Firewall

Luiz Arthur

As redes de computadores tal como a **Internet**, trazem a sociedade uma grande **evolução** pois tais redes conseguem tornar o mundo mais globalizado através, por exemplo, da disseminação de informações de forma rápida e eficiente. Ou seja, através da Internet podemos ter acesso a informações disponíveis em milhões de hosts da Internet.

Porém, as redes de computadores além dos benefícios trazem grandes problemas, tal como o acesso indevido e não autorizado em sistemas de empresas ou mesmo micros pessoais, pois várias máquinas da Internet querem manter algumas informações confidências. O acesso indevido a hosts tornou-se uma prática muito mais fácil com o advento da Internet, pois assim como um host A tem acesso a milhões de hosts, estes mesmos hosts da Internet podem acessar este host A. **Então a grande maioria das redes precisam de mecanismos para evitar tais acessos e tornar os sistemas mais seguros e confidenciais**. Para esta tarefa normalmente é utilizado um Firewall.

Firewalls são umas das ferramentas de seguranças mais utilizadas, normalmente o **firewall é a primeira linha de defesa de ataques externos, mas estes também podem impedir alguns tipos de ataques internos**.

Firewalls podem ser um misto de hardware e software colocados em pontos estratégicos da redes, principalmente em pontos de fusão intra-redes, e observar em um pacote de rede pode ou não trafegar de uma rede para outra, através de regras (políticas) pré-definidas.

A capacidade de **conectar um computador a vários outros através da Internet** é uma faca de dois gumes. **É muito divertido** para as pessoas navegarem pela Internet quando estão em casa. **Mas, para os gerentes de segurança das empresas, trata-se de um pesadelo**. Muitas empresas têm grandes quantidades de informações confidenciais on-line — segredos comerciais, planos de desenvolvimento de produtos, estratégias de marketing, análises financeiras etc. A revelação dessas informações para um concorrente poderia ter terríveis conseqüências.

Além do **perigo das informações virem a público**, também há o perigo do vazamento dessas informações dentro da empresa. Em particular, **vírus, vermes e outras pestes digitais podem burlar a segurança**, destruir dados valiosos e consumir muito tempo dos administradores, que tentam eliminar a confusão causada por eles.

Os firewalls são apenas uma adaptação moderna de uma antiga forma de segurança medieval: **cavar um fosso profundo em torno do castelo**. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas. Nas redes, é possível usar o mesmo artifício: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou de entrada da empresa é feito através de uma **ponte levadiça eletrônica** (firewall).

O tipo de Firewall mais tradicional é o de filtro de pacote, que analisa pacotes de redes e usando regras permite ou bloqueia pacotes em redes ou máquinas.

Mas os Firewalls atualmente agregam inúmeras outras funcionalidades, tal como a de tradução de endereços de redes com NAT (Network Address Translation, normalização de pacotes, filtragem por estados de conexão de rede, registros de pacotes (logs), dentro outras.

A palavra Firewall em sua tradução literal quer dizer parede de fogo, mas na verdade **o termo Firewall vem da construção civil e quer dizer parede corta-fogo ou anti-chamas**, no qual existe uma parede que é resistente ao fogo e permite em caso de incêndio que as pessoa possam fugir através de escadas que ficam guardadas pela parede anti-chamas que evita a propagação do calor e fumaça. É justamente assim que um Firewall trabalha, mantendo-se no meio de duas redes, e bloqueando o perigo (fogo) de uma rede (Internet por exemplo) de outra rede (uma rede privada, por exemplo).

Os Firewalls evoluirão muito desde a sua invenção, mas uma coisa é certa **um bom Firewall só é possível com uma boa configuração por parte de um ótimo administrador do Firewall**, administrador este que deve conhecer fundamentalmente com funciona uma rede e como os pacotes trafegam nesta rede. Caso contrário um Firewall nunca fará sua função de forma consistente.

Cada Firewall filtro de pacotes normalmente é um roteador padrão equipado com algumas funções complementares, que permitem a inspeção de cada pacote de entrada ou de saída. Os pacotes que atenderem a algum critério serão remetidos normalmente, mas os que falharem no teste serão descartados.

Em geral, **os filtros de pacotes são baseados em tabelas de regras** configuradas pelo administrador do sistema. Essas tabelas listam as origens e os destinos aceitáveis, as origens ou destinos bloqueados e as regras padrão que orientam o que deve ser feito com os pacotes recebidos de outras máquinas ou destinados a elas.

No caso comum de uma configuração TCP/IP, uma origem ou destino consiste em uma porta e um endereço IP.

As portas indicam qual é o serviço desejado. Por exemplo, a porta 23 do TCP é para telnet, a porta 79 é para finger e a porta 119 é para notícias da USENET. Uma empresa poderia bloquear os pacotes recebidos em relação a todos os endereços IP combinados com uma dessas portas. Dessa forma, ninguém fora da empresa poderia estabelecer login via telnet ou procurar alguém usando o daemon Finger.

