(11) Número de Publicação: **PT 1735983 E**

(51) Classificação Internacional:
H04L 29/06 (2007.10)

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

(22) Data de pedido: **2004.04.14**

(30) Prioridade(s):

(43) Data de publicação do pedido: **2006.12.27**

(45) Data e BPI da concessão: **2008.02.06**
095/2008

(73) Titular(es):
TELECOM ITALIA S.P.A.
PIAZZA DEGLI AFFARI, 2 20123 MILANO **IT**

(72) Inventor(es):
EUGENIO MARIA MAFFIONE **IT**
GIOVANNI GAMBARO **IT**

(74) Mandatário:
MANUEL GOMES MONIZ PEREIRA
RUA ARCO DA CONCEIÇÃO, N.º 3, 1º ANDAR 1100-028
LISBOA **PT**

(54) Epígrafe: **MÉTODO E SISTEMA PARA GERIR DISTRIBUIÇÃO DE CONTEÚDOS EM REDES DE COMUNICAÇÃO**

(57) Resumo:

DESCRIÇÃO

MÉTODO E SISTEMA PARA GERIR DISTRIBUIÇÃO DE CONTEÚDOS EM REDES DE COMUNICAÇÃO

Campo da Invenção

A presente invenção refere-se à distribuição de conteúdos em redes de comunicações.

A invenção foi desenvolvida dando a atenção específica à aplicação possível numa situação de Internet, por exemplo para controlar o acesso aos conteúdos dos meios nos contextos operacionais em que uma ou mais tecnologias "verticais" são usadas para entregar e aceder a conteúdos de meios dentro de uma rede móvel e/ou fixa.

Descrição das técnicas relacionadas

Nos últimos anos, os serviços disponíveis na Internet e/ou dentro das intranets das empresas e baseados na distribuição de conteúdos dos meios (em especial do tipo multimédia) conseguiram um significado particular. Isto é suportado quer pela disponibilidade de larguras de banda maiores de transmissão para o acesso, quer pelo constante aumento no número e nos tipos dos conteúdos que se encontram disponíveis para serem entregues.

Para além dos conteúdos tradicionais da Internet, outros conteúdos de multimédia "ricos" tais como as transmissões de vídeo (tanto o que é feito a pedido como o que é transmitido ao vivo) fornecem agora serviços que são particularmente importantes para os utilizadores (o E-learning, a transmissão da Internet, o vídeo a Pedido...). Esta situação torna-se

cada vez mais rica devido aos tipos novos de conteúdos que são suportados tipicamente pelas plataformas verticais fornecidas por fornecedores específicos e especializados: exemplos do afirmado são as plataformas para os jogos a pedido e para as aplicações à medida.

Os conteúdos são fornecidos a partir de um centro de serviços de fornecedor de conteúdos (CP) para um Local de Utilizador (US) onde reside um Solicitador de Conteúdos (CR) através de uma rede N (Acesso+Metro+Transporte).

Como regra, de modo a tornar um serviço disponível para ser distribuído, é necessário que o conteúdo, o servidor de conteúdos CP e o Solicitador de Conteúdos CR satisfaçam as limitações específicas em termos de compatibilidade. Em termos práticos, os componentes localizados nas posições de extremidade (que é o servidor CP e o solicitador CR) devem usar programas informáticos que sejam correspondentes/ compatíveis com uma tecnologia comum.

Por este motivo, mesmo referindo-se somente à transmissão de conteúdos, existem vários tipos de tecnologias como as que se encontram descritas em "Windows Media 9 Series Deployment Guide", Microsoft, Dezembro de 2002, páginas 47- 51 ou em "Helix Universal Server Admninistration Guide, Version 9.0", Real Networks, 19 de Maio de 2003, páginas 247-299.

Cada uma das referidas tecnologias é caracterizada por características específicas em temos das plataformas de programas informáticos disponíveis (por exemplo, terminais móveis, PCs, PDAs, Caixas Descodificadoras), estando os programas informáticos disponíveis com o servidor e com os correspondentes mecanismos de autorização.

Uma tal técnica foi definida como sendo uma técnica "vertical" enquanto um utilizador final pode ter instalado no seu sistema um programa informático adaptado para fazer pelo menos a "leitura" de uma tecnologia do conteúdo, sendo a tarefa mais relevante colocada no centro de serviços CP. De facto, o centro de serviços deve estar equipado com servidores de entrega assim como com processos de autorização e sistemas que são especificamente dedicados a cada tecnologia dedicada a ser suportada pelo centro.

Uma disposição típica referenciada como sendo uma arquitectura "centralizada" encontra-se ilustrada na figura 1. Isto inclui essencialmente dois blocos funcionais que se encontram localizados fisicamente em pontos diferentes:

- por um lado, o Solicitador de Conteúdos CR inclui um terminal de utilizador e os programas informáticos relacionados que são carregados no mesmo, estando ambos os componentes localizados no utilizador (possivelmente incluindo um telefone celular), e

- por outro lado, o centro de serviços CP inclui baterias de servidores 10, 12, cada uma delas disposta de modo a proporcionar um determinado conjunto de serviço em relação a uma determinada tecnologia, dependendo do número de pedidos em simultâneo destinados a serem geridos. Cada bateria 10, 12 associou um servidor de autorização respectivo 10a, 12a assim como uma base de dados de autorizações associada 10b, 12b. Cada um dos conjuntos constituído por uma bateria de servidores, sendo o servidor de autorizações correspondente e a base de dados associada actualmente referenciados como sendo a "quinta dos conteúdos".

De um modo resumido, na disposição centralizada ilustrada na figura 1, o centro de serviço CP terá de incluir - por necessidade - uma pluralidade de quintas de conteúdos diferentes correspondentes ao número de tecnologias diferentes destinadas a serem suportadas pelo centro.

Ao fazer-se especificamente referência às tecnologias da Microsoft e da Real Networks referenciadas de seguida, uma disposição como a ilustrada na figura 1 requer procedimentos e mecanismos respectivos para a gestão da autorização do acesso aos conteúdos respectivos. Estes procedimentos e estes mecanismos não são directamente compatíveis: por exemplo, o acesso e/ou a autorização podem ser controlados por intermédio de acessórios do proprietário que efectuam o controlo ao longo do sistema de ficheiros que armazenam o conteúdo dos endereços de IP dos utilizadores que lhes acedem.

Em outras tecnologias, a autorização é baseada na verificação de uma tabela externa, a qual pode ser constituída por um simples ficheiro de texto, por uma base de dados num formato de proprietário ou numa base de dados de SQL (Structured Query Language) aberta.

De um modo resumido, uma disposição de acordo com a revelada na figura 1 requer que não somente as baterias de servidores 10, 12 são univocamente dedicadas a uma única tecnologia de conteúdos: a mesma separação aplica-se, de facto, também ao processo e ao sistema que efectuam as tarefas de autorização. Isto exige componentes de gestão e de controlo que são especializados e dedicados a cada uma das tecnologias, em que cada componente é de facto incompatível com os componentes

homólogos para as outras tecnologias que possivelmente se encontram presentes no centro de serviços.

Isto significa, entre outras coisas, que quando uma nova tecnologia de distribuição de conteúdos é adicionada ao centro não existe possibilidade prática de extrair vantagem de qualquer instalação já instalada e, deste modo, beneficiando de quaisquer factores de escala.

Devido à perspectiva mais ampla do tipo novo de conteúdos (jogos a pedido, pedidos por pedido, e assim por diante) e à oferta possível de soluções verticais novas por parte de vendedores tecnológicos, pelos componentes da autorização de programas de informática/material físico e por processos correm o risco de se transformarem num problema real para os fornecedores que fazem funcionar os centros de serviços.

Para além das arquitecturas centralizadas baseadas no conceito do centro de serviço, uma evolução foi seguida em épocas recentes para conseguir a disposição mostrada na figura 2. Este é essencialmente uma designada disposição de rede de conteúdos (CDN).

Num contexto CDN (de acordo com o revelado, por exemplo, em "Cisco ACNS 5.1 Caching And Streaming Configuration Guide, Release 5.1", 2003, Cisco, páginas 227-270, Text Part N.OL-4070-01), os servidores periféricos designados como servidores “hospedeiros” 14 tomam o lugar dos servidores centralizados da disposição da figura 1. Os servidores hospedeiros estão fisicamente mais próximos dos utilizadores (em que a rede N ilustrada na figura 2 é essencialmente constituída pelo acesso e pela rede metropolitana e de um modo geral não compreendem já a própria rede de transporte).

Deste modo, os servidores hospedeiros 14 estão numa posição para distribuir os conteúdos através da exploração de uma maior largura de banda.

Na disposição que se encontra ilustrada na figura 2, qualquer pedido apresentado pelo Solicitador de Conteúdos CR é encaminhado de novo através de um sistema central (designado como encaminhador de conteúdos CDNCR) na direcção de um servidor 14 em que os conteúdos solicitados e encontram disponíveis. Um tal servidor 14 é seleccionado como sendo o mais adequado em termos de recursos disponíveis e da "distância" ao longo da rede. Após um tal processo de reencaminhamento (encaminhamento de conteúdo), o processo de acesso ao conteúdo do servidor hospedeiro seleccionado é essencialmente análogo ao processo que tem lugar na disposição de acordo com a figura 1.

Numa forma de realização habitual, a arquitectura CDN pertence e é gerida por um operador de rede que oferece aos vários fornecedores de conteúdos a possibilidade de usarem a infra-estrutura CDN para tornar mais fácil a distribuição e a entrega dos conteúdos respectivos.

Uma característica típica dos servidores hospedeiros 14 num CDN é que eles não se encontram dedicados a uma única tecnologia de conteúdo: eles são de facto concebidos de modo a servirem ao mesmo tempo pedidos de diferentes tipos de conteúdos (por exemplo, Real, Windows Media entre outros). Deste modo, comportam-se essencialmente como servidores de tecnologia múltipla devido à sua capacidade de integrarem componentes de serviço das várias tecnologias, deixando deste modo estes componentes coexistirem no interior de um único servidor hospedeiro 14.

A arquitectura de CDN mostrada em figura 2 não é isenta de um determinado grau de complexidade. Além dos problemas do factor de escala relacionados com a gestão dos processos de autorização para as tecnologias diferentes usadas (com a necessidade inerente de ter um módulo específico 14a de autorização disponível para cada tecnologia específica), um problema adicional levanta-se devido à probabilidade de os conteúdos de cada servidor hospedeiro 14 se encontrarem relacionados com os diferentes fornecedores de conteúdos, tendo políticas diferentes de autorização/ licenciamento.

Isto vai de facto aumentar a complexidade do processo de autorização do acesso, tornando assim praticamente impossível fazer a distribuição de uma maneira exacta e "granular" os critérios e os métodos da autorização aos conteúdos tornados disponíveis por fornecedores de conteúdos diferentes. Ao adicionarem-se novas tecnologias de conteúdos (como os jogos a pedido ou as aplicações à medida) a uma arquitectura distribuída como a mostrada na figura 2 pode revelar-se ser ainda mais complexo do que no caso da distribuição centralizada mostrada na figura 1.

De facto, em ambas as arquitecturas mostradas nas figuras 1 e 2, o controlo do acesso aos conteúdos transforma-se num assunto de importância crítica para o operador de rede e para o fornecedor de conteúdos, em especial em relação à facturação pelo operador. Isto torna-se particularmente evidente caso se considere o exemplo de um serviço que, com base numa subscrição ao próprio serviço, forneça um acesso não diferenciado aos conteúdos. Este pode ser o exemplo típico de uma subscrição a um serviço de ADSL residencial. Ao passar desse serviço para o acesso baseado numa facturação pré-paga em que a facturação se encontra diferenciada em

função dos conteúdos específicos pedidos (como pode ser o caso para o acesso pré-pago através de um telefone celular), a possibilidade de detectar sob circunstâncias em tempo real - isto é, quando o pedido é feito - as tentativas possíveis de um acesso fraudulento transformam-se num assunto de importância estratégica (se não vital).

O controlo em tempo real possível não se encontra por si univocamente relacionado com a intervenção em tempo real contra à tentativa fraudulenta. De facto um operador pode decidir - sob circunstâncias específicas - tolerar uma tentativa fraudulenta durante uma determinada quantidade de tempo, ao mesmo tempo que se reserva no direito de tomar as acções mais apropriadas tendo em vista, por exemplo, técnicas de comercialização específicas.

Relativamente a este ponto, a maioria das disposições da técnica anterior são baseadas em técnicas em que um dispositivo do controlo é fornecido já adaptado para agir de uma maneira transparente no fluxo de dados entre o utilizador e o servidor que fornece o serviço ao efectuar o controlo de acesso baseado em determinadas regras internas.

Por exemplo em "Cisco Content Service Switch Basic Configuration Guide, Version 7.20", Março de 2003, Cisco, Capítulos 3 e 5, Text part number 78-13886-05, é revelado um conjunto de dispositivos designados CSS (Content Service Switch) e que se encontram adaptados para funcionar sobre o fluxo de dados entre um cliente e um servidor. Os dispositivos definem regras estáticas aplicadas ao tráfego cliente/ servidor. Estes são adaptados para ser aplicados a grupos de clientes (tendo determinados endereços de sub-rede ou de IP, servidores, tendo um determinado endereço de IP ou

domínios de DNS), tipos de conteúdos (por exemplo extensão do nome de arquivo ou URL), baseados nas listas que podem ser definidas antecipadamente, configuradas nos vários aparelhos. Baseados em tais regras (programadas a partir do exterior), o dispositivo analisa o tráfego e decide como este deve ser distribuído, ou seja se algum tráfego deve ser enviado sem modificação, filtrado para obstruir o seu trânsito ou redirigido para destinos alternativos (este é o caso típico quando o serviço é incapaz de alcançar determinados conteúdos).

Tais dispositivos requerem obrigatoriamente que as regras de autorização sejam previamente configuradas nos próprios dispositivos. Isto revela-se ser uma solução crítica por pelo menos duas razões.

Uma primeira razão está relacionada com o número máximo de autorizações que podem ser configuradas. Este número pode alcançar um valor muito elevado, de um modo geral superior à capacidade do próprio sistema (25 000 regras no total) tendo de ser tomadas em linha de conta todas as combinações possíveis de utilizadores/ conteúdos. Numa forma de realização habitual, 100 listas de acesso designadas como Listas de Controlo de Acesso (ACL) podem ser definidas, estando cada uma delas adaptada para incluir, no máximo, 254 “cláusulas”. Dentro de cada uma das cláusulas há a possibilidade de definir um utilizador isolado e um conteúdo isolado ou grupos de utilizadores e/ ou de conteúdos. Em termos práticos, todos estes grupos são estáticos por si e não são de modo algum úteis para compor regras.

Um segundo factor crítico centra-se no facto da pré-configuração de tais regras não permitir o controlo dinâmico

das autorizações. Não é possível activar ou desactivar um determinado utilizador em relação a um determinado conteúdo dependendo da condição de poder variar de um modo rápido ou externo em relação ao próprio dispositivo, por exemplo em consequência de uma subscrição nova que está a ser activada, de um crédito que está a ficar esgotado, de um crédito novo que está a ser adquirido, de campanhas promocionais.

O documento WO-A-99/57866 divulga um sistema do redireccionamento dos dados para dirigir de novo os dados do utilizador com base num conjunto de regras armazenado. A aproximação correspondente é baseada num Proxy da Aplicação. Isto é particularmente incómodo em termos das exigências do dispositivo, pois requer um módulo de emulação para cada serviço/ tecnologia suportado pelo sistema. Um módulo dedicado do programa informático, dependente da tecnologia é deste modo requerido para cada tecnologia a ser distribuída. Um problema adicional reside no facto de que tal módulo específico do programa informático pode não estar disponível para a integração no sistema. Este pode ser o caso quando as tecnologias de distribuição do conteúdo envolvidas são tecnologias do proprietário, uma situação bastante actual para por exemplo jogos a pedido ou aplicações à medida.

Uma outra disposição alternativa encontra-se revelada em vários documentos cedidos a Nomadix, Inc., como sejam as Patentes US-B-6 130 892, US-B-6 636 894, WO-A-01/31886 ou a WO-A-02/35797.

A solução Nomadix pode ser aplicada à rede de acesso para a filtragem dos conteúdos distribuídos por uma arquitectura de Distribuição de Conteúdos através do preenchimento de três requisitos básicos:

- análise do conjunto de pedidos do Solicitador de Conteúdos sem requerer módulos adicionais de programas informáticos dedicados ao protocolo ou à tecnologia de distribuição de conteúdos,

- envio e recepção do pedido de autorização enviado para um servidor externo, e

- actuar sobre a autorização para possivelmente negar ou redireccionar o pedido original do utilizador (o qual no entanto necessita de módulos de programas informáticos específicos para o redireccionamento da aplicação).

Para além do problema da proporcionalidade escalar da aplicação, que é relacionado com o redireccionamento, o dispositivo da Nomadix apresenta um número de pontos críticos no que diz respeito ao uso de serviços de Distribuição de Conteúdos nos contextos considerados anteriormente.

Como primeiro ponto, o dispositivo da Nomadix é situado na rede de acesso de telecomunicações do operador. Isto representa uma penalidade séria de realização para o operador. Isto é particularmente verdadeiro no caso de uma rede fixa que requer um número elevado de dispositivos em comparação com outras disposições em que a posição está mais perto da origem (ou seja com o Local de Conteúdos do CDN ou com o Centro de Serviço numa arquitectura centralizada).

