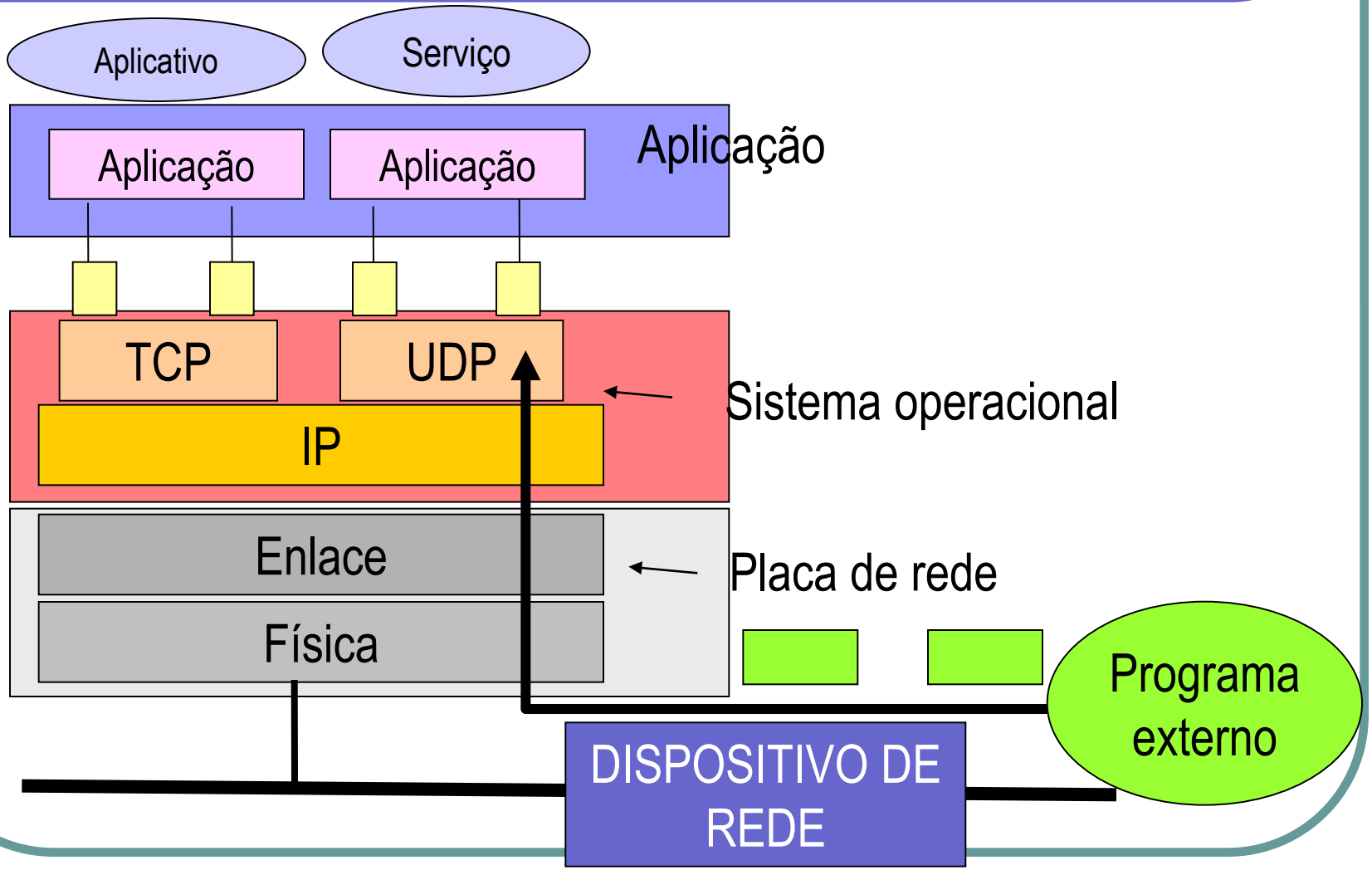
FIREWALLS

Firewalls

- Definição:
  - Termo **genérico** utilizado para designar um tipo de **proteção de rede** que restringe o acesso a certos serviços de um computador ou rede de computadores pela **filtragem dos pacotes** da rede.
- Os firewalls podem ser de dois tipos:
  - **Sem estado (stateless)**
    - A decisão sobre a passagem ou não de um pacote considera apenas as informações carregadas **no próprio pacote.**
  - **Com estado (stateful)** – Stateful Inspection
    - A decisão sobre a passagem ou não de um pacote leva em conta **outros pacotes** que atravessaram anteriormente o firewall.

