Firewalls

Objetivos

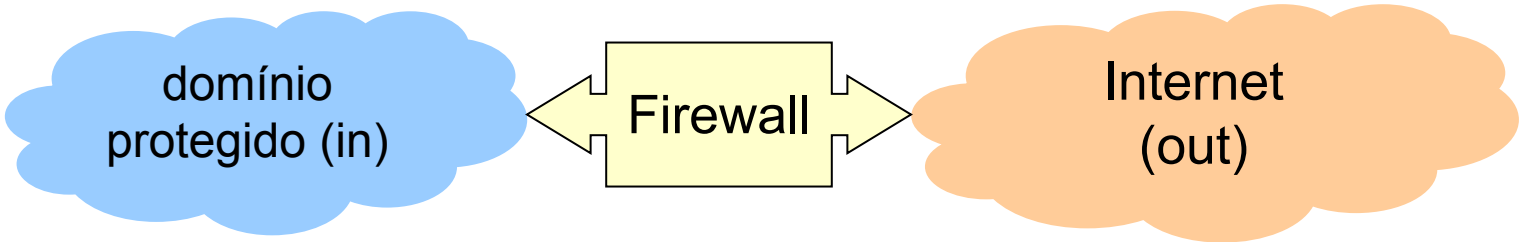
- **É um elemento indispensável na ligação de um domínio de rede**
  - Controlo de acesso
  - Controlo de fluxo
  - Controlo de conteúdos

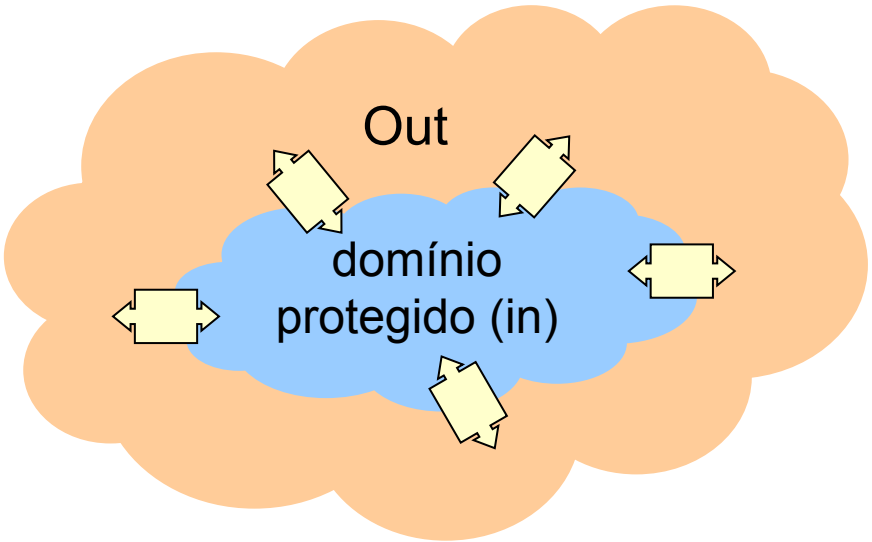
- **Concretização centralizada de políticas de segurança**
  - Minimiza o impacto de vulnerabilidades locais
    - Conhecidas ou desconhecidas
  - Facilita a tomada de posições mais drásticas
  - Centraliza a deteção de problemas
    - e o seu tratamento

Definição (Cheswick & Bellov)

- **Elo de ligação entre redes**
  - de um perímetro protegido (conjunto de redes e máquinas)
  - a uma rede insegura (Internet)
- **Conjunto de componentes**
  - Hardware e software
- **Propriedades**
  - Está no caminho de todo tráfego in <-> out
  - Controla o tráfego que por ela passa
  - É imune à penetração (por definição)

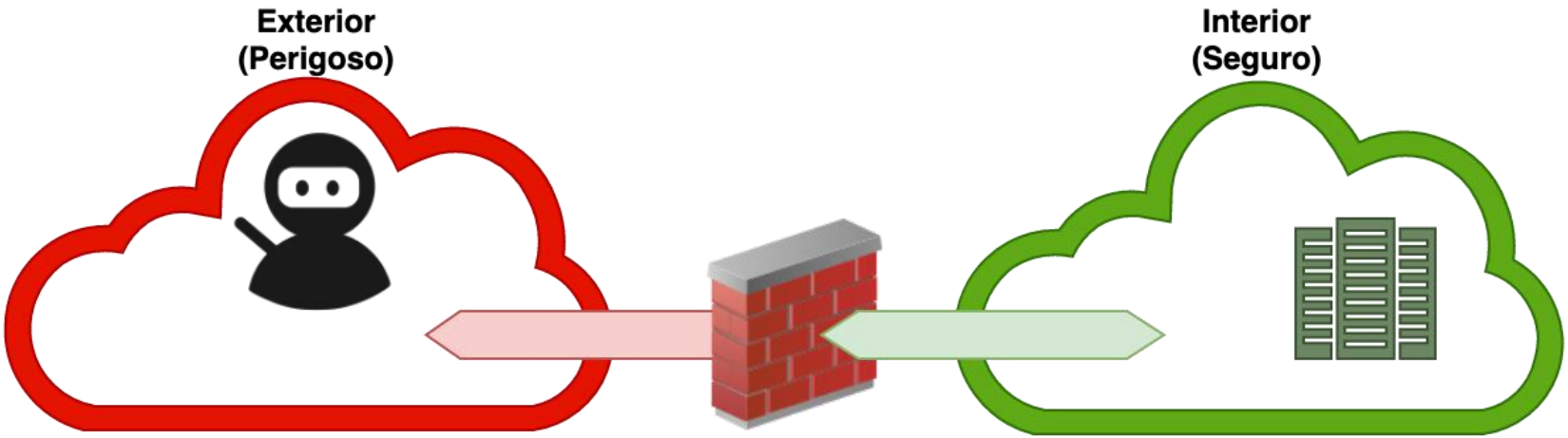
Definição (Cheswick & Bellov)





