- Firewall

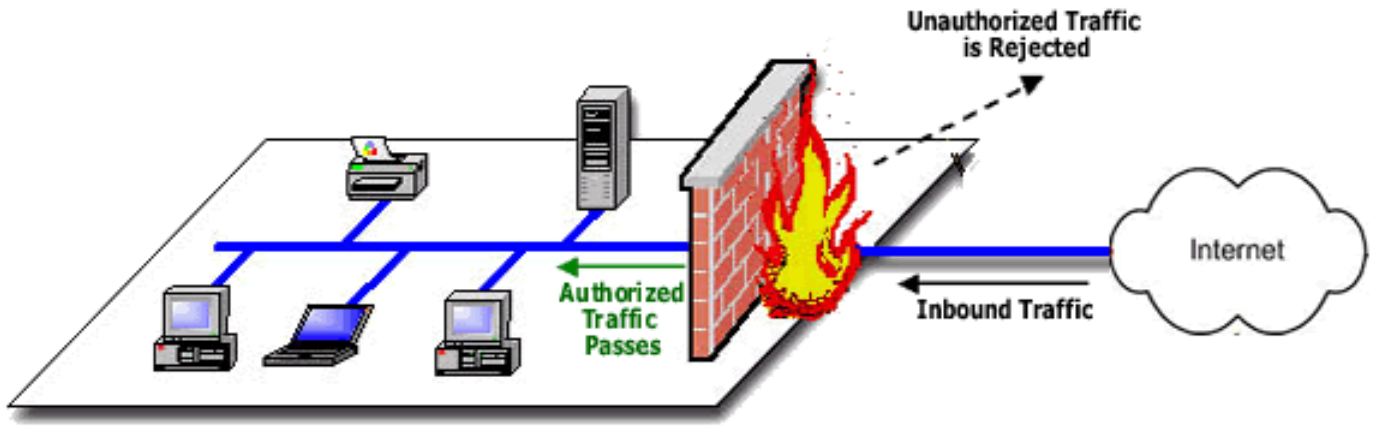
Firewalls

- Um **firewall** forma uma barreira através da qual o tráfego indo em cada direção precisa passar. Uma **política de segurança** de firewall dita qual tráfego tem autorização para passar em cada direção.

- Um firewall pode ser projetado para operar como um **filtro** no nível de pacotes IP ou pode ser operar em uma camada de protocolo mais alta.

Função do Firewall

- O Firewall é inserido entre a rede local e a Internet, para estabelecer um enlace controlado e erguer uma parede ou um perímetro de segurança externo.



Firewall de Filtragem de Pacotes

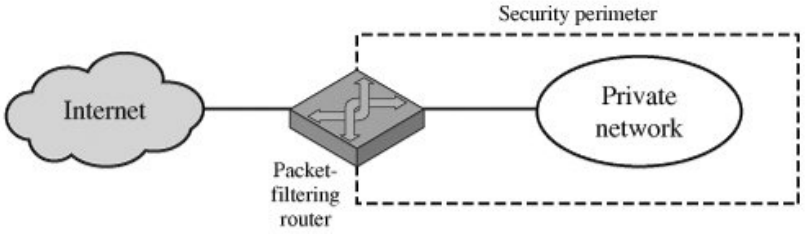
- Um roteador de filtragem de pacotes aplica um conjunto de regras a cada pacote IP que entra e sai e depois encaminha ou descarta o pacote.

- As regras de filtragem são baseadas nas informações:
  - IP de origem.
  - IP de destino.
  - Porta de origem (PO) e porta de destino (PD). Nível de transporte.
  - Protocolo de Transporte.

- Políticas padrões para tomada de decisão.
  - Descartar (Aquilo que não é expressamente permitido é proibido).
  - Encaminhar (Aquilo que não é expressamente proibido é permitido).

Firewall de Filtragem de Pacotes

- A vantagem de um firewall de filtragem de pacotes é sua simplicidade. Porém, este toma decisões de filtragem com base em um pacote individual e não leva em consideração qualquer contexto de camada superior.



