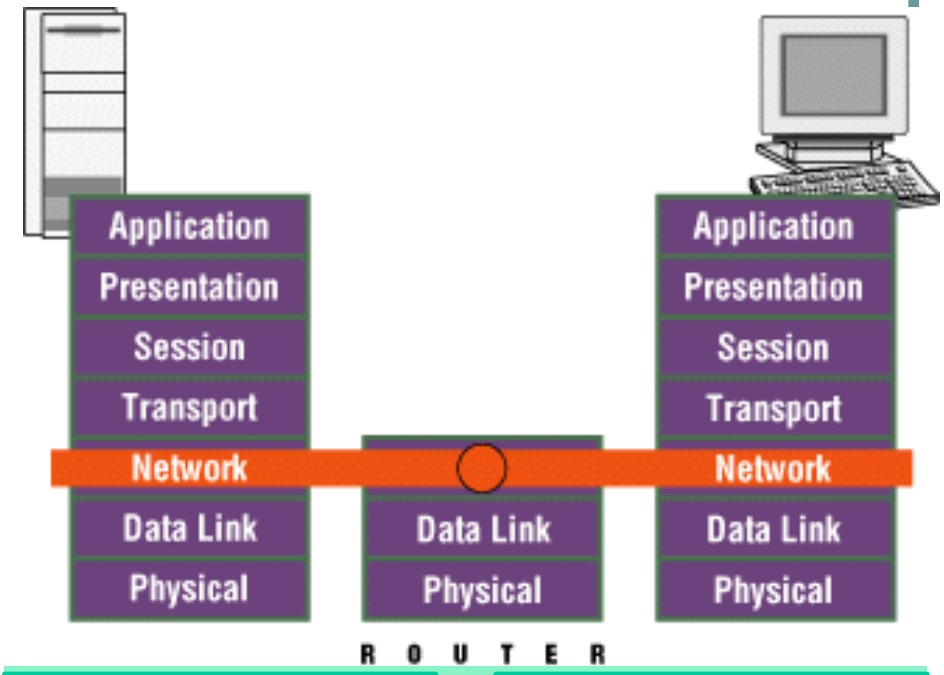
Proxy e FIREWALL

Firewall - Inspeção com estado. (Stateful Inspection)

- As primeiras gerações de firewall eram ditos "stateless".
  - Cada pacote é **analisado individualmente**, **sem** levar em conta pacotes anteriores trocados na mesma conexão.
  - Os firewalls baseados em filtros de pacotes **não** olham o conteúdo dos protocolos de aplicação.

Firewall - Filtro de Pacotes

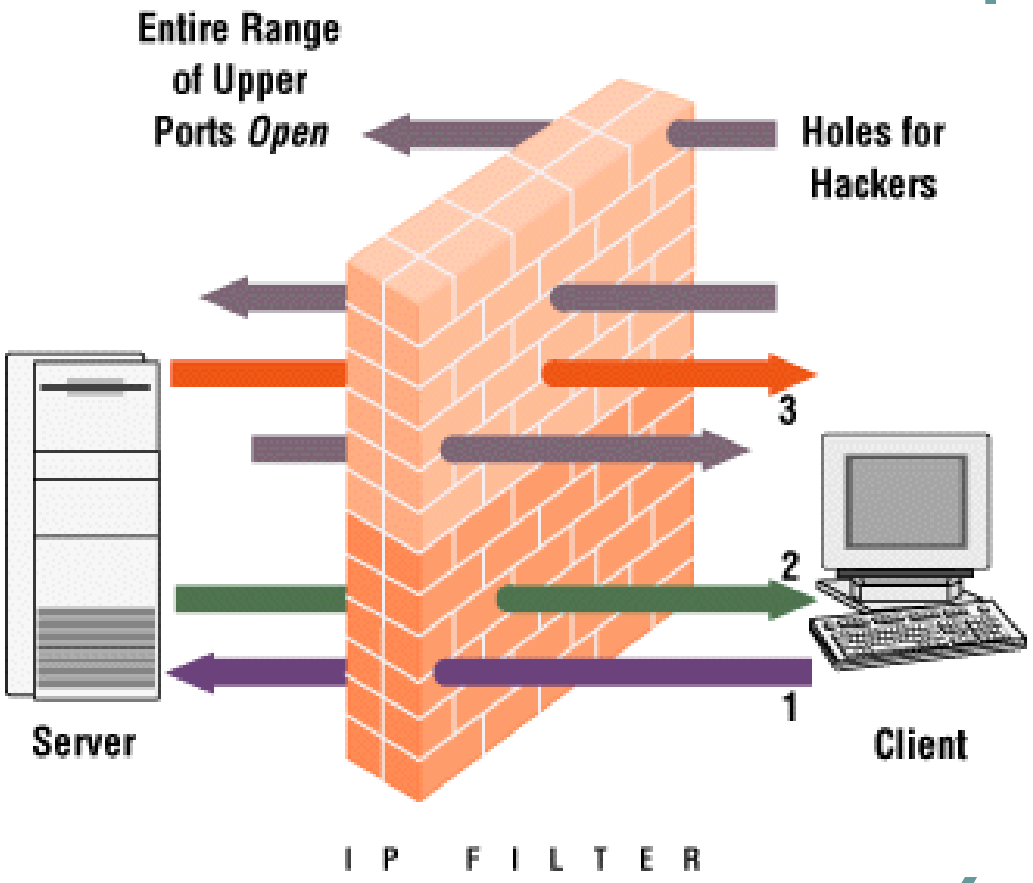
- Usualmente implementado em roteadores.
- São **independentes** da aplicação (analisam apenas informações de IP e Porta).
- **Tem alto desempenho**.