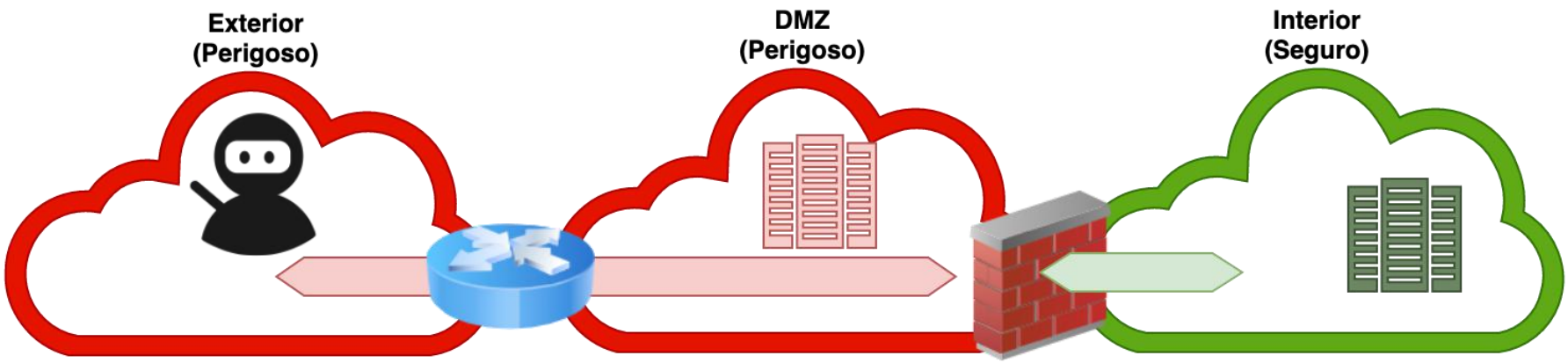
- **Supervisão de toda a comunicação in <-> out**
  - Controlo
    - do uso dos recursos protegidos por máquinas exteriores
    - do uso da rede exterior pelas máquinas do perímetro protegido
  - Defesa
    - contra ataques externos ao domínio protegido
    - contra ataques iniciados no interior lançados para o exterior
- **Acionamento de mecanismos próprios de gateways**
  - Para esconder a estrutura do perímetro protegido
    - NAT (Network Address Translation)
      - Masquerading e Port forwarding
  - Para estender o perímetro de segurança
    - Encapsulamento seguro (VPN)

Estrutura Genérica



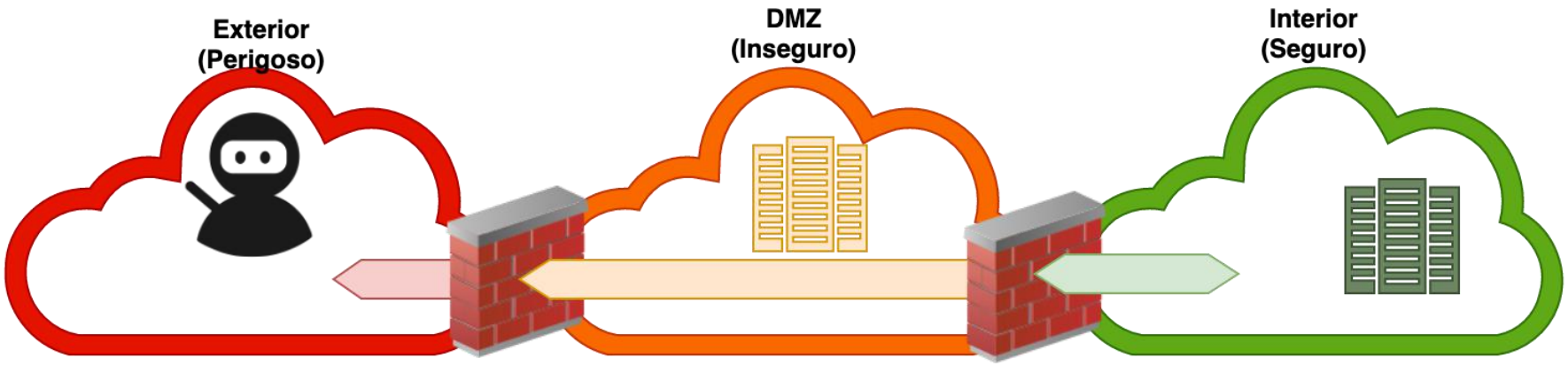
- **Defesa em perímetro (do domínio)**
  - Pode fazer parte de uma estratégia de defesa em profundidade
- **Considera um ambiente inseguro e um seguro**
  - Fora: outros domínios ou a Internet
  - Dentro: rede interna
- **Um único servidor = Bastião**

Estrutura Genérica



- **DMZ: DeMilitarized Network ou Perimeter Network**
  - Rede insegura
  - Contém servidores expostos ao mundo
    - Por vezes necessário para utilizar serviços/aplicações específicas