Firewall = Bloqueio de Pacotes

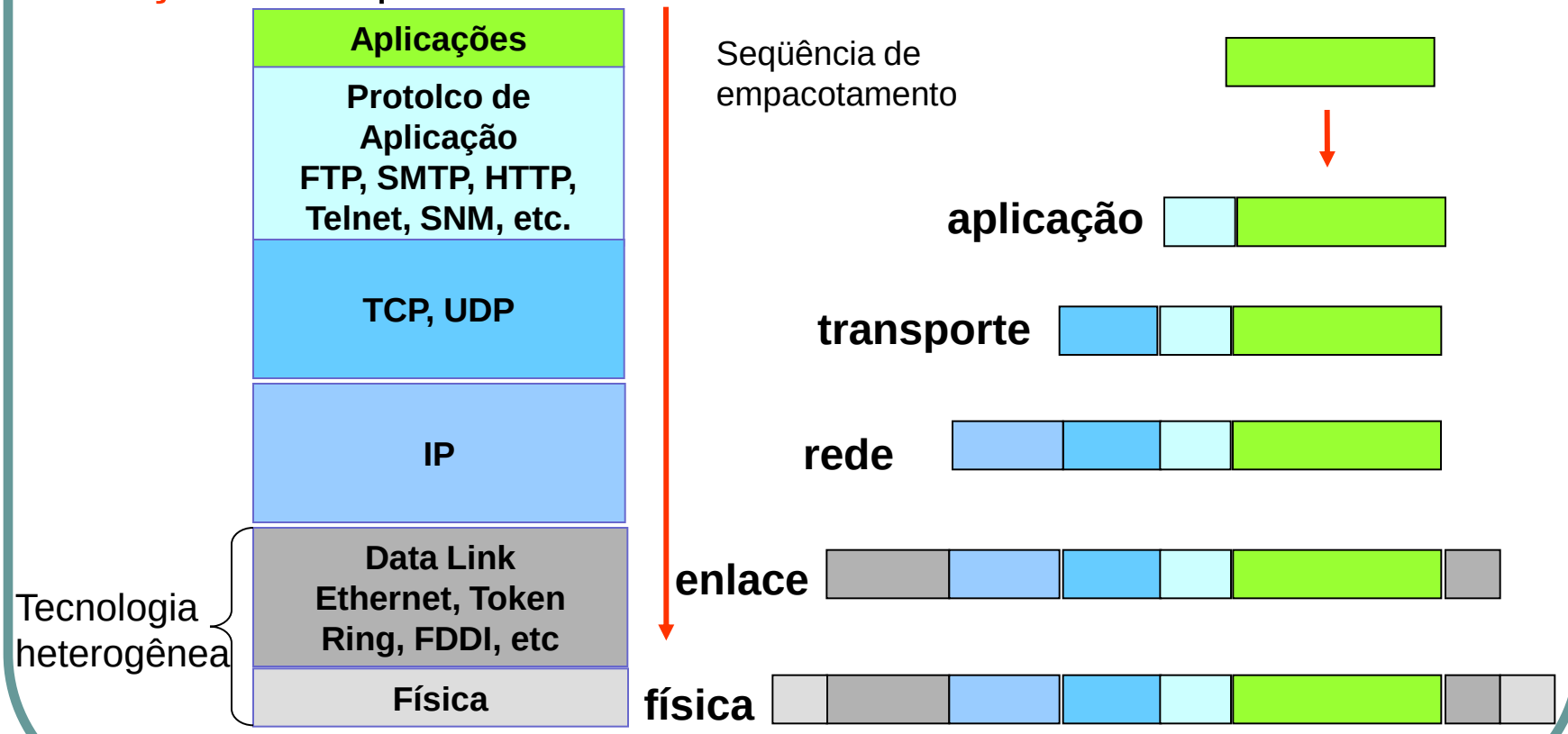


Firewalls Sem Estado

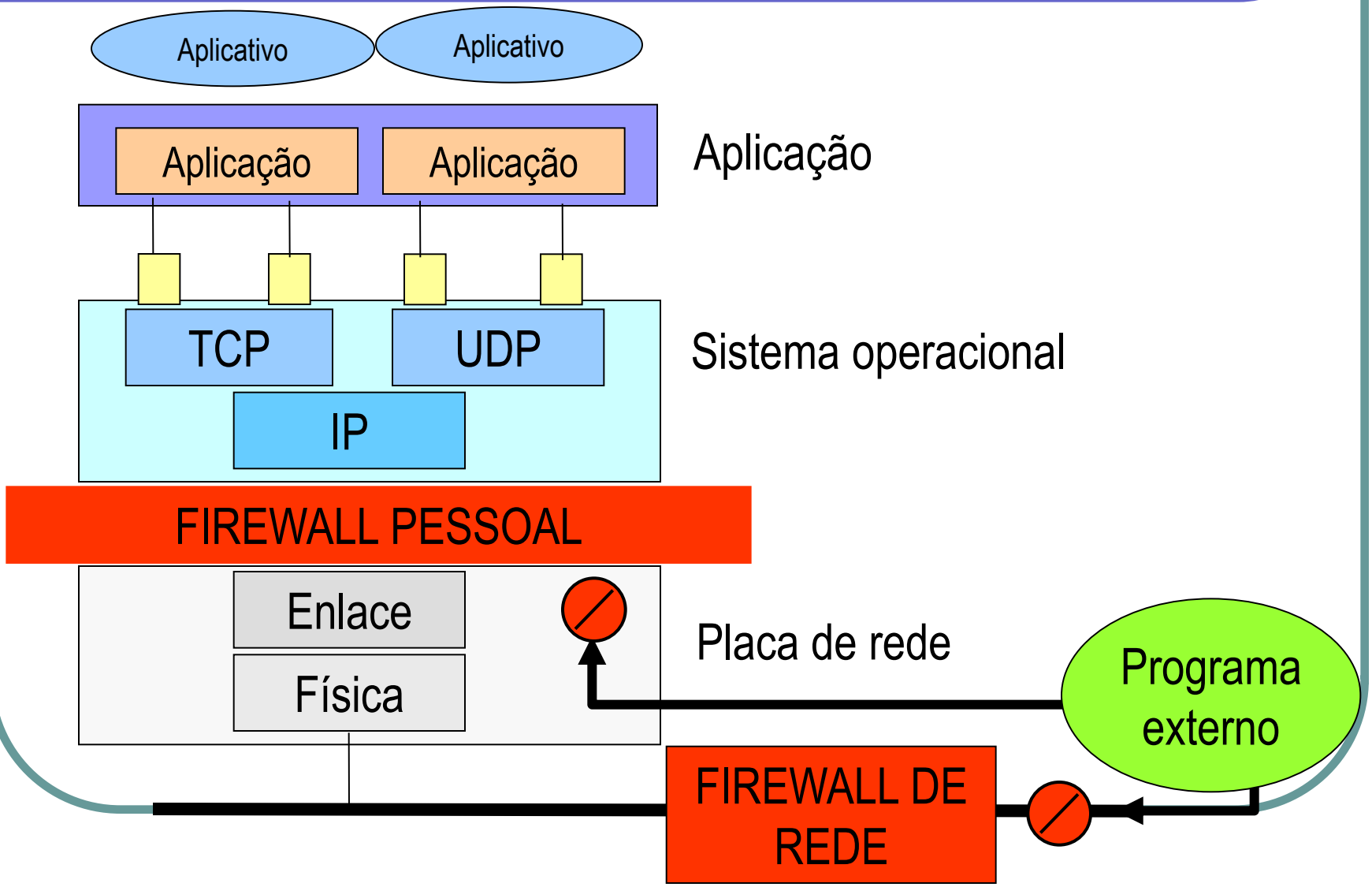
- O tipo mais comum de firewall é o sem estado:
  - A decisão sobre a passagem ou não de um pacote considera apenas as informações carregadas no **próprio** pacote.
- Utiliza usualmente apenas informações das camadas de rede e transporte.
  - Essa simplificação permite:
    - Tornar o firewall **mais rápido**.
    - Tornar o firewall **independente** do protocolo transportado.
    - Tornar o firewall **independente** de criptografia e tunelamento.

Filtragem de Pacotes sem Estado

A **filtragem** de pacotes é feita com base nas informações contidas no **cabeçalho** dos protocolos.

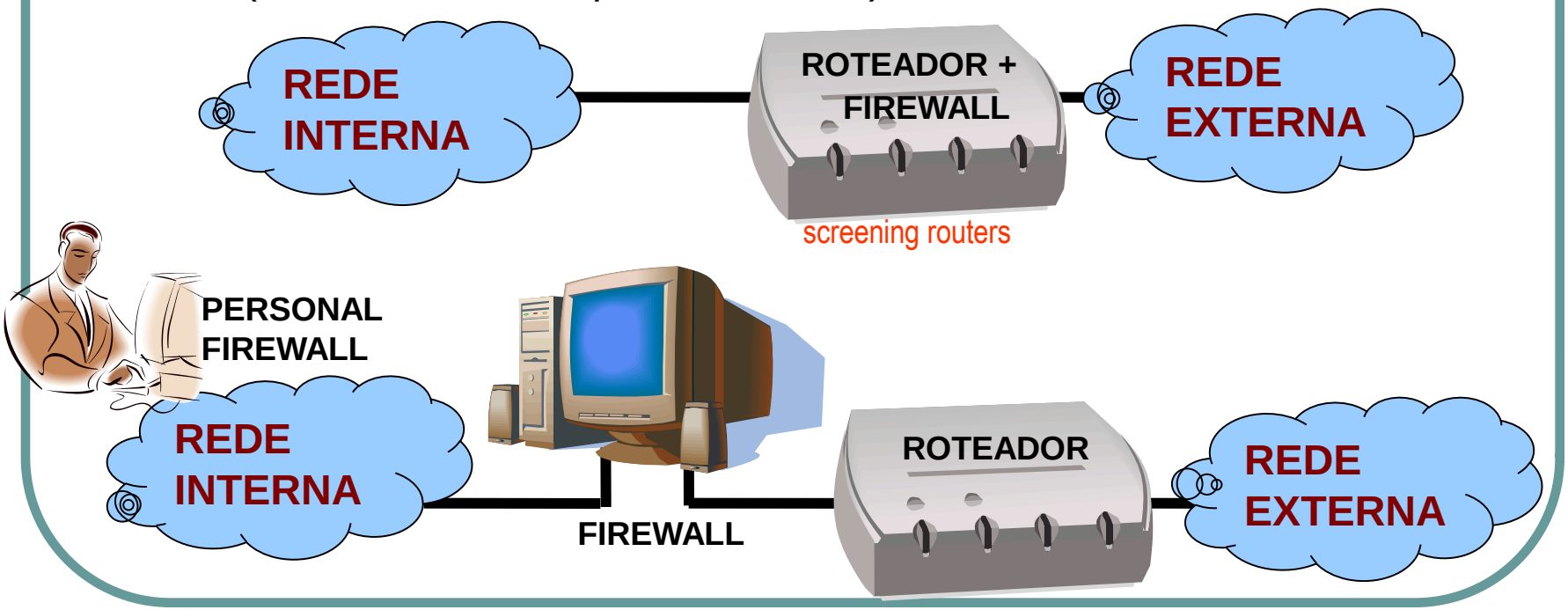


Filtragem de Pacotes



Implementação Física

- No software do **Roteador**: ‘screening routers’
  - Um roteador que executa filtragem de pacotes e é usado como firewall.
- No software de uma **estação dedicada**
  - (um PC com duas placas de rede).