O **bloqueio de pacotes de saída é mais complicado** porque, embora **muitos sites adotem as convenções padrão para numeração de portas, eles não são obrigados a fazê-lo**.

Além disso, para **alguns serviços** importantes, como FTP (File Transfer Protocol), **os números de portas são atribuídos dinamicamente**.

Outro, é que embora o bloqueio das conexões TCP seja difícil, **o bloqueio de pacotes UDP é ainda mais complicado**, **porque se sabe muito pouco** (a priori) **sobre o que eles farão**. Muitos filtros de pacotes simplesmente não aceitam tráfego UDP.

A segunda metade do mecanismo de firewall é o gateway de aplicação (que pode ser feito pelo Firewall ou por Proxy's). **Que em vez de apenas examinar pacotes brutos, o gateway opera na camada de aplicação.**

Por exemplo, um gateway pedido de página HTTP pode ser configurado de forma a examinar cada mensagem recebida ou enviada. O gateway toma a decisão de transmitir ou descartar cada página, com base nos campos da página HTTP, no tamanho da mensagem ou até mesmo em seu conteúdo (por exemplo, a presença de palavras impróprias como "sexo" ou "playboy" pode provocar algum tipo de ação especial).

O que um Firewall não protege

A primeira coisa que qualquer pessoa tem que ter em mente é que um Firewall não é uma caixa mágica que deixa uma rede 100% segura, na verdade nenhum software ou hardware de segurança faz isto, já que não existe um sistema 100% seguro.

Um Firewall pode controlar conexões de rede, mas não pode prevenir, por exemplo, que alguém pegue documentos de um servidor de páginas (HTTP), se você liberar tal acesso no firewall. Um Firewall também dificilmente impedirá que um usuário de sua rede privada **acesse um site com vírus** ou **receba um e-mail com vírus** e este infecte a máquina deste usuário (já que muitos Firewalls não fará filtros quanto aos dados trafegados em pacotes de redes).

Implementando Firewalls

Existem inúmeras formas de se implementar Firewalls e **cada ambiente** a ser protegido por Firewall **pode ter um requisito diferente**, depender de políticas de segurança, estrutura da rede, softwares usados, culturas do ambiente e recursos financeiros. Então **antes de iniciar a implementação de um Firewall faz se necessário definir o que deve ser protegido, o que é prioritário e o que não é**. Caso esta analise do ambiente não seja feita o Firewall não terá muito sentido e dificilmente conseguirá atingir o seu objetivo (manter a rede segura).

Definindo a Política de Filtragem de Pacotes

Como já foi dito qualquer Firewall de rede a principio é um sistema de filtro de pacotes, este tipo de Firewall trabalha com o conceito de política (**policy**), uma política basicamente **diz ao Firewall qual é a forma padrão de se tratar o tráfego da rede**. Existem duas políticas básicas que são:

Política de permitir tudo o que não for negado por regras do Firewall: Nesta política qualquer pacote pode passar pelo Firewall, a menos que exista uma regra pré-definida que proíba a passagem deste pacote. Ou seja, quando um pacote de rede chega ao Firewall este vai procurar por uma regra impedindo a passagem deste pelo Firewall, caso esta regra não exista o pacote irá passar por padrão pelo Firewall. Este tipo de política **geralmente é a política padrão** na grande maioria dos Firewalls, mas é uma política muito **flexível e permissiva** o que a torna incerta e possivelmente insegura;

Política negar tudo o que não for permitido via regras do Firewall: Nesta política nenhum pacote pode passar pelo Firewall, exceto se existir regras que permitam sua passagem. Ou seja, aqui tudo está proibido a menos que o administrador do Firewall cria regras dizendo o contrário e liberando um ou outro acesso. Está regra normalmente é tida como muito segura porém não é flexível.

Com a política de negar tudo, consegue-se na teoria mais segurança que na política de liberar tudo, já que tudo que for esquecido está negado por padrão, porém este tipo de política de Firewall é mais complexa de se construir e manter, pois é menos flexível e amigável, principalmente para administradores que não compreendem como funcionam a transmissão de dados em uma rede (ida-e-volta) e o inter-relacionamentos de serviços de redes.

Podem ser implementadas outras políticas de Firewall, mas as duas apresentadas anteriormente são as duas mais comumente utilizadas.