Estrutura Genérica



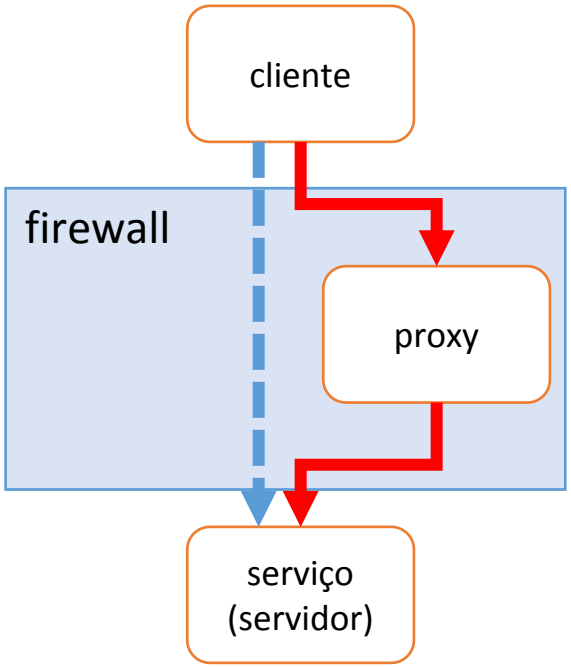
- **DMZ pode possuir alguma proteção**
  - Sistema de duas Firewalls com regras diferenciadas
- **Firewall externa: bastante permissiva**
  - Controla acesso a todas as redes
- **Firewall interna: mais restrita**
  - Controla acesso à rede interna

Tipos: Filtros de Pacotes

- **Rejeitam interações não autorizadas segundo o conteúdo dos datagramas IP**
  - Endereços IP (de origem e/ou destino)
  - Opções dos cabeçalhos IP/transporte
  - Protocolos e portos de transporte (origem e/ou destino)
  - Sentidos de criação de circuitos virtuais
  - Dados enviados através do protocolo de transporte
  - Dimensão dos datagramas
- **Podem analisar comportamento de fluxos**
  - exemplo: detetar port scans (com nmap)
- **Normalmente suportadas por componentes do núcleo do SO**
  - Exemplo: iptables, ipfw, pf

Tipos: Gateways Aplicacionais

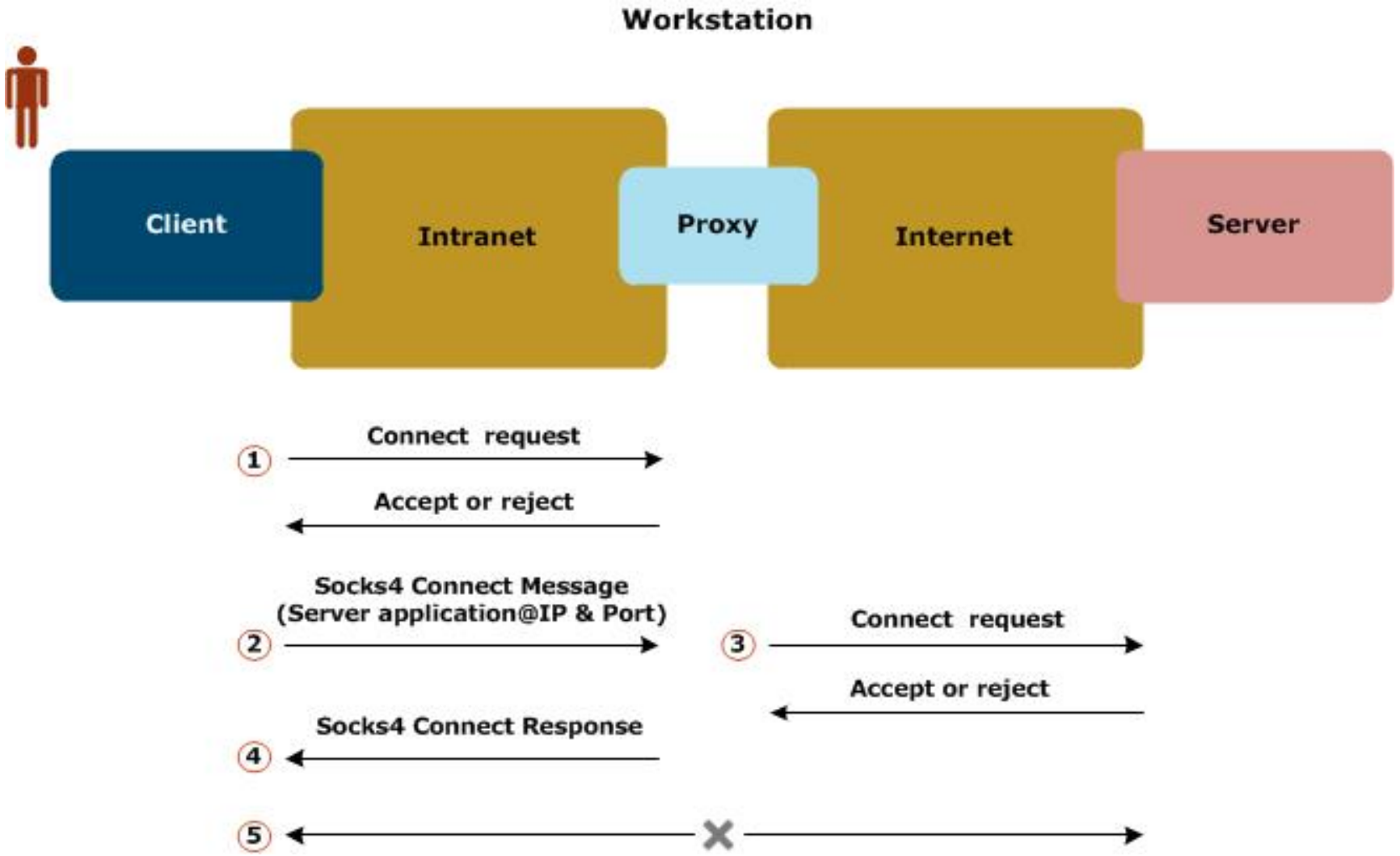
- **Controlam interações ao nível aplicação**
  - Mas transparentes para as aplicações interatuantes
  - Existe normalmente uma firewall diferente por protocolo
    - Protocol proxy
- **Cliente -> Proxy -> serviço (servidor)**
  - Os proxy são servidores
- **Aspetos da operação de um proxy**
  - Controlo de acesso por utilizador
  - Análise e alteração de conteúdos
  - Registo (logging) detalhado
  - Representação (proxying)
    - Substituição transparente de um dos interlocutores