Prós	Contra
• Independentes da aplicação. • Alta performance. • Escalavel.	• Baixa segurança. • Não entende informações de camadas acima do transporte.

Firewall - Filtro de Pacotes:
Problemas de Segurança

- São stateless:
  - Precisam liberar todas as portas de cliente (> 1023) para permitir uma comunicação FTP.
- Apenas duas opções:
  - Ou libera-se todas as portas ou bloqueia-se o serviço todo.

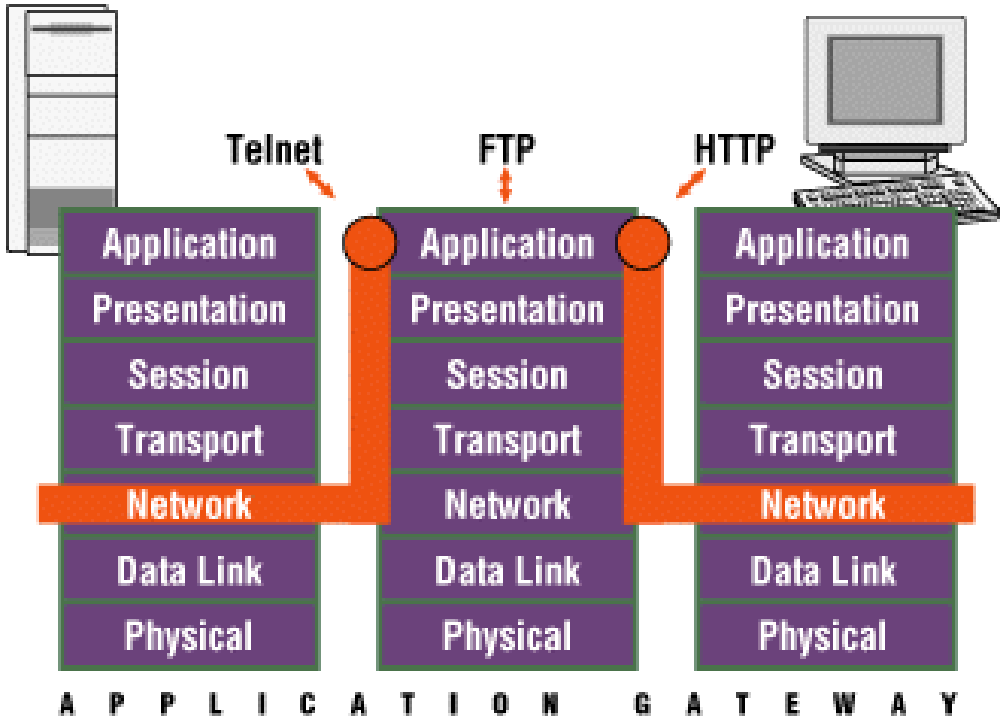


Gateways de Aplicação - Proxy

- Uma alternativa para os filtros de pacotes são os gateways de aplicação.
  - Gateways de aplicação (Proxy) são "statefull": Isto é, eles guardam o estado das conexões iniciadas pelos clientes.
  - Alguns tipos de gateways de aplicação (Proxy) são capazes de analisar o conteúdo dos pacotes.
  - Todavia, são dependentes da aplicação (**não funcionam para aplicações desconhecidas**) e tem baixo desempenho.

