os dados de atualização de ACL 680 para implementação da ACL.

Embora a invenção tenha sido descrita em referência às modalidades

exemplificativas, diversas adições, exclusões, substituições ou outras modificações podem ser efetuadas sem sair do espírito e escopo da invenção. Consequentemente, a invenção não deve ser considerada limitada pela descrição precedente, porém, apenas limitadas pelo escopo das reivindicações em anexo.

REIVINDICAÇÕES

1. Sistema para controlar dinamicamente comunicações de rede, **CARACTERIZADO** pelo fato de que o sistema compreende:

um dispositivo de rede configurado para receber tráfego de rede e produzir uma pluralidade de registros de fluxo que descrevem o dito tráfego de rede;

um armazenamento de registro de fluxo configurado para receber os ditos registros de fluxo do dito dispositivo de rede e armazenar os ditos registros de fluxo; e

uma ferramenta de análise de dados configurada para acessar o dito armazenamento de registro de fluxo para recolher os ditos registros de fluxo armazenados e avaliar cada um dos ditos registros de fluxo de acordo com os critérios predefinidos para identificar dinamicamente um endereço, sendo que a ferramenta de análise de dados é configurada adicionalmente para implementar modelos estatísticos configurados para resolver problemas relacionados ao uso da rede, e sendo que a ferramenta de análise de dados usa os registros de fluxo e modelos estatísticos para gerar um resultado estatístico que então é armazenado no armazenamento de registro de fluxo;

sendo que cada um da dita pluralidade de registros de fluxo compreende um número de sequência identificando o registro de fluxo, um endereço de nó de origem, um endereço de nó de destino, um endereço de porta de origem, um endereço de porta de destino, e número de bytes ou pacotes transmitidos em cada fluxo associado, e

sendo que os critérios predefinidos compreendem o número total de bytes transmitido no fluxo associado para cada um dos endereços de nó ou porta,

sendo que o dispositivo de rede é configurado para receber o dito endereço identificado e adicionar o dito endereço identificado em uma lista de controle de acesso para evitar tráfego de encaminhamento associado com o dito endereço identificado; e

um dispositivo de entrada/saída configurado para exibir a um usuário o dito endereço identificado recebido da ferramenta de análise de dados, e sendo que a ferramenta de análise de dados é configurada para encaminhar o endereço identificado para o dispositivo de rede para ser adicionado à lista de controle de acesso apenas se o usuário proporcionar uma entrada para aceitar do endereço identificado.

2. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que compreende adicionalmente um armazenamento de lista de controle de acesso configurado para armazenar o dito endereço identificado e proporcionar o dito endereço identificado para o dispositivo de rede.

3. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que os ditos registros de fluxo são agregados de acordo com os ditos endereços de nó e/ou porta.

4. Sistema, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que o dispositivo de entrada/saída adquire e exibe adicionalmente os dados de registros de fluxo associados ao dito endereço identificado.

5. Método para gerenciar rede, **CARACTERIZADO** pelo fato que compreende:

monitorar o tráfego através dos componentes na rede;

receber os registros de fluxo a partir dos ditos componentes que descrevem o dito tráfego;

analisar os registros de fluxo e identificar um endereço que atenda um critério predefinido, em que o critério predefinido compreende um número total máximo de bytes associados a um endereço;

exibir para um usuário o dito endereço identificado; e

após o usuário aprovar o endereço identificado, encaminhar o endereço identificado para um dos componentes de rede, sendo que o dito componente adiciona o endereço identificado a uma lista de controle de

acesso associada, sendo que a dita lista de controle de acesso direciona o componente para evitar o tráfego de encaminhamento associado ao dito endereço identificado.

6. Método, de acordo com reivindicação 5, **CARACTERIZADO** pelo fato de que o dito endereço identificado é automaticamente removido da lista de controle de acesso após um período de tempo predefinido.

7. Método, de acordo com reivindicação 5, **CARACTERIZADO** pelo fato de que o dito endereço identifica pelo menos um entre um nó de origem, um nó de destino, uma porta de origem e uma porta de destino.

