



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

(11) PI 0923742-9 B1



(22) Data do Depósito: 23/12/2009

(45) Data de Concessão: 05/01/2021

(54) Título: SERVIDOR DE PORTA DE LIGAÇÃO COM MICRONÚCLEO E PROCESSO DE CONTROLE DESTESERVIDOR

(51) Int.Cl.: H04L 29/06; H04L 29/08; G06F 9/46.

(52) CPC: H04L 63/02; H04L 69/12; H04L 69/32; G06F 9/46.

(30) Prioridade Unionista: 30/12/2008 FR 0859143.

(73) Titular(es): EADS SECURE NETWORKS.

(72) Inventor(es): GUILLAUME MEIER; MARC CHALAND; NICOLAS CLERMONT; FRANCIS HAUGUET.

(86) Pedido PCT: PCT FR2009052687 de 23/12/2009

(87) Publicação PCT: WO 2010/076523 de 08/07/2010

(85) Data do Início da Fase Nacional: 29/06/2011

(57) Resumo: SERVIDOR DE PORTA DE LIGAÇÃO COM MICRONÚCLEO. A presente invenção refere-se a um servidor de porta de ligação (27) munido de um primeiro subsistema que compreende um nível mídia (22), um nível (24) de comunicação e um nível (26) de controle, esse servidor (27) compreendendo também um micronúcleo (38) e um controlador de IPC (25) que gere comunicações entre os recursos do servidor atribuídos ao primeiro subsistema (22, 24, 26), caracterizado pelo fato de que ele compreende: um segundo subsistema (32, 34, 36), que compreende um segundo nível mídia (32), um segundo nível (34) de comunicação e um segundo nível (36) de controle tais como o micronúcleo (38) e o controlador de IPC (25) gere também comunicações entre os recursos do servidor atribuídos a esse segundo subsistema (22, 24, 26); e uma memória (29) partilhada em leitura e escrita, estabelecida sob controle do primeiro subsistema (22, 24, 26) e o nível de controle do segundo subsistema (22, 24, 26).

Relatório Descritivo da Patente de Invenção para **"SERVIDOR DE PORTA DE LIGAÇÃO COM MICRONÚCLEO E PROCESSO DE CONTROLE DESTESERVIDOR"**.

[0001] A presente invenção refere-se a um servidor de porta de ligação munido de um micronúcleo. Ela se refere também a um processo de transmissão de dados entre redes via um tal servidor de porta de ligação.

[0002] Os sistemas de exploração clássicos, tais como Microsoft Windows ou GNU/Linux, não foram projetados com grandes restrições de segurança. O resultado é uma concepção pouco segura sob a forma de um sistema de exploração que utiliza camadas operativas que podem ser representadas de acordo com diversos modelos, tal como o modelo OSI, do inglês "Open Systems Interconnection".

[0003] No âmbito de um servidor de porta de ligação 17 (figura 1), também denominado mandatário ou "proxy" em inglês, essa representação pode ser simplesmente efetuada em três níveis:

- um primeiro nível 16 de controle compreende um núcleo que gera as operações efetuadas pelas aplicações do sistema de exploração, notadamente atribuindo para isso recursos a esses aplicativos e controlando as comunicações entre esses recursos. O núcleo é tipicamente um núcleo monolítico, mesmo se uma abordagem modular pode ser escolhida para gerir especialmente cada recurso oferecido pelo sistema de exploração.

[0004] Um tal núcleo monolítico inclui softwares de baixo nível, tais como o planejador, o gestor de processos, o gestor de memória, assim como os programas de controle dos periféricos e alguns serviços de alto nível tais como os sistemas de arquivo e dos algoritmos criptográficos ou de filtragem.

- Um segundo nível 14 de comunicação compreende os aplicativos de software, notadamente que forma as pilhas de protocolo

exigidas para emitir ou receber dados via uma rede de telecomunicação que utiliza um protocolo de comunicação.