Gateways de Aplicação - Proxy

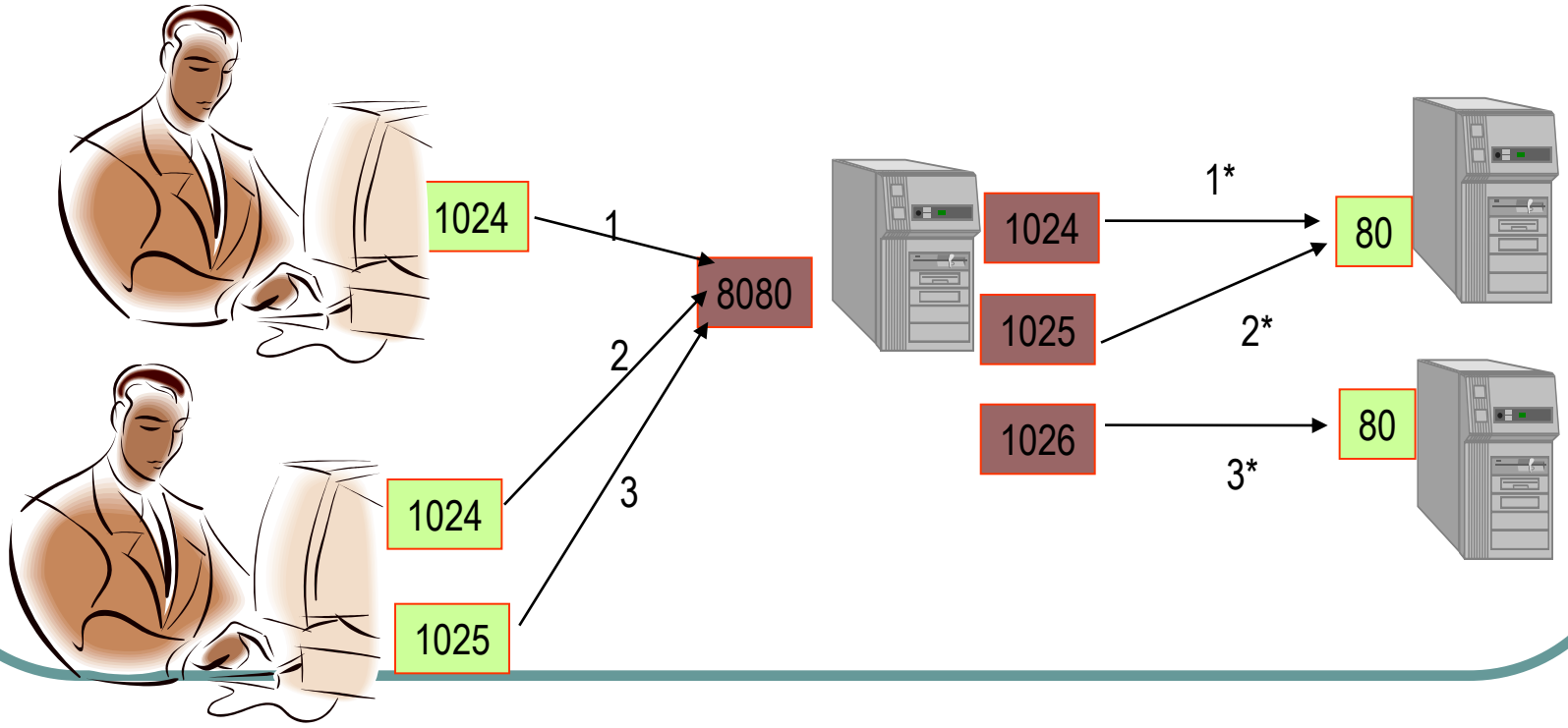
- Usualmente Implementados como serviços.
- O Gateway de Aplicação é visto pelos clientes como um Servidor.
- Abrem apenas a porta do cliente utilizada para fazer a conexão com o servidor.