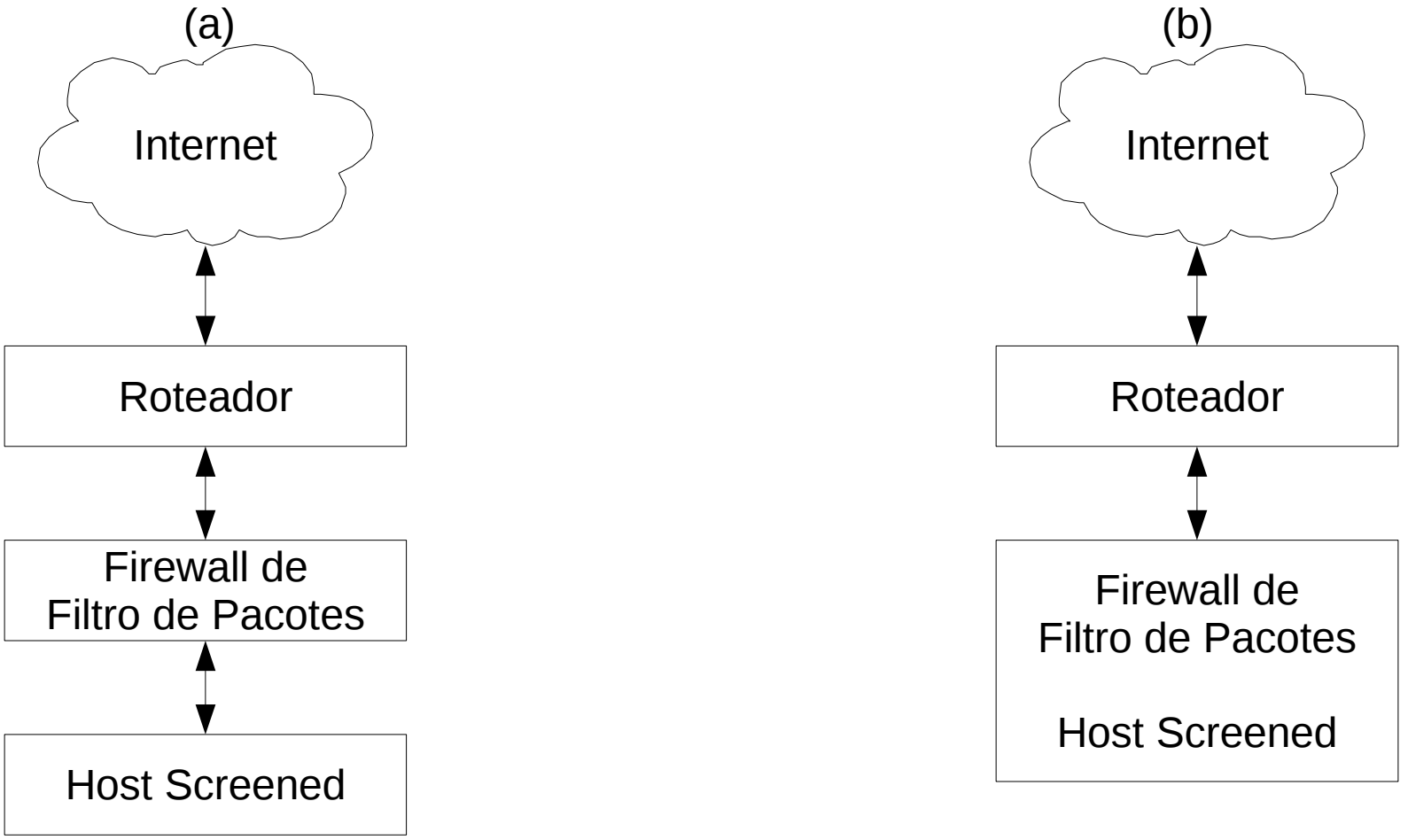
Projetos de Firewalls

Existem várias formas de se planejar o uso de Firewalls, isto depende do tamanho da rede e do nível de segurança que se deseja, é claro que também da quantia de dinheiro a ser investida. Alguns projetos de Firewall são:

Host Screened (host filtrado)

Um host screened é uma máquina que deve ser protegida de ataques externos. Sua Implementação é simples e segura já que este tipo de Firewall filtra pacotes destinados a ele como servidor, ou seja, este tipo de host só pode acessar serviços de servidores e nunca ser um servidor.

Um exemplo de implementação de Sreened Hosts:



No exemplo (a) o Firewall e o host a ser protegido estão em máquinas diferentes, mas o Firewall e o host a ser protegido podem ser os mesmos como mostra (b). Os hosts Sreened são geralmente PC's, notebooks, e geralmente é usado em casa ou em pequenos ambientes empresariais.

Os **hosts screened podem usar** tanto endereços **IP's públicos quanto privados**. Se o roteador estiver configurado como bridged o host irá receber um endereço válido da Internet, o que pode representar um grande problema de segurança, já que a máquina é acessada direta da Internet. Mas é possível usar IP's privados que podem ocultar tanto o Firewall quanto o host atrás do roteador aumentando a segurança (na teória), mas neste caso é necessário o uso de **NAT** o que pode deixar o tráfego de pacotes mais lento que o apenas roteado.