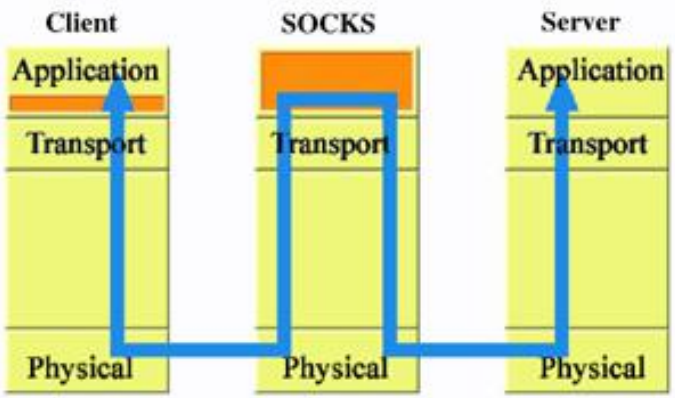
Tipos: Gateways de Circuitos

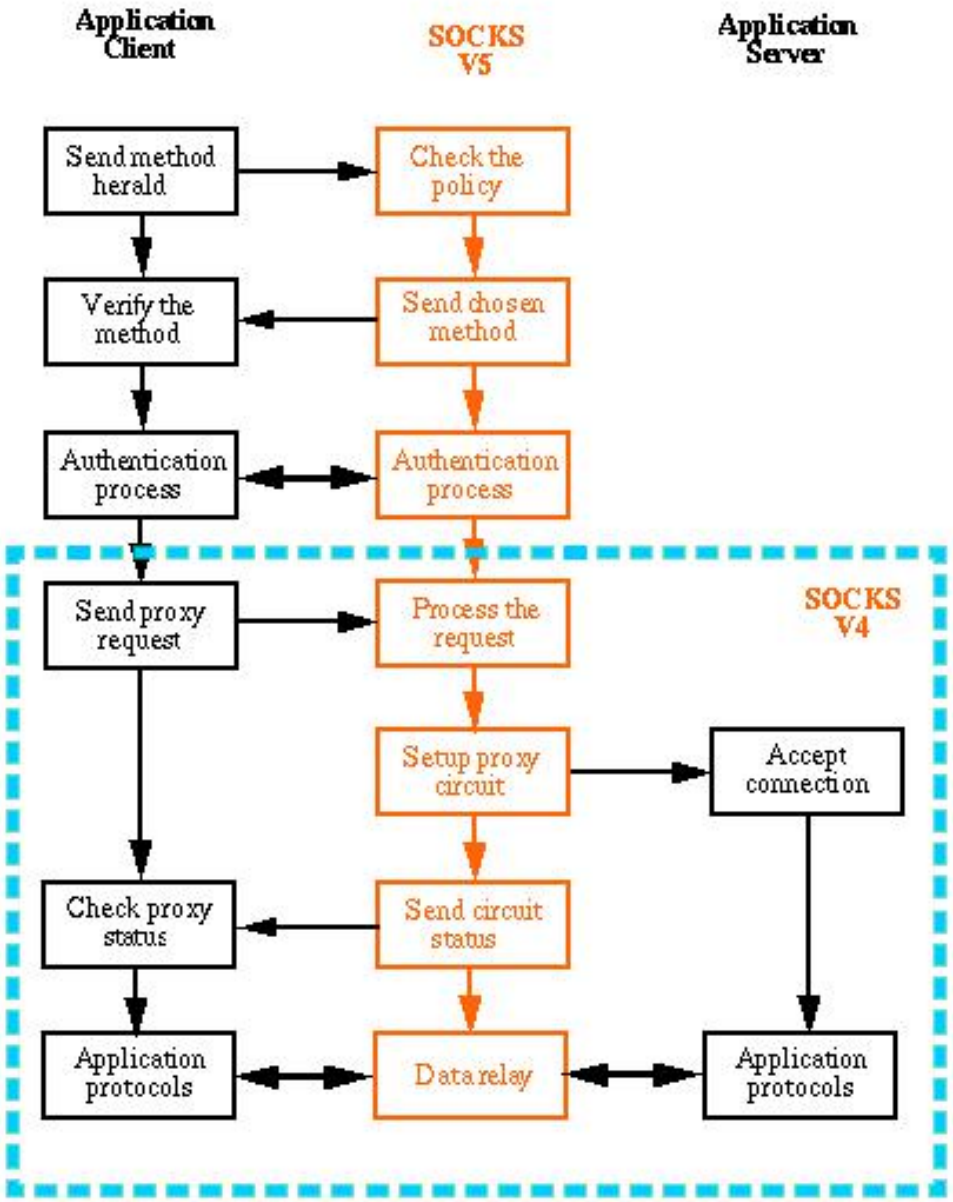
- **Espécie de gateway aplicacional**
  - Contactadas diretamente pelos clientes
- **Interposição não transparente**
  - Para autenticação e autorização próprias
- **Normalmente requer a alteração das aplicações clientes**
  - Exemplos: SOCKS e Proxy HTTP

Tipos: Gateways de Circuitos



SOCKS


Client
SOCKS
Server
Application
Transport
Physical
Application
Transport
Physical
Application
Transport
Physical


Application Client
SOCKS V5
Application Server
Send method herald
Check the policy
Verify the method
Send chosen method
Authentication process
Authentication process
SOCKS V4
Send proxy request
Process the request
Setup proxy circuit
Accept connection
Check proxy status
Send circuit status
Application protocols
Data relay
Application protocols