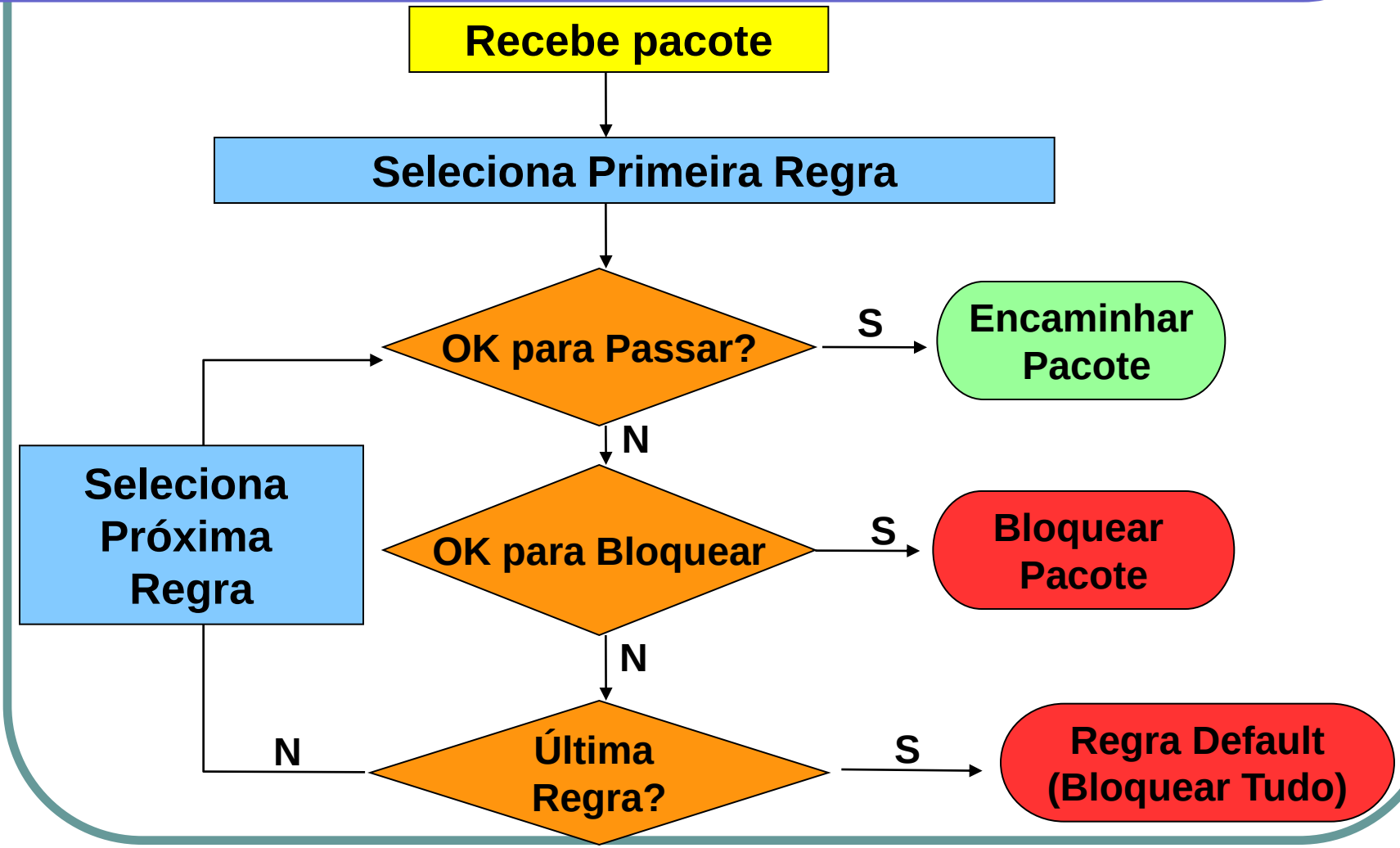
Exemplo

- Roteadores Cisco
  - PIX Firewall
  - Firewall
  - Roteador
  - Proxy
  - Detector de ataques (SMTP, etc)
  - Defesa contra fragmentação de IP
  - Implementa VPN com IPsec
  - Mais de 256K sessões simultâneas.

Exemplo

- Implementação por Software
  - **Check Point Firewall**
    - Interface Gráfica
    - Módulo de Firewall
    - Módulo de Gerenciamento
    - **Mútiplas Plataformas**
      - Windows, Solaris, Linux, HP-UX, IBM AIX
    - Controle de Segurança e Qualidade de Serviço.

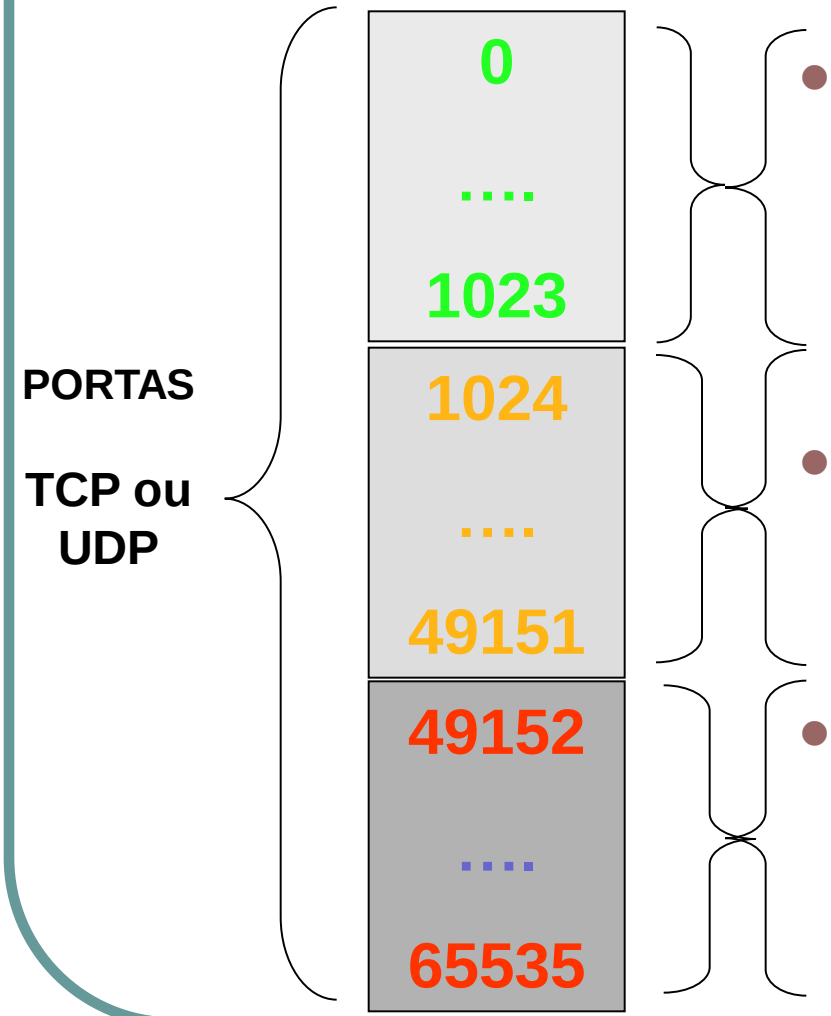
Algoritmo dos Firewalls sem Estado



Filtragem por Aplicação

- Os firewalls **sem estado não** analisam o protocolo de aplicação para determinar o tipo de serviço transportado pelo pacote.
- **A dedução do tipo de serviço é feito indiretamente**:
  - Pelo campo "**Protocol Type**" do IP
    - RFC 1700: Assigned Numbers
      - TCP = 6, UDP = 17, ICMP = 1, etc.
  - Pelas portas quando o tipo de protocolo for 6 ou 17
    - http://www.iana.org/assignments/port-numbers
- **Todas as numerações são padronizada pela IANA (*The Internet Assigned Numbers Authority*)**

Distribuição das Portas



- Portas Bem conhecidas (*well known ports*):
  - Geralmente usada pelos servidores de serviços padronizados.
- Portas Registradas
  - Geralmente usada por servidores proprietários.
- Portas Dinâmicas ou Privadas:
  - Usadas pelos clientes e pelos serviços não padronizados.