[0006] Em uma pilha de protocolos, cada camada resolve um certo número de problemas relativos à transmissão de dados, e fornece serviços bem- definidos às camadas superiores do primeiro nível 16. Essas camadas altas estão mais próximas do utilizador e geram dados mais abstratos, utilizando para isso os serviços das camadas baixas que conformam esses dados a fim de que eles possam ser emitidos em um meio físico.

[0007] - Um terceiro nível 12 média que efetua a interface do servidor 17 com uma rede exterior 10 ou 11. Esse nível 12 é tipicamente conforme ao protocolo Ethernet implementando uma camada física e uma subcamada lógica, a saber a camada Media Access Control (MAC) do modelo OSI.

[0008] Uma tal porta de ligação 17 pode ter uma função de filtragem destinada a assegurar a transmissão de dados 13 recebidos, por exemplo, de uma rede não segura 10 tal como a rede Internet com destino a uma rede sensível 11. Nesse caso, esses dados 13 são tratados:

[0009] - Pelo nível 12 Ethernet do servidor de porta de ligação 17 a fim de permitir o tratamento dos mesmos no servidor, e depois

[00010] - Pelo nível 14 de comunicação que compreende uma pilha de protocolos TCP/IP, para "Transmission Control Protocol" e "Internet Protocol" em inglês, a fim de gerar dados, transmitidos de acordo com protocolos de transporte, conforme a protocolos aplicativos, e depois finalmente

[00011] - Pelo nível 16 de controle que emprega serviços de filtragem de alto nível que permitem, por exemplo, decodificar os dados antes da transmissão dos mesmos à rede sensível 11.

[00012] A presente invenção resulta da constatação que um tal ser-

vidor, e o processo exigido para sua utilização, apresentam inconvenientes. Notadamente, eles apresentam fraquezas próprias à complexidade de um núcleo monolítico e à arquitetura de um sistema informático que não permite uma verificação formal da vulnerabilidade de um servidor de porta de ligação.

[00013] Mais precisamente, nenhum mecanismo permite provar que os dados que vêm de 10 passam sucessivamente por todas as etapas da filtragem realizadas pelos níveis 12, 14 e 16. Assim, uma disfunção 15, voluntária ou acidental, pode se produzir em um desses níveis 12 ou 14 e chegar a um contornamento do nível 16 de controle.

[00014] É então possível ter acesso à rede 11 independentemente das regras de transmissão que devem ser aplicadas pelo nível 16 de controle, o que representa uma falha do servidor 17 dificilmente aceitável.

[00015] Para responder a esse problema, a presente invenção se refere a um servidor de porta de ligação munido de um primeiro subsistema que compreende um nível média, um nível de comunicação e um nível de controle, esse servidor compreendendo também um micronúcleo e um controlador de IPC que gere comunicações entre os recursos do servidor atribuídos ao primeiro subsistema, caracterizado pelo fato de que ele compreende:

- um segundo subsistema, que compreende um segundo nível média, um segundo nível de comunicação e um segundo nível de controle tais como o micronúcleo e o controlador de IPC gere também comunicações entre os recursos do servidor atribuídos a esse segundo subsistema, e

- uma memória partilhada em leitura e escrita, estabelecida sob controle do micronúcleo e do controlador de IPC, entre o nível de controle do primeiro subsistema e o nível de controle do segundo subsistema.

[00016] Um tal servidor de porta de ligação responde ao problema da ausência das funções de controle de transmissões devidas a disfunções provocadas ou acidentais, do nível média e/ou do nível comunicação de um servidor de porta de ligação.

[00017] De fato, uma tal disfunção não pode chegar à transmissão de dados entre redes em um servidor de acordo com a invenção, somente o nível de controle podendo transmitir dados entre essas redes via a memória partilhada.

[00018] Um tal servidor apresenta portanto numerosas vantagens. Por um lado, ele permite responder a um defeito de regras de segurança claramente estabelecidas na rede sensível visto que essas regras podem ser implementadas por seu nível de controle.