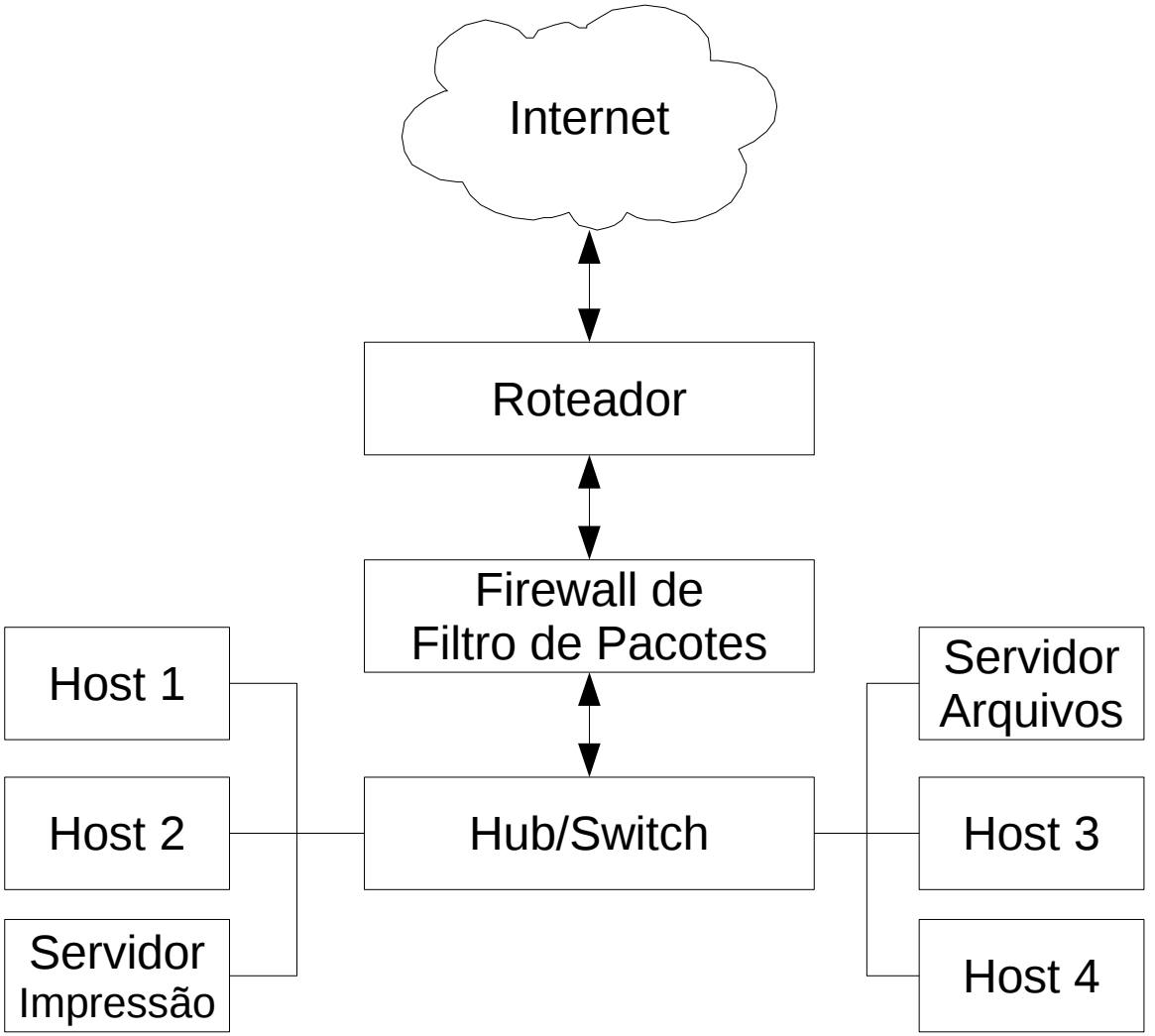
Em alguns casos mais específicos os hosts screened podem ter mais de uma interface de rede (**multi-homed**) o que exige um pouco mais de configuração principalmente se o Firewall não estiver na mesma máquina que o host a ser protegido.

LAN screened ou Segmento de LAN Screened

No Host screened nós protegemos apenas um computador, já no LAN screened (LAN ou segmento de LAN Filtrado) faz-se a proteção de uma rede (vários computadores) ou várias LAN's. Assim, LAN screened é similar ao Host screened mas este protege várias máquinas.