Tipos: Filtros de Pacotes com Contexto

- **Filtro de pacotes dinâmico (ou com contexto)**
  - Espécie de filtro de pacotes com contexto histórico
  - O contexto é fundamental para certas decisões
  - Termo comum: Stateful Packet Filter/Inspection (SPI)

- **Exemplos de contexto:**
  - Decisões tomadas para fragmentos de pacotes IP
    - Desfragmentação prévia à filtragem
  - Circuitos virtuais TCP estabelecidos
    - Os pedidos de estabelecimento de circuito são controlados
    - Os circuitos virtuais estabelecidos são permitidos
  - Tabelas NAT dinâmicas
    - Criação de entradas consoante o tráfego observado

Tipos: Filtros de Pacotes com Contexto

- **Exemplos de contexto (cont.):**
  - Interações pedido/resposta sobre UDP
    - Autorização dinâmica de respostas a pedidos autorizados
    - Exemplo: resolução de nomes DNS
  - Mensagens de erro ICMP
    - Relacionados com pacotes TCP / UDP antes enviados
  - Identificação de protocolos aplicacionais através do fluxo de dados
    - Para lidar com fluxos que usem portos dinâmicos ou "roubados"
    - Exemplos: FTP, protocolos RPC, protocolos P2P
    - Utilidade: filtragem, transparent proxying, QoS

Bastião

- **Deve executar versões seguras de sistemas operativos**
  - Com uma configuração segura
  - Tem instalados apenas os serviços essenciais
  - Proxy de Telnet, DNS, FTP, SMTP e autenticação

- **Servidores públicos não devem executar num bastião**
  - Exemplos: DNS, SMTP, HTTP, FTP, SSH, RAS, etc.
  - Devem executar em máquinas isoladas dentro de DMZs
    - Preferencialmente uma por serviço
  - O bastião apenas encaminha tráfego para as máquina apropriadas dentro de uma DMZ
    - E permite um tráfego limitado a partir das DMZ

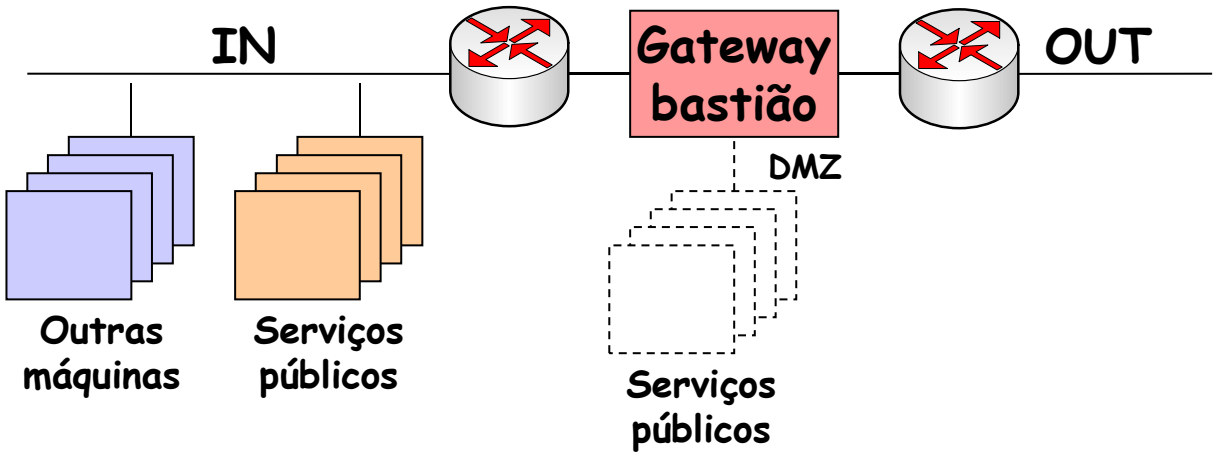
Bastião

- **Muitas vezes é plataforma para gateways aplicacionais**
  - Mas quanto mais proxies houver no bastião, menor será o seu desempenho
  - Os proxies podem ser executados em máquinas específicas
    - Security appliances
  - O bastião apenas encaminha tráfego de e para as appliances

- **Execução segura dos gateways aplicacionais**
  - Independência
    - O comprometimento de um não afeta os restantes
  - Sem privilégios especiais
    - O seu comprometimento não permite afetar a máquina

Topologia: Dual-homed (com ou sem DMZ)

- **Arquitetura**
  - Uma única máquina
  - Gateway bastião
  - Um par de routers adicionais
    - Para isolar o bastião de endereçamentos diretos
  - Servidores internos e públicos
- **Problemas**
  - O comprometimento do bastião desativa a firewall
  - A carga de processamento da firewall está toda sobre o bastião
  - Os serviços públicos estão dentro da rede protegida
- **Vantagens**
  - Simplicidade
  - Economia de recursos



Serviços de Segurança

- **Autorização**
  - De fluxos de dados (filtros de pacotes)
    - Nível transporte ou rede
  - De utentes (gateways aplicacionais / circuitos)

- **Redirecionamento de tráfego**
  - Para máquinas dedicadas
    - Serviços locais (e.g. mail, www, ftp, etc.)
    - Proxies em security appliances
  - Representação
    - Explícita (e.g. gateways de circuitos)
    - Transparente (e.g. traduções de endereços NAT)

Serviços de Segurança

- **Processamento de conteúdos aplicacionais**
  - Análise de conteúdos
    - Exemplo: deteção de vírus
  - Alteração de protocolos de alto nível
    - Exemplo: remoção de vírus