[00019] Ele permite também prevenir um ataque que emana de uma rede não sensível e que visa contornar o nível de segurança de um servidor de porta de ligação por contornamento de seu nível de controle.

[00020] Um servidor de acordo com a invenção permite assim proteger uma rede sensível de agressões externas, voluntárias ou não. Desse modo ele permite assegurar uma política de segurança entre redes de sensibilidades diferentes, por exemplo, entre uma rede não segura e uma rede sensível.

[00021] Em uma realização, cada subsistema compreende meios para codificar informações, recebidas em uma solicitação de acordo com um protocolo de comunicação rede, em uma estrutura binária de acordo com um protocolo de comunicação entre os níveis de controle do primeiro subsistema e do segundo subsistema.

[00022] Nesse caso, cada subsistema pode compreender meios para codificar as informações em uma estrutura binária depois de tratamento dessas últimas no nível de comunicação e depois no nível de controle desse subsistema.

[00023] De acordo com uma realização, o servidor compreende meios para identificar, em função da natureza da solicitação, dados característicos da solicitação que devem ser codificados na estrutura binária.

[00024] Em uma realização, o servidor compreende meios para associar a solicitação recebida a uma solicitação predefinida em uma lista limitada de solicitações autorizadas.

[00025] De acordo com uma realização, o micronúcleo compreende meios para associar cada aplicação executada por um subsistema ao controle de um recurso do servidor.

[00026] Em uma realização, o servidor compreende meios para limitar as comunicações de tal modo que nem o nível média nem o nível de comunicação de um subsistema possa se comunicar diretamente nem com o nível média nem com o nível de comunicação do outro subsistema sem o intermediário dos níveis de controle dos subsistemas.

[00027] De acordo com uma realização, o servidor compreende meios para analisar a sintaxe e a validade dos protocolos filtrados por cada camada utilizada no servidor.

[00028] A invenção também se refere a um processo de controle de um servidor de porta de ligação munido de um primeiro subsistema que compreende um nível média, um nível de comunicação e um nível de controle, esse servidor compreendendo também um micronúcleo e um controlador de IPC que gere comunicações entre os recursos do servidor atribuídos ao primeiro subsistema, caracterizado pelo fato de que, o servidor sendo também munido de um segundo subsistema, que compreende um segundo nível média, um segundo nível de comunicação e um segundo nível de controle tais como o micronúcleo e o controlador de IPC gere também comunicações entre os recursos do servidor atribuídos a esse segundo subsistema, é utilizada uma memória partilhada em leitura e em escrita, estabelecida sob controle do mi-

cronúcleo, para transmitir solicitações entre o nível de controle do primeiro subsistema e o nível de controle do segundo subsistema com o auxílio de um servidor de acordo com uma das realizações precedentes.

[00029] Finalmente, a invenção também se refere a um produto programa de computador que compreende instruções de código de programa registradas em um suporte legível por um computador para executar um processo de acordo com a invenção quando o dito programa funciona em um computador.

[00030] A invenção será melhor compreendida com a leitura da descrição que se segue, dada unicamente a título ilustrativo e não limitativo, e feita em referência aos desenhos em anexo nos quais:

- a figura 1, agora descrita, é uma vista esquemática do funcionamento de um servidor de porta de ligação de acordo com a técnica anterior;

- a figura 2 é uma vista esquemática do funcionamento de um servidor de porta de ligação de acordo com a invenção, e

- a figura 3 representa o tratamento de uma solicitação HTTP por um servidor de acordo com a invenção.

[00031] Com referência à figura 2, um servidor de porta de ligação 27 de acordo com a invenção compreende dois níveis média 22 e 32, dois níveis de comunicação 24 e 34 e dois níveis de controle 26 e 36.

[00032] No entanto, um único micronúcleo 38 é empregado para efetuar algumas funções de base entre as quais a gestão das comunicações entre os recursos do servidor, notadamente por transferência de mensagem IPC para "Inter Process Communication" em inglês.