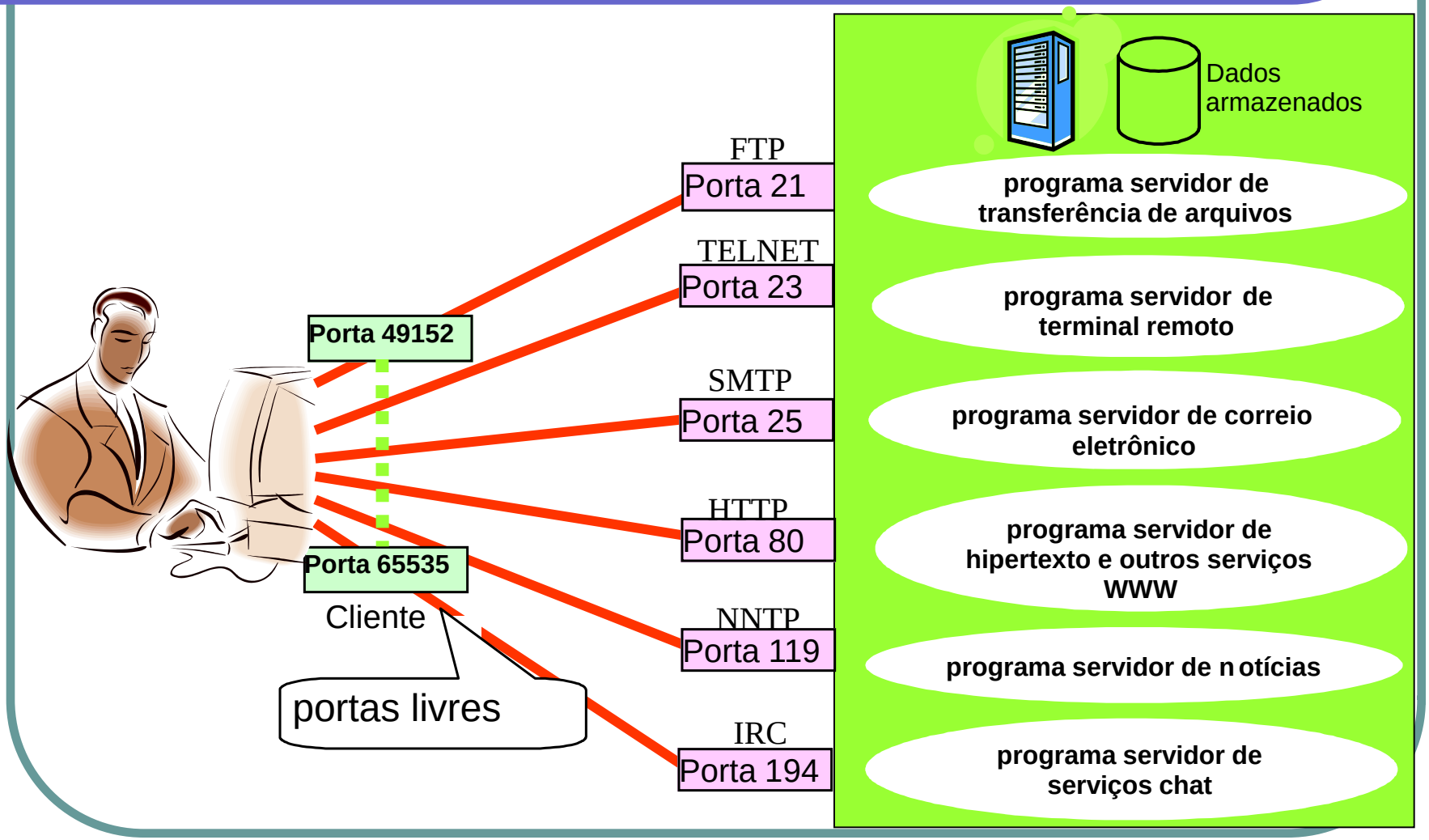
Distribuição das Portas

- Portas Bem Conhecidas:
  - Definidas pela IANA
  - Acessíveis **apenas** por processos de sistema
    - (que tenham privilégios do tipo **root**).
  - Designa serviços padronizados para Internet:
    - FTP (21), HTTP (80), DNS (53), etc.
  - **Range**: 0 a 1023
  - Geralmente, a porta é mapeada a um serviço em **ambos** os protocolos (TCP e UDP), mesmo que usualmente só seja **utilizado um** deles.

Distribuição de Portas

- Portas Registradas:
  - Listada pela IANA
  - Serviço oferecido para conveniência da comunidade.
  - Acessíveis por processos de usuário.
  - Usadas geralmente para designar serviços proprietários:
    - Corba Management Agente (1050), Microsoft SQL Server (1433), Oracle Server (1525), etc.
  - Range: 1024 a 49151.

Exemplos de portas bem conhecidas



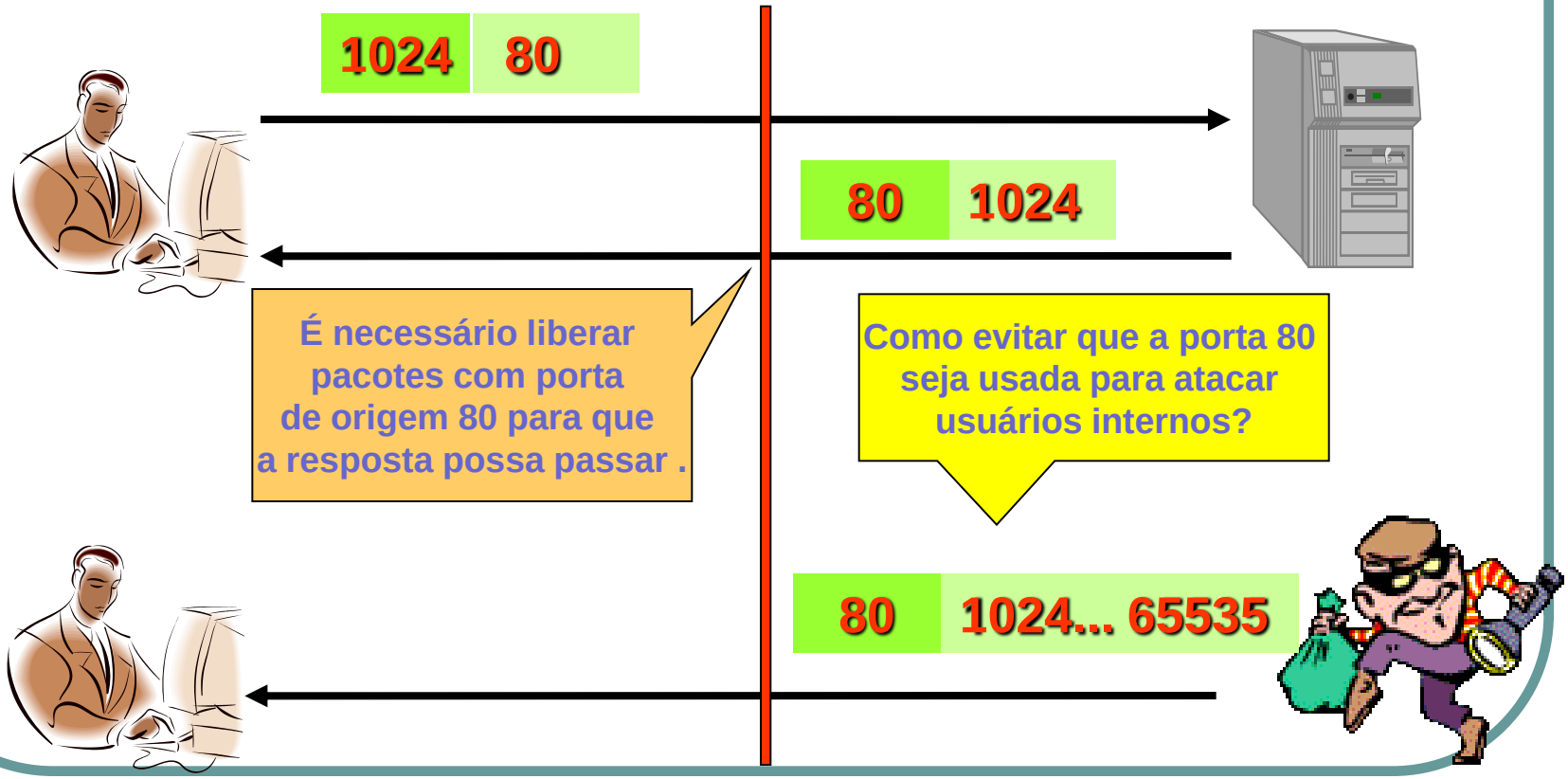
Exemplo de Regras de Filtragem

regra	ação	interface/ sentido	protocolo	IP origem	IP destino	Porta origem	Porta destino	Flag ACK
1	aceitar	rede interna/ para fora	TCP	interno	externo	> 1024	80	*
2	aceitar	rede externa/ para dentro	TCP	externo	interno	80	> 1023	1
3	rejeitar	*	*	*	*	*	*	*

O símbolo "*" indica que qualquer valor é aceitável para regra.

Problema: Spoofing de Porta

- Como diferenciar um ataque externo de uma resposta solicitada por um usuário interno?