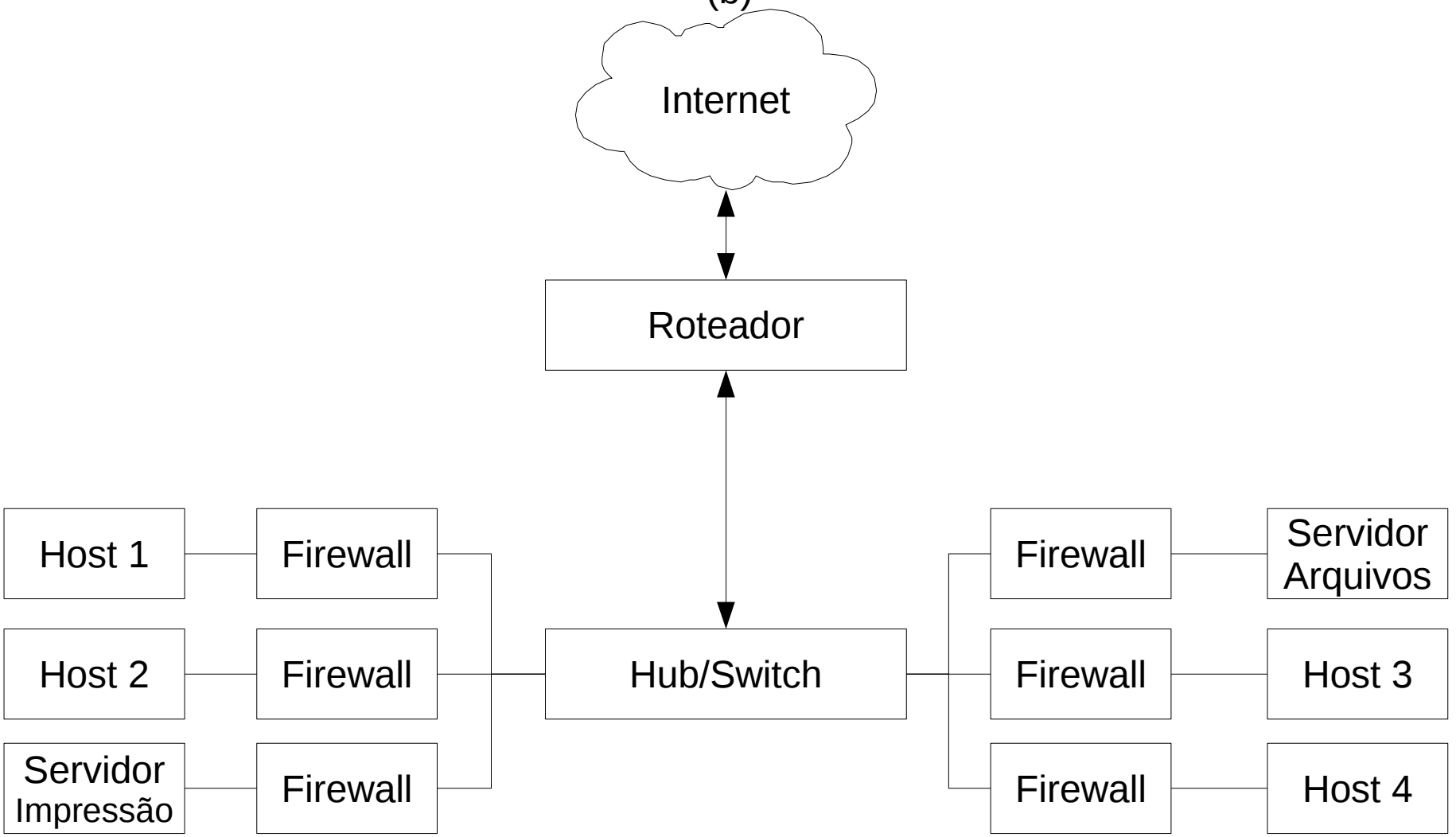
A política de pacotes assim como do Host screened continua sendo a de bloquear qualquer pacote que entra na LAN a menos que este seja uma resposta de um pedido interno da LAN (nenhuma máquina da rede pode ser um servidor).

Exemplos de LAN screened:



Neste exemplo, a grande vantagem é a segurança, pois cada host tem um Firewall próprio, é claro que a desvantagem é o custo, como sugestão ficaria montar um modelo hibrido onde somente os servidores teriam Firewall próprio e rede também teria um Firewall global como no exemplo anterior.

(b)



Host Bastion

O projeto do host bastion é parecido com o do host screened, a única diferença é na configuração do Firewall de filtro de pacotes e nos tipos de serviços que estão em execução no host, que são tipicamente aplicações de servidores, tal como: DNS, FTP, HTTP, SNMP, SSH, etc. Assim, **no host bastion é permitido a entrada de tráfego da Internet**, por exemplo, tentando acessar serviços permitidos pelo Firewall de filtro de pacotes. Ou seja, ao contrário do host screened que podia ser apenas cliente de uma rede, **o host bastion pode desenvolver o papel de servidor**, o que é claro torna este tipo de configuração menos segura, e é somente recomendada quando existe a necessidade ser servir algum serviço para terceiros.