8. Método, de acordo com reivindicação 7, **CARACTERIZADO** pelo fato de que o dito endereço identifica um nó de origem.

9. Método, de acordo com reivindicação 5, **CARACTERIZADO** pelo fato de que compreende adicionalmente exibir para o usuário os dados de registros de fluxo associados ao dito endereço identificado.

10. Sistema para controlar dinamicamente o tráfego em uma rede, **CARACTERIZADO** pelo fato de que o sistema compreende:

um dispositivo de geração de registro de fluxo configurado para proporcionar os registros de fluxo que descrevem o dito tráfego de rede;

um sistema de armazenamento de registro de fluxo configurado para receber e armazenar os registros de fluxo;

um dispositivo de análise de dados configurado para acessar o sistema de armazenamento e avaliar os registros de fluxo armazenados de acordo com os critérios predefinidos;

sendo que o dispositivo de análise de dados é configurado para identificar dinamicamente pelo menos um endereço que satisfaz os ditos critérios predefinidos, o dito pelo menos um endereço compreendendo um endereço de porta ou de nó associado ao tráfego; e

sendo que o pelo menos um endereço identificado é adicionado a uma lista de controle de acesso e os componentes na rede não irão encaminhar o tráfego associado aos endereços na lista de controle de

acesso,

sendo que cada um dos ditos registros de fluxo compreende um carimbo de data/hora, e sendo que os critérios predefinidos compreendem uma janela de tempo.

11. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o sistema de armazenamento de dados de fluxo é configurado para agregar os registros de fluxo.

12. Sistema, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que compreende adicionalmente uma interface de usuário configurada para exibir para um usuário o dito endereço identificado, e por meio do qual o endereço identificado é adicionado à lista de controle de acesso somente após o usuário aceitar o endereço identificado.

13. Sistema, de acordo com a reivindicação 12, **CARACTERIZADO** pelo fato de que a interface de usuário é adicionalmente configurada para exibir para o usuário os dados de registros de fluxo associados ao dito endereço identificado.

14. Método para avaliar um endereço em uma lista de controle de acesso, **CARACTERIZADO** pelo fato de que método compreende:

monitorar o tráfego através dos componentes na rede;

receber os registros de fluxo a partir dos ditos componentes que descrevem o dito tráfego;

analisar qualquer um dos ditos registros de fluxo recebidos associados ao dito endereço na lista de controle de acesso de acordo com um critério predefinido;

renovar o endereço na lista de controle de acesso se o dito endereço satisfizer o dito critério predefinido; e

exibir para um usuário o dito endereço, e por meio do qual a renovação do endereço ocorre após o usuário aprovar o endereço.

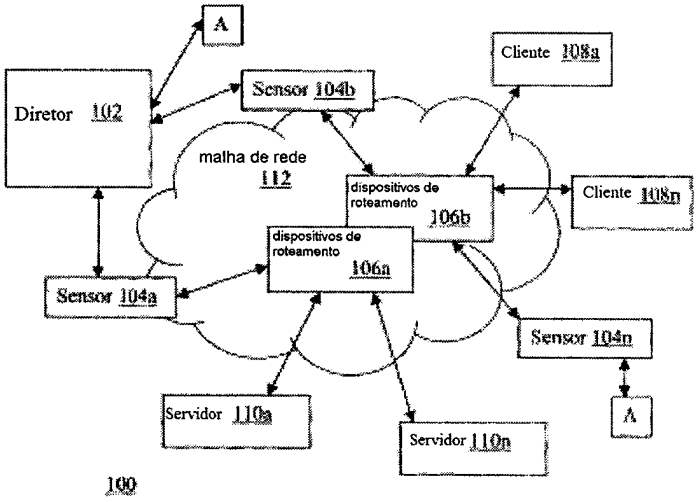
15. Método, de acordo com reivindicação 14,

CARACTERIZADO pelo fato de que compreende adicionalmente exibir para o usuário os dados de registros de fluxo associados ao dito endereço.

16. Método, de acordo com reivindicação 14, **CARACTERIZADO** pelo fato de que o dito endereço identifica pelo menos um entre um nó de origem, um nó de destino, uma porta de origem e uma porta de destino.