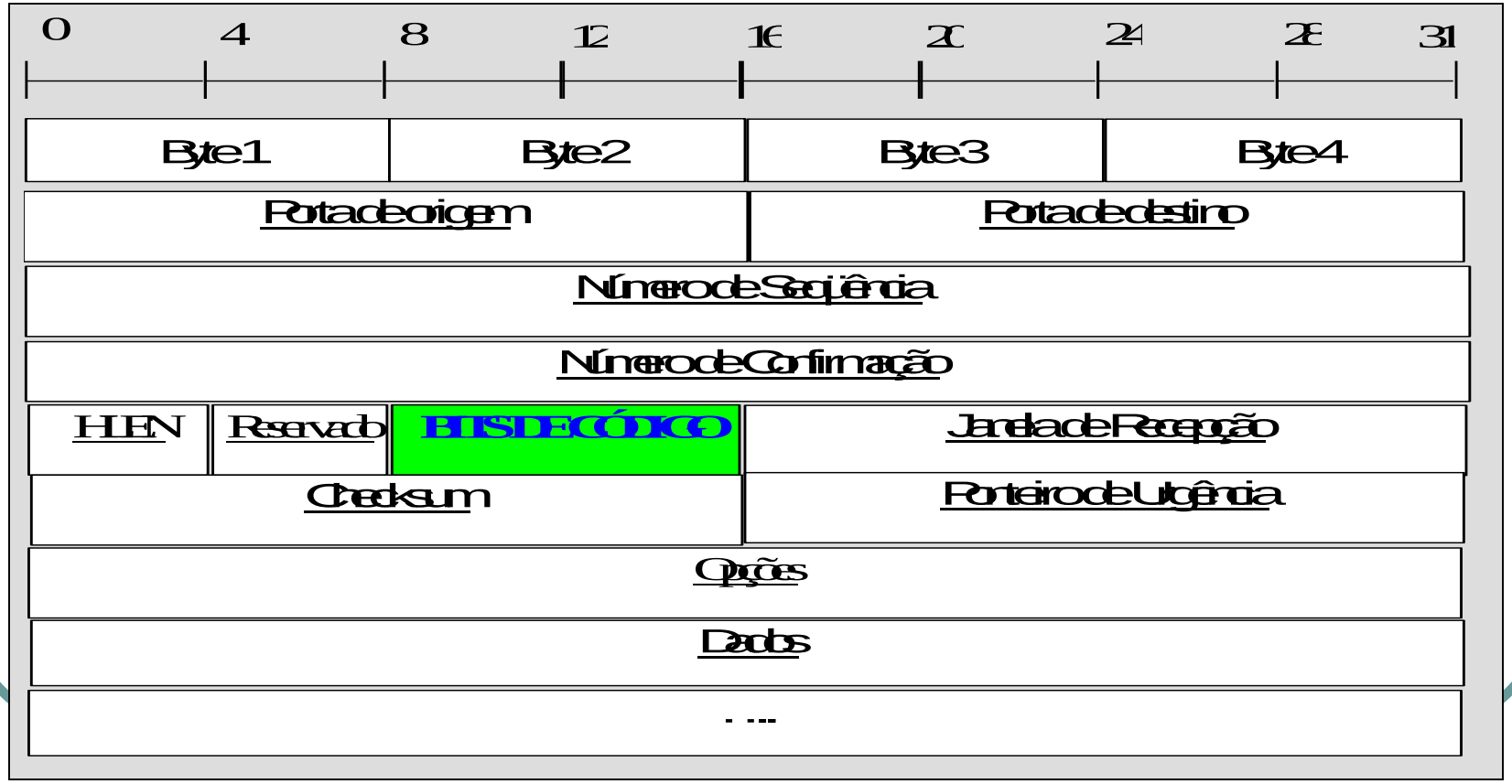


Característica da Comunicação TCP

- Comunicação bidirecional, confiável e orientada a conexão.
  - O destino recebe os dados na mesma ordem em que foram transmitidos.
  - O destino recebe todos os dados transmitidos.
  - O destino não recebe nenhum dado duplicado.
- O protocolo TCP **rompe** a conexão se algumas das propriedades acima não puder ser garantida.

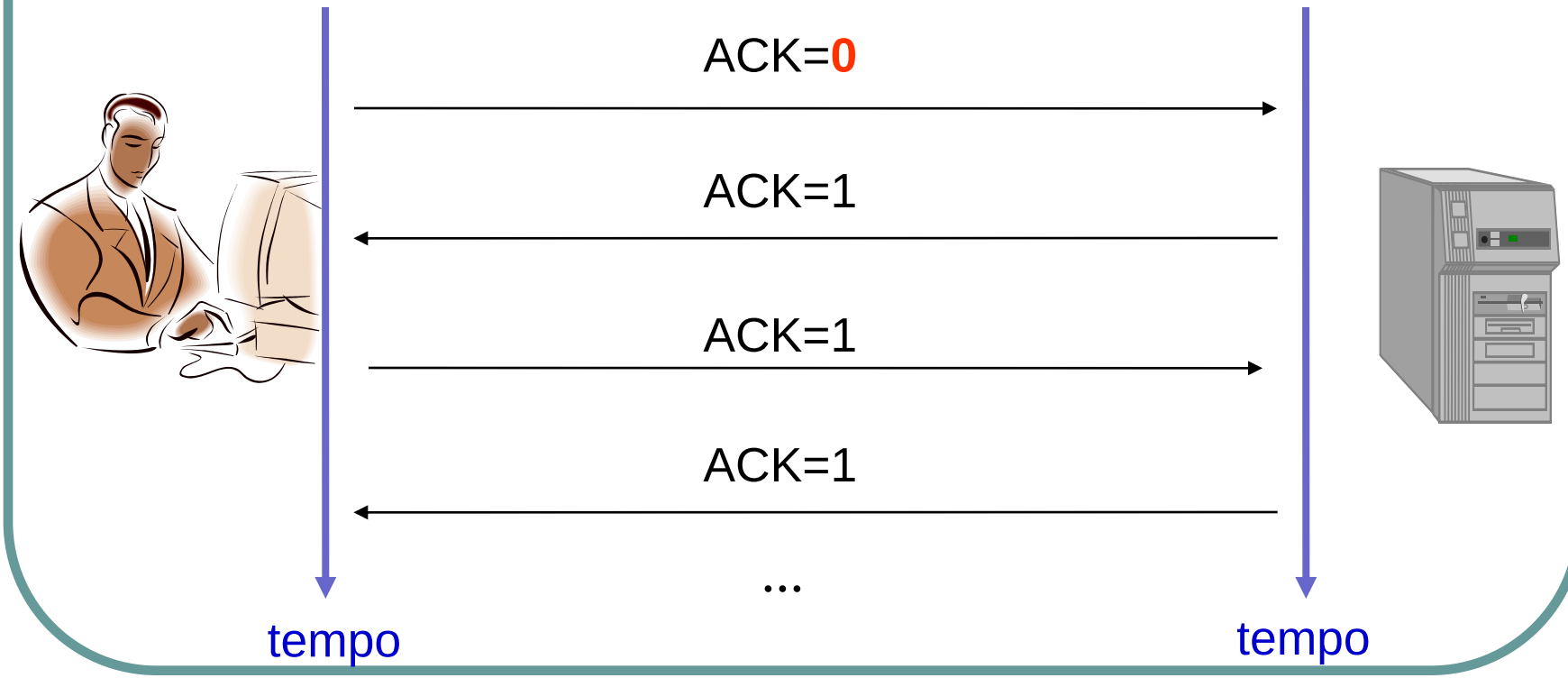
Flags TCP

- **RES: Reservado (2 bits)**
- **URG: Urgent Point**
- **ACK: Acknowlegment**
- **PSH: Push Request**
- **RST: Reset Connection**
- **SYN: Synchronize Seqüence Number**
- **FIN: Mais dados do transmissor**



Flag ACK

- Uma conexão TCP sempre se inicia com o cliente enviando um pacote com o *flag* ACK= 0.