[00033] Além dessa gestão, um micronúcleo de segunda geração compreende um programa de controle de relógio e um planejador de tal modo que um tal micronúcleo compreende menos de 20 000 linhas de código.

[00034] Comparativamente, um núcleo monolítico compreende milhões de linhas de código com um risco proporcional de ok bugs (erros) e de defeitos de segurança. Ele pode dificilmente ser verificado como de acordo com as especificações dos verificadores de códigos e dos sistemas de prova formal atuais.

[00035] Além disso, os núcleos monolíticos têm más propriedades de isolamento. De fato, os processos utilizador podem quebrar o isolamento de diferentes modos graças aos tubos, aos arquivos, à memória partilhada, etc. A gestão das comunicações interprocessos não é confiável.

[00036] De fato, como precedentemente indicado, não existe isolamento, na parte de dentro de um núcleo monolítico, entre subsistemas do núcleo como por exemplo entre os programas de controle e as pilhas rede. Assim, um programa de controle de um componente material errado ou corrompido pode colocar em perigo todo o sistema.

[00037] A utilização de micronúcleos ditos de segunda geração resolve o problema ligado a uma falha dentro do nível de controle. Esses micronúcleos têm um tamanho que permite mantê-los facilmente e verificá-los formalmente a fim, por exemplo, de certificá-los a um nível elevado tal como o nível 7 do padrão internacional EAL para "Evaluation Assurance Level" em inglês.

[00038] A título de exemplo, os micronúcleos de segunda geração mais conhecidos, e atualmente utilizados em diferentes variantes, se apoiam em uma aplicação de programação, ou API para "Application Programming Interface" em inglês comum – L4 projetada sob o impulso de Jochen Liedtke.

[00039] Assim, um servidor de porta de ligação munido de um tal micronúcleo permite responder à complexidade, e vulnerabilidade, dos núcleos monolíticos. Em termos de segurança, um tal sistema se beneficia da solidez do micronúcleo.

[00040] No entanto, a segurança dos servidores depende também da solidez das comunicações IPC pois essas últimas representam um meio possível de transmissão de dados perigosos. Ora, por razões de eficácia, a gestão da segurança das comunicações é tradicionalmente deixada ao nível dos servidores, o micronúcleo se contentando de transmitir as mensagens.

[00041] É por essa razão que, nessa realização, o micronúcleo 38 compreende um controlador 25 IPC que oferece um mecanismo de direitos de comunicação de tal modo que duas aplicações só podem se comunicar entre si se o controlador 25 reconhece que essas aplicações possuem os direitos apropriados.

[00042] De fato, o micronúcleo considera cada aplicação, por exemplo de serviços ou de programas de controle, como o sujeito dos critérios de segurança que lhe são fornecidos previamente.

[00043] A partir desses critérios, o micronúcleo 38 pode atribuir recursos do sistema às aplicativos que ele gere de acordo com uma regra estabelecida em sua partida enquanto que seu controlador de IPC 25 atribui ou recusa direitos de comunicação entre essas aplicações.

[00044] Em outros termos, o micronúcleo 38 identifica, por um lado, recursos a atribuir – tais como a memória, as entradas e saídas, privilégios para níveis de gestão de – e por outro lado comunicações em espera de autorização do controlador de IPC 25.

[00045] Assim, quando uma aplicação exige uma comunicação IPC entre diferentes elementos, o controlador de IPC 25 determina a partir dessa lista se a aplicação solicitante tem um direito de comunicação com a aplicação destinatária.

[00046] O controlador de IPC 25 efetua portanto a função de controlador IPC para, por exemplo, fornecer direitos de comunicação a aplicações especiais sob demanda. Do mesmo modo, esse controlador IPC pode detectar tentativas de violação dos critérios de segurança e

fornecer uma auditoria sobre o potencial de violação.

[00047] Nessa realização, o micronúcleo 38 tem também como função manter para cada aplicação as comunicações previamente autorizadas.