Prós	Contra
• Boa segurança • Conhecimento do comportamento da aplicação.	• Baixa performance. • Suporte a aplicação limitada. • Baixa escalabilidade

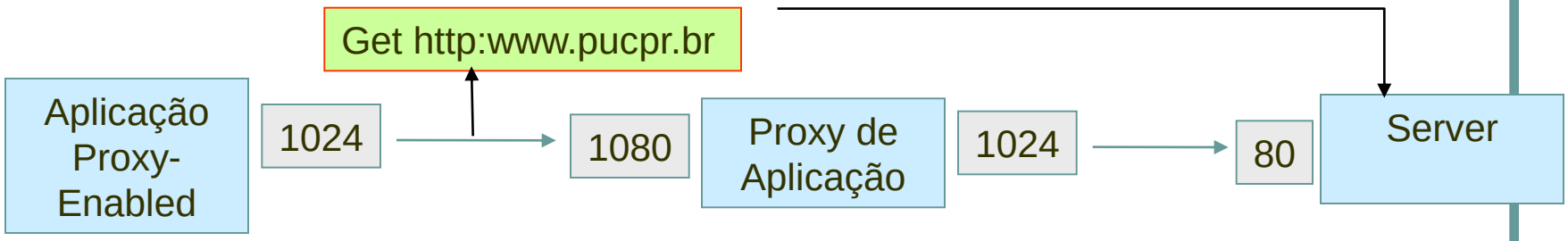
Gateways de Aplicação - Proxy

- Dependentes de Aplicação
  - Examinam o conteúdo dos pacotes, incluindo os protocolos de aplicação.
    - Exemplo: Proxy HTTP
- Independentes da Aplicação
  - Não precisa examinar o conteúdo.
    - Exemplo: Socks

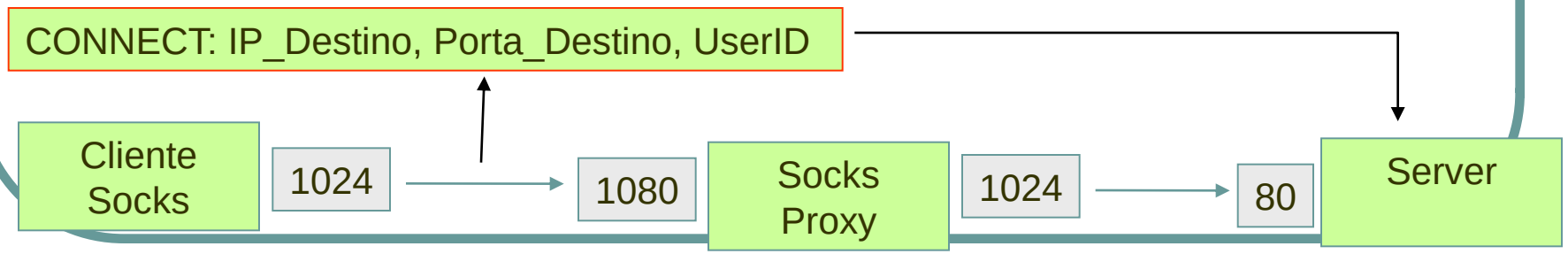


Proxy Socks X Proxy de Aplicação

O **proxy** de aplicação localiza o Servidor de Destino analisando as informações do protocolo de aplicação.



O **cliente SOCKS** inclui automaticamente informações adicionais (durante a conexão TCP ou nos pacotes UDP), que são utilizadas pelo **Proxy SOCKs** para localizar o Servidor de Destino.