Em segundo lugar, o dispositivo da Nomadix controla e bloqueia o pedido que vem do cliente. Em consequência, o tempo envolvido no processo de receber o pedido do cliente, de obtenção da autorização com um sistema centralizado, de fornecimento de uma resposta subsequente e do envio do pedido

pode ser muito longo para dar origem a um desligar da aplicação por parte do Solicitador de Pedido e do Servidor de Conteúdo. Tal disposição não se encontra adaptada para o uso em um contexto móvel onde a conformidade com exigências em tempo real seja vital para assegurar a segurança contra os comportamentos fraudulentos quando, por outro lado, as latências da transmissão não podem ser menores.

Finalmente quando o dispositivo da Nomadix suporta de comunicação serviços de contabilidade, ele emite um registo de contabilidade baseado exclusivamente no pedido de conteúdos. No caso de uma anomalia na resposta pelo servidor de distribuição, isto pode resultar numa falsa sinalização (e na facturação incorrecta) quando não existir a possibilidade de fornecer uma contagem do tempo efectivamente distribuído desde que o fim da entrega não é detectado.

Objecto e resumo da invenção

É deste modo sentida a necessidade de disposições adaptadas para ultrapassar as limitações das disposições de acordo com as técnicas anteriores acima indicadas adicionando, por exemplo, outras funções mais adaptadas para a contabilidade, dando ao mesmo tempo origem a uma autorização (e a uma contabilidade) em tempo real adaptados para o controlo ao acesso aos conteúdos. De um modo específico sente-se a necessidade de unidades em que os critérios de controlo dinâmico independentes da tecnologia permitem um elevado grau de liberdade na selecção da "granularidade" da acção de controlo. Isto vai permitir que seja livremente referido em relação a parâmetros como sejam o agrupamento lógico de sub-rede/URL/servidor de conteúdos numa combinação seleccionada de um modo livre actuando indiferentemente tanto no fluxo de

pedido como no fluxo de resposta (conteúdos a serem distribuídos) ao fornecerem em paralelo um suporte mais completo para fins de contabilidade.

O objecto da presente invenção é proporcionar uma disposição que satisfaça estas necessidades.

De acordo com a presente invenção, esse objecto é conseguido por meio de um método que tem as características determinadas nas reivindicações que se seguem. A invenção refere-se também a um sistema correspondente, a uma rede relacionada assim como a um produto de programa de computador que pode ser carregado na memória de pelo menos um computador e incluindo parcelas do código do programa informático para executar as etapas do método da invenção quando o produto é feito correr num computador. Como usado no presente, a referência a tal produto do programa de computador é destinada a ser equivalente à referência a um meio que pode ser lido por um computador e que contém instruções para controlar um sistema de computador para coordenar o desempenho do método da invenção. A referência a "pelo menos um computador" é evidentemente destinada a destacar a possibilidade de a presente invenção ser executada em uma forma distribuída/ modular.

Uma forma de realização preferida da presente invenção é assim um sistema para processar transacções numa rede de comunicação, em que transacções incluem pelo menos um pedido dependente da tecnologia para um dado conteúdo feito por um solicitador a pelo menos um utilizador. O sistema opera com base no acesso de uma lista de conteúdos incluindo as cláusulas de permissão/ negação de acesso que regulam o acesso dos solicitadores aos conteúdos fornecidos pelo

servidor. Um módulo de processando é fornecido estando configurado para a detecção do pedido dependente da tecnologia, e extraindo do mesmo as informações que identificam o solicitador que faz o pedido e o conteúdo solicitado. Uma entrada independente da tecnologia correspondente ao conteúdo do acesso pode assim ser gerada adaptada para ser verificada por comparação com a lista de conteúdo de acesso para deduzir as informações de permissão/ negação a respeito do pedido detectado. O pedido é distribuído como uma função das informações de permissão/ negação derivadas e assim por exemplo i) enviadas para o servidor, ou ii) ou abandonadas ou enviadas para um destino alternativo. O acesso aos vários conteúdos distribuídos é controlado de uma maneira que é independente das tecnologias específicas usadas para a distribuição dos conteúdos de meios.

A disposição aqui descrita encontra-se, deste modo, adaptada para efectuar uma acção de controlo em relação a qualquer um dos que se seguem:

- o tipo de conteúdo (imagem, ficheiro, transmissão de vídeo, páginas da Internet),

- o tipo de protocolo usado para a distribuição de conteúdos para o utilizador (http, https, http progressivo, mms, rtsp, ftp, …),

- a arquitectura de distribuição (servidor centralizado, servidores hospedeiros ou CDN),

- o tipo de cliente que solicita a distribuição de conteúdos (Caixa descodificadora, computador pessoal, telefone celular, …),

- o tipo de ligação de IP (sem fios, GPRS, Ethernet, …)

Uma forma de realização particularmente preferida da presente invenção proporciona a presença de um componente centralizado de controlo (agindo como um servidor de conteúdo e de política de segurança) adaptado para verificar as condições em tempo real e as autorizações de utilizador/ conteúdos para gerir de uma maneira unitária as autorizações para todas as tecnologias e tipos os tipos de conteúdos (actuais e futuros). Isto funciona primeiramente no identificador do utilizador e na referência ao conteúdo pedido, unificando assim o método de autorização.

De um modo adicional, pelo menos um dispositivo de rede é de preferência fornecido e actua como uma porta de comunicação de acesso de conteúdo condicional dinâmico (DCCA). Uma tal porta de comunicação pode estar adaptada para desempenhar, para todas as tecnologias (actuais e futuras) as seguintes funções:

- análise de tráfego transparente, ao por em vigor uma lógica de controlo bilateral para o pedido, actuando sobre os próprios pedidos ou agindo sobre o trafico que retorna para o utilizador, ao mesmo tempo que toma em consideração - a todos os níveis (ligação de dados, rede, transporte e aplicação) - as informações derivadas do mesmo. Esta análise é referida como sendo “transparente” desde que seja capaz de agir sem modificar a arquitectura de IP, e é capaz de agir numa disposição de comutação em posta (nível 2 da pilha OSI);

- a recepção e o envio de pedidos de autorização ao componente de controlo central com base num formato unitário para todos os tipos de conteúdos ao identificar o conteúdo solicitado e o utilizador de um modo que é completamente independente das características específicas das tecnologias adaptadas para a distribuição de conteúdos (tipo de conteúdos, protocolo, cliente, servidor, arquitectura, capacidade de ligação);

- a implementação da autorização no fluxo com uma técnica bilateral interrompendo o fluxo de pedido sem o enviar para o servidor de conteúdos (por exemplo o controlo em linha sobre o pedido) ou bloqueando o fluxo de retorno para solicitador de conteúdos (por exemplo, controlo activo atrasado na resposta), ao mesmo tempo que se controla o próprio fluxo para suportar a função de contabilidade;

- a possibilidade de redireccionar o pedido, quando o controlo é efectuado a pedido, com base nos mesmos critérios transparentes considerados para fins de análise, modificando deste modo a referência ao conteúdo solicitado contido no conjunto de carga ao mesmo tempo que é mantida activa a sessão de comunicações estabelecida com o servidor de conteúdos, sem a intervenção de qualquer módulo de um programa informático especialmente dedicado a uma dada tecnologia.

Uma forma de realização preferencial da disposição descrita na presente proporciona o dispositivo de rede em questão de modo a que o mesmo seja empregue em associação com a bateria ou conjunto de servidores de conteúdos do centro de serviços, ou através da sua colocação com o mesmo ou através da sua disposição em ligação com os servidores hospedeiros em cada

um dos locais da arquitectura CDN ao serem localizados no mesmo ponto. Desta forma a disposição resultante é significativamente mais eficaz em comparação com as disposições baseadas no local num ponto de acesso à própria rede, sendo, no entanto, esta ultima disposição implementada em caso de necessidade.

Em resumo, a disposição descrita na presente satisfaz todas as necessidades possíveis para o controle dinâmico do acesso de conteúdos anteriormente indicado.

De um modo específico, a disposição descrita na presente proporciona uma solução que é:

- completamente transparente em relação à arquitectura de distribuição de conteúdos, em relação ao cliente e ao conteúdo assim como à arquitectura de PI usada devido, entre outros, à possibilidade de funcionar como uma disposição de comutação/ em ponte;

- escalonável, na porção dedicada ao processamento da autorização (de um modo centralizado) é diferente da parte dedicada à acção de desencadeamento/ filtragem;

- de um tipo muito granular pois permite uma definição das permissões de acesso ao conteúdo com base em quaisquer itens de informações adaptados para serem derivados numa ligação de dados, numa rede, em níveis de transporte e de aplicação;

- muito configuráveis pois permitem a gestão em tempo real das autorizações de acesso tanto com base no pedido de conteúdo como numa maneira desfasada actuando sobre o fluxo de retorno, sendo deste modo compatível com serviços baseados

no conteúdo dos novos tipos que requerem facturação em tempo real como sejam os baseados na facturação pré-paga, ao mesmo tempo que são permitidas as latências não negligenciáveis de ligação; e

- independentes do vendedor pois podem facilmente suportar novos protocolos e tecnologias de conteúdos sem requererem módulos adicionais de programas informáticos, estando ao mesmo tempo numa posição que permite interceptar qualquer protocolo de pedido (e do fluxo de retorno relacionado) assim como a gestão de um modo unitário dos pedidos de autorização e dos acontecimentos de contabilidade num servidor centralizado.

Breve descrição dos desenhos

A presente invenção será agora descrita, a título meramente exemplificativo, fazendo referência às figuras anexadas, em que:

- as figuras 1 e 2 foram já anteriormente descritas de um modo resumido,

- a figura 3 é um diagrama em blocos que representa, usando essencialmente a mesma disposição das figuras 1 e 2, a estrutura básica da disposição descrita na presente,

- as figuras de 4 a 6 representam, de um modo esquemático, a aplicação do mesmo esquema básico ilustrado na figura 3 a diferentes contextos operacionais,

- a figura 7 é um fluxograma de um controlo lógico básico adaptado para ser implementado na disposição aqui descrita,

- a figura 8 é um diagrama em blocos que representa o fluxo de dados correspondente ao fluxograma da figura 7,

- a figura 9 é um outro fluxograma que representa um outro controlo lógico alternativo adaptado para ser implementado na disposição aqui descrita,

- a figura 10 é um diagrama em blocos que representa o fluxo de dados correspondente ao fluxograma da figura 9,

- as figuras 11 e 12 são diagramas em blocos lógicos que representam o controlo de permissão da forma que se encontra implementada dentro do âmbito da disposição aqui descrita,

- as figuras de 13 a 17 são vários diagramas em blocos que representam o funcionamento de vários módulos envolvidos em várias fases de funcionamento da disposição aqui descrita;

- a figura 18 representa uma estrutura de acesso de conteúdo adaptada para gerir um pedido de gestão de conteúdo e um possível redireccionamento do mesmo dentro da disposição aqui descrita, e

- as figuras 19 e 20 são exemplos de possíveis formas de realização prática da disposição aqui descrita.

Descrição detalhada de formas de realização preferenciais da invenção

A figura 3 dos desenhos anexos ilustra uma localização possível dos componentes de um sistema de acordo com o descrito na presente em relação a outros objectos e elementos envolvidos no funcionamento do mesmo. Em temos gerais, as

partes, os componentes ou os elementos idênticos, semelhantes ou equivalentes a partes, componentes ou elementos homólogos já descritos em relação às figuras 1 e 2 são designados pelas mesmas letras e/ ou pelos mesmos números referência.

De um modo específico, a disposição da figura 3 inclui uma porta de comunicação 20 (de seguida definido como porta de comunicação de Acesso de conteúdo Condicional Dinâmico ou DCCA) disposta no trajecto da ligação entre o CR solicitador de conteúdos no local US do utilizador e um servidor de conteúdos 26 (adaptado para ser configurado de acordo com disposições diferentes, como se encontra melhor detalhado de seguida) situado no local de distribuição de conteúdos 24.

A porta de comunicação 20 é configurada executando um número de funções tais como o desencadeamento, o desenvolvimento de regras, a filtragem, a oscilação e injecção de novo em relação ao tráfego que flui através da mesma. A porta de comunicação 20 é configurada para cooperar com um servidor 22 que desempenha o papel de uma política de conteúdos e de um servidor de segurança. Isto é posicionado ao nível do controlo da rede, por exemplo num centro de serviço do operador de telecomunicações que controla a rede. O servidor 22 tem a tarefa principal de validar os pedidos que entram e possivelmente de activar mecanismos específicos da contabilidade.

Os blocos representativos do solicitador CR e o sistema satisfeito 26 de servidor de conteúdos estão representados em linhas tracejadas pois representam elementos da arquitectura pré-existentes.

As figuras 4 a 6 mostram como os elementos básicos representados na figura 3 podem ser dispostos de um modo diferente dentro das várias arquitecturas adaptadas para a distribuição de conteúdos de meios.

Especificamente, a disposição mostrada na figura 4 refere-se a uma arquitectura centralizada em que a porta de comunicação 20 de DCCA é disposta "em frente" da bateria/ do conjunto de servidores de conteúdos 10, 12 discutidos já em relação a figura 1.

A porta de comunicação 20 e a política de conteúdos e o servidor de segurança 22 são dois componentes situados no centro de serviço 24 do fornecedor de conteúdos, isto é o centro de serviço para a entrega dos conteúdos. Nesse caso, o elemento de ligação representado pela rede N está compreendido geralmente pela rede de acesso, (à qual o solicitador de conteúdos CR e o fornecedor de conteúdos são 24 ligados), da rede metropolitana, e da rede do transporte no caso de ligações de longa distância.

Figura 5 refere-se, por outro lado, a uma arquitectura da entrega com base em CDN. Nesse caso a porta de comunicação 20 é disposta em frente dos servidores hospedeiros 14 fornecidos em cada local da rede de distribuição de conteúdos (por exemplo nos pontos metropolitanos de presença). Pelo outro lado, a política de conteúdos e o servidor de segurança 22 da são situados no centro de serviço do operador da rede de distribuição de conteúdos, possivelmente em conjunto com os outros componentes de controlo dessa rede, tais como o encaminhador de conteúdos 23 de CDN.

Nesse caso, o ponto óptimo da posição para a porta de comunicação 20 é, como indicado, na frente do servidor hospedeiro (ou da bateria/ conjunto de servidores hospedeiros) que entregam os conteúdos. Outras posições são possíveis, mas estas são geralmente prováveis de tornar o sistema de controlo mais vulnerável às tentativas dos utilizadores para funcionarem de um modo fraudulento contornando a porta de comunicação de controlo.

A Figura 6 refere-se a uma arquitectura "genérica" incluindo os servidores 28 dispostos em várias posições na rede e vindo para baixo para proprietários diferentes. Nesse caso, a porta de comunicação 20 tem a tarefa de filtrar e de controlar todo o tráfego na fonte, a saber, na proximidade do ponto de acesso à rede usada pelo solicitador de conteúdo CR.

A disposição descrita na presente não está de nenhuma maneira limitada ao uso possível de uma arquitectura com CDN ou de uma arquitectura que possibilite o uso de um centro de serviço. De facto, a disposição da presente está adaptada para funcionar em relação às arquitecturas "mistas", onde a necessidade de autorizar/ possibilitar que um utilizador receba um serviço fornecido por um ou mais servidores ao mesmo tempo que fornece a sustentação necessária para a contabilidade.

A seguinte descrição de uma forma de realização preferida da disposição descrita na presente irá em primeiro lugar referir-se a uma execução possível dentro de uma situação de CDN, isto é a um contexto genérico de arquitectura de CDN. Nesse respeito, ao fazer referência à figura 5, o servidor de conteúdos hospedeiro deve ser compreendido na sua forma mais genérica como sendo um "conjunto de" servidores que fornecem

um serviço de conteúdos, enquanto o encaminhador de conteúdos 23 pode ser substituído por outros sistemas, por exemplo um DNS (Servidor de Nomes de Domínios) ou estar ausente.

De facto, os elementos básicos das disposições descritas na presente, a saber a porta de comunicação 20 (que executa as acções de desencadear, de filtrar e de redireccionar) e a política de conteúdos e o servidor de segurança 22 (que verifica os direitos de acesso aos conteúdos em tempo real aquando do pedido pela porta de comunicação 20 e fornecendo o resultado à própria porta de comunicação 20) são independentes do tipo de arquitectura e - mais em concreto - da tecnologia usada no solicitador de conteúdos CR/ do solicitador. Isto significa que - qualquer - acesso ao servidor hospedeiro 14 pode ser interceptado pela porta de comunicação 20 e ser processado executando as funções indicadas anteriormente.

Os mecanismos de desencadeamento e de filtragem implementados pela porta de comunicação 20 podem ser configurados com base numa descrição e conseguem um grau de granularidade ao nível de um nome de domínio ou de um único conteúdo. Este mecanismo é implementado por meio das descrições da lista designados das listas de acesso de conteúdo (ACL) a ser descrita em detalhe de seguida com referência à figura 18.