[00048] Uma tal estrutura permite um controle preciso sobre a utilização dos recursos enquanto que, simultaneamente, cada aplicação é associada ao controle de um recurso, quer dizer de um componente ou mecanismo hardware, o que reforça o controle para bloquear a propagação de um ataque ou de um bug(erro).

[00049] No servidor 27, o tratamento dos dados utiliza portanto dois subsistemas, a saber:

- por um lado um subsistema formado pelo nível 22 mídia, pelo nível 24 de comunicação e pelo nível 26 de controle, ligado à rede 20 não seguram por exemplo a rede Internet, e

- por outro lado um subsistema seguro formado pelo nível 32 mídia, pelo nível 34 de comunicação e pelo nível 36 de controle, ligado à rede 21 sensível, por exemplo uma rede aviônica, um intranet de defesa e/ou um nó central de comunicação.

[00050] De fato, cada subsistema gera um fluxo de dados, por exemplo ao nível de sua interface rede ou de sua pilha de protocolos, utilizando para isso seus próprios recursos físicos que são isolados do outro subsistema, exceto entre o nível de controle dos mesmos como descrito ulteriormente.

[00051] Assim, o micronúcleo 38 e seu controlador de IPC 25 só autorizam comunicações do nível 22, respectivamente 32, mídia com o nível 24, respectivamente 34, esse último nível só podendo se comunicar como nível de controle 26, respectivamente 36.

[00052] Assim, supondo-se que um ataque ou um bug(erro) proveniente da rede 20 consiga se infiltrar através de uma falha em uma das camadas do nível 22 mídia e/ou do nível 24 de comunicação, por

exemplo na aplicação de um programa de controle e/ou da pilha de protocolos, dados não podem ser transmitidos para a rede sensível 21 sem seu tratamento pelo nível 26 e 36 de controle.

[00053] Por outro lado, a arquitetura do servidor permite efetuar uma filtragem em profundidade da rede, essa filtragem utilizando uma análise da sintaxe e da validade dos protocolos filtrados por cada camada do servidor, por exemplo: Ethernet, IP, TCP, nível aplicação.

[00054] Devido a isso, uma solicitação recebida pelo subsistema não seguro é transformada, por ocasião de seu tratamento progressivo pelo nível de comunicação 24 e depois pelo nível de controle 26, de uma solicitação em uma simples estrutura binária claramente definida.

[00055] Uma tal transformação é representada na figura 3 que ilustra a decomposição de uma solicitação protocolar HTTP em dados binários que codificam as informações transmitidas por essa instrução HTTP.

[00056] Mais precisamente, esses dados compreendem uma instrução "Get", um endereço URL, a versão do protocolo HTTP utilizado e os formatos de arquivo levados em consideração por um software de exploração ou software de navegação.

[00057] Esses dados binários, representados sob a forma de uma tabela por preocupação com a clareza, são em seguida transmitidos ao nível 36 de controle do subsistema seguro por intermédio de uma memória partilhada 29 entre os dois subsistemas.

[00058] Para isso, um protocolo limitativamente definido é utilizado. Um tal protocolo defini o conjunto das solicitações que podem ser emitidas pelo nível 26 de controle da rede não segura, de tal modo que os campos de dados exigidos para essas solicitações podem, por um lado, ser predeterminados e, por outro lado, ser preenchidos por dados binários que codificam as informações identificadas na solicitação recebida.

[00059] Assim, as solicitações transmitidas pela rede 20 não segura via o servidor de porta de ligação 27 são tratadas pelo subsistema não seguro para extrair dessas últimas dados característicos das solicitações, esses dados característicos sendo transmitidos ao subsistema seguro via o nível de controle 26 desse subsistema não seguro.

[00060] Na sequência, o subsistema seguro reescreve a solicitação de acordo com seu nível 34 de comunicação, por exemplo de acordo com um protocolo HTTP, com base nos dados característicos previamente extraídos. Na sequência, essa solicitação é transmitida via o nível 32 de comunicação ao servidor destinatário que pode então ser validamente e seguramente forçado.