Demilitarized Zone – DMZ (Zona desmilitarizada)

Este é um tipo de projeto usado para conectar uma LAN a Internet e expor alguns recursos para o mundo, tal LAN acomoda normalmente servidores HTTP, FTP ou outros serviços de rede. Este cenário geralmente acumula todo tipo de perigo que uma rede ou um Firewall pode sofrer, já que as máquinas ficam praticamente expostas na Internet. Mas **a DMZ isola os serviços que vão ser oferecidos na Internet da rede local (LAN) o que proporciona mais segurança a rede local**.

Uma DMZ simples normalmente tem três interfaces de redes, uma que conecta o Firewall a redes externar (Internet), outra conectando a LAN screened e a última do segmento DMZ.

O Firewall de Filtro de Pacotes pode ter implementadas as seguintes políticas:

•Hosts da LAN screened tem acesso as redes externas (Internet);

•Hosts da LAN screened tem acesso limitado aos hosts bastion na DMZ;

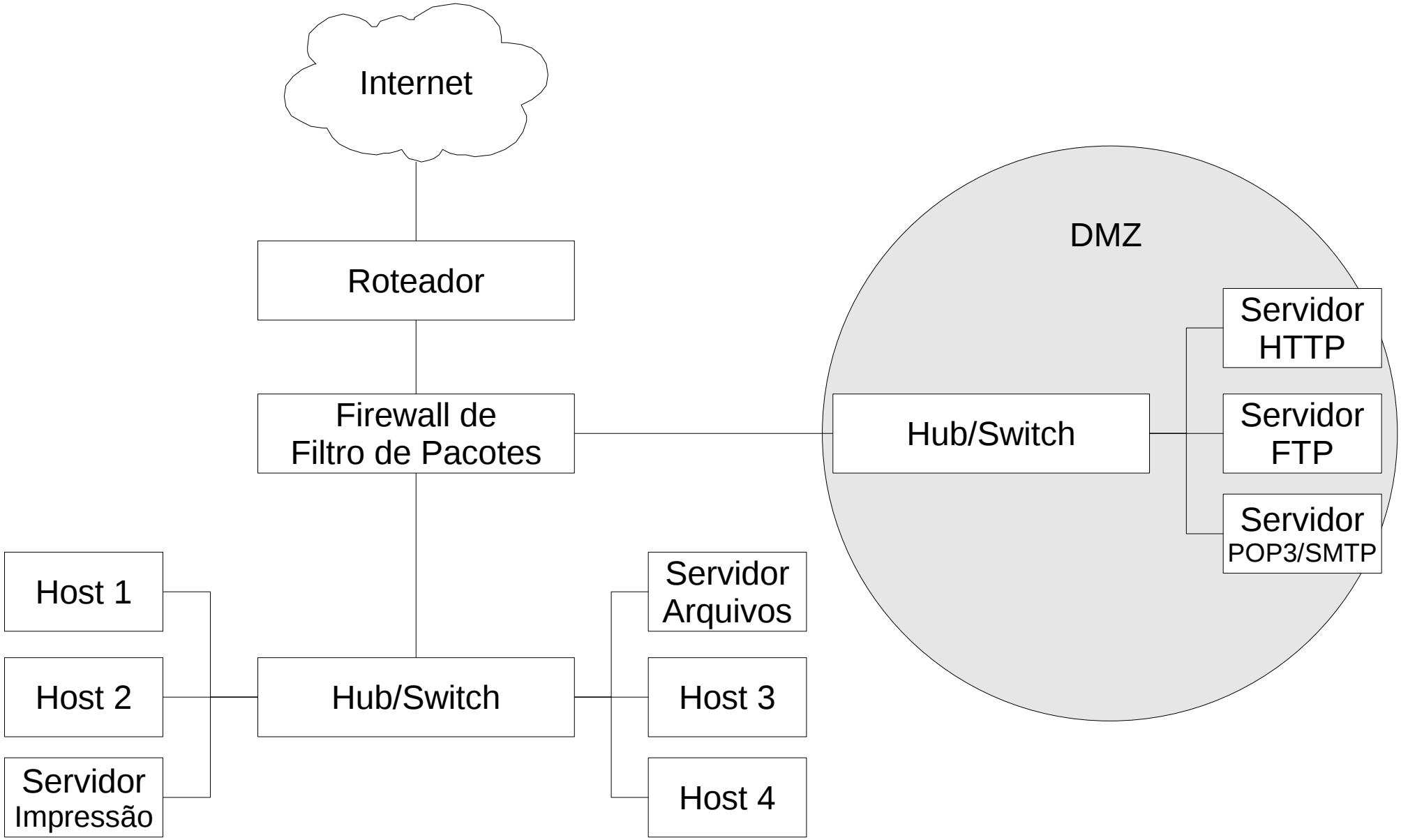
•Hosts externos tem acesso limitado aos hots bastion na DMZ;

•Hosts bastion da DMZ não tem acesso a LAN screened;

•Hosts Bastion na DMZ tem acesso limitado a redes externas (Internet);

•Hosts Externos não tem acesso a LAN screened.