17. Método, de acordo com reivindicação 14, **CARACTERIZADO** pelo fato de que o dito endereço é automaticamente removido da lista de controle de acesso após um período de tempo predefinido.

Figura 1A


A
Diretor 102
Sensor 104b
Cliente 108a
malha de rede
112
dispositivos de
roteamento
106b
Cliente 108n
dispositivos de
roteamento
106n
Sensor 104a
Sensor 104n
A
Servidor 110a
Servidor 110n
100

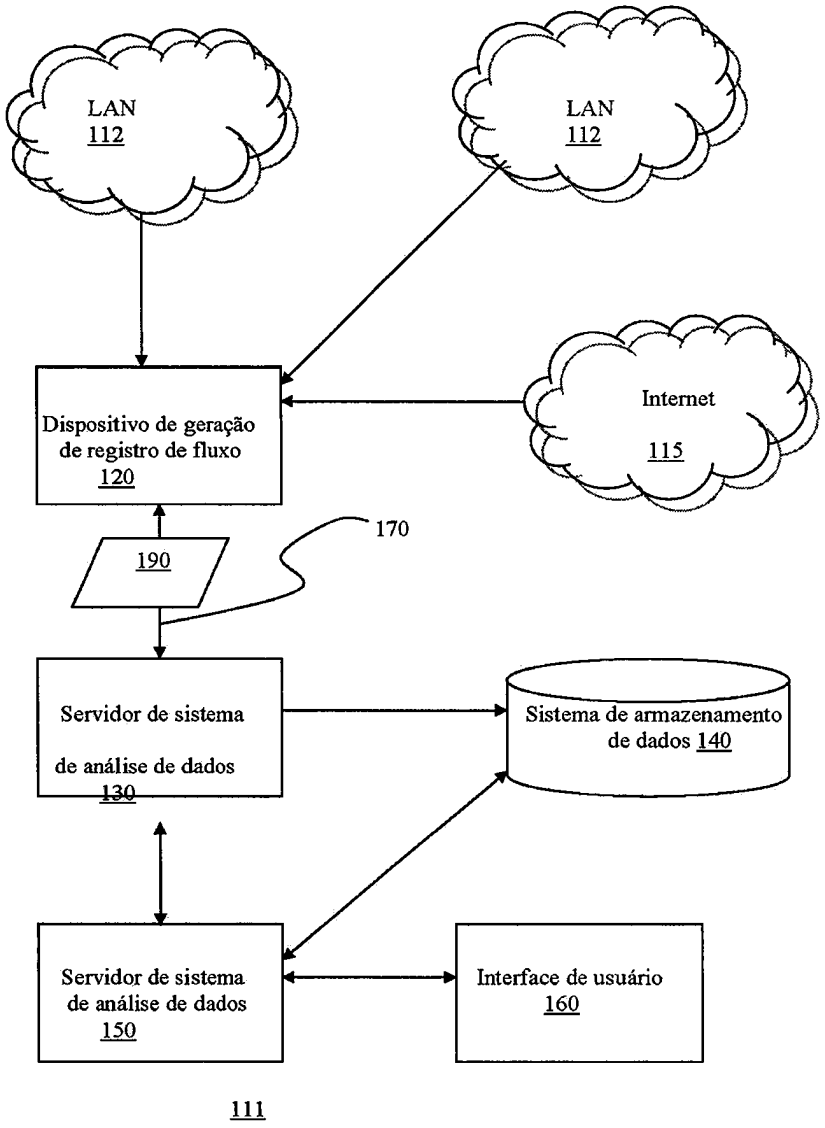


Figura 1B
(Técnica Anterior)

Registro de fluxo exemplificativo
200

número de versão de fluxo	210
número de sequência	220
índices SNMP de interface de entrada e saída	230
carimbos de data/hora para o tempo de início e término	240
número de bytes e pacotes observado no fluxo	250
cabeçalhos de 3 camadas, que incluem endereços IP de origem & destino, números de porta de origem e destino, protocolo IP e valor de Tipo de Serviço (ToS)	260
para fluxos TCP, a união de todos os sinalizadores TCP observados ao longo da vida útil do fluxo.	270

Figura 2

(Técnica Anterior)