[00061] Uma tal conformação dos dados é representada na figura 3 a partir dos dados binários precedentemente obtidos a partir de uma solicitação HTTP.

[00062] Em retorno, a resposta do servidor destinatário é recebida pelo nível média 32, e depois 34 de comunicação a fim de chegar ao nível 36 de controle.

[00063] Esse nível 36 de controle pode então transmitir os dados binários, obtidos a partir da resposta, através da memória partilhada 29 a fim de que essa última os transmita ao requerente via os níveis 26, 24 e depois 22 do subsistema não seguro.

[00064] É evidente que um servido de porta de ligação de acordo com a invenção não visa bloquear bugs(erros) e/ou ataques mas sim limitar suas consequências sobre a rede sensível visto que o conjunto das solicitações emitidas na rede sensível por esse servidor são solicitações validadas por sua reescrita, essas solicitações validadas não correspondendo exatamente à solicitação inicial. A segurança da porta de ligação é assim assegurada pela arquitetura do servidor.

[00065] Em resumo, cada subsistema age como uma comporta que só pode se comunicar com o outro subsistema por intermédio de uma

memória na qual são registrados dados binários que codificam as informações identificadas em uma solicitação recebida na entrada de um dos subsistemas em campos predefinidos.

[00066] Desse modo, os subsistemas só se comunicam por intermédio de seu nível de controle, especialmente confiável pela presença de um micronúcleo, e com o auxílio de dados dos quais o alcance está limitado ao campo definido.

[00067] A presente invenção é suscetível de numerosas variante. Notadamente, a descrição efetuada abaixo da invenção apresenta um micronúcleo 38 que compreende o controlador IPC 25 mas, em função das variantes e dos critérios utilizados para definir um micronúcleo, esse controlador 25 IPC pode estar localizado fora do micronúcleo 38.

REIVINDICAÇÕES

1. Servidor de porta de ligação (27) caracterizado por compreender:

- um primeiro subsistema que compreende um nível mídia (22), um nível de comunicação (24) e um nível de controle (26),
- um segundo subsistema (32, 34, 36), que compreende um segundo nível mídia (32), um segundo nível de comunicação (34) e um segundo nível de controle (36)
- um micronúcleo (38) e um controlador de IPC (25) configurados para gerenciar comunicações entre os recursos do servidor atribuídos ao primeiro subsistema (22, 24, 26), por um lado, e também para gerenciar as comunicações entre os recursos do servidor atribuídos ao segundo subsistema (32, 34, 36), por outro lado, e
- uma memória (29) compartilhada em leitura e escrita, estabelecida sob controle do micronúcleo (38) e do controlador de IPC (25), entre o nível de controle do primeiro subsistema (22, 24, 26) e o nível de controle do segundo subsistema (32, 34, 36).

2. Servidor de acordo com a reivindicação 1, caracterizado pelo fato de que cada subsistema (22, 24, 26; 32, 34, 36) compreende meios para codificar as informações, recebidas em uma solicitação de acordo com um protocolo de comunicação de rede, em uma estrutura binária de acordo com um protocolo de comunicação entre os níveis de controle do primeiro subsistema (26) e do segundo subsistema (36).

3. Servidor de acordo com a reivindicação 2, caracterizado pelo fato de que cada subsistema (22, 24, 26; 32, 34, 36) compreende meios para codificar as informações em uma estrutura binária depois de tratamento dessas últimas no nível de comunicação (24; 34) e depois no nível de controle (26; 36) desse subsistema.

4. Servidor de acordo com a reivindicação 2 ou 3, caracteri-

zado pelo fato de que ele compreende meios para identificar, em função da natureza da solicitação, dados característicos da solicitação que devem ser codificados na estrutura binária.