Um esquema de DMZ:



Normalmente a LAN screened é formada por IP's privados e a DMZ pode ser formado por IP's privados ou válidos na Internet.

Embora a DMZ seja mais complexa e conseqüentemente mais cara, não é recomendado fazer economia colocando hosts bastian e hosts screened na mesma rede, esta economia é geralmente de curto prazo, mas é rapidamente consumida pelos problemas de segurança que este tipo de implementação vai trazer a informação que trafega nesta rede, por exemplo.

LANs de larga escala

LANs de larga escala são normalmente configuradas com uma mistura de todas as implementações de rede e Firewall vistas anteriormente. Cada LAN pode ser protegida por seu próprio Firewall local sendo que para agrupar todas as LANs pode existir um Firewall global. É claro que cada caso é um caso, e uma configuração de Firewall pode e deve ser diferente da outra dependendo dos requisitos do cenário e das informações.

Hosts e Firewalls invisíveis

Com o crescimento drástico da Internet os endereços IPv4 estão se esgotando, para resolver este problema surge o IPv6 que utiliza endereçamento de 128 bits o que acaba com o problema de faltas de IPs no planeta Terra.

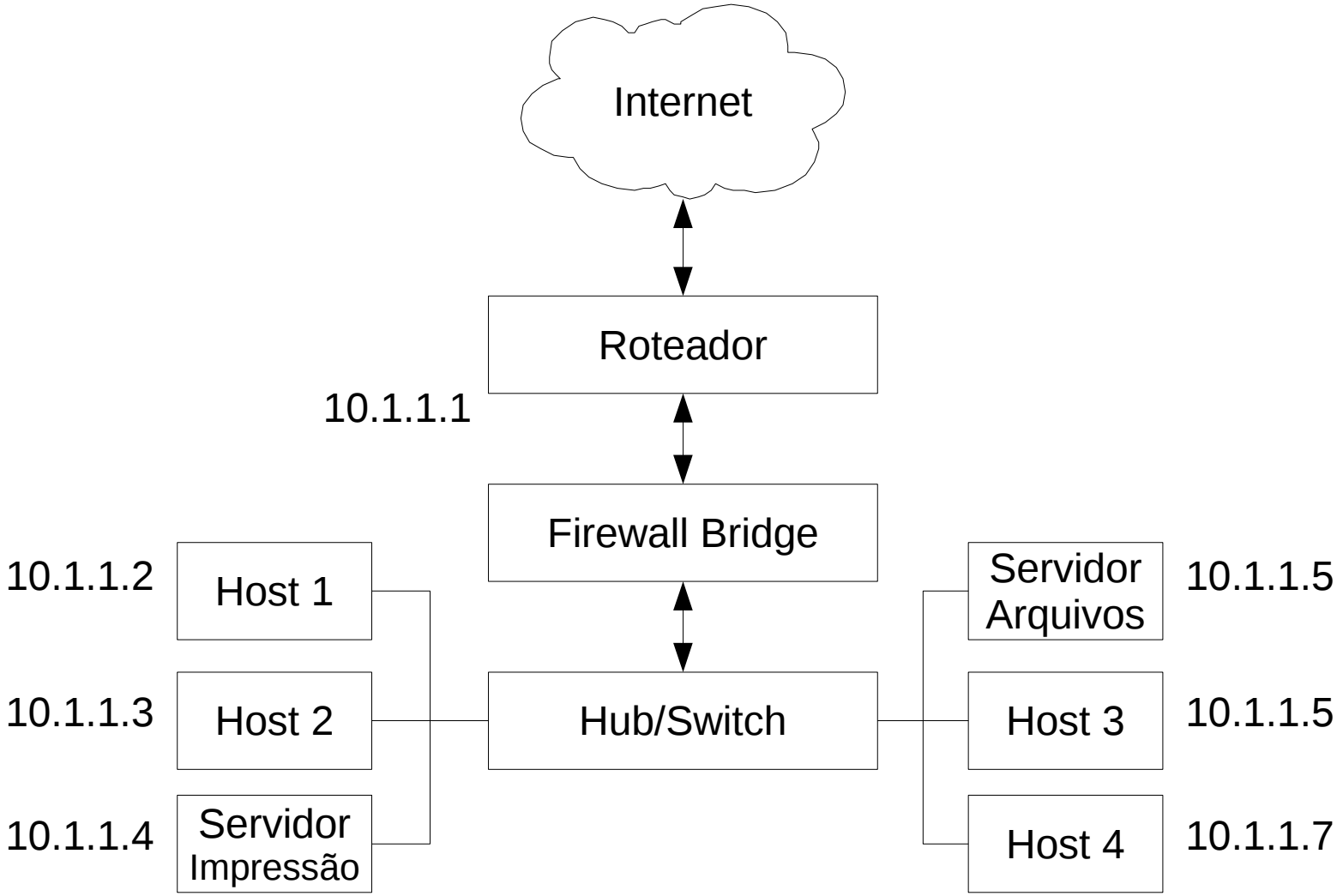
Então ficar dando IPs a Firewall pode ser um problema, quando os IPs e estão escaços e por conseqüência caros, mas **existem duas soluções**, fora IPv6 que diminuem os problemas com IPv4 e melhor aumentam (teoricamente) a segurança, são estas: **Filtragem Bridge e NAT**.