Um filtro do ACL controla por meio das cláusulas de permissão/ negação os seguintes artigos: a fonte de IP e os endereços de destino + a máscara da sub-rede + o VPN ID, o tipo do protocolo de transporte (TCP/UDP), a porta de comunicação de comunicação (origem/ destino) e a referência ao conteúdo pedido.

Os filtros de ACL são mantidos ao nível da porta de comunicação 20, o que opera com base na intercepção do pedido de utilizador e é activado (num modo de permissão/ negação) em consequência da validação da activação executada pelo servidor 22. Isto é baseado na emissão dos atributos do identificador do utilizador (por exemplo o endereço IP), o conteúdo do serviço (por exemplo o URL) e, possivelmente, os atributos correspondentes do servidor hospedeiro 14 que fornece o serviço.

A porta de comunicação 20 da figura 5 intercepta o tráfego do utilizador (pedido para o conteúdo de multimédia, que - em regra geral - é "dependente da tecnologia "), numa modalidade transparente, ou seja sem o afectar ou modificar. Os extractos da porta de comunicação de cada pedido dependente da tecnologia pedem os conteúdos para os quais a gestão foi configurada, isto é o endereço IP do CR do solicitador, o URL associado com o conteúdo pedido, o endereço IP do servidor hospedeiro, e as características do protocolo usado.

Estes dados são usados para criar (como se encontra melhor detalhado mais adiante em referência à figura 18) uma entrada de acesso de conteúdo " independente da tecnologia " (ACL), para que o qual a validação é pedida acedendo ao servidor 22. O servidor 22 verifica a credencial do utilizador em relação ao pedido feito e deriva uma informação correspondente de permissão/ negação.

Quando o utilizador está activado ("permissão"), o fluxo de dados do utilizador para o servidor hospedeiro e do servidor hospedeiro para o utilizador permanece inalterado.

Se o usuário não estiver activado ("negação") para receber o conteúdo pedido, pelo menos duas intervenções diferentes podem ocorrer.

Como uma primeira opção, o pedido do cliente pode ser obstruído, isto é o pedido não é enviado ao servidor hospedeiro 14 que fornece o serviço.

Como uma opção alternativa, o fluxo descendente (do servidor hospedeiro para o cliente) pode ser obstruído.

Especificamente, fazendo referência ao fluxograma da figura 7, a referência 100 designa uma etapa onde a porta de comunicação 20 extrai do tráfego emitido pelo solicitador de conteúdo CR para o servidor 14 (o tráfego designado como 1 na figura 8) o endereço IP (ES) e a(s) URL(s). Estes dados extraídos são sujeitos na etapa 102 a uma verificação em relação às capacidades do utilizador.

O resultado de tal verificação é esperado numa etapa 104 e um teste final é feito na etapa 106. Se o teste der origem a um resultado positivo (utilizador activado - "permissão") o pedido respectivo é enviado ao servidor hospedeiro 14 numa etapa 108.

No caso a verificação de etapa 106 dá origem a um resultado negativo (utilizador não activado - "negação"), o pedido é abandonado/ redireccionado na etapa 110.

De um modo mais concreto, os números de referência de 1 a 6 da figura 8 identificam a sequência de tempo dos vários fluxos de tráfego. Especificamente, essa sequência à origem às seguintes etapas:

- o pedido do solicitador de conteúdo CR é enviado para a porta de comunicação 20 (fluxo 1).

- a porta de comunicação 20 intercepta o pedido (enquanto que o resto do tráfego passa através dela de um modo inalterado) e coloca o pedido numa condição de espera sem fazer o seu envio para o servidor hospedeiro 14. Entretanto, a porta de comunicação 20 prepara um pedido para o servidor 22 incluindo as referências do solicitador (endereço de IP) e o conteúdo solicitado, o qual é de seguida enviado para o servidor 22 (fluxo 2);

- o servidor 22 efectua a verificação da capacidade do utilizador relativamente ao conteúdo solicitado e responde à porta de comunicação 20 por intermédio de uma mensagem de permissão/ negação (fluxo 3);

- se o resultado for positivo, a porta de comunicação 20 envia o pedido original para o servidor hospedeiro 14 (fluxo 4); em caso contrário pode dispensar o pedido ou fazer o seu envio de um modo modificado (dentro do âmbito da mesma sessão de TCP). De um modo adicional, pode configurar um ACL interno de modo a optimizar os pedidos seguintes;

- o servidor hospedeiro responde ao pedido recebido (fluxo 5), e

- o fluxo de resposta passa através da porta de comunicação 20 na direcção do solicitador de conteúdo (fluxo 6). Esta forma de funcionamento, permite o redireccionamento em linha do conteúdo.

As figuras 9 e 10 descrevem uma técnica alternativa já considerada anteriormente.

Neste caso, após ter extraído (na etapa 100) as informações a respeito da potencialidade do utilizador e fazendo a sua porta de comunicação para o servidor 22 para a verificação (numa etapa 102), a disposição alternativa considerada nas figuras 9 e 10 fornece o pedido de utilizador que está a ser emitido (na etapa 112) como um pacote de utilizador para o servidor 14 sem ser de modo algum alterado. Desse modo, o servidor 14 pode começar a fornecer o utilizador com o serviço pedido. Isto ocorre numa etapa 114 que é continuada (pelo menos) desde que o resultado da verificação efectuada na etapa 102 seja recebido do utilizador 22.

Nesse ponto a capacidade do utilizador é testada na etapa 116.

Se a etapa 116 der origem a um resultado positivo, o sistema evolui para a etapa “não fazer nada” 118, deixando desse modo o servidor 114 continuar a etapa 114 entregando deste modo o conteúdo ao CR solicitado.

Se, por outro lado, a verificação da etapa 116 der origem a um resultado negativo, um sinal de bloco é enviado para o servidor 114 interrompendo deste modo a distribuição do serviço para o CR solicitador.

Uma vez mais, no diagrama da figura 10, os vários fluxos de informações encontram-se indicados por números de referência que identificam a sua sequência de tempo.

De um modo específico, na disposição da figura 10:

- o pedido do utilizador é enviado para a porta de comunicação 20 (fluxo 1);

- a porta de comunicação 20 intercepta o pedido (enquanto que o resto do tráfego passa através do mesmo de um modo não alterado) e coloca o pedido numa condição de espera sem o enviar para o servidor hospedeiro 14. Entretanto, a entrada prepara um pedido para o servidor 22 incluindo as referências ao solicitador (endereço IP) e o conteúdo solicitado, o qual é então enviado para o servidor 22 (fluxo 2);

- entretanto, o pedido é enviado (sem alteração) para o destino final, que é o servidor 1 (fluxo 3);

- o servidor 14 começa a satisfazer o pedido, enviando de volta tráfego de resposta (fluxo 4),

- o tráfego de resposta é deixado passar sem alteração desde a porta de comunicação 20 na direcção do solicitador de conteúdos CR (fluxo 5);

- após a verificação da activação do utilizador em relação ao conteúdo requerido, o servidor 22 responde à porta de comunicação 20 através de uma mensagem de permissão/ negação (fluxo 6).

No caso da permissão, a porta de comunicação 20 não efectua qualquer tipo de operação; ao invés, no caso de uma negação, insere um filtro que bloqueia o fluxo de resposta do servidor hospedeiro 14 ao solicitador de conteúdo CR (pelo que os fluxos 4 e 5 são descontinuados).

A vantagem desta disposição alternativa reside no facto de permitir controlar a capacidade do utilizador mesmo nos casos em que a latência da transmissão e a possibilidade de desligar a aplicação possivelmente derivando são aspectos críticos. Isto pode ser habitualmente o caso de uma rede móvel.

A figura 11 é um diagrama de blocos exemplificativo de uma estrutura interna possível do servidor 22. Na forma de realização exemplificativa que se encontra ilustrada, o servidor 22 é essencialmente um sistema que acede a diferentes bases de dados de modo a identificar, com base nas operações de união da base de dados, as políticas a serem aplicadas para um determinado utilizador em relação a um determinado conteúdo.

É obviamente possível conceber diferentes formas de realização para este tipo de servidor. Formas de realização alternativas podem ser, possivelmente, baseadas nos servidores de um tipo de autenticação, de autorização e de contabilidade (AAA) como as que são conhecidos como RADIUS, TACACS, TACACS+, DIAMETER ou outros sistemas como sejam os servidores LDAP, adaptados para detectar o perfil do utilizador e decidir se um certo pedido que é proveniente de uma entrada pode ser ou não autorizado.

Na forma de realização exemplificativa ilustrada, o servidor 22 inclui três bases de dados, nomeadamente:

- uma base de dados 30 de identidade do utilizador que alberga as informações relativas aos utilizadores (em linha ou não),

- uma base de dados 32 de conteúdos que alberga as informações relativas aos conteúdos disponíveis e geridos pelo sistema (por exemplo o URL respectivo, o domínio hospedeiro, o fornecedor de conteúdos, o custo, a duração e assim por diante), e

- uma base de dados 34 de políticas de conteúdos que alberga as informações de activação para o conteúdo dos utilizadores simples (ou grupos de utilizadores).

Conforme se encontra ilustrado na figura 11, um servidor simples 22 pode cooperar com diferentes portas de comunicação 20, incluídas num CDN. Conforme foi explicado anteriormente, a porta de comunicação 20 encontra-se configurada para detectar as informações relativas ao solicitador (como seja o endereço de IP), o conteúdo solicitado (como seja o respectivo URL) e possivelmente o endereço do servidor hospedeiro para o qual o pedido foi enviado.

O número de referência 36 designa como um todo a lógica principal do servidor 22, o qual inclui, entre outros, um módulo 38 de verificação de ACL assim como um controlador 40 de entrada.

Com base nos itens de informações recebidos da, ou de cada uma das, portas de comunicação 20, o módulo 38 de verificação do ACL é questionado de modo avaliar a “consistência” do acesso ao conteúdo em relação à capacidade proporcionada ao utilizador.

Deste modo, o módulo 38 de verificação efectua as seguintes tarefas:

- identificação do utilizador com base nos respectivos atributos conforme os passados desde a porta de comunicação 20 (por exemplo usando o endereço IP de modo a calcular a partir de uma tabela o nome de utilizador do utilizador activado, função que é actualmente disponível para uma série de sistemas AAA), isto ocorre como resultado do acesso à base de dados 30 de identidade do utilizador,

- identificação de macro-famílias possíveis com as quais o conteúdo solicitado se encontra relacionado assim como informações adicionais pertinentes (por exemplo a duração da largura de banda requerida), acendendo à base de dados 32 de conteúdos, e

- verificando as activações associadas com o utilizador em relação aos conjuntos de conteúdos relacionados com o conteúdo solicitado acedendo à base de dados 34 de políticas de conteúdos.

O resultado de uma tal operação, que pode ser de um tipo de permissão ou de negação, é enviado a partir do controlador de entrada 22 para a porta de comunicação 20 de pedido.

Por exemplo, um tal caso, a árvore de base de dados associada inclui:

Identidade do utilizador DB 30

Endereço IP	**Nome de Utilizador**	**Crédito**
10.10.10.10	Utilizador1	10 Euro
10.10.10.11	Utilizador2	1 Euro
10.10.10.12	Utilizador3	1 Euro

Conteúdo DB 32

Referência de Conteúdo	Duração	Custo	Macrofamílias
www. milan.it/ultimigoal.rm	120	1 €	desporto, futebol
www.rai.it/montalbanol.rm	2500	2 €	ficção
fictionwww.formulal.it/monza.rm	500	1 €	desporto, corridas de automóveis

Políticas de Conteúdos DB 34

ChavedoNomedeUtilizador	Macrofamília
Utilizador1	ficção
Utilizador2	futebol
Utilizador3	desporto

Os seguintes pares de pedido/ resposta podem resultar de/ provocar a porta de comunicação de solicitação 20

Ped (10.10.10.10,www.milan.it/ultimigoal.rm)=> Resp (Negar: conteúdo não permitido)
Ped (10.10.10.11,www.milan.it/ultimigoal.rm)=> Resp (Permitir, durante 120 segundos)
Ped (10.10.10.12 www.milan.it/ultimigoal.rm)=> Resp (Negar, por crédito insuficiente)
Ped (10.10.10.12 www.formula1.it/monza.rm)=> Resp (Permitir, durante 500 segundos)

Deste modo, em conjunto com a resposta, o servidor 22 pode enviar para a entrada, ou para cada uma das portas de comunicação, 20, alguns itens de informações adicionais derivados das bases de dados interrogadas. Estas podem incluir, por exemplo, a duração do conteúdo (que se torna o

tempo de vida do próprio ACL), o crédito residual, ou outras informações úteis para controlar a distribuição do serviço.

Como regra será de um modo geral suficiente transmitir para a porta de comunicação de solicitação 20 mesmo só a mensagem adequadamente associada com o pedido original.

Do mesmo modo, a etapa em que as agregações em macro famílias são verificadas pode ser dispensada se a base de dados 34 tiver politicas de conteúdo ao nível do conteúdo simples (URL) e não ao nível das macro famílias. Deste modo, um grau máximo de granularidade pode ser conseguido ao controlar-se o acesso ao conteúdo.

Deve notar-se que, de um modo preferencial, a função de gestão dos ACLs activos e o seu armazenamento não são proporcionados com o servidor 22 mas ao invés com a porta de comunicação 20 respectiva, através da implementação de somente duas primitivas:

- ObterACL pela porta de comunicação 20, e
- ConfigurarACL por um servidor 22.

Em outras formas de realização pode ser útil implementar um servidor 22 adaptado de modo a armazenar os ACLs criados de um modo centralizado de forma a permitir voltar ao ponto de partida numa etapa posterior em caso de falha dos acontecimentos por parte da porta de comunicação 20. De um modo preferencial, nesse tipo de arquitectura, é fornecida uma primitiva adicional do tipo:

- RealinharACL tanto pela porta de comunicação 20 como pelo servidor 22, o que cuida do envio a partir da porta de

comunicação 20 e na direcção do servidor 22 dos ACLs disponíveis no local (por exemplo, de modo a assegurarem o regresso ao início após uma falha nesse componente) ou o seu inverso (do servidor 22 para cada porta de comunicação 20, de um modo selectivo)

- LargarACL da porta de comunicação 20 para o servidor 22 quando terminar o tempo de vida do próprio ACL.

A figura 12 destaca a estrutura interna da porta de comunicação 20, enquanto as subsequentes figuras de 13 a 17 se destinam a detalhar a sua operação.

Na forma de realização ilustrativa que se encontra apresentada, a porta de comunicação 20 é implementada como um componente separado. No entanto, tendo em conta o que foi descrito anteriormente, e ainda tendo em conta o restante desta descrição, será evidente que as funções por si efectuadas, nomeadamente o desencadeamento, a filtragem, o policiamento e o redireccionamento (Oscilação + Re-injecção) dos conjuntos podem ser implementadas sob a forma de módulos de acréscimos associados com outros aparelhos de rede como sejam um comutador de rede, um comutador de conteúdos, um aparelho de encaminhador ou directamente com um ou mais servidores hospedeiros.

O sistema é disposto sobre uma pluralidade de camadas duas das quais (a mais baixa e a mais elevada) são essencialmente compreendidas por pontos de ligação de rede 50 e 52 que cooperam com o solicitador de conteúdos CR e com o servidor hospedeiro, respectivamente, mais um ponto de ligação adicional 54 na direcção do servidor 22.

As camadas intermédias incluem essencialmente uma camada inferior 56 no nível Núcleo e um nível mais elevado 58 no nível do conteúdo da aplicação.

Na camada de núcleo 56 a função básica de um Núcleo semelhante a Unix é providenciada no que diz respeito a ligação em rede, em ponte e filtragem ao nível do IP (até ao nível 4).

Uma implementação típica da camada 56 inclui todas as funções típicas localizadas no sistema FreeBSD tal como disponível no IPFW (Dispositivo de segurança de IP (IP Firewall)) de um sistema FreeBSD.

Especificamente, os seguintes elementos estão incluídos:

- um módulo de filtro 60 tendo associado um correspondente submódulo de controlo confiado com uma tarefa de filtragem (até ao nível 4) de pacotes IP. Este módulo funciona com pacotes transmitidos em ponte entre as duas interfaces de rede destacadas pelo nível inferior e um submódulo de Desvio 62 e um submódulo de re-injecção 64. O módulo 62 tem a tarefa de redireccionar os pacotes Ethernet (quadros) para uma aplicação de sistema ao nível do utilizador para o se processamento. O módulo 64 tem a tarefa de re-injectar, sempre através de uma aplicação de sistema ao nível de utilizador, com re-computação do código de correcção cíclico (CRC) para correcto envio para a rede. Estes módulos 62 e 64, que actualmente não se encontram disponíveis para interfaces de transmissão em ponte, podem ser também activados para o tráfico de transmissão em ponte alterando correspondentemente o núcleo básico do FreeBSD.

As referências 66 e 68 designam duas regras de IP dinâmico e regras de IP estático de bases de dados hospedeiras, respectivamente.

O uso do FreeBSD como base para este sistema operativo da porta de comunicação 20 tem inúmeras vantagens.

Primeira de todas permite uma segurança de IP transparente por meio de transmissão em ponte. De modo adicional, leva a cabo as acções de filtragem e accionamento ao nível Núcleo com um desempenho melhorado. Existe a possibilidade de implementar mecanismos de desvio selectivos relacionados com as regras de segurança para enviar pacotes específicos para um ou mais conectores Núcleo ligados a uma aplicação de espaço de utilizador.