- **Comunicação segura**
  - Virtual Private Networks (VPNs)
    - Cifra e controlo de integridade de fluxos de dados sobre redes públicas (inseguras)
  - Encapsulamento (tunneling)
    - Extensão do domínio IP para nós distantes
    - ex. PPTP, L2TP, IPSec

Serviços de Segurança

- **Defesa contra tentativas de DoS**
  - Deteção de ataques
    - Volumes de tráfego anormais, de volume alto, etc...
  - Filtragem de datagramas perigosos ou mal formados
    - ex. Land attack, Ping-of-Death
  - Acionamento de medidas paliativas
    - ex. SYN flooding relay/semi-gateway

- **Defesa contra fugas de informação**
  - Deteção de tráfego anormal
  - Controlo do comportamento contra modelos conhecidos

Limitações

- **Não resolvem o problema dos atacantes dentro da rede interna**
  - A menos que a rede interna seja segmentada em múltiplas sub-redes
  - Os switches normalmente não suportam operações de uma firewall
  - As VLANs fornecem um segregação mínima (do tipo DMZ)
- **Eficácia Ť controlo de todas as ligações ao exterior**
  - Que podem ser feitas paralelamente de inúmeras maneiras:
  - PSTN & modems
  - WLANs & APs não cadastrados
- **Falta de controlo sobre interações camufladas/escondidas**
  - Interações camufladas multiplexadas por VPNs
  - Túneis IP sobre HTTP, ICMP, DNS, etc.
- **São difíceis de administrar em ambientes com interesses heterogéneos**
  - Universidades, ISPs

Firewalls Pessoais

- **Têm sido adotadas para a proteção de máquinas individuais / pessoais**
  - Defesa em profundidade vs. defesa de perímetro
- **Os donos podem definir políticas de controlo adicionais**
  - As aplicações autorizadas a aceder à rede
  - Os protocolos que as aplicações podem usar
  - As máquinas/redes que os protocolos/aplicações podem contactar
- **Reduzir o risco de compromisso entre máquinas de uma rede**
  - Permite que uma máquina se proteja independentemente da proteção dada pela sua rede
    - Não fazer assunções relativamente às demais proteções de rede
  - Úteis para máquinas que migram entre redes

Firewalls Pessoais: Problemas

- **Os utilizadores normais não são especialistas de segurança em redes**
  - Não percebem normalmente como funcionam as redes IP
    - Endereços IP, portos de transporte, protocolos de transporte, etc.
  - Não sabem avaliar se uma determinada interação é normal, aceitável, etc.
  - Não sabem as políticas de segurança elementares que devem aplicar
- **Bloquear interações suspeitas pode anular funcionalidades**
  - A comunicação em rede é atualmente banal
  - As aplicações não informam os utentes das suas necessidades de comunicação

Firewalls Pessoais: Problemas

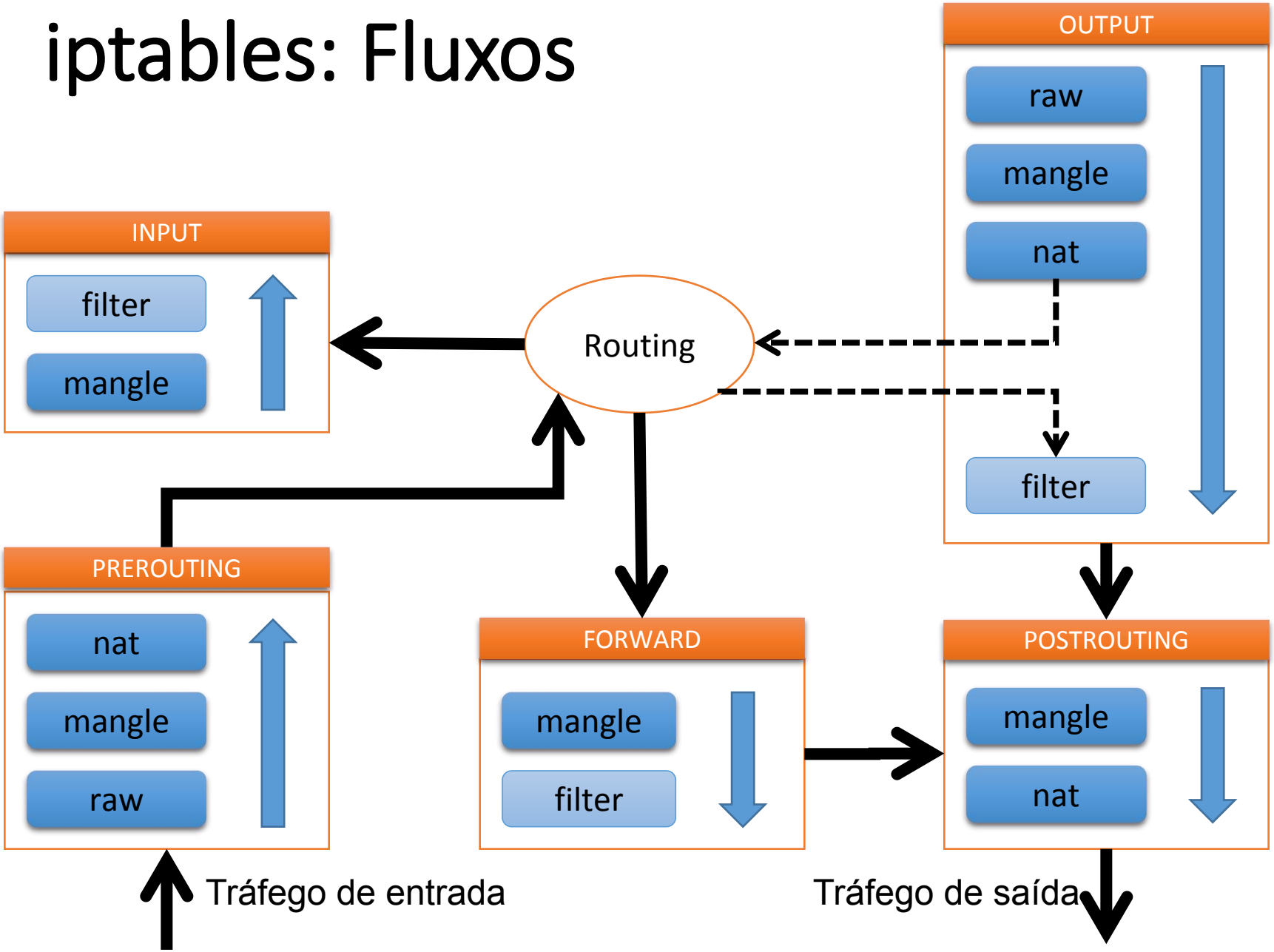
- **Complexidade operacional**
  - Diferentes ambientes operacionais -> diferentes políticas
  - Diferentes interfaces de rede -> diferentes políticas