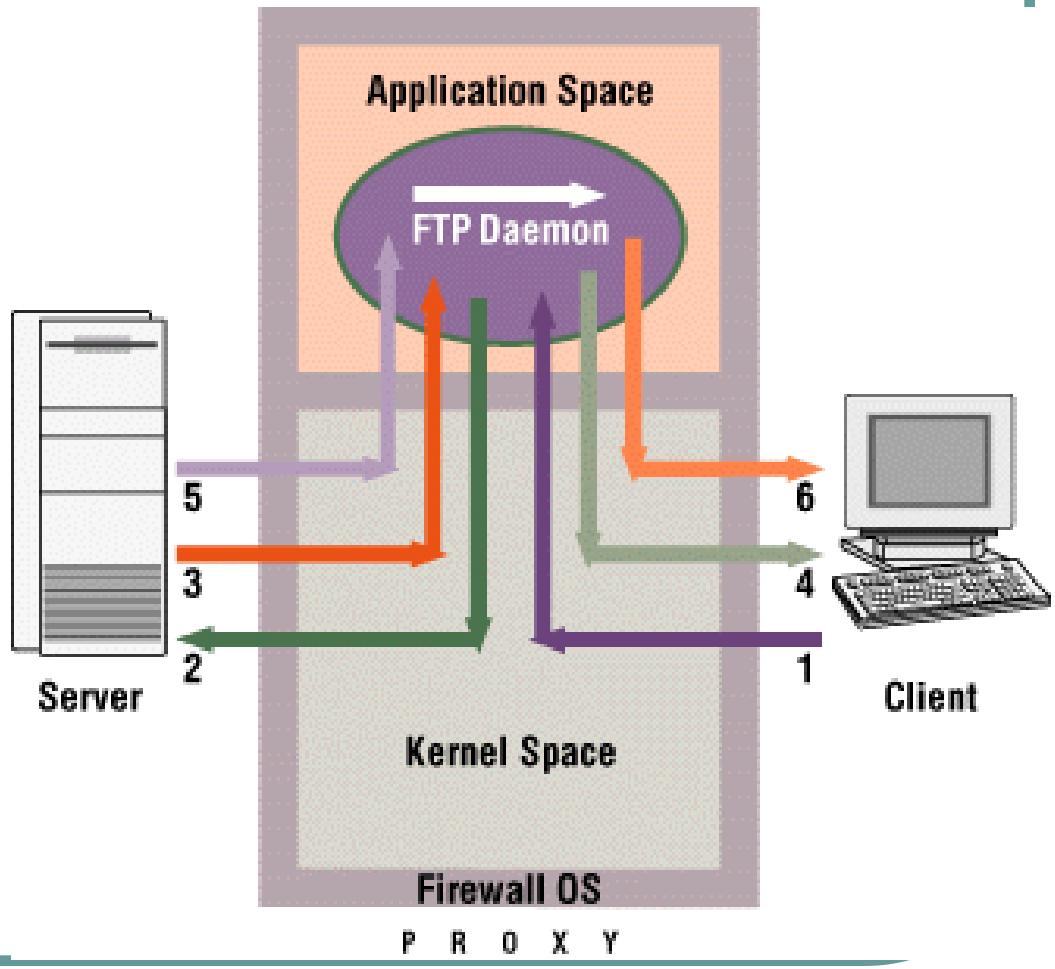
Limitações dos Gateways de Aplicação

- Proxys de Aplicação
  - **Limitam** o tipo de aplicativo que pode ser utilizado na rede.
  - Funcionam apenas para os aplicativos que foram re-escritos para utilizar o Proxy.
- Proxy Socks
  - A versão corrente do protocolo SOCKs é 5.0
    - RFC1928: suporta TCP , UDP e autenticação
  - A versão 4 suporta apenas TCP.
  - Algumas soluções proprietárias suportam também ICMP.

Gateway de aplicação – Proxy

Problemas de Desempenho

- **Quebram o esquema cliente-servidor** (o proxy cria uma nova conexão para cada cliente).
  - O número de sessões no Gateway é **duplicado**.
  - Cada conexão mantém um processo no Proxy.



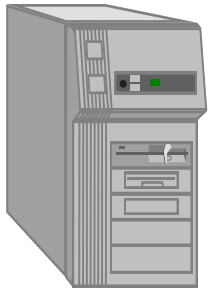
Firewall - Stateful Inspection

- Tecnologia Desenvolvida pela CheckPoint.
- Implementa o conceito de estado sem criar novas conexões no roteador.
  - Um módulo de software analisa permanentemente o conteúdo dos pacotes que atravessam o firewall.
  - As informações relevantes dos pacotes são armazenadas em tabelas dinâmicas para posterior uso.
  - A decisão quanto a passagem ou não de um pacote leva em conta o conteúdo de pacotes anteriormente trocados na mesma conexão.

Firewall - Stateful Inspection

- Para poder criar regras sobre quem inicia uma comunicação, o firewall armazena informações sobre as portas utilizadas pelo cliente.