De modo adicional, existe a possibilidade no FreeBSD de levar a cabo um mecanismo de re-injecção de pacote por meio dos conectores Núcleo tidos em conta anteriormente. Isto permite a uma aplicação do espaço de utilizador lidar exclusivamente aqueles pacotes especificamente identificados pelas regras de segurança aceitando, modificando ou rejeitando-as ou lidando de um modo retardado o fluxo de retorno.

De modo adicional, FreeBSD é um software disponível gratuitamente, pelo que a porção de segurança segue os actuais desenvolvimentos de software de código aberto, enquanto preservam a porção ao nível da aplicação. As alterações possíveis necessárias na rede de comunicação de núcleo de modo a gerar as funções de desviar/re-injectar, disponíveis também para os pacotes que são transmitidos em ponte possam ser facilmente levados a cabo.

Finalmente, as implementações TCP da BSD são actualmente tidas em conta como os empilhamentos TPC mais robustos no contexto Unix.

O módulo de lógia 58 inclui um número de submódulos de aplicação. Estes incluem um módulo de análise 70 que desempenha (nível 7) as análises dos pacotes recebidos do módulo de desvio núcleo 62 através da extracção do endereço IP e da URL (ou, de um modo mais geral, as referências úteis para autorização), enquanto também exemplifica o pedido para enviar autorização para o servidor 22 (através da interface 54) e gerindo a resposta correspondente forçando a politica de filtragem por meio de comandos enviados para o submódulo de controlo núcleo 60a. Isto essencialmente envolve a presença de um submódulo de política de controlo 72 e um submódulo de requisito vigilante. Possível manipulação do pacote requerido e controlo do submódulo re-injectado de núcleo é levado a cabo por um pacote de submódulo de balanceamento 74. Especificamente, o submódulo de controlo regulador 72 leva a cabo o momento de acção para os ACLs e possível remoção após expiração do tempo de deixar o servidor 22.

A camada lógica principal 58 da porta de comunicação de saída 20 coopera ainda com dois repositores de informação 78 e 80.

O repositório anterior, designado 78, essencialmente inclui as definições de configuração da porta de comunicação 20. Estas são essencialmente inerentes a:

- regras estáticas para accionar os pedidos e determinar os protocolos, as portas de comunicação e os atributos que são característicos dos pacotes sobres os quais a

informação contida é escrutinada (tal como usado pelo filtro IP 60 para o nível de filtração 4);

- regras de análise da Ethernet Framework para localizar a informação URL e IP destinada a ser usada pelos submódulos 70 para propósitos de análise; e
- possível re-direccionamento de regras com base no protocolo, domínio ou rejeição de tipo (por exemplo crédito insuficiente, permissão não disponível e por aí adiante) para possível uso pelo submódulo de balanceamento de pacote 74 de modo a substituir a URL ou pedido original do utilizador com um destino alternativo. Será muito apreciado que tal destino alternativo passe pelo servidor hospedeiro dentro da mesma sessão TPC. Por um lado, isto assegura a existência no servidor enquanto por outro lado melhora a eficiência do próprio sistema.

O repositório 80 essencialmente inclui as listas de conteúdo de acesso (ACLs), destinado a descrever ao nível 7 a filtragem activa num determinado momento e desempenho de mapeamento com as regras correspondentes ao nível 4 dos módulos de filtro IP 60 armazenados na base de dados de Regras de IP dinâmico 68.

A fase de configuração da porta de comunicação 20 é detalhada mais adequadamente na figura 13 onde os módulos/submódulos directamente envolvidos são destacados em linhas ponteadas.

Essencialmente, a porção principal da fase de configuração ocorre na porta de comunicação 20 antes do sistema ser usado. De facto, a configuração do servidor 22 está limitada para indicar as referências para ligação à porta de comunicação

(s) e bases de dados usadas. Irá ser geralmente assumido que estas já estão pré-carregadas com a necessária informação tal como previamente destacado.

Essencialmente, a fase de configuração da porta de comunicação 20 envolve um número de etapas de definição de configurações.

Uma primeira etapa de configuração envolve definição do endereço do servidor 22 e as portas de comunicação correspondentes para a informação para requer autorização (pelo menos endereço de IP de utilizador e URL) e recepção das respostas correspondentes (tais como recusado/autorizado ou limite de tempo). Isto é essencialmente simétrico com a configuração desempenhada no servidor 22. Exemplos disto são como se seguem:

```
CP&SSERVER=10.10.15.156
ServerCommPort=22222
NetworkCommPort=33333
```

Numa etapa de definição de configuração subsequente, envolve a definição das interfaces físicas para controlo e transmissão em ponte, nomeadamente aqueles interfaces por meio dos quais a porta de comunicação 20 recebe e comunica com o servidor 22 e os conteúdos solicitados CR bem como o servidor hospedeiro.

Exemplos destes são:

```
DCCAControlIf=fxp2
TowardsUserIf=fxp0
TowardsContentIf=fxp1
```

Subsequentemente, a lógica de filtragem/accionamento estático ao nível 4 (regras de IP estático) são definidas tal como são para ser implementadas pelo módulo de filtro IP 60 para os pacotes entre os dois interfaces de transmissão em ponte. Isto inclui preferivelmente todos os quadros de interesse para capturar o pedido do utilizador (e preferivelmente apenas estes quadros) para cada protocolo sobre o qual a função é para ser implementada. Isto enquanto é indicado a porta de comunicação de desvio ao nível do Núcleo onde os módulos 70 (L7 análises) e 74 (pacote balanceamento) pode receber e re-injectar pacotes na transmissão em ponte entre o solicitador de conteúdo CR e o servidor hospedeiro. Tais definições podem também incluir as definições referentes ao bloqueamento das respostas actuais para o protocolo. Por exemplo, no caso do protocolo Real de RealNetworks esta configuração pode incluir:

TriggerL4DivertRule=divert 11111 tcp de qualquer um para qualquer um 554,7070,7071 via fxp1 estabelecida

InitL4FilterRule=deny udp de qualquer um para qualquer um 6979-7170 via fxp0

Subsequentemente, o nível 7 análise lógica é definido de modo a extrair a referência ao conteúdo para ser enviada para objectivos de autorização para o servidor 22. Isto ocorre através do destaque do padrão de prefixo para pesquisar no quadro (sem levar em conta o carácter de código adoptado), disposto antes da sequência reportada de comunicação nos conteúdos. No caso do Real este pode assumir a forma:

TriggerL7PrefixString="PLAY rtsp:_//"

Subsequentemente, a lógica de balanceamento de pacote para os objectivos de aceitar/recusar o pacote é definido para cada protocolo gerido de uma maneira diferente possível para cada domínio hospedeiro. Será apreçado que neste caso, para os protocolos indicados, a porta de comunicação 20 adopte uma lógica de filtragem do tipo activa no pedido tal como indicado nas figuras 7 e 8. No caso de Real isto pode ser:

ReinjectAccept=<none>
ReinjectDeny=sorry.rm (per hosted domain = "rai.cdn.telecomitalia.it"
ReinjectDeny = please__subscribe.rm (per hosted domain = "cnn.cdn.telecomitalia.it")

Como uma alternativa à regra previamente indicada, o modelo de regra ao nível 4 é definido para ser automaticamente inserido no caso de aceitação ou recusa é definido para gerir a acção de filtragem activa atrasada na resposta. Bastante frequentemente, estas regras são simples na forma de negação de uma regra definida tal como InitL4FilterRule, adequadamente instanciada entre o endereço IP do solicitador de conteúdo CR e o endereço de IP do servidor hospedeiro indicado no pedido. Se o modelo for diferente uma definição útil pode ser:

TemplateAcceptRule=accept udp 6979-7170
que no caso de aceitação produz a inserção (pelo módulo de regra de controlo 72) de um nível de regra 4 para ser gerida pelo filtro de IP 60 do tipo:

> accept udp from <Surrogate Server> to <Content Requester> 6970-7170 via <TowardsContentIf>

e similar para a recusa

TemplateDenyRule=deny udp 6970-7170

Nos exemplos de configuração aqui feitos pode tornar-se supérfluos conforme vão ficando abrangidos pelas regras de estatísticas da base de dados 66.

As Figuras da 14 à 16 destacam os componentes da porta de comunicação 20 que entra em acção durante várias fases de operação da porta de comunicação 20.

De um modo específico, a figura 14 destaca os componentes da porta de comunicação 20 que desempenha a acção de accionamento do pedido.

Primeiro que tudo, por meio das regras contidas na base de dados 66, o (“dependente de tecnologia”) quadro vindo do solicitador de conteúdo CR é analisado ao nível 4 pelo módulo de filtro IP 60. Se isso for de interesse, ao invés de ser enviado directamente (pelo filtro IP 60) para a interface 52 para o servidor hospedeiro, o quadro é interceptado e enviado através o submódulo 62 para o módulo de análise 70 no nível de aplicação.

Através do uso das regras de análise para os pacotes contidos na base de dados 78 (especificamente no que diz respeito ao protocolo prefixo) o módulo de análise 70 envia para o solicitador regulador 76 o conjunto inclui:

- o <os atributos identificado do Solicitador de Conteúdo>
- o <os atributos de identificação do Conteúdo Solicitado>
- o <os atributos de identificação d Servidor Hospedeiro>

Esta definição pode de facto ser limitada para o endereço de Ip do utilizador e a URL bem como o endereço de IP do servidor hospedeiro.

Será apreciado que dessa forma um mecanismo de autorização unitária é levada a cabo que é “independente de tecnologia”, isto é, totalmente independente da tecnologia de distribuição de conteúdo usada na rede.

O diagrama da figura 15 destaca o componente da porta de comunicação 20 que implementa comunicação para o servidor 22. Esta actividade é completamente gerida pelo módulo de solicitador de regulador 76 que desempenha as tarefas de:

- empacotamento do pedido usando os dados contidos no módulo de análise 70, e
- enviando o pedido usando a porta de comunicação de comunicação 52 para o servidor.

Simultaneamente, o módulo 76 gere as respostas vindas do servidor. Estas respostas (tipicamente na forma de mensagens de aceitação/recusa possivelmente têm associadas algumas características adicionais relacionadas ao conteúdo tais como duração, largura de banda necessária e por aí fora) são enviadas para os módulos de aplicação. Estes módulos gerem a criação de vias de regra de filtração dinâmica (através do módulo de controlo regulador 72) e o pacote de manipulação (através do módulo de balanceamento 74).

Na ausência de uma resposta do servidor 22 dentro de um certo período de tempo, o módulo de requisição regulador 76 aplica

as regras definidas pelo administrador, tais como destinadas a evitar a entrega do conteúdo.

Uma fase de filtragem subsequente faz com que a informação a ser passada ou a não ser passada do solicitador de conteúdo CR para o servidor hospedeiro e vice-versa. Por essa razão os elementos destacados na figura 16 (uma vez mais destacados por linhas ponteadas) dão destaque a uma estrutura de suporte interna, contida na base de dados 80 actualmente designada lista de conteúdo de acesso (ACL). Esta estrutura descreve as cláusulas activas de permissão/negação para um determinado utilizador e um determinado conteúdo e outros atributos úteis para o nível de filtragem 7. Estas cláusulas adicionais referem-se a um nível 4 cláusula gerida pelo módulo de filtro IP 60 e os submódulos próximos.

A Figura 18 descreve o possível seguimento para memorização das listas de conteúdo de acesso ACLs na porta de comunicação 20. Tal estrutura pode também ser usada no servidor 22 para centralizar o armazenamento dos ACLs existentes.

Tal como descrito anteriormente, uma lista ACL define parâmetros para uma ligação/pedido. Baseado nessas regras pode ser definido para o acesso ser aceite ou recusado para certas fontes de rede.

A Figura 18 é um exemplo de campos de informação usado para implementar a decisão lógica (lógica de filtragem) na porta de comunicação 20. No caso do exemplo mostrado na figura 18, os campos indicados têm o seguinte sentido/função:

- Acção: descrever a acção a ser desempenhada na presença de certos parâmetros de ligação (aceitar/recusar);

- Src IP e Dst IP: estes representam o endereço IP das entidades que estabelecem a ligação e incluem, se necessário, informação relativa ao ID da correspondente Rede Privada Virtual (VPN) e mascara sub-rede;
- Protocolo: identificação o tipo de protocolo de transporte usado para ligação (TCP/UDP);
- Porta de comunicação de ENTRADA e porta de comunicação de SAÍDA: Estas definem as portas de comunicação lógicas usadas para comunicação entre os processos que estabelecem ligação;
- H.D.: representa o Domínio de Hospedagem em que o conteúdo foi requerido (por exemplo cdn.telecomitalia.it);
- Conteúdo: identifica a URL do único conteúdo requerido como resultado da ligação (por exemplo: /recent/promo.asf);
- TTL: define o tempo de validação da cláusula ACL, para além do qual tal cláusula será automaticamente removida.

A figura 16 destaca os componentes usados pela porta de comunicação 20 para permitir o controlo o requerido através da definição de um filtro atrasado actuando na resposta tal como apresentado na figuras 9 e 10.

Nesse caso, o módulo de balanceamento de pacote 74 envia o pacote requerido para o interface de saída 52 sem qualquer modificação. De modo a faze-lo, é imediatamente activado pelo módulo de solicitador de política 76 antes de enviar o pedido para o servidor hospedeiro.

Maior parte da actividade é levada a cabo pelo módulo de controlo político 72. Este módulo recebe a informação requerida pelo módulo solicitador de política 76 baseado no

critério estabelecido no nível de configuração para um determinado protocolo através da interacção com o módulo de controlo de filtro IP 60. O módulo de controlo regulador 72 tem a tarefa de manter/reparar os ACLs contidos na base de dados 80, em especial no que diz respeito à função de gestão dos valores TTL para as regras.

A Figura 17 destaca os componentes da porta de comunicação 20 que entra em acção durante a fase onde um pedido modificado é re-injectado. Tal como descrito anteriormente isto corresponde à solução alternativa considerada nas figuras 7 e 8.

As duas opções podem ser configuradas para um único protocolo e permitir diferentes características a serem obtidas dependendo das necessidades do operador. Dois factores básicos a esse respeito são representados por uma sensibilidade baixa/elevada para os atrasos na resposta pelo servidor e o tempo excedido da aplicação, ou a personalização baixa/elevada de gestão das recusas do pedido.

Neste último caso, o módulo de balanceamento de pacote 74 desempenha a maior parte da actividade relacionada. Dependendo da resposta (aceite/recusada) recebida do solicitador de regra 76, o módulo de balanceamento de pacote 74 determina se e como o pacote de pedido original (continua em “standby”) é para ser re-injectado ao nível Núcleo de modo a ser enviado para o servidor hospedeiro.

Nesse caso, a criação de um local ACL leva à optimização de qualquer pedido subsequente do mesmo tipo, através da criação de um tipo de cache evitando assim contínuos pedidos do servidor.

Uma vantagem básica deste esquema reside na permissão do redireccionamento em linha do pacote para o chamado “destinos sentimos muito” (estes são usualmente na forma de páginas html, filmes ou outros, depende do tipo de pedido), enquanto é mantido a ligação TCP com o servidor hospedeiro activo e sem requerer a presença de um módulo de software de simulação para ensinar tecnologia destinada a ser manuseada.

Formas de realização práticas da porta de comunicação 20 concentrada num sistema onde a acção de accionamento e o seguinte filtro de acção, são desempenhados com um elevado grau de granularidade, de modo nocional em ligação com cada e todos os conteúdos requeridos por um utilizador especifico.

Nesse respeito, ambos i) disposições que funcionam como proxies através da avaliação das suas características em termos de transparência no que diz respeito ao impacto do agente - ou o componente desempenha o papel do agente - na rede (a chamada segurança “transparente”).

Como uma extensão, os componentes de accionamento e filtragem podem ser considerados de modo a estender as análises também para aqueles pacotes de análise e sistemas de inspecção de pacote existentes nos sistemas de filtragem de Web que são suficientemente configuráveis e granulares.

Finalmente, vários modos possíveis de deturpar/re-injectar são considerados.

Uma primeira observação é que o FreeBSD e Linux dão a possibilidade de filtragem de pacotes IP até ao nível 4, redireccionando-os num conector Núcleo onde também permitem gestão ao nível de aplicação. Esta capacidade é explorada por

muitos sistemas de análise de rede. De modo adicional, FreeBSD dá a possibilidade de enviar pacotes IP que satisfazem uma determinada regra de segurança para uma aplicação de utilizador que pode decidir se estes pacotes são para ser modificados ou re-injectados na rede (regra de desvio). Nesse caso, o sistema toma conta de remontagem dos quadros de Ethernet de uma forma correcta.

De um modo adicional, quer o FreeBDS quer o Linux oferecem a possibilidade de configuração de um par de interfaces de rede num modo de transmissão em ponte. Este esquema, no entanto, já não oferece a possibilidade de desvio dos pacotes.

As análises de pacotes não requerem por necessidade a disponibilidade de um proxy de camada de aplicação. As análises podem ser efectuadas através de mecanismos de análises de expressões regulares (as chamadas “análises de imitação”), tal como tipicamente usadas por sistemas de detecção de intrusão. Alguns sistemas de detecção de intrusão providenciam um mecanismo de accionamento de uma assinatura predefinida for detectada no pacote Ethernet.