- **A combinação de cenários operacionais, interfaces de rede e interações aceitáveis para cada caso levam a uma enorme quantidade de regas**
  - Confusão, incoerência -> difícil de detetar vulnerabilidades

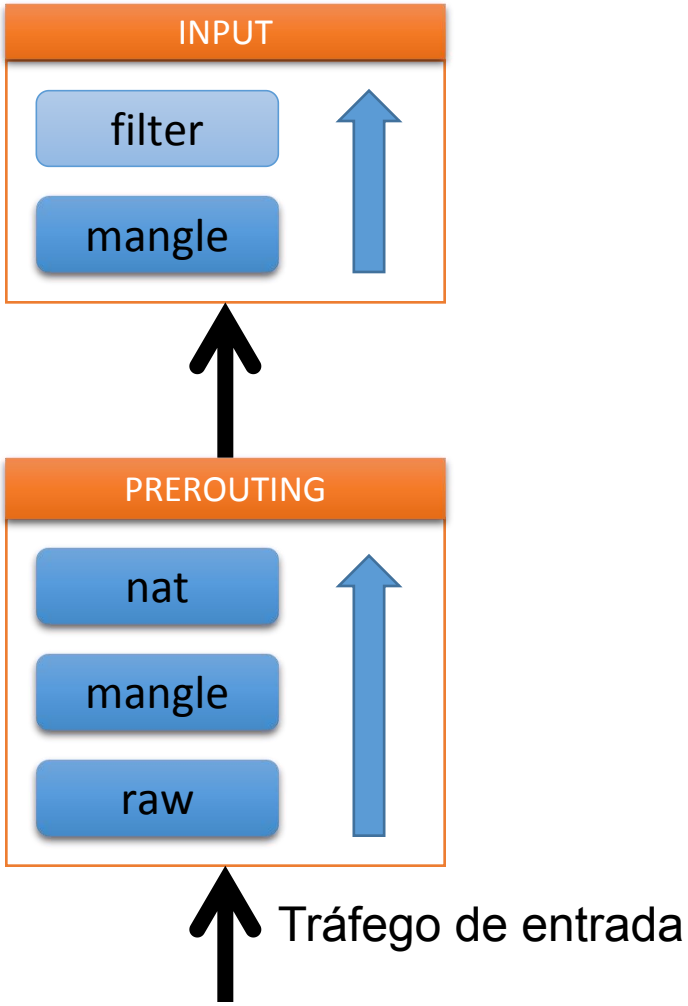
iptables

- **Filtro de pacotes (com contexto)**
  - Integrado com o TCP/IP do núcleo do Linux
  - Pode ser estendida de várias formas
    - Novos módulos do núcleo
    - Aplicações em modo utilizador
- **5 cadeias**
  - INPUT, OUTPUT, FORWARD
  - PREROUTING, POSTROUTING
- **4 tabelas (por cadeia, mas não para todas as cadeias)**
  - raw mangle, nat, filter
- **Vários módulos extra**
  - e.g. estado (seguidor de fluxos)