200.0.0.1:
1024
>>> 210.0.0.2:
53



200.0.0.1:1024 >>> 210.0.0.2:53

210.0.0.2:53 <<< 200.0.0.1:1024

210.0.0.2:53 <<< 200.0.0.1:1026

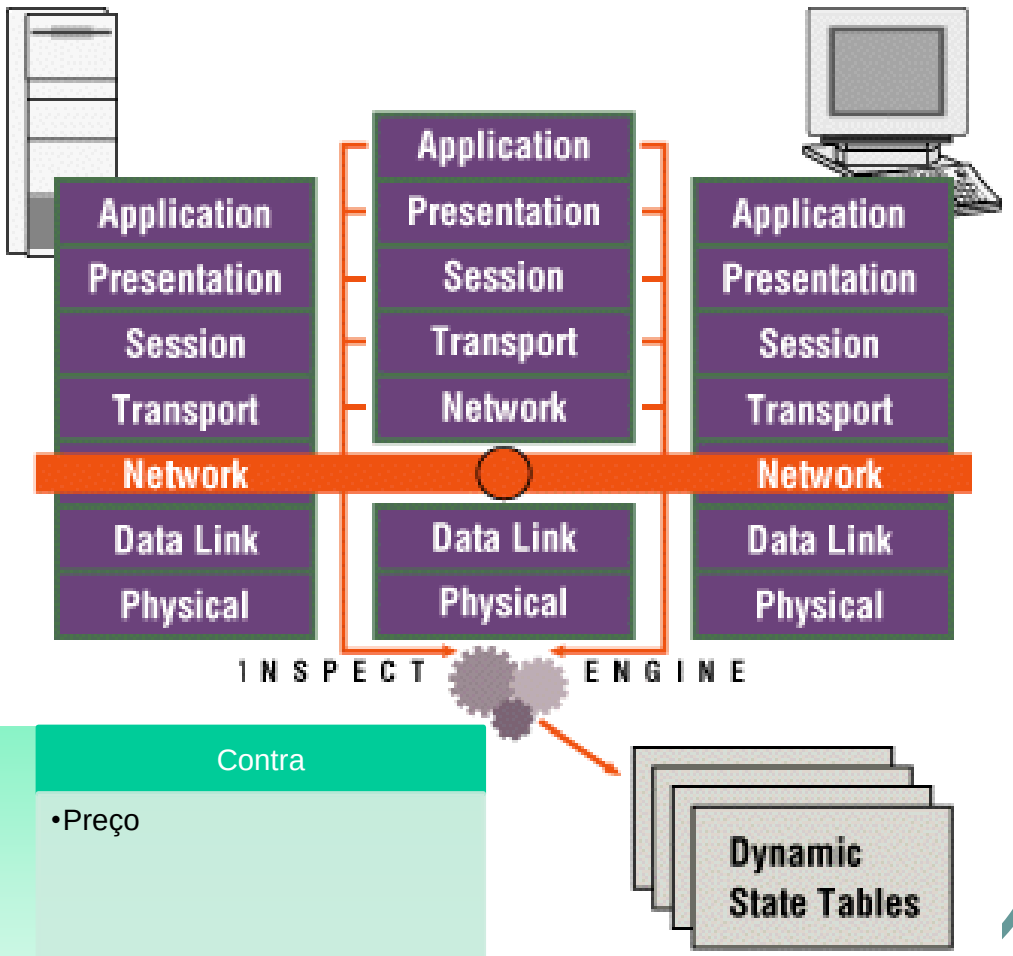
210.0.0.2:53 <<< 200.0.0.2:1024

tempo

tempo

Firewall - Stateful Inspection

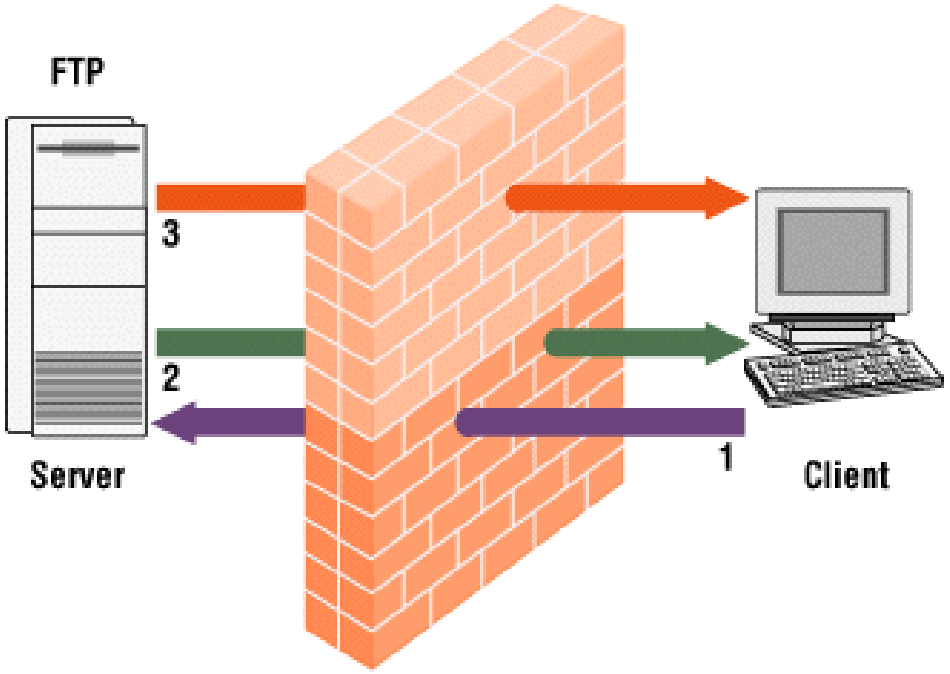
- Analisa o conteúdo dos pacotes sem quebrar o modelo cliente servidor.
- A informação de estado é capturada quando o pacote através o firewall e armazenadas em tabelas dinâmicas.



Prós	Contra
•Boa segurança •Conhecimento do comportamento da aplicação. •Alta performance •Escalavel •Transparente	•Preço

Firewall - Stateful Inspection

- Quando o cliente requisita um serviço FTP, o Firewall armazena a porta utilizada numa tabela dinâmica, **não liberando** nenhuma outra porta do cliente.



Maquina de inspeção

Firewall - Stateful Inspection
Segurança de Conteúdo

- Além das informações de portas, as informações de conteúdo também são utilizadas pelo Firewall.
- Normalmente, apenas os protocolos mais comuns são analisados.
  - HTTP: Permite Filtrar:
    - Métodos de acesso (GET, POST), URLs ("*.sk"), etc
    - TAGS em HTML com referências a Applets em Java ou Objetos ActiveX.
    - Download de certos tipos MIME.
  - FTP: Permite Filtrar
    - Comandos específicos (PUT, GET), Nomes de Arquivo
    - Pode disparar antivírus para verificação de arquivos.
  - SMTP: Permite criar regras de Filtragem baseadas
    - Nos campos FROM e TO
    - Tipo MIME
    - Etc.

Firewall - Stateful Inspection

Integração com Métodos de Autenticação