Outros sistemas usam o mecanismo de assinatura para desempenhar uma concepção inteligente dos pacotes, operando ao nível 7.

O diagrama de bloco da figura 19 destaca as várias fases de operação do esquema aqui descrito sem expressamente referir ao posicionamento dos módulos nos vários dispositivos.

Numa etapa 100 um pacote genérico entra na porta de comunicação DCCA 20.

Numa etapa de análise 102 de nível 4 (por exemplo direcção, protocolo e porta de comunicação) são detectados alguns pacotes para serem redireccionados (desviados) para a análise de nível 7. Esses pacotes que não são filtrados pelo nível de regra 4 seguem (após algumas bases de controlos possíveis noutras regras de nível 4 para outros protocolos no bloco 102), uma ponte típica flui através do bloco 118 de uma maneira inalterada.

A análise de nível 7 é representada por um bloco 106.

No exemplo de forma de realização aqui descrito esta análise é levada a cabo em território do utilizador e não no nível Núcleo. Em qualquer dos casos, tais análises determinam as características do pedido e envia o pedido de autorização para o módulo de autorização (bloco 108). No exemplo de forma de realização descrito aqui isto é implementado pelo servidor 22. Em qualquer dos casos, o nível 7 análises pode requerer autorização temporária do pedido (no caso do modo de operação baseado em autorização atrasada com controlo de resposta. Nesse caso, o dispositivo pode definir uma regra baseada o tempo.

A fase de definição de regra é representada por um bloco 110. Isto geralmente envolve activação de regras para permitir tráfico em duas direcções e, em geral, outras regras relacionadas que permitem gestão contabilística no tráfico de resposta (isto é geralmente desempenhado por um módulo externo designado 112).

A fase de autorização tal como levada a cabo no módulo 108 pode derivar (por exemplo, como um resultado de uma resposta

de recusa) em redirecção em linha do pedido actuando na fase de redireccionamento (bloco 114).

Subsequentemente, a fase de re-injecção 104 reinsere o pacote previamente sujeito a uma acção de desvio (modificado como possível como resultado de redireccionamento). Finalmente, numa etapa designada 116 o pacote (quer transmitido em ponte quer re-injectao) deixa o dispositivo.

A Figura 20 mostra o tráfico de entrada da rede (pedido para conteúdos multimédia), interceptado e filtrado ao nível Núcleo (por meio de regras de dispositivo de segurança IP) e trazido para um espaço de utilizador. Lá, os módulos JAVA encarregam-se da tarefa de autorizar pedidos e re-injecta o tráfico ao nível do núcleo para servir o pedido de um modo tradicional.

Como indicado, uma localização preferida da porta de comunicação 20 está em frente do servidor. Desse modo, o servidor pode ser controlado assegurando que o caminho de rede para o alcançar, começa em qualquer cliente considerado, é - por necessidade - apenas um, passando através do dispositivo.

De outro modo, um FreeBSD 4.8 O núcleo pode ser modificado de modo a assegurar que alguns sub-componentes do comando ipfw (relacionado com desvio e re-injecção dos pacotes para e a partir do nível de aplicação) possam operar também correctamente com os pacotes de transmissão em ponte.

Os pedidos pelos utilizadores finais são interceptados na entrada da interface de rede e passam, através do empilhamento de protocolo de rede, para o módulo núcleo (IP

firewall) para filtragem de pacote. Um tal módulo analisa e filtra o tráfico de rede definindo regras do tipo:

0400 aceita do 192.168.0.1 22222 para 192.168.0.2 33333 tcp por via fxp0 estabelecida.

O primeiro parâmetro representa o identificador para a regra IP Firewall, o segundo a acção a ser desempenhada (permissão/negação/desvio), seguido pela fonte e endereços de IP de destino e as respectivas portas de comunicação lógicas, o protocolo de transporte, o interface de entrada para o tráfico e, no caso considerado, (protocolo TCP) o controlo da sinalização SYN para controlar se a ligação está configurada ou não.

O dispositivo de segurança IP oferece uma função adicional que permite envio de tráfico satisfazendo as condições da regra para o espaço de utilizador usando um conector específico (CONECTOR_DESVIO). Desse modo, quaisquer tarefas de processamento relacionadas ao tráfico de rede podem ser dispostas para o nível de aplicação.

Para esse propósito, é o suficiente indicar a opção “desvio” tal como no campo de acção na regra de IP Firewall:

0400 desvia 44444 de 192.168.0.1 22222 para 192.168.0.2 33333 tcp via fxp0 estabelecida

Isto indica também a porta de comunicação lógica do conector-desvio (44444) para o tráfico de rede satisfazendo a regra de ser enviado.

Um módulo desenvolvido em C (C_para_JAVA) assegura um interface adequado dos conectores_desvio com aplicações JAVA para analisar e processar o pedido do nível de núcleo.

Por exemplo, tal tipo de esquema pode ser aplicado ao tráfico ICMP (do tipo de pedido com entrada de informações) usando a regra do dispositivo de segurança de IP para intercepção:

0400 desvio 44444 de 192.168.2.2 para 192.168.2.1 icmp via fxp1 icmptype 8.

Isto tem o propósito de intercepção de pedidos ICMP do cliente na interface “fxp1”, passando tais pacotes para um módulo de software JAVA ouvindo na porta de comunicação “44444” para saída vídeo dos pacotes de dados e re-injectando o tráfico na interface de saída (fxp0).

O filtro é assim transparente para o cliente solicitador, enquanto correctamente intercepta (e possivelmente imprime) os pacotes ICMP

Experiências alternativas foram levadas a cabo usando o protocolo “mmst” (mmst terminou o transporte TCP) usando como REGRA de dispositivo de segurança de IP:

> 0400 desvia 44444 de 192.168.2.2 para 192.168.2.1 tcp via fxp estabelecido.

Isto tem o propósito de interceptar todos os pacotes de dados que requerem conteúdos multimédia do servidor Windows Media™ (sessões TCP definidas: SYN=0), passando-as para um módulo de software JAVA em espaço de utilizador para saída vídeo e re-injecção no tráfico no interface de saída (fxp0).

O fluxo de áudio/vídeo foi deixado inalterado durante o processo de intercepção e re-injecção. Durante a operação, é possível visualizar as URLs contidas nos pedidos do servidor. Comunicando com o servidor de segurança, o módulo JAVA no agente verifica se o endereço IP que solicitou um determinado conteúdo está autorizado para receber o conteúdo da url solicitada.

Nesse caso, o trafico desvio para um espaço de utilizador é re-injectado ao nível do núcleo usando os conectores_desvio e o pedido é subsequentemente enviado através dos interfaces de saída para um aparelho de armazenamento relacionado.

No caso onde o teste foi levado a cabo pelo módulo JAVA produz um resultado negativo, duas possibilidades existem:

- o tráfico é descartado ou redireccionado para a página "lamentamos muito" (lógica positiva),
- por outro lado o tráfico é re-injectado ao nível de Núcleo e permitido qu alcance os dispositivos de armazenamento enquanto a resposta flui dos caches é subsequentemente bloqueada (lógica negativa).

Redireccionamento do tráfico de rede do espaço Núcleo para o espaço de utilizador via dos conectores_desvio é possível através da modificação do módulo Núcleo relacionado ao IP Firewall. Isto originalmente desempenha um controlo na consistência dos pacotes de IP antes da operação de desvio (que assim sendo não é permitida nos pacotes não IP). A modificação remove esse tipo de controlo, dando assim a possibilidade de levar a cabo uma acção de desvio em quadros de Ethernet "puros"

O sistema aqui descrito autoriza pedidos através da exploração de um paradigma PULL: o utilizador avança com o pedido; este é também interceptado directamente ou o fluxo de retorno associado é interceptado e listas de controlo num sistema de rede são finalmente gerados.

De modo adicional, o mecanismo intercepta o pedido ou o fluxo de retorno identifica um inicio de conta, nomeadamente, o inicio de entrega. Subsequentemente, a geração automática da entrada na lista de controlo leva o sistema na rede a monitorizar a actividade através de possível geração de outros tipos de registo de uso (temporário e para). A informação disponível inclui todos os itens que permitem pagar, nomeadamente:

- facturação com base no consumo, graças aos dados de trafico capturados da entrada da lista de controlo,
- facturação baseada no tempo, graças à gestão do iniciar e terminar eventos, e
- facturação baseada no evento/conteúdo, graças à indicação da referência aos conteúdos.

Desse modo, a possibilidade é dada ao operador de facturar baseado no tráfico assim facturação de tempo para serviços ao vivo, facturação de eventos para serviços de vídeo a pedido e semelhantes, enquanto é desagregado da conta total o componente de tráfico de modo a evitar facturação em duplicado.

Este sistema pode ser aplicado de uma forma transparente para diferentes tipos de conteúdos de arquitecturas de entrega (ambas centralizadas e descentralizadas).

O mesmo sistema pode ser usado, sem o accionamento de sistema, para levar a cabo autorização com base num paradigma PUSH (ENVIAR), que é por meio de pré provisionamento por um servidor central baseado em lógicas de controlo não directamente accionado pela rede, mas ao invés accionado por aplicações externas.

O paradigma PULL (OBTER) é significante na medida em que providencia certos melhoramentos “instantâneos” para o serviço de entrega de conteúdo. Isto é uma forma que é completamente transparente em relação aos dois pontos envolvidos, nomeadamente o solicitador de conteúdo CR e o servidor que providencia o serviço. Baseado nas características do dispositivo de accionamento/filtragem e as funções de controlo possivelmente providenciadas por um servidor externo, o sistema aqui descrito pode ser usado para outros propósitos.

Exemplo disso é como se segue.

A qualidade dinâmica de suporte de serviço (QoS). Na sequência de um pedido para aceder a determinado conteúdo, o servidor 22 pode detectar os requisitos específicos e gerar um pedido de reserva para um sistema de gestão QoS, para a largura de banda requerida e para a duração do conteúdo, através do uso do servidor hospedeiro e o solicitar de conteúdo como ponto final. De modo alternativo, a possibilidade existe de comunicar directamente com a porta de comunicação 20 de modo a marcar os quadros de retorno do servidor de conteúdos com um certo nível de serviço.

De um modo alternativo, o mesmo sistema pode ser usado para suportar portais de aplicação externa, através do controlo e

autorização de um modo transparente, o acesso por uma terceira parte aos conteúdos de um portal sem a necessidade de providenciar esta função de um modo nativo.

Pode continuar a ser de um modo alternativo, o mesmo sistema pode ser para as redirecções controladas de pedidos para atributos prefixados de tempo real. Isto leva a um mecanismo de redireccionamento do pedido de utilizador por reconstrução de apagar a URL. Desse modo, um pedido pode ser adaptado de acordo com atributos específicos do utilizador e determinados critérios que podem possivelmente derivar de sistemas externos tais como:

- informação em tempo real no que diz respeito a localização de modo a alterar, por exemplo, um pedido para www.restaurants.it em restaurantes.it/Milan;
- dependendo da altura do dia, transformando possivelmente um pedido do tipo www.rai.it/lastnews em um pedido mais geral tal como rai.it/eveningnews;

- dependendo da largura de banda disponível, transformando o pedido do tipo www.trailer.it/mickey num pedido www.trailer.it/30Kb/mickey;

- dependendo das características do terminal de utilizador. Isto pode ser por exemplo baseado na detecção de um contexto de rede móvel por meio do endereço IP e do IMEI (International Mobile Equipment Indentity) enquanto identificador que deriva de características de hardware especifico (mostrador, capacidades e por ai a diante). Um pedido genérico para um determinado contexto pode ser assim transformado num pedido adaptado às características de hardware do receptor.

Tal como uma regra, o mecanismo de accionamento e intercepção disponível com a porta de comunicação 20 avalia determinadas características em tempo real, enquanto permite que uma decisão seja tomada como a melhor maneira de servir o conteúdo solicitado.

Uma porta de comunicação como descrito anteriormente pode ser implementada, de modo opcional:

- directamente no servidor hospedeiro (agegado),
- directamente num elemento de rede incluído no fluxo de trafico entre o utilizador e o servidor (agregado),
- por meio de uma equipamento dedicado inserido de um modo transparente na infra-estrutura de rede no fluxo de trafico entre o utilizador e o servidor hospedeiro (agregado), esta opção é considerada um forma de realização preferida.

O servidor de segurança que implementa o mecanismo de verificação no acesso pode ser implementado de modo opcional:

- como uma derivação de um servidor AAA genérico com uma extensão de acesso para as capacidades de utilizador para o conteúdo,
- como uma derivação de um servidor de segurança genérico com uma extensão semelhante, e
- como um sistema dedicado para alerta de conteúdos de segurança, isto é actualmente considerado como uma forma de realização preferida.

O dispositivo é preferivelmente disposto e ainda de preferivelmente co-localizado, conjuntamente com o servidor de conteúdo (centro de serviço ou sítios CDN). Como

alternativa, pode ser disposto na rede de acesso, abaixo do primeiro dispositivo de IP existente.

É então evidente que, sem prejudicar os princípios básicos da invenção, os detalhes e formas de realização podem variar, também de um modo significativo, em relação ao que foi descrito, apenas a título de exemplo, sem sair do âmbito da invenção como definido pelas reivindicações que se seguem.

06-05-2008

REIVINDICAÇÕES

1. Método de gestão de transacções numa rede de comunicação, as referidas transacções incluem pelo menos um pedido dependente de tecnologia para um determinado conteúdo efectuado através de um solicitador (CR) a pelo menos um servidor (14), o método inclui as etapas de:

- disponibilização de uma lista de conteúdos de acesso (80) incluindo permissão/negação que são as cláusulas de acesso do referido solicitador (CR) a conteúdos providenciados por pelo menos um servidor (14),
- detecção (56) do referido pedido dependente de tecnologia
- extracção (58) do referido pedido dependente de tecnologia de informação que identifica o solicitador (CR) que faz o pedido e o conteúdo pedido,
- geração (58) a partir da informação extraída do referido pedido dependente de tecnologia que pede uma entrada de conteúdo de acesso de independente tecnologia correspondente,
- verificação (22) da referida entrada contra a referida lista para derivar informação de permissão/negação no que diz respeito ao pedido detectado, e
- gestão dos referidos pedidos como uma função da referida informação de permissão/negação derivada, caracterizada por a referida gestão do referido pedido incluir, aquelas da referida informação de permissão/negação derivada, a etapa de envio (116) do referido pedido para o referido pelo menos um servidor (14) e, como uma função da referida informação de permissão/negação derivada, as etapas alternativas de:

- i) bloqueamento de transacção associada com o referido pedido detectado, se a informação de permissão/negação indicar que o solicitador não está autorizado, ou

- ii) deixar que a transacção associada ao referido pedido continue, se a informação de permissão/negação indicar que o solicitador está autorizado.

2. Método da reivindicação 1, caracterizado por a referida etapa de bloqueamento ser levada a cabo pelo bloqueamento de um fluxo de dados de resposta (4, 5) a partir de pelo menos um servidor (14) para o solicitador (CR) fazer o referido pedido detectado.

3. Método das reivindicações 1 e 2, caracterizado por a referida etapa de bloqueamento ser atrasada (114) em relação à derivação da referida informação de permissão/negação.

4. Método da reivindicação 1, 2 ou 3, caracterizado por a referida entrada de conteúdos de acesso incluir:

- atributos de identificação do solicitador (CR) que apresenta o pedido detectados,
- atributos de identificação do conteúdo pedido, e
- atributos de identificação do referido pelo menos um servidor (14) para o qual o pedido é feito.

5. Método de qualquer uma das reivindicações precedentes, caracterizado por incluir a etapa de providenciar uma função de porta de comunicação (20) entre o referido solicitador (CR) e o referido pelo menos um servidor (14).

6. Método da reivindicação 5, caracterizado por incluir as etapas de:

- configuração da referida função porta de comunicação (20) para levar a cabo pelo menos um das referidas etapas de detecção, extracção, geração e gestão, e
- associação com a referida função porta de comunicação (20) uma função de servidor de regra de conteúdo (22) para desempenhar a referida etapa de verificação.

7. Método da reivindicação 6, caracterizado por incluir a etapa de fornecimento da referida função de porta de comunicação (20) com funções de interface (50, 52, 54) com os referidos solicitadores (CR) e o referido pelo menos um servidor (14) bem como em relação à referida função de servidor regulador de conteúdo (22), respectivamente.

8. Método da reivindicação, 6 ou 7, caracterizado por incluir a etapa de providenciar na referida função de porta de comunicação (20) uma pluralidade de níveis incluindo:

- um nível de núcleo baixo (56) na pluralidade de níveis, providenciando rede de comunicação, filtragem do nível de IP, funções relacionadas à detecção do referido pedido, e
- um nível de aplicação (58) acima do nível de núcleo baixo na pluralidade de níveis para levar a cabo as referidas etapas de extracção e geração.

9. Método da reivindicação 8, caracterizado por o referido nível de núcleo baixo (56) levar a cabo pelo menos uma das etapas de:

- filtragem (60) dos fluxos de dados trocados entre os referidos solicitadores (CR) e o referido pelo menos um servidor (14),
- desvio (62) dos referidos fluxos de dados para o referido nível de aplicação, e
- re-injecção (64) dos referidos fluxos de dados na referida rede.