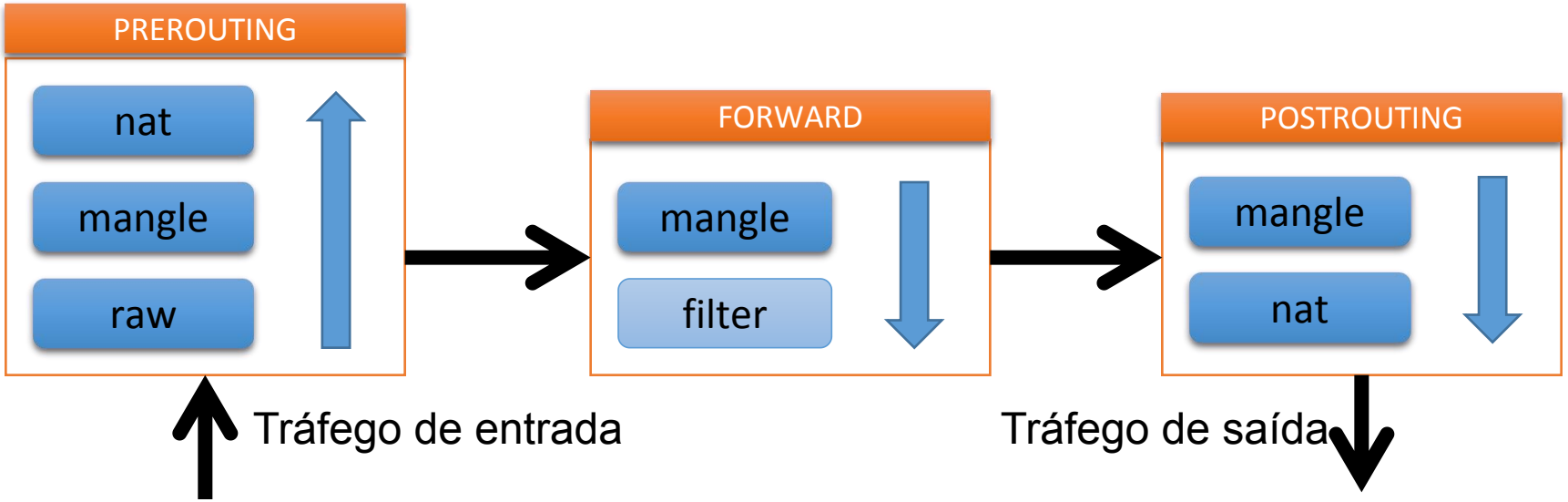
iptables: Fluxos



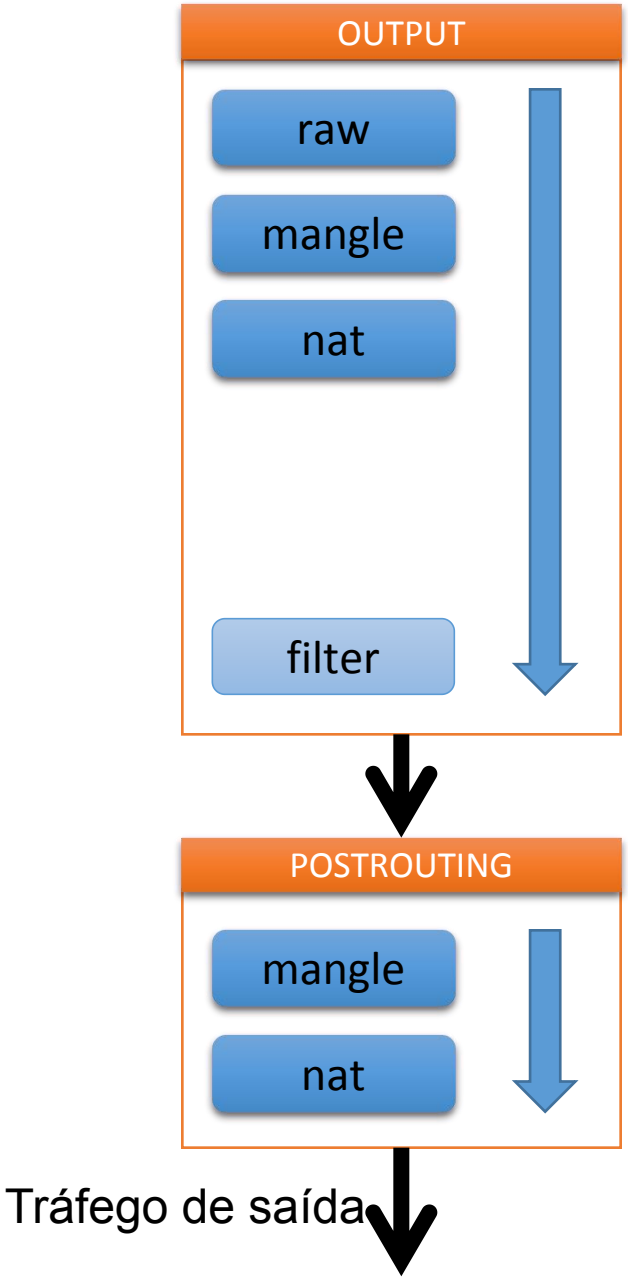
iptables: Tráfego para a máquina local



iptables: Tráfego reencaminhado



iptables: Tráfego originário na máquina local



iptables: decisões

- **Decisões base**
  - ACCEPT
    - Deixa o pacote prosseguir
  - DROP
    - Descarta o pacote
  - CONTINUE
    - Usar decisões de outras regras
- **Decisões reutilizáveis**
  - Novas cadeias
  - Saltar para uma nova cadeia
    - O nome da cadeia é a decisão
  - RETURN
    - Abandona a cadeia atual
- **Outras decisões**
  - LOG
  - MARK
    - Com marca interna
    - Útil para tomar decisões coerentes em diferentes cadeias
  - REJECT
    - Rejeição com mensagem de erro
  - SNAT, MASQUERADE
    - NAT da origem (masquerading)
  - DNAT, REDIRECT
    - NAT do destino (port fwd)
- **Ações por aplicações**
  - QUEUE

exploração de iptables: fail2ban

- **Agente que observa registos, comparando-os com padrões**
  - Pode prevenir alguns DoS, ataques por força bruta (SSH), scans
  - Reativo: Não previne o início do ataque
    - Pode não prevenir ataques com poucas interações
  - Pode ser utilizado com qualquer serviço que crie registos
- **Jail: um contexto composto por várias regras**
  - Define o que observar e que ação aplicar
- **Ação: implementação de uma resposta específica**
  - exemplo: bloquear comunicações na firewall
  - Pode usar uma firewall local ou remota
- **Filter: um conjunto de regexps que sinalizam um comportamento anómalo**
  - Composto por expressões a considerar e a ignorar (white list)

Importância das Firewalls

Extrema!

- **Os ataques a sistemas públicos são constantes**
  - Por atacantes especializados
  - Por aplicações autónomas
- **Sistemas nem sempre possuem mecanismos de segurança adequados**
  - Bloqueio após demasiadas tentativas incorretas
  - Validação das comunicações
  - Controlo de Acesso
- **Necessário aplicar mecanismos definidos pelo administrador, de acordo com políticas do domínio**
  - Programador de uma aplicação não tem conhecimento destas

exploração de iptables: fail2ban

- **Servidor “anónimo”, sem conteúdos.Núm. IPs bloqueados por tentativa de acesso a SSH**