5. Servidor de acordo com a reivindicação 2, caracterizado pelo fato de que ele compreende meios para associar a solicitação recebida a uma solicitação predefinida em uma lista limitada de solicitações autorizadas.

6. Servidor de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que o micronúcleo (38) compreende meios para associar cada aplicação executada por um subsistema (22, 24, 26; 32, 34, 36) ao controle de um recurso do servidor.

7. Servidor de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que ele compreende meios para limitar as comunicações de tal modo que nem o nível mídia (22) nem o nível de comunicação (24) de um subsistema possa se comunicar diretamente nem com o nível mídia (32) nem com o nível de comunicação (34) do outro subsistema sem o intermediário dos níveis de controle (26, 36) dos subsistemas.

8. Servidor de acordo com qualquer uma das reivindicações 1 a 7, caracterizado pelo fato de que ele compreende meios para analisar a sintaxe e a validade dos protocolos filtrados por cada camada utilizada no servidor.

9. Processo de controle de um servidor de porta de ligação caracterizado por compreender um primeiro subsistema que compreende um nível mídia (22), um nível de comunicação (24) e um nível de controle (26), assim como um segundo subsistema (32, 34, 36), que compreende um segundo nível mídia (32), um segundo nível de comunicação (34) e um segundo nível de controle (36), o servidor (27) também compreendendo um micronúcleo (38) e um controlador de IPC (25) gerenciando comunicações entre os recursos do servidor

atribuídos ao primeiro subsistema por um lado, e também gerenciando comunicações entre os recursos de servidor atribuídos ao segundo subsistema (32, 34, 36), por outro lado, no qual o processo de memória (29) partilhada em leitura e escrita é usado, estabelecido sob controle do micronúcleo e do controlador de IPC, para transmitir solicitações entre o nível de controle do primeiro subsistema (22, 24, 26) e o nível de controle do segundo subsistema (32, 34, 36) usando os meios do servidor como definido em qualquer uma das reivindicações 1 a 8.