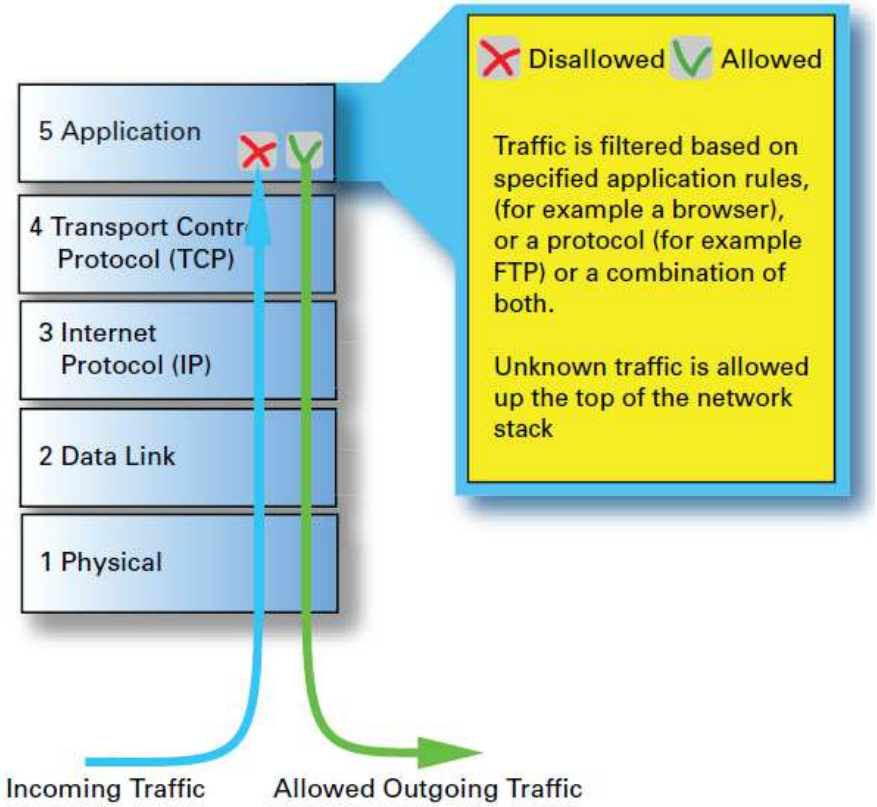
- Exemplo de tabela de filtragem.

Ação	Host Interno	Porta	Host Externo	Porta	Comentário
Bloquear	-	-	SPIGOT	-	Host não confiável
Permitir	Próprio GW	25	-	-	Conexão com própria porta SMTP

Ação	Host Interno	Porta	Host Externo	Porta	Flags	Comentário
Permitir	Hosts próprios	-	-	25	-	Envio de pacotes SMTP para a porta de outros hosts
Permitir	-	25	-	-	Ack	Resposta

Firewall em nível de Aplicação

- Firewall em nível de aplicação (ALG – *Application Level Gateways*), também chamado de Proxy, pode filtrar pacotes na camada de Aplicação. Pacotes de entrada ou saída não podem acessar serviços que não estão especificados no Proxy.