10. Método da reivindicação 9, caracterizado po incluir a etapa de levara a cabo a referida filtragem como uma filtragem de pacotes.

11. Método da reivindicação 10, caracterizado por incluir a etapa de levar a cabo a referida filtragem de IP como uma filtragem de pacotes até ao nível 4.

12. Método da reivindicação 8, caracterizado por incluir a etapa de levar a cabo o referido nível de aplicação (58) as operações de:

- extracção (70) da referida informação de pedido que identifica o referido solicitador (CR) e o conteúdo solicitado,
- envio (76) da referida informação extraída para a referida função de servidor regulador de conteúdo (22), e
- controlo (72, 60a) do referido nível núcleo baixo (56).

13. Método de qualquer uma das reivindicações precedentes, caracterizado por incluir a etapa de detecção do referido pedido deixando o referido pedido não afectado.

14. Método de qualquer uma das reivindicações precedentes, caracterizado por a etapa de extracção incluir a análise de pacotes incluídos no referido pedido.

15. Método da reivindicação 14, caracterizado por as referidas análises serem levada a cabo na forma de análises de nível 7.

16. Método de qualquer uma das reivindicações precedentes, caracterizado por incluir a etapa de geração, baseada na referida informação de permissão/negação, e pelo menos um pedido de reserva para um sistema de gestão de qualidade de serviço (QoS).

17. Método de qualquer uma das reivindicações precedentes, caracterizado por incluir a etapa de redireccionamento do referido pedido de utilizador e através de um modo selectivo modificar um identificador (URL) a ele associado.

18. Método da reivindicação 1, caracterizado por incluir as etapas de:

- detecção de informação do terminal associado ao solicitador (CR) sendo o referido pedido detectado, e
- modificação do referido pedido detectado como uma função da referida informação tal como ao terminal associado com o solicitador (CR).

19. Sistema para gerir transacções numa rede de comunicação, as referidas transacções incluem pelo menos um pedido dependente de tecnologia para um determinado conteúdo feito por um solicitador (CR) a pelo menos um servidor (14), o sistema inclui uma lista de conteúdo de acesso (80) incluindo clausulas de acesso de permissão/negação que regulam o acesso

do referido solicitador (CR) a conteúdos providenciados pelo referido pelo menos um servidor (14), e pelo menos um modulo de processamento de pedido (20, 22) incluindo submódulos configurados para:

- detecção (56) do referido pedido de dependente tecnologia,
- extracção (58) do referido pedido de dependente tecnologia que identifica o solicitador (CR) efectuando o pedido e o conteúdo pedido,
- gerar (58)de informação extraída do referido pedido de dependente tecnologia de uma entrada de conteúdo de acesso de independente tecnologia correspondente,
- verificação (22) da referida entrada contra a referida lista para informação de permissão/negação derivada relativa ao pedido detectado , e
- gestão do referido pedido como uma função da referida informação de permissão/negação derivada, caracterizada por o referido pelo menos um modulo (20, 22) é configurado para desempenhar, independente de da referida informação de permissão/negação derivada, a etapa de envio (116) do referido pedido detectado para o referido pelo menos um servidor (14), como função da referida informação de permissão/negação derivada, as etapas alternativas de:
  - -i) bloqueamento de transição associado com os referidos pedidos detectados, se a informação de permissão/negação indica que o solicitador não está autorizado, ou
  - - ii) deixar a transição associada com o referido pedido continuar, se a informação de permissão/negação indicar que o solicitador se encontra autorizado.

20. Sistema da reivindicação 19, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para levar a cabo a referida etapa de bloqueamento bloqueando um fluxo de dados de resposta (4, 5) do referido pelo menos um servidor (14) e o solicitador (CR) faz o referido pedido detectado.

21. Sistema das reivindicações 19 ou 20 caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para levar a cabo a referida etapa de bloqueamento como uma etapa atrasada (114) em relação á derivação da referida informação de permissão/negação.

22. Sistema da reivindicação 19, 20, 21, caracterizado por a referida entrada de conteúdo de acesso incluir:

- atributos de identificação do solicitador (CR) que apresenta o pedido detectados,
- atributos de identificação do conteúdo pedido, e
- atributos de identificação do referido pelo menos um servidor (14) para o qual o pedido é feito.

23. Sistema de qualquer uma das reivindicações da 19 à 22, caracterizado por incluir uma porta de comunicação (20) entre o referido solicitador (CR) e o referido pelo menos um servidor (14).

24. Sistema da reivindicação 23, caracterizado por a referida porta de comunicação (20):

- ser configurada para levara a cabo pelo menos uma das referidas etapas de detecção, extracção, geração e gestão, e

- ter um servidor regulador de conteúdos associado 822) para levara a cabo a referida etapa de verificação.

25. Sistema da reivindicação 24, caracterizado por a referida porta de comunicação (20) ser dotada de funções de interface (50, 52; 54) com os referidos solicitadores (CR) e pelo menos um servidor (14) bem como uma função de servidor regulador de conteúdos (22), respectivamente.

26. Sistema de qualquer uma das reivindicações da 23 à 25, caracterizada por a referida porta de comunicação (20) incluir:

- um nível de núcleo baixo (56) providenciando rede de comunicação, transmissão em ponte funções de filtragem de nível relacionadas com a detecção do referido pedido, e
- um nível de aplicação (58) para levar a cabo as referidas etapas de extracção e geração.

27. Sistema da reivindicação 26, caracterizado por o referido nível núcleo baixo (56) ser configurado para levar a cabo pelo menos uma das etapas de:

- filtragem (60) dos fluxos de dados trocados entre os referidos solicitadores (CR) e o referido pelo menos um servidor (14),
- desvio (62) dos referidos fluxos de dados para o referido nível de aplicação, e
- re-injecção (64) dos referidos fluxos de dados na referida rede.

28. Sistema da reivindicação 27, caracterizado por a referida porta de comunicação (20) ser configurada para levar a cabo a referida filtragem como filtragem de pacote de IP.

29. Sistema da reivindicação 28, caracterizado por a referida filtragem de IP compreender filtragem de pacotes de IP até ao nível 4.

30. Sistema da reivindicação 26, caracterizado por o referido nível de aplicação (58) ser configurado para:

- extracção (70) da referida informação de pedido que identifica o referido solicitador (CR) e o conteúdo solicitado,
- envio (76) da referida informação extraída para a referida função de servidor regulador de conteúdo (22), e
- controlo (72, 60a) do referido nível núcleo baixo (56).

31. Sistema da reivindicação 19, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para detectar o referido pedido deixando o referido pedido não afectado.

32. Sistema da reivindicação 9, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para analisar pacotes na forma das análises do nível 7.

33. Sistema da reivindicação 32, caracterizado por o referido pelo menos um módulo de processamento (20, 22) ser configurado para levar a cabo a referida análise na forma de análises de nível 7.

34. Sistema da reivindicação 19, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para gerar, com base na referida informação de permissão/negação pelo menos um pedido de reserva para um sistema de gestão de qualidade de serviço (QoS).

35. Sistema da reivindicação 19, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para redireccionar o referido pedido de utilizador modificando de um modo selectivo um identificador (URL) a ele associado.

36. Sistema da reivindicação 19, caracterizado por pelo menos um módulo de processamento (20, 22) ser configurado para:

- detecção de informação para o terminal associado com o solicitador (CR) fazendo o referido pedido detectado, e
- modificando o referido pedido detectado como função da referida informação para o terminal associado com o solicitador (CR).

37. Rede de comunicação incluindo um sistema de acordo com qualquer uma das reivindicações da 19 à 36.

38. Produto de programa de computador carregável na memória de pelo menos um computador e incluindo porções de código de software para levara cabo o método de qualquer uma das reivindicações da 1 á 18.