Exemplo de Regras de Filtragem

regra	ação	interface/ sentido	protocolo	IP origem	IP destino	Porta origem	Porta destino	Flag ACK
1	aceitar	rede interna/ para fora	TCP	interno	externo	> 1024	80	*
2	aceitar	rede externa/ para dentro	TCP	externo	interno	80	> 1023	1
3	rejeitar	*	*	*	*	*	*	*

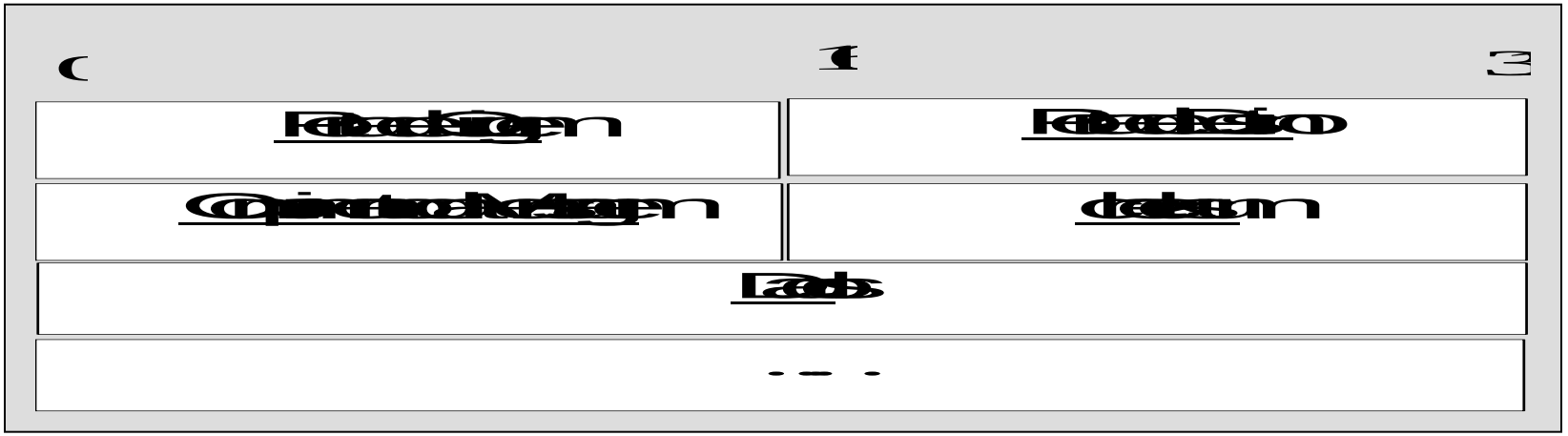
O símbolo "*" indica que qualquer valor é aceitável para regra.

Filtragem com Protocolo UDP

- Comunicação bidirecional, sem nenhum tipo de garantia.
  - Os pacotes UDP podem chegar fora de ordem.
  - Pode haver duplicação de pacotes.
  - Os pacotes podem ser perdidos.
- Cada pacote UDP é independente e não contém informações equivalentes ao flag ACK dos pacotes.

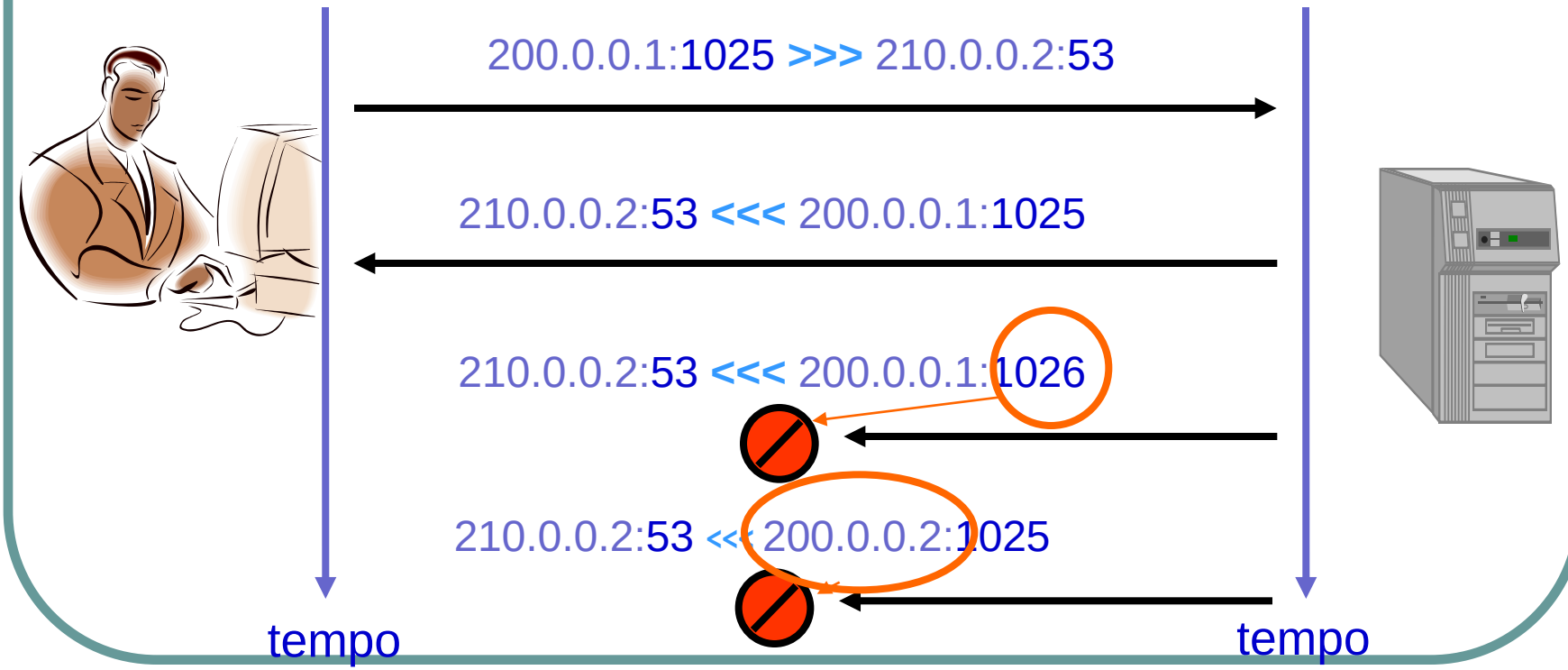
Mensagem UDP

- As mensagens UDP não possuem flags de controle pois o protocolo UDP não oferece a mesma qualidade de serviço que o protocolo TCP.



Dynamic Packet Filtering com UDP

- Para poder criar regras sobre quem inicia uma comunicação no protocolo UDP, os roteadores precisam se lembrar das portas utilizadas.



Regras para Filtragem de Pacotes

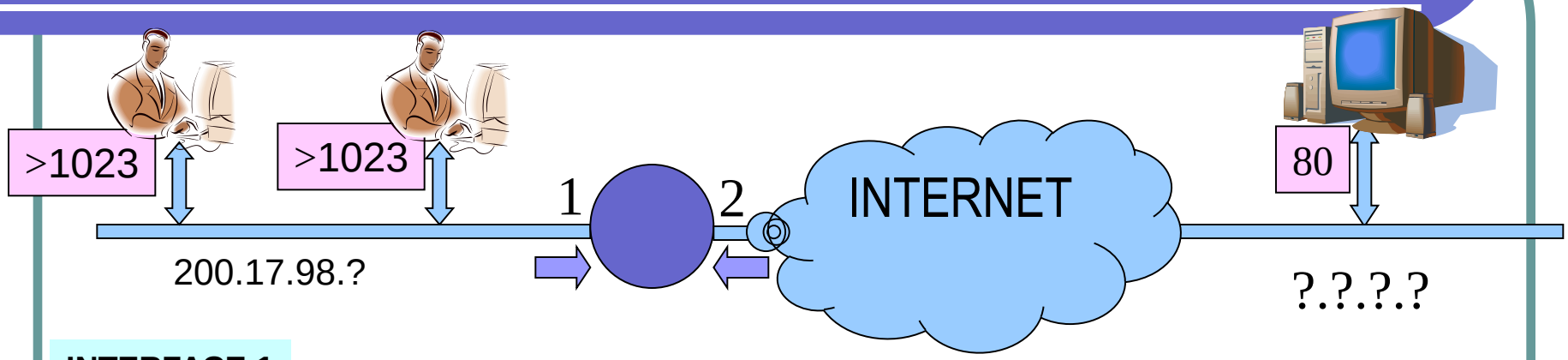
- **Implementação**:
  - Analisar o cabeçalho de cada pacote que chega da rede externa, e aplicar uma série de regras para determinar se o pacote será bloqueado ou encaminhado.
- **ESTRATÉGIAS**
  - 1) TUDO QUE NÃO É **PROIBIDO** É **PERMITIDO**.
  - 2) TUDO QUE NÃO É **PERMITIDO** É **PROIBIDO**.