- Firewalls com Tecnologia Stateful permitem criar regras de filtragem baseados no login do usuário ao invés do endereço IP.
- Estas técnicas simplificam o processo de criar regras de filtragem pois o usuário pode acessar o serviço independentemente da máquina que estiver usando.
- Esta tecnologia só é possível para firewalls "Stateful".
- Três métodos são usualmente disponíveis:
  - User Authentication (transparente)
  - Session Autentication
  - Mapeamento Transparente do Usuário em Endereço

Firewall - Stateful Inspection

Integração com Métodos de Autenticação

- User Authentication (transparente)
  - Permite a usuário remoto acessar um serviço da rede independente do seu IP.
  - O firewall reconhece o login do usuário analisando o conteúdo dos protocolos FTP, HTTP, TELNET e RLOGIN.
- Session Authentication
  - Quando o usuário tenta acessar um serviço da rede o Firewall envia para o cliente um pedido de login (challange message).
  - O cliente deve ter um software especial para confirmar a senha.
  - Só então o acesso é permitido (ou negado).

Firewall - Stateful Inspection

Integração com Métodos de Autenticação

- Mapeamento Transparente entre Usuário e Endereço
  - O Firewall captura mensagens DHCP para as máquinas.
  - O Firewall captura as mensagens de login trocadas entre o usuário e o servidores de domínio da rede.
    - CHECK POINT, por exemplo, suporta as mensagens do Windows NT.
    - O usuário não se loga no Firewall, o sucesso do login é identificado pelo Firewall também capturando as mensagens do servidor.