Número de registro de fluxo 310	Endereço IP de origem 320	Carimbo de data/hora 330	Tamanho de byte 340
1	xxx.xxx.x.1	t_1	10
2	xxx.xxx.x.1	t_2	20
3	xxx.xxx.x.2	t_3	1000
4	xxx.xxx.x.2	t_4	2000
5	xxx.xxx.x.1	t_5	30
6	xxx.xxx.x.3	t_6	10
7	xxx.xxx.x.1	t_7	40

Tabela de fluxo exemplificativa 300

Figura 3

Números de registro de fluxo 410	Endereço IP de origem 420	Tamanho de byte total 430
4	xxx.xxx.x.1	100
2	xxx.xxx.x.2	3000
1	xxx.xxx.x.3	10

Tabela de fluxo agregada 400

Figura 4

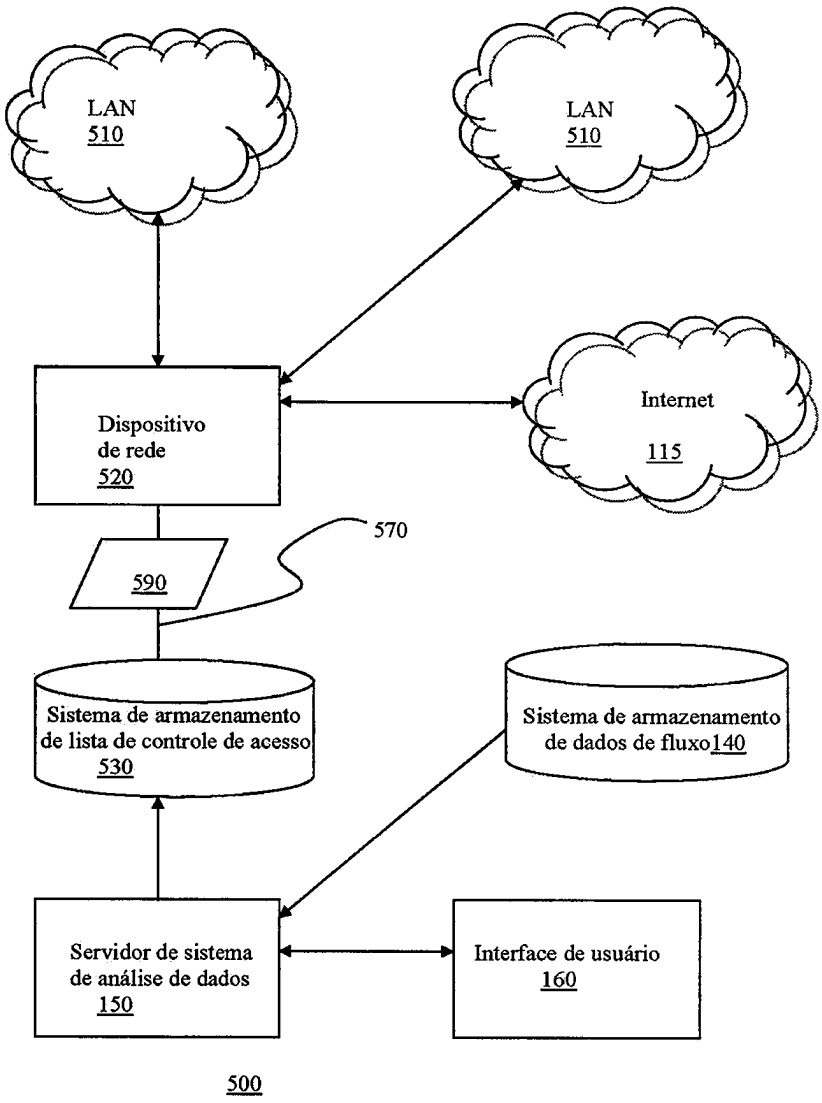
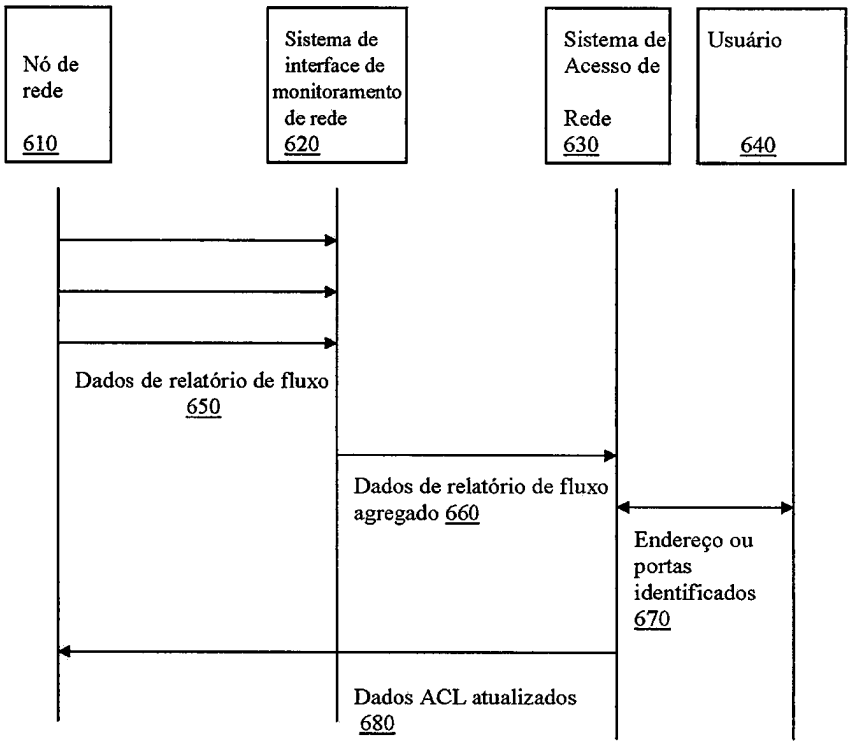