1/2

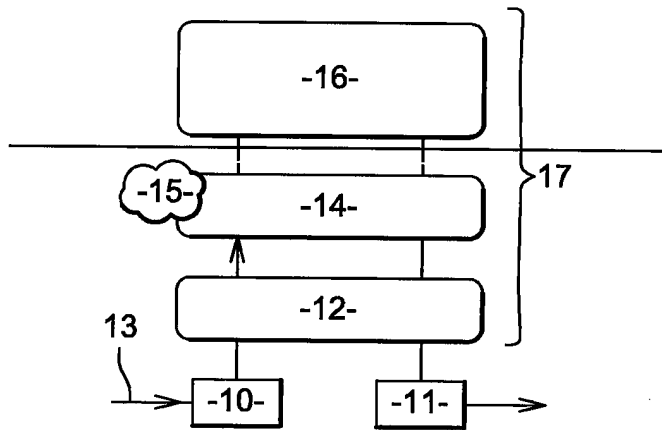


Fig. 1

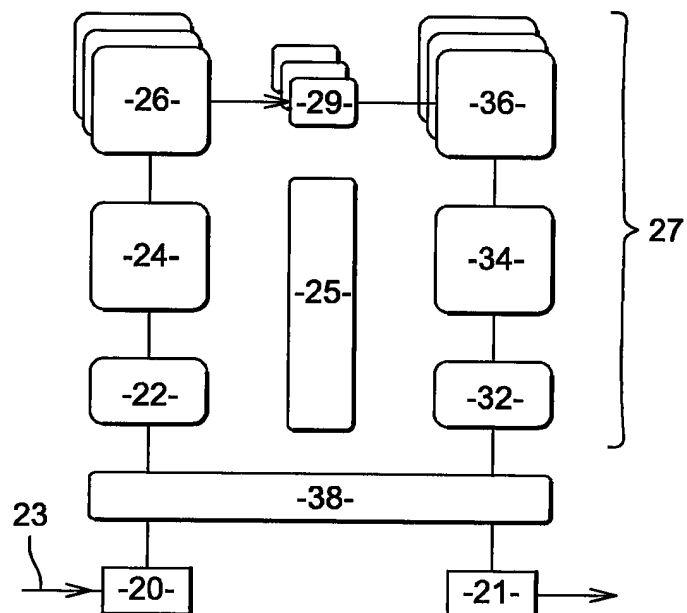
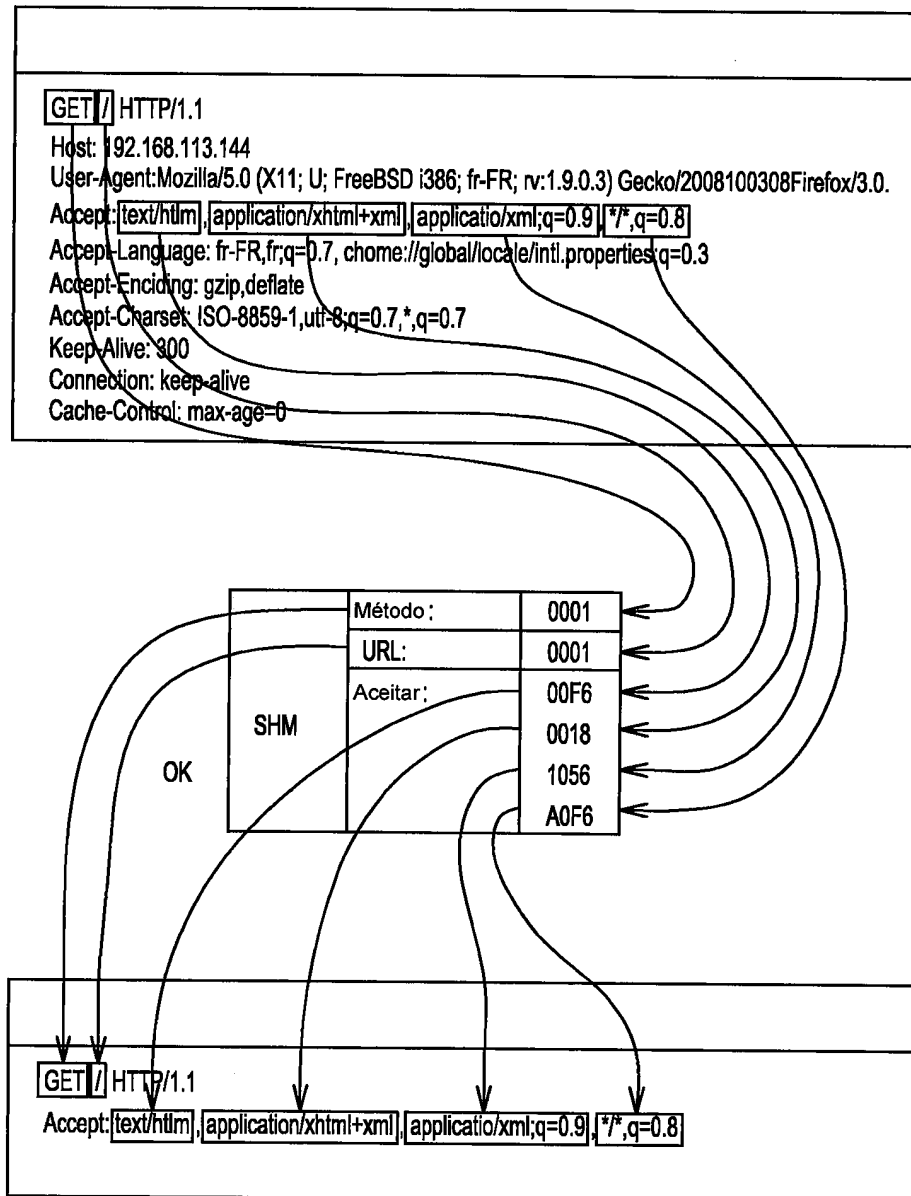


Fig. 2

**Fig. 3**