Exemplo: TUDO QUE NÃO É PERMITIDO É PROIBIDO

regra	ação	interface/ sentido	protocolo	IP origem	IP destino	Porta origem	Porta destino	Flag ACK
1	aceitar	rede interna/ para fora	TCP	interno	*	> 1023	23	*[1]
2	aceitar	rede externa/ para dentro	TCP	*	interno	23	> 1023	1
3	rejeitar	*	*	*	*	*	*	*

- Interpretação:
  - Hosts Internos podem acessar servidores de telnet internos ou externos.
  - Hosts externos podem apenas responder a requisições, não podem iniciar um diálogo (estabelecer uma conexão).

Exemplo: WEB



INTERFACE 1

Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
tcp	200.17.98.0:24	*	> 1023	80	*
*	*	*	*	*	*

INTERFACE 2

Ação	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	tcp	*	200.17.98.0:24	80	> 1023	1
negar	*	*	*	*	*	*

Exemplo

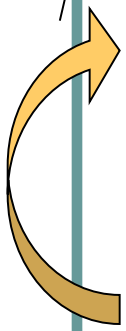
Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	23	*
permitir	In	tcp	*	interno	23	> 1023	1
permitir	In	tcp	*	interno	> 1023	80	*
permitir	Out	tcp	interno	*	80	> 1023	1
negar	*	*	*	*	*	*	*

- Interpretação:
  - Hosts Internos podem acessar servidores de telnet internos ou externos.
  - Hosts externos podem acessar servidores de web internos.

Seqüência de Criação de Regras

- A seqüência na qual as regras são aplicadas pode alterar completamente o resultado da política de segurança. Por exemplo, as regras de aceite ou negação incondicional devem ser sempre as últimas regras da lista.

O deslocamento de uma regra genérica para cima anula as demais.



Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	23	*
permitir	In	tcp	*	interno	23	> 1023	1
permitir	In	tcp	*	interno	> 1023	80	*
permitir	Out	tcp	interno	*	80	> 1023	1
negar	*	*	*	*	*	*	*

Desempenho do Filtro de Pacotes

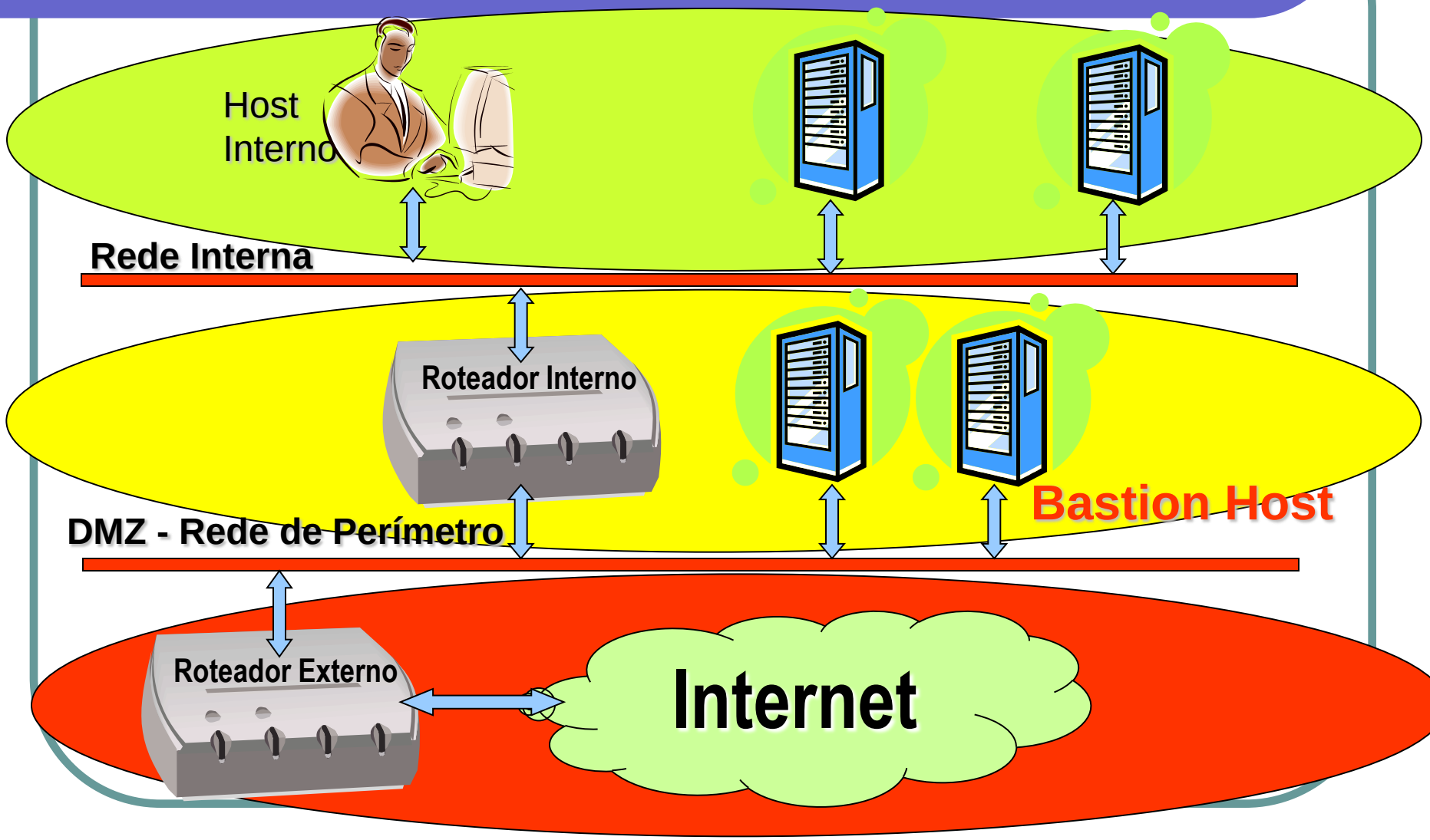
- **O processo de filtragem de pacotes exige que um certo processamento adicional seja executado pelo roteador para cada pacote que chega ou precisa ser transmitido.**
- **Dependendo da velocidade da linha de transmissão, esse processamento pode ou não causar uma degradação do desempenho da rede.**

Conexão	Pacotes/s (20 bytes)	Tempo disponível	Ciclos CPU 1 GHz
56 Kbit/s	350	2.86 ms	2860000
2 Mbit/s	12500	80 μs	80000
10 Mbit/s	62500	16 μs	16000
100 Mbit/s	625000	1.6 μs	1600
1Gbit/s	**6250000**	**0.16 μs**	**160**

Arquitetura DMZ

- Perimeter Network
  - Uma rede adicionada entre a rede protegida e uma rede externa, com o objetivo de proporcionar uma camada a mais de segurança.
  - Também chamada de **DMZ** (De-Militarized Zone).
- Bastion Host
  - Um computador que precisa ser altamente protegido, pois é suscetível a sofrer ataques.
  - O bastion host é um computador exposto simultaneamente a Internet e a rede interna.

Exemplo de DMZ



Roteador Interno (Choke Router)

- Protege a rede interna da rede externa e da rede de perímetro (DMZ).
- É responsável pela maioria das ações de filtragem de pacotes do firewall.

Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	*	*
permitir	In	tcp	*	interno	*	> 1023	1
negar	*	*	*	*	*	*	*