LAN
510
LAN
510
Internet
115
Dispositivo
de rede
520
570
590
Sistema de armazenamento
de lista de controle de acesso
530
Sistema de armazenamento
de dados de fluxo140
Servidor de sistema
de análise de dados
150
Interface de usuário
160
500

Figura 5


Nó de rede
610
Sistema de interface de monitoramento de rede
620
Sistema de Acesso de Rede
630
Usuário
640
Dados de relatório de fluxo
650
Dados de relatório de fluxo agregado 660
Endereço ou portas identificados
670
Dados ACL atualizados
680

600

Figura 6

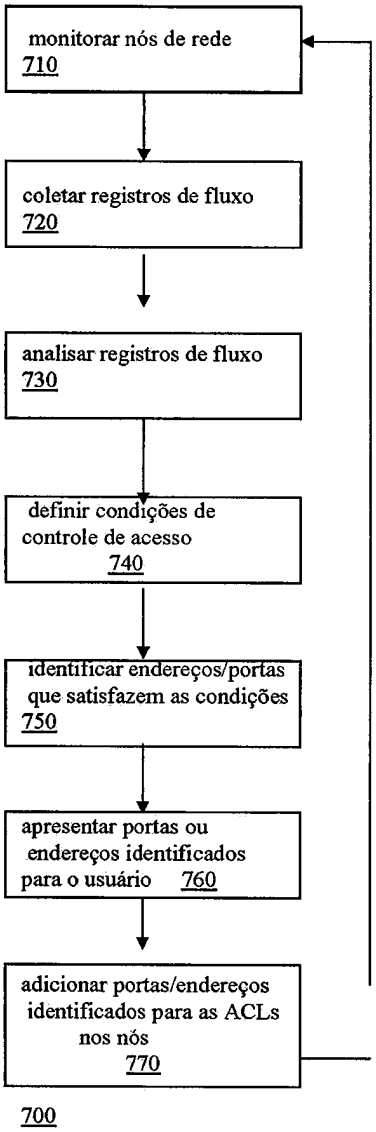

monitorar nós de rede
710
coletar registros de fluxo
720
analisar registros de fluxo
730
definir condições de
controle de acesso
740
identificar endereços/portas
que satisfazem as condições
750
apresentar portas ou
endereços identificados
para o usuário 760
adicionar portas/endereços
identificados para as ACLs
nos nós
770
700

Figura 7