06-05-2008

Fig.1

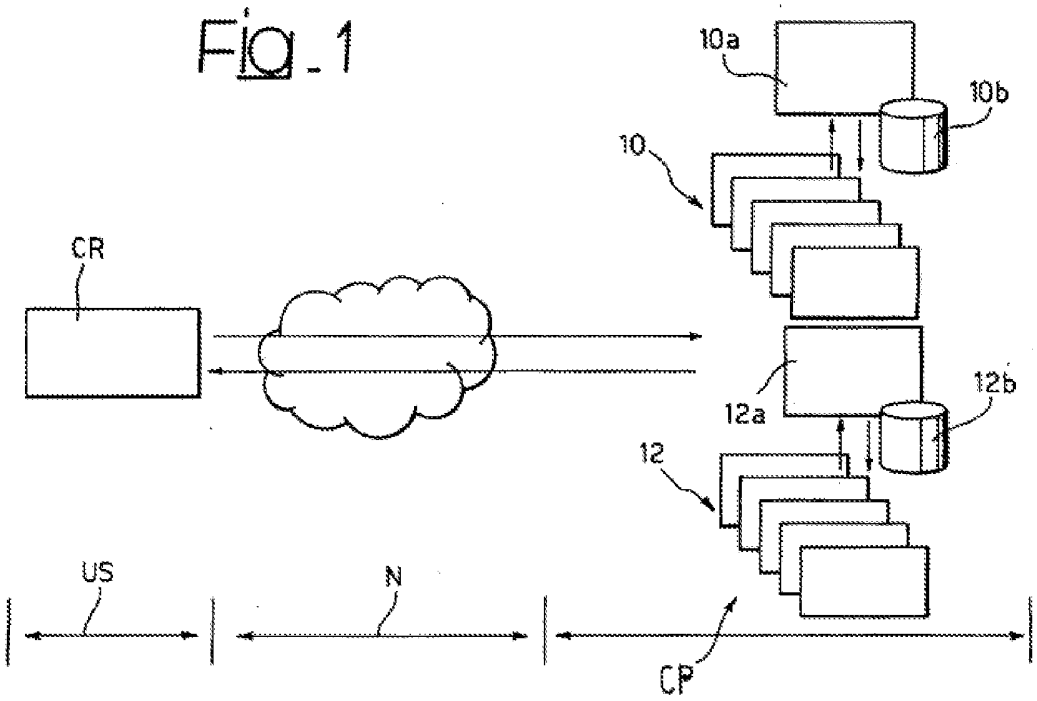


Fig.2

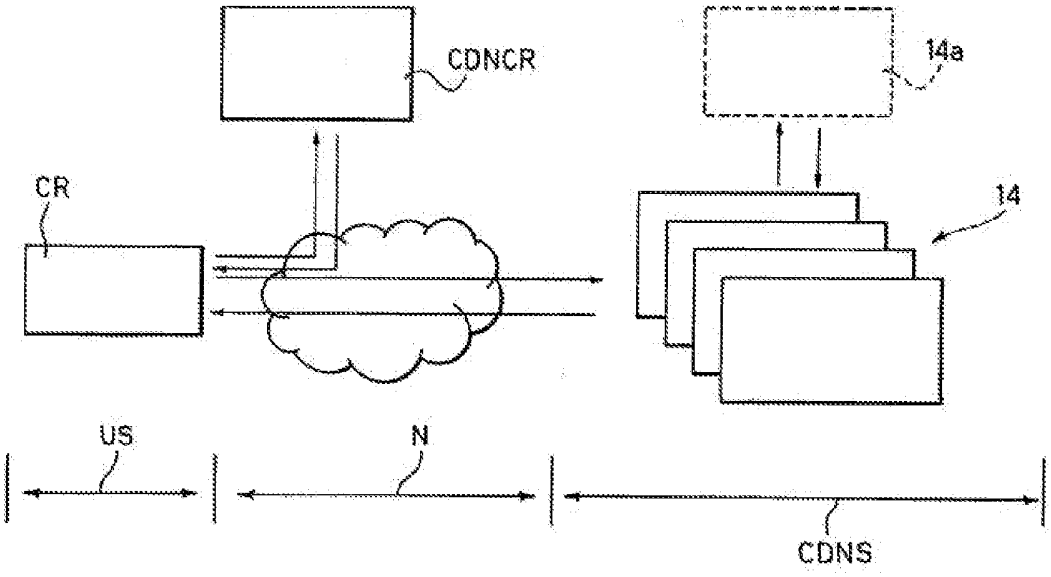


Fig.3

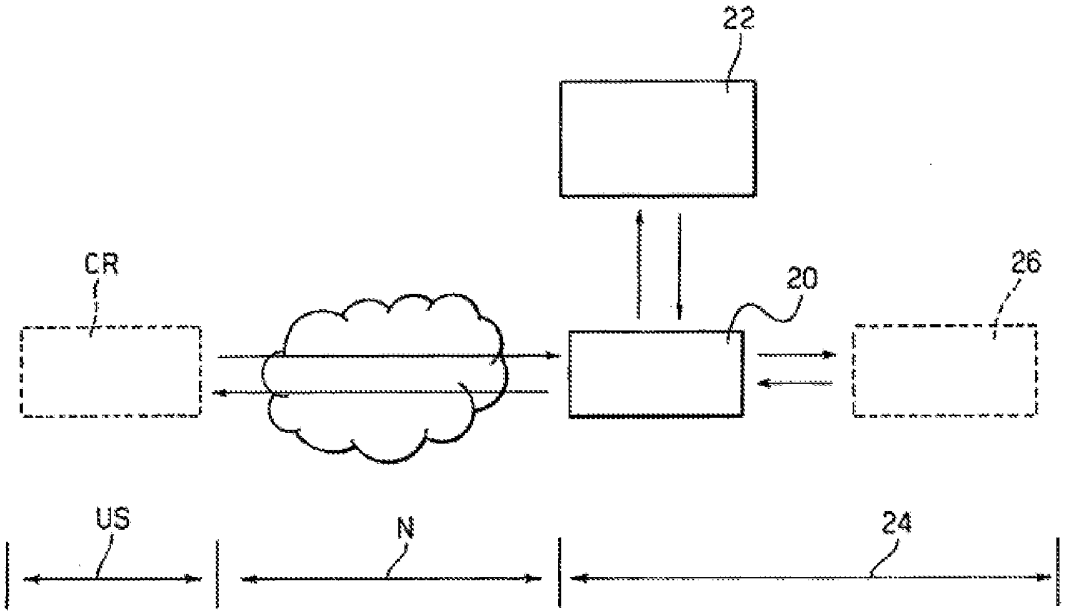


Fig. 4

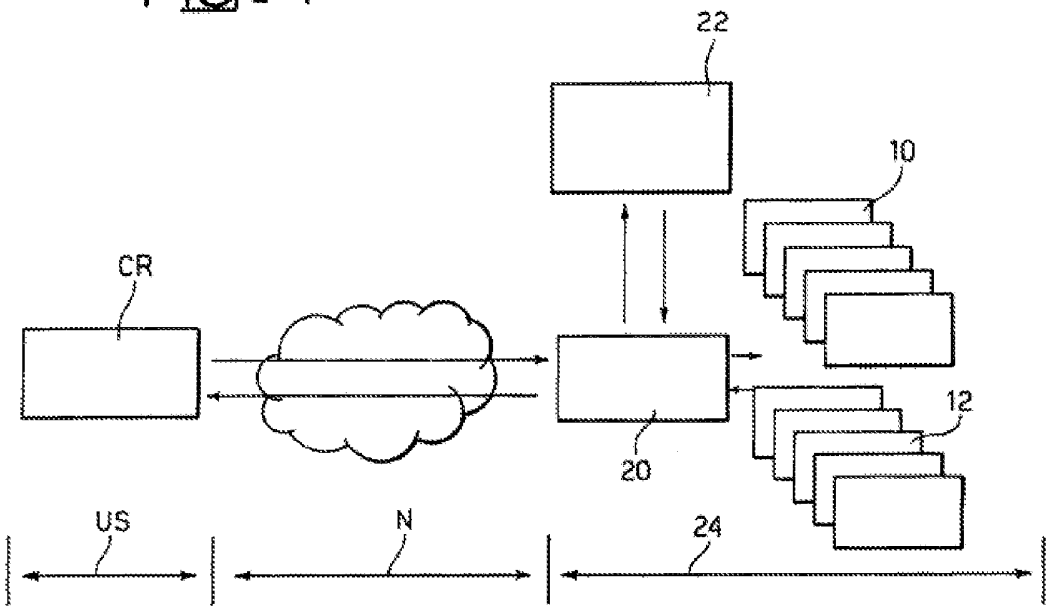


Fig.5

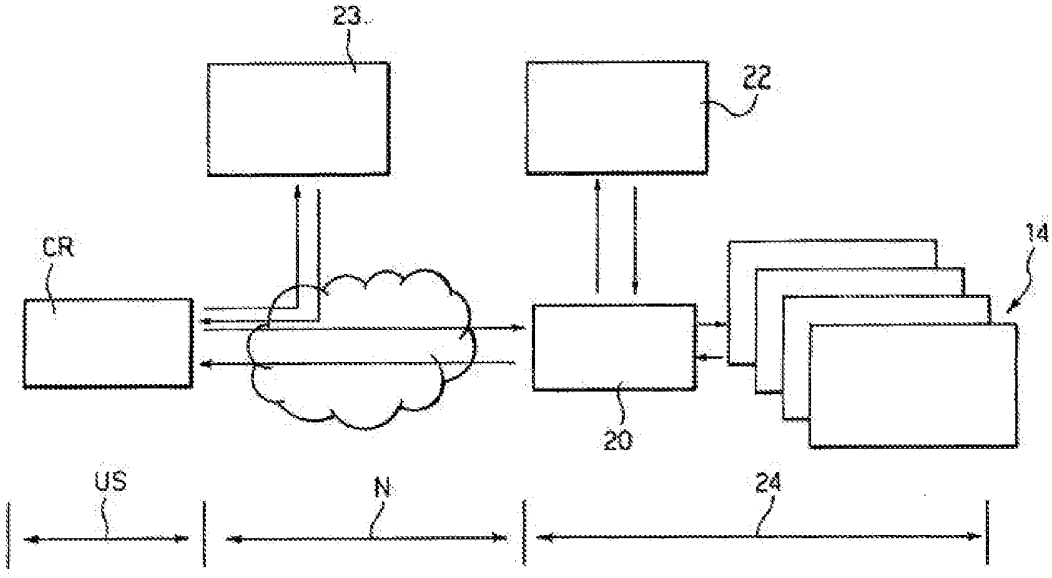


Fig.6

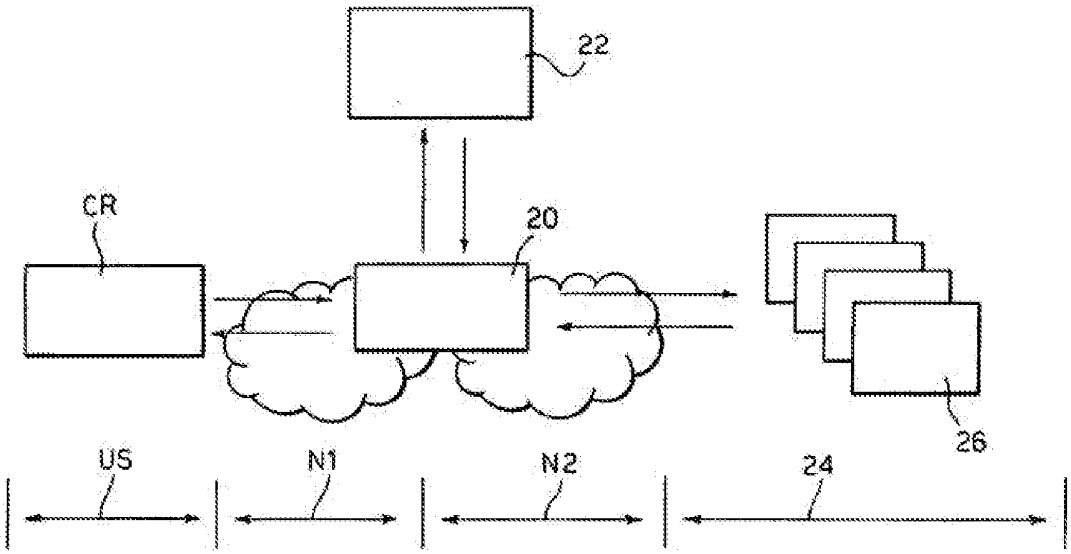


Fig. 7

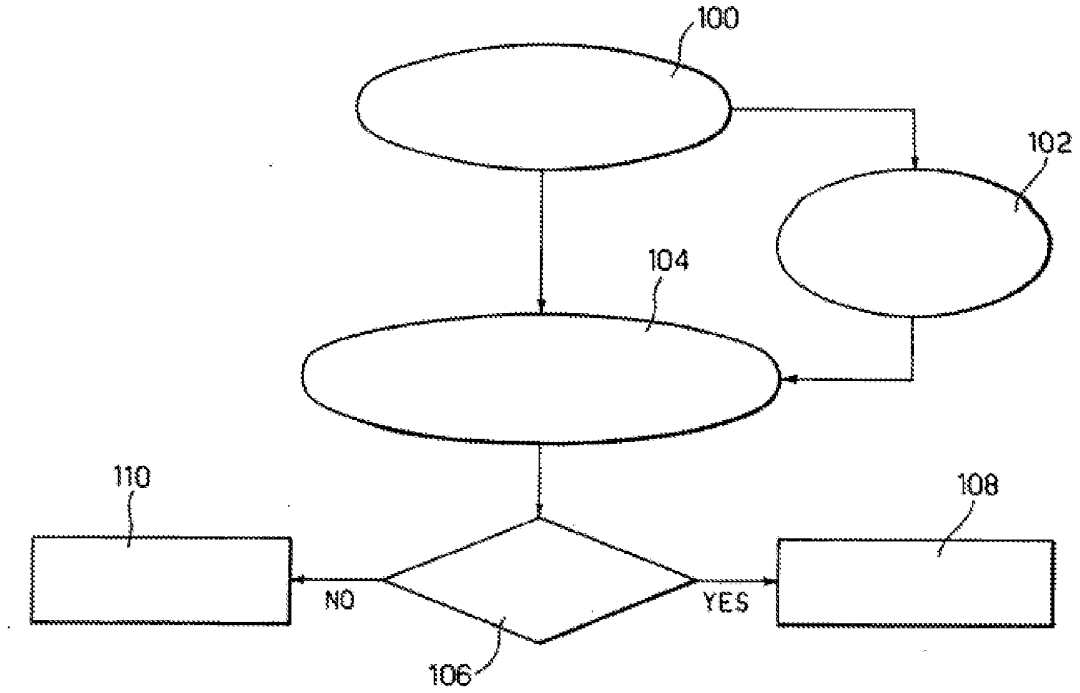


Fig.8

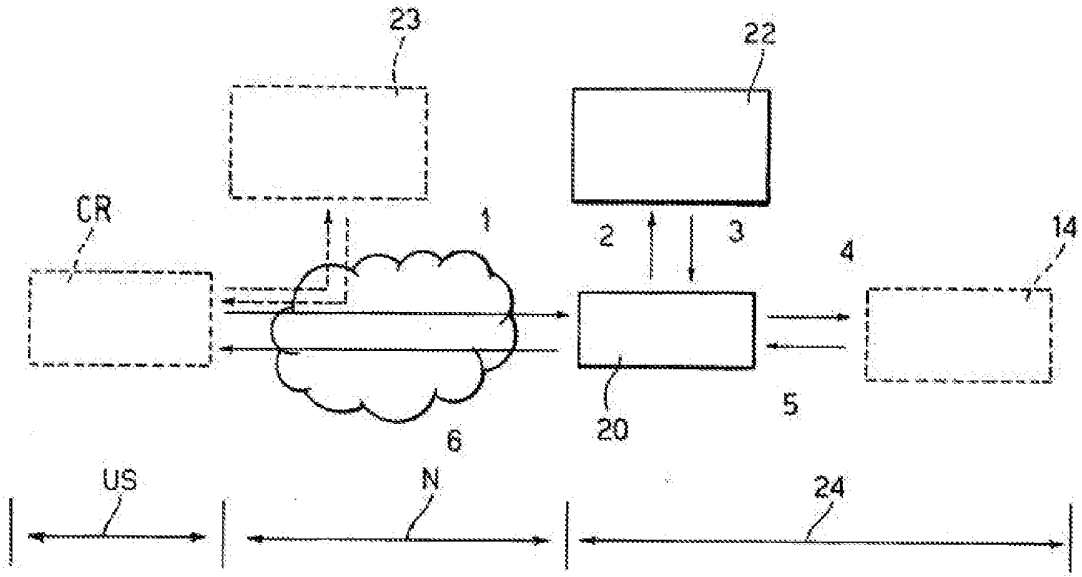


Fig.9

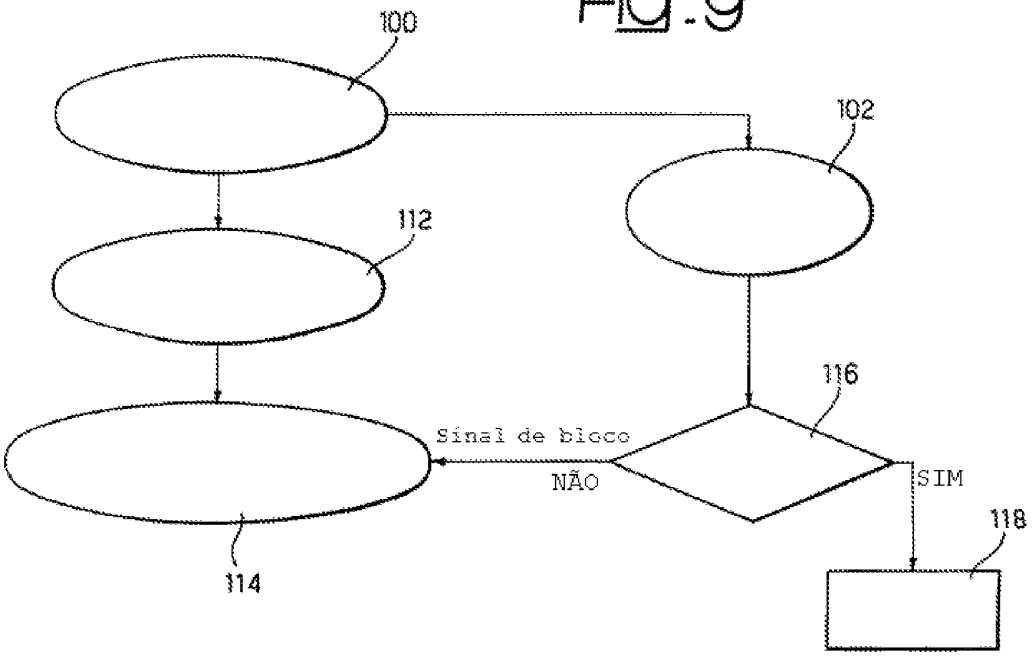


Fig.10

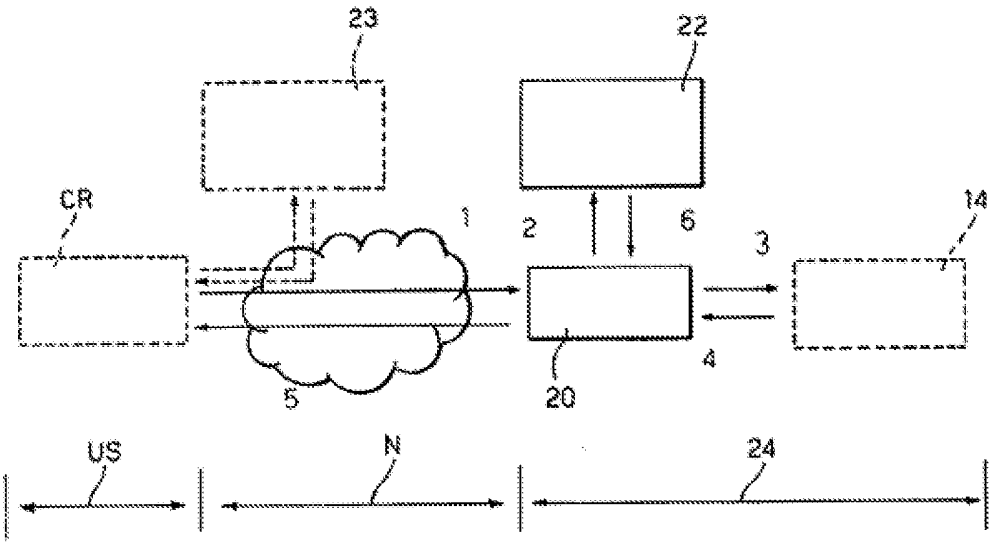


Fig. 11

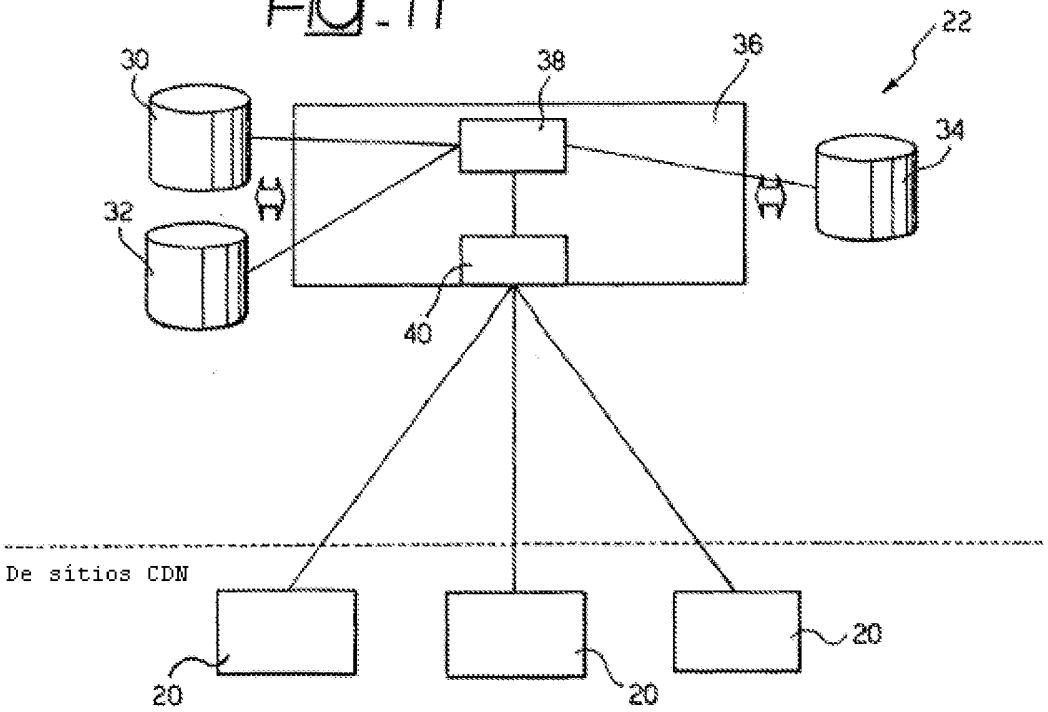


Fig. 12

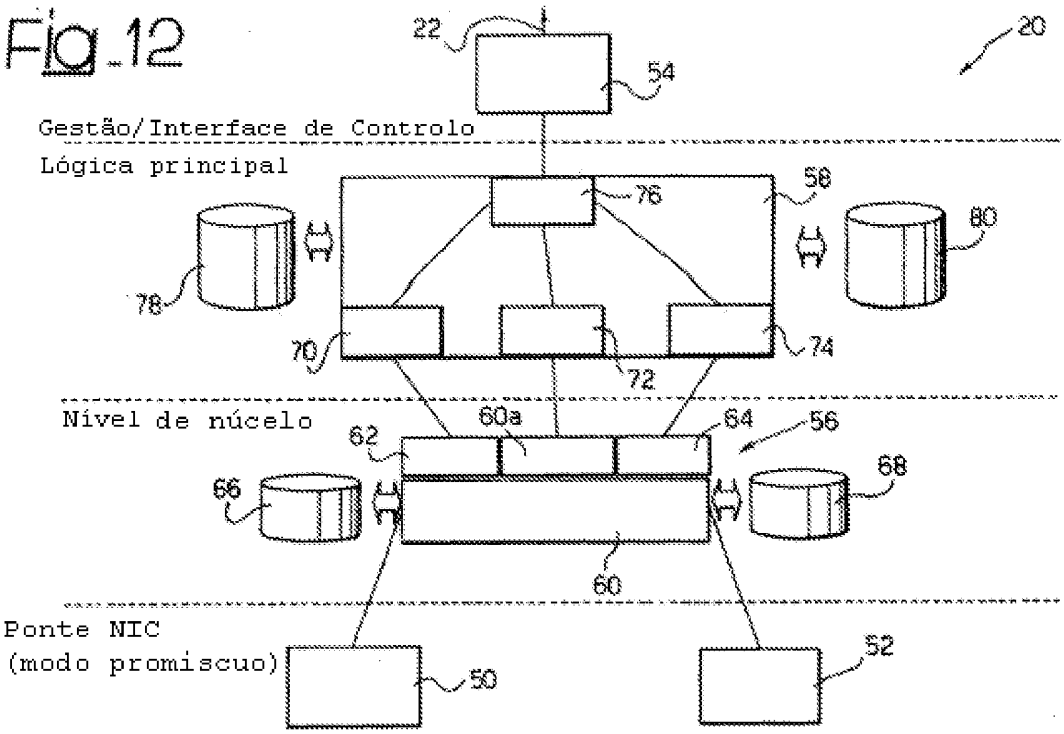

22
54
20
Gestão/Interface de Controlo
Lógica principal
76
58
80
78
70
72
74
Nível de núcelo
60a
62
64
56
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig. 13