EXEMPLO DE REGRAS PARA O CHOKE ROUTER

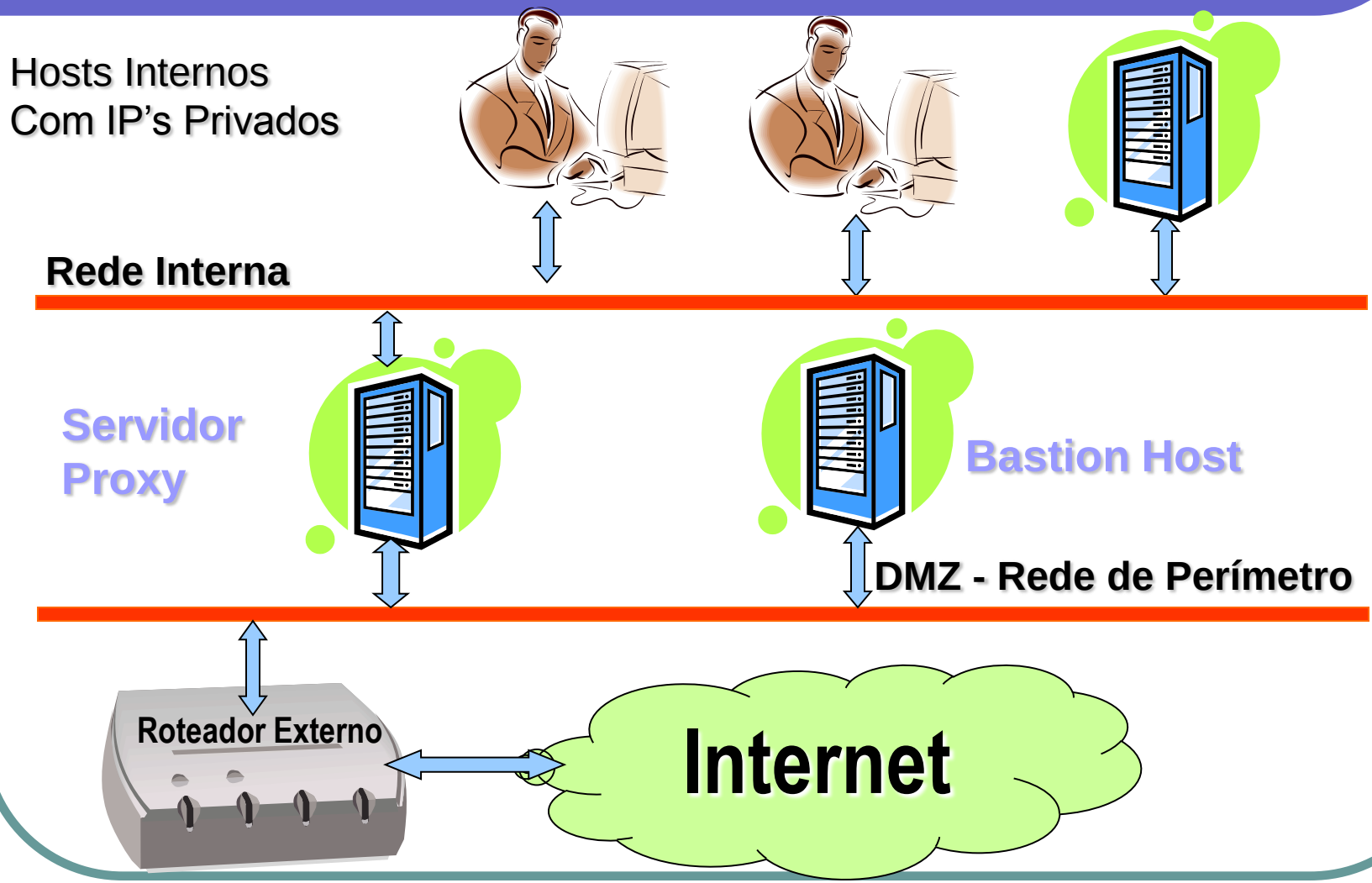
Roteador Externo (Access Router)

- Protege a rede interna e a rede de perímetro da rede externa.
- Muitas vezes, a função o roteador externo está localizado no provedor de acesso.
- Em geral, utiliza regras de filtragem pouco severas.

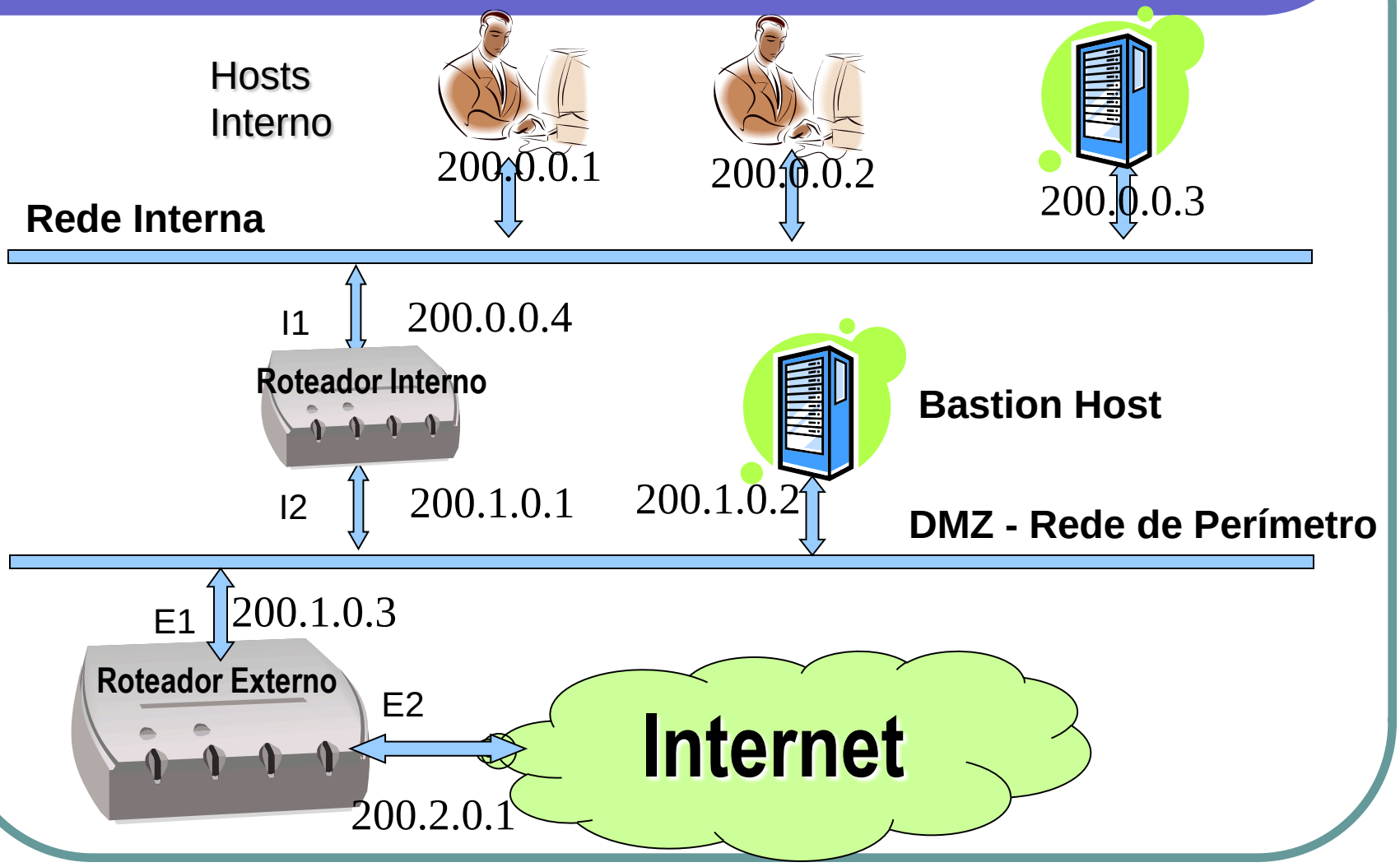
Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	*	*
permitir	In	tcp	*	interno	*	> 1023	1
permitir	In	tcp	*	dmz	> 1023	*	*
permitir	Out	tcp	dmz	*	*	> 1023	*
negar	*	*	*	*	*	*	*

EXEMPLO DE REGRAS PARA O ACCESS ROUTER

Rede de Perímetro com Proxy



EXERCÍCIO


Hosts
Interno
200.0.0.1
200.0.0.2
200.0.0.3
Rede Interna
I1
200.0.0.4
Roteador Interno
Bastion Host
I2
200.1.0.1
200.1.0.2
DMZ - Rede de Perímetro
E1
200.1.0.3
Roteador Externo
E2
Internet
200.2.0.1

DEFINIÇÃO DAS ROTAS

- Indique as Rotas que Devem Existir:

- A) Computadores da Rede Interna
- B) Roteador Interno
- C) Bastion Host
- D) Roteador Externo

EXERCÍCIO

- Defina as regras para filtragem de pacotes dos roteadores da arquitetura DMZ para:
  - A) Permitir aos computadores externos acessarem o serviço HTTP no bastion HOST.
  - B) Permitir aos computadores externos acessar o serviço SMTP no bastion HOST.
  - C) Permitir aos usuários internos acessarem o serviço POP, SMTP e HTTP no bastion HOST.
  - D) Permitir aos usuários internos acessarem qualquer servidor HTTP externo.
  - E) Proibir todos os demais acessos.

Roteador Interno

AÇÃO	INTERFACE	PROTOCOLO	IP ORIGEM	IP DESTINO	PORTA ORIGEM	PORTA DESTINO	FLAG ACK

Roteador Externo

AÇÃO	INTERFACE	PROTOCOLO	IP ORIGEM	IP DESTINO	PORTA ORIGEM	PORTA DESTINO	FLAG ACK