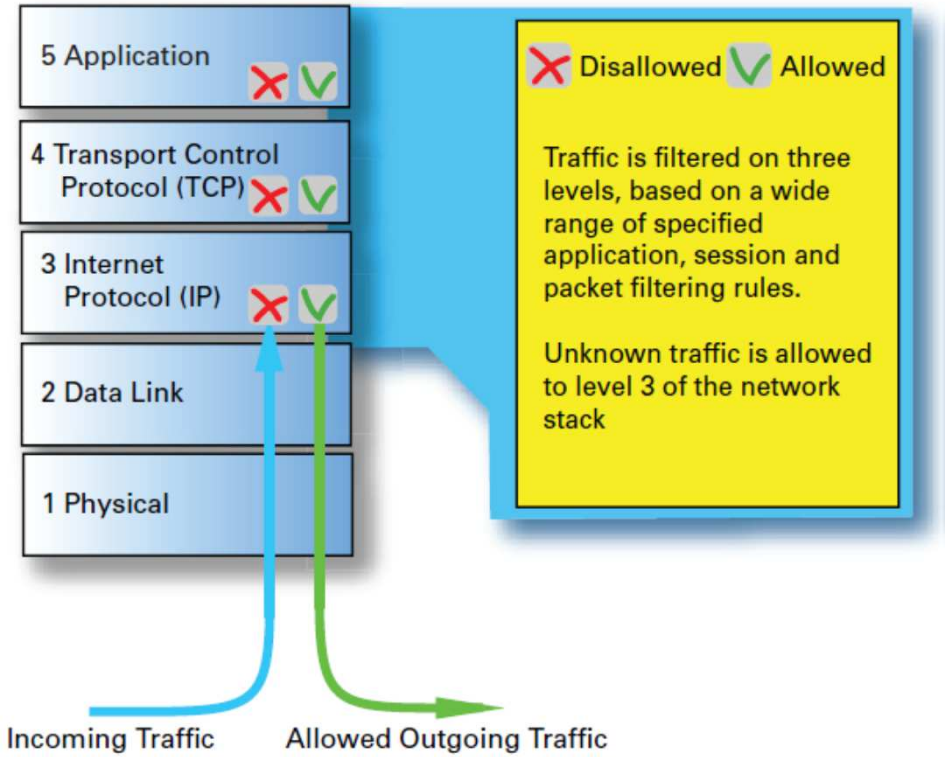
Firewall em nível de Aplicação

- Vantagens.
  - ALG tendem a ser mais seguros.
  - Não é necessário explorar todas combinações dos filtros de pacote.
  - Somente examina algumas aplicações permitidas.
  - Fácil registrar e auditar todo o tráfego.

- Desvantagem.
  - Overhead de processamento adicional em cada conexão.

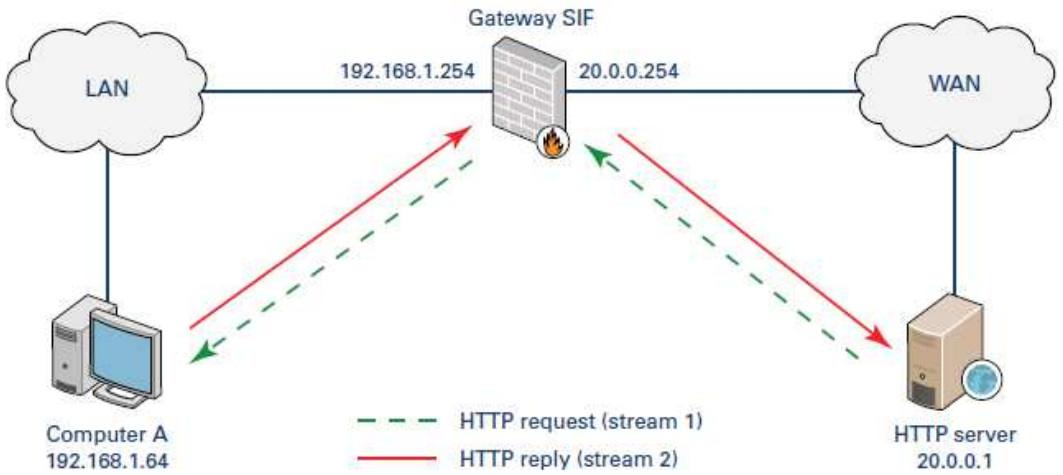
Firewall de Inspeção com Estado

- O Firewall de Inspeção com Estado (*Stateful Inspection Firewalls*) estreita as regras para o tráfego TCP, criando um catálogo de conexões de saída. Existe uma entrada para cada conexão estabelecida atualmente.



Firewall de Inspeção com Estado

- Um exemplo de como funciona um SIF pode ser visto na figura em questão.



Stream/Connection Table

Connection	Streams	Protocol	SRC IP	DST IP	SRC Port	DST Port
Connection 1	Stream 1 Stream 2 (expected)	HTTP HTTP	192.168.1.64 20.0.0.1	20.0.0.1 192.168.1.64	1026 80	80 1026