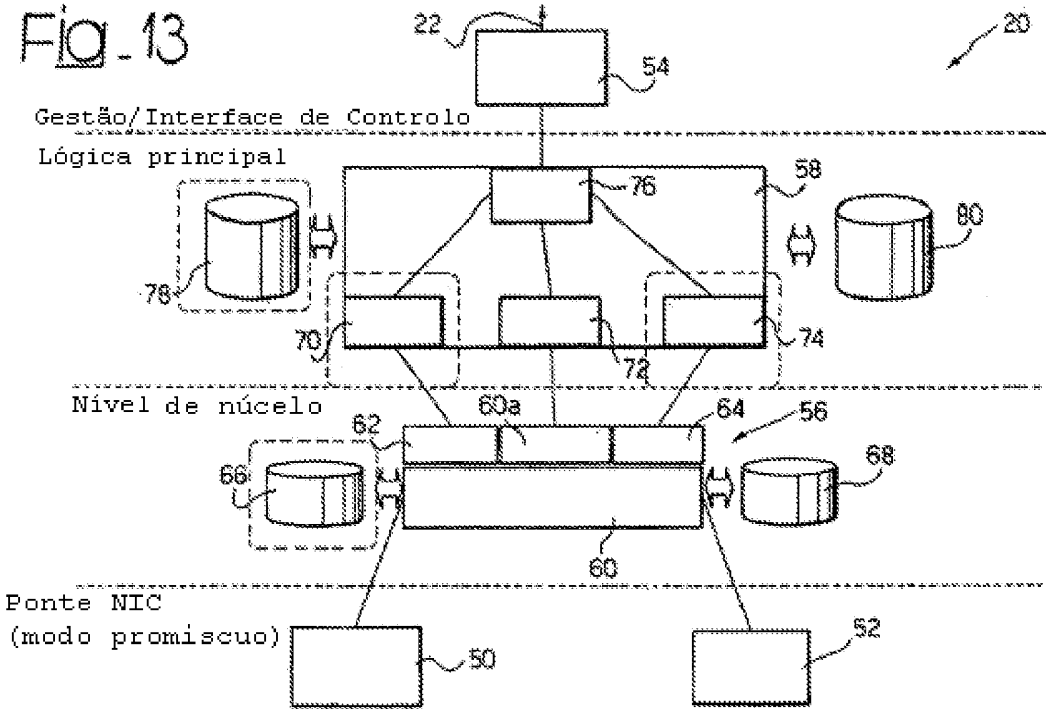

22
54
20
Gestão/Interface de Controlo
Lógica principal
76
58
80
78
70
72
74
Nível de núcelo
60a
62
64
56
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig.14

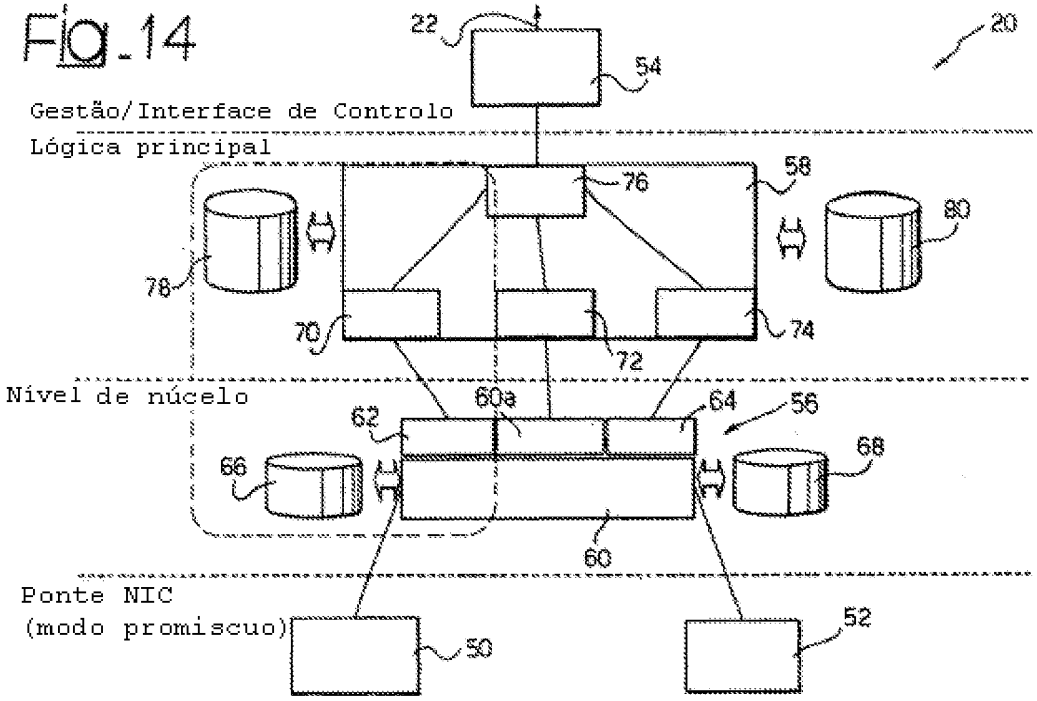

22
20
54
Gestão/Interface de Controlo
Lógica principal
76
58
80
78
70
72
74
Nível de núcelo
62
60a
64
56
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig. 15

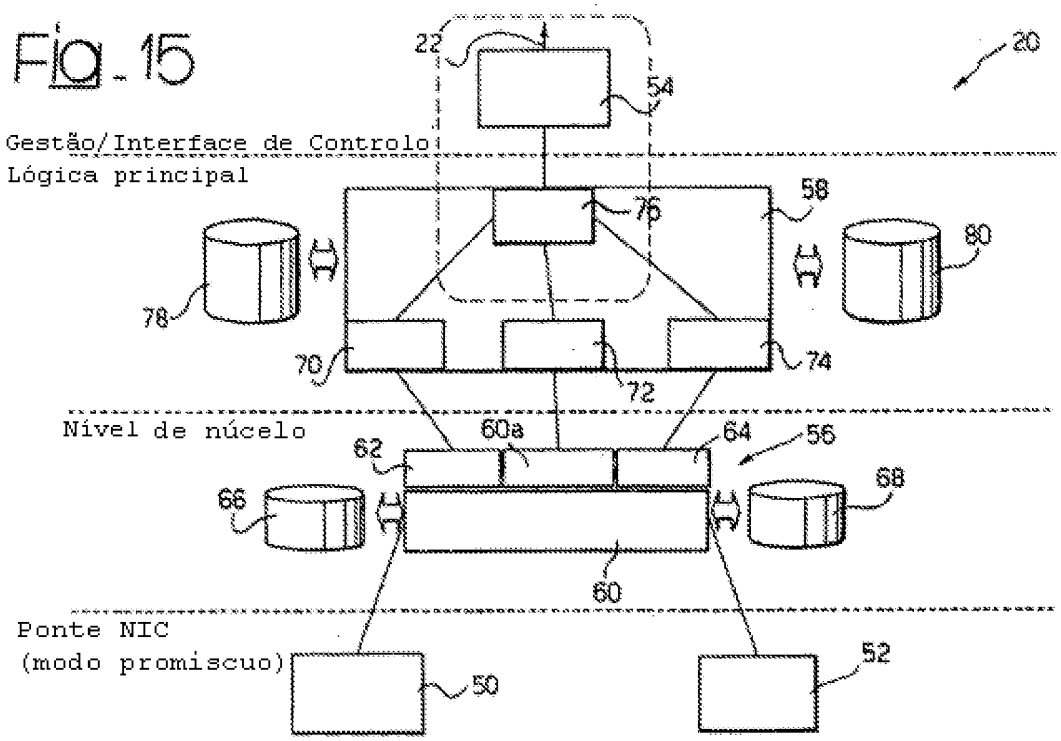

22
20
54
Gestão/Interface de Controlo
Lógica principal
58
76
78
80
70
72
74
Nível de núcelo
60a
62
64
56
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig. 16

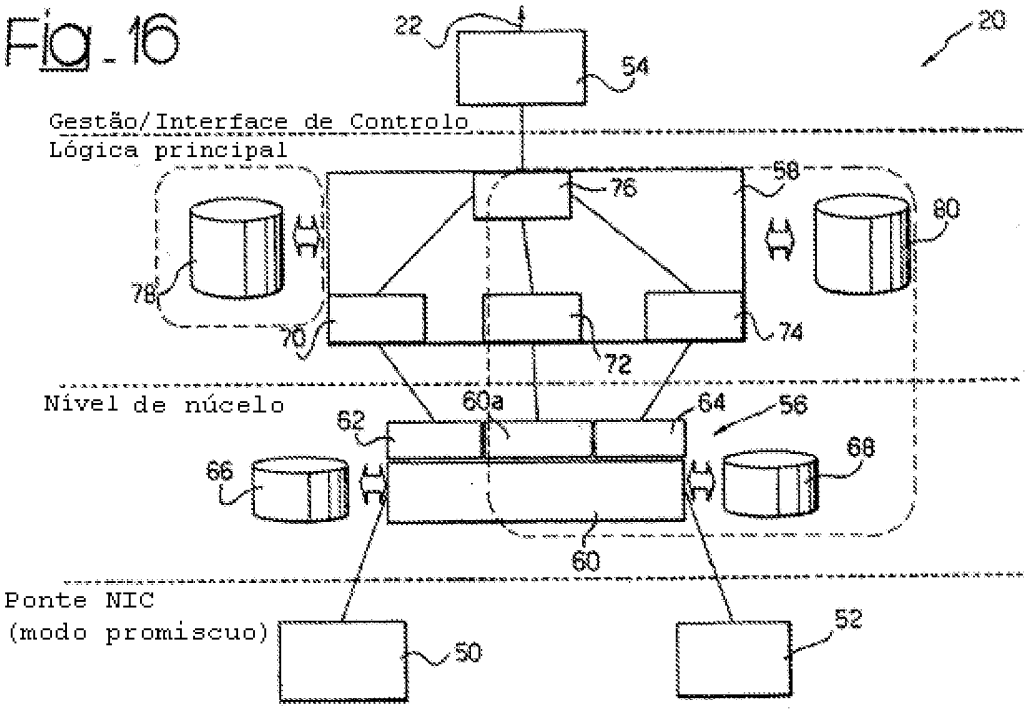

22
20
54
Gestão/Interface de Controlo
Lógica principal
76
58
80
78
70
72
74
Nível de núcelo
60a
64
56
62
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig. 17

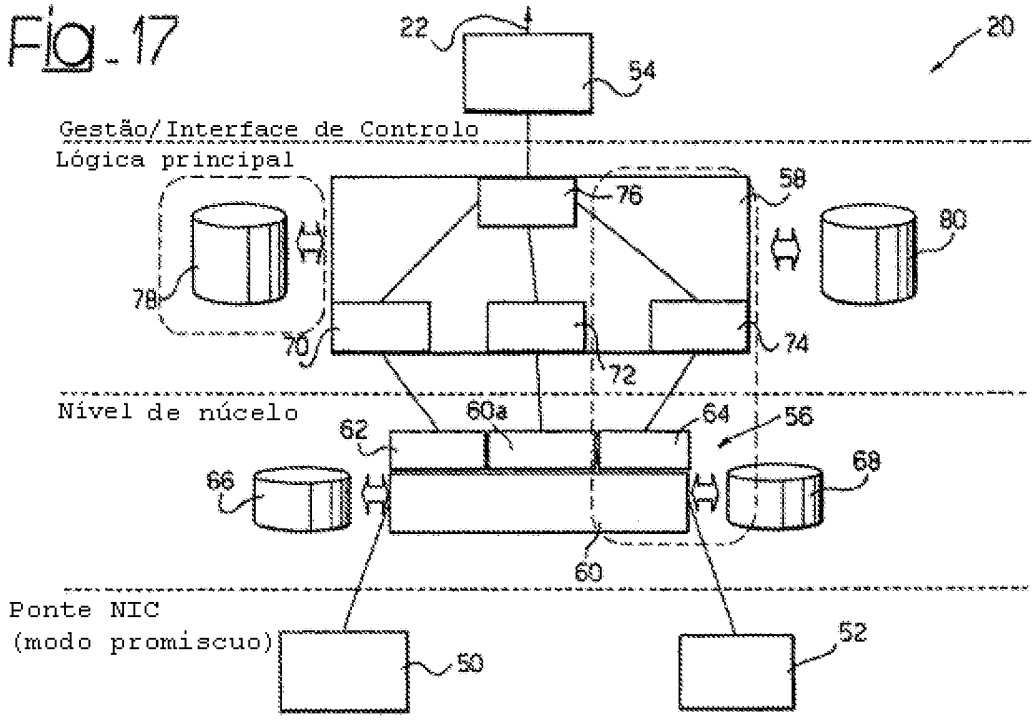

22
54
20
Gestão/Interface de Controlo
Lógica principal
76
58
80
78
70
74
72
Nível de núcelo
60a
64
56
62
66
68
60
Ponte NIC
(modo promiscuo)
50
52

Fig.18

Acção	Src IP	Dst IP	Protocolo	Porta de Entrada	Porta de Saída	N.D.	Conteúdo	TTL
Aceite/ Rejeitado	Endereço IP	Endereço IP	TCP/ UDP	Porta N°	Porta N°	Domínio	URL	secs

Fig.19

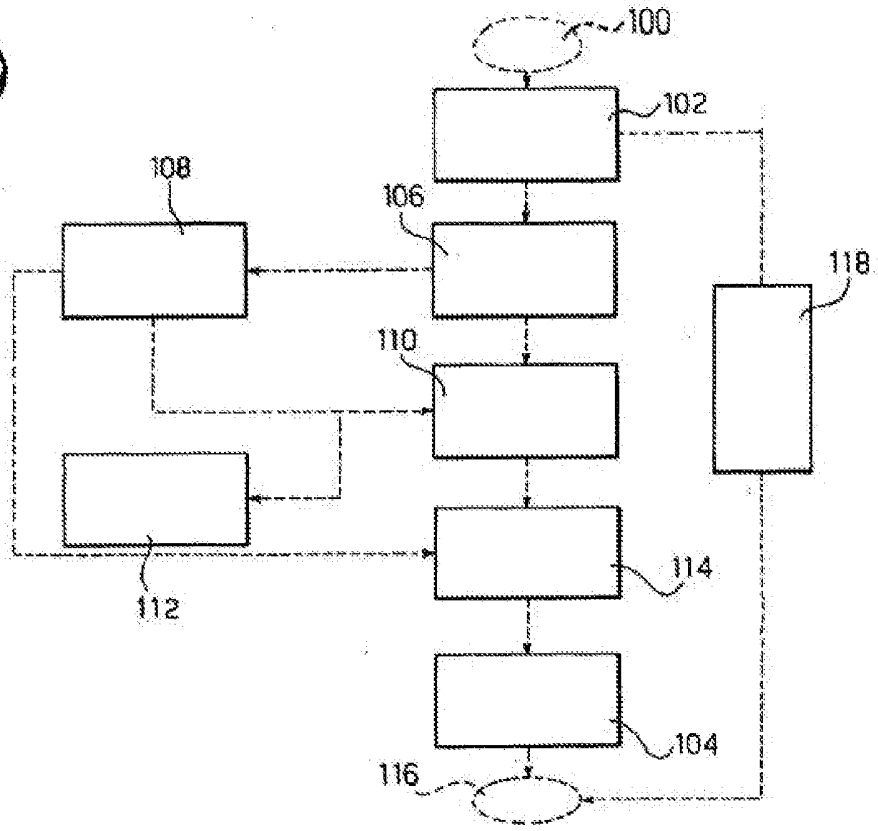
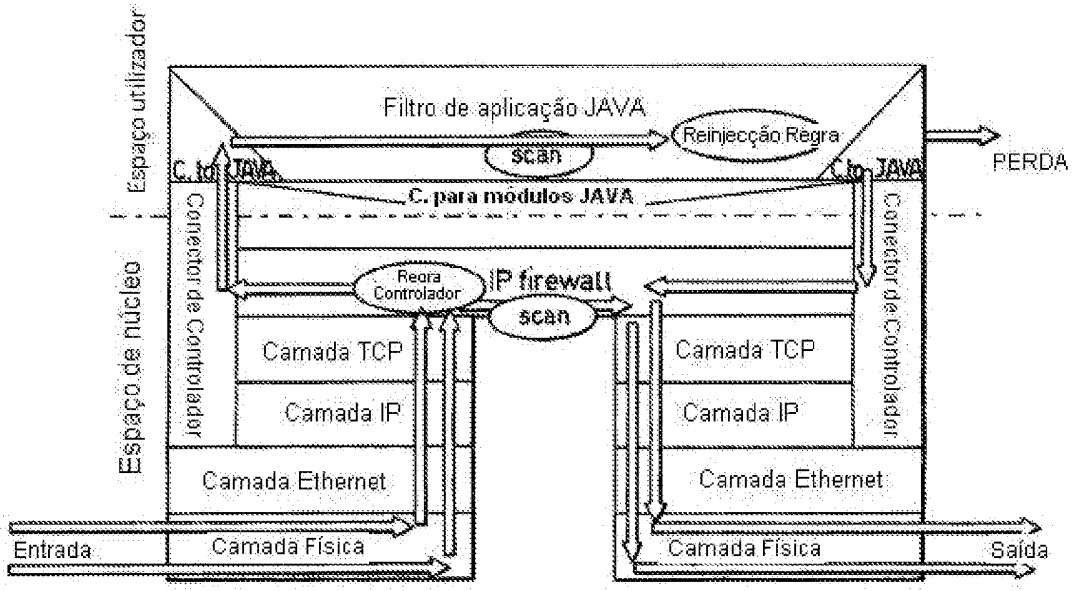


Fig.20


Espaço utilizador
Espaço de núcleo
Filtro de aplicação JAVA
Reinjecção Regra
scan
PERDA
C. JAVA
C. para módulos JAVA
Conector de Controlador
Regra Controlador
IP firewall
scan
Camada TCP
Camada IP
Camada Ethernet
Camada Física
Entrada
Saída