Filtragem Bridge

Uma bridge Ethernet é um dispositivo que conecta dois segmentos de redes. Está técnica é bem **parecida com o que faz um switch Ethernet**. Isto quer dizer que não é necessário separar os segmentos com redes IP's distintas, e sim pela **Camada de Enlace**. Assim, **o Firewall filtra o que passa de um segmento para outro e o melhor o firewall é invisível, já que não necessita ter um endereço IP**, o que diminui muito a chance de ser invadido.

É claro que ser invisível tem seus problemas em um Firewall, tal como: não ser possível gerenciar ou monitorar o Firewall remotamente já que este não tem um IP. É claro que é possível colocar uma placa de rede isolada só para isto, mas a segurança já diminui.

Um exemplo, de Firewall Bridge que fica entre o roteador e a rede:



NAT (Network Address Translation)

NAT é uma técnica que esconde vários hosts de uma LAN atrás de um único endereço IP válido na Internet, isto ajuda a conservar endereços válidos na Internet. Assim, **todas as máquinas de uma rede local chegam a Internet através de um mesmo IP**, o que esconde o layout da LAN, e para alguém da Internet acessar a LAN deverá existir o redirecionamento de porta para IP's/portas da LAN, caso isto não aconteça a única máquina a ser acessada da Internet é o roteador (normalmente o modem ADSL).

A grande maioria dos Firewalls implementam soluções de NAT, junto com o Firewall de filtro de pacotes, mas estão funções são distintas.

Então podemos concluir que o NAT fornece um nível maior de segurança pois torna invisíveis os hosts que estão atrás da máquina que faz NAT. Mas as máquinas atrás do NAT não podem ser acessadas diretamente, ao contrário de máquinas que tem IP's válidos na Internet, o que pode ser um problema em alguns casos.

Funcionalidades adicionais presentes em muitos Firewalls

Embora os Firewalls sejam basicamente filtro de pacotes de redes, estes adquiriram ao longo do tempo várias outras funcionalidades, como já foi visto NAT.

Assim alguns Firewalls podem vir a assumir as seguintes funções:

• **Proxy** – Muitos Firewalls fazer o serviço de proxy e podem fazer pedidos de conexão em nomes de outros hosts;

• **Gerador de logs** – Em termos de segurança, quanto mais informações sobre sua rede e Firewall melhor. Então a grande maioria dos Firewalls possuem mecanismos de log, que registram desde um pacote passando pela rede, até atividades anormais, é claro que tudo configurável (o administrador escolhe o que vai registrar ou não);

• **Balanceamento de carga, Qualidade de Serviço (QoS) e Tolerância a Falhas**: Alguns Firewalls conseguem priorizar serviços de redes, fazer balanceamento de carga de dados serviços de redes, ou mesmo tomar alguma atitude em caso de falhas de serviços de redes;

• **IDS**: Alguns Firewalls possuem capacidade de interagir com Sistemas de Dectecção de Intrusão de redes ou de hosts.

A lista de funcionalidades poderia ser enorme, tanto é que muita gente hoje não sabe mais qual é a função básica de um Firewall, de tantas funcionalidades que este agregou ao longo do tempo;

Mas uma coisa é certa o uso de Firewalls é indispensável para qualquer rede de computadores.

Este material é retirado dos seguintes livros:

TANENBAUM, Andrew S. **Redes de Computadores**. Editora Campus, 4 Edição.
2003.

ARTYMIAK, Jacek. **Building Firewalls with OpenBSD and PF**. 2 Edição. 2003.

Todos os slides são apenas uma base para a disciplina e não dispensa a leitura dos próprios livros para compreensão do assunto como um todo.

Fim