Tecnologias de Redes de Computadores - 90293

Apresentação 14 – Proxies de rede

Pedro Gonçalves

pasg@ua.pt

Sumário

- Proxies
- Proxies web;
  - Configuração da Proxy HTTP Squid:
  - Definição de Access Control Lists no Squid.
  - Implementação de proxies transparentes.
  - Utilização de disco pela proxy Squid.
  - Requisitos da proxy http.
  - Resolução de problemas de configuração da proxy squid.
- Proxies inversos:
- Configuração de clientes da proxy web;

Razões para utilizer proxies

- Monitorização e filtragem
  - Software de controlo de conteúdos
  - Filtragem de conteúdos cifrados
  - Contorno de filtros ou de censura
  - Registo de utilização ou escuta

- Melhoria de performance
  - Racionalização da largura de banda de acesso à rede;
  - Aumento de rapidez no acesso à rede;
  - caching proxy acelera o acesso

- Tradução
  - Adaptação de conteúdos, de fornecedores
    - Em tese até tradução de língua poderia ser feita

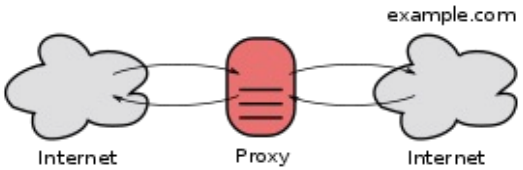
- Anonimização de acessos

- Controlo de acessos:
  - Controlo de tempo de acesso
  - Limitação das horas de acesso
  - Aumento de Segurança

Servidor proxy

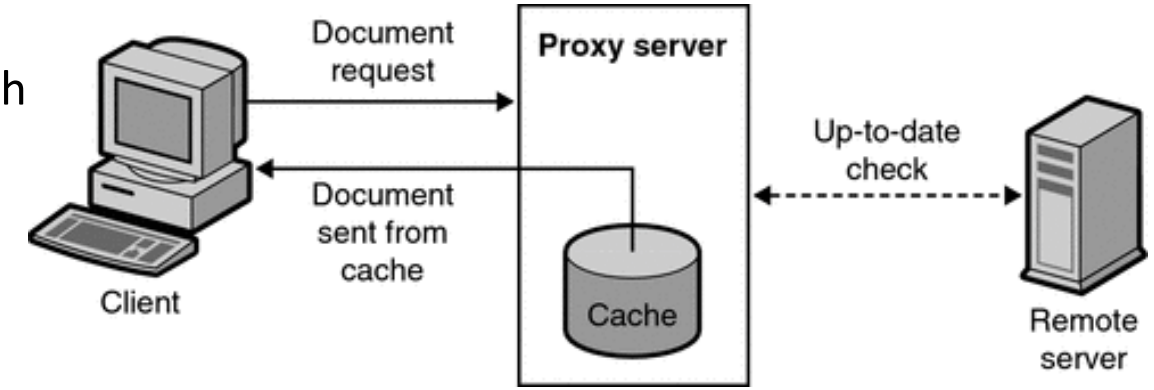
- Aplicação servidora que funciona como intermediária
  - Recebe pedidos de clientes
  - Reencaminha pedidos para servidores
- opera em nome do cliente pedindo os recursos, eventualmente escondendo o cliente.

- Analisa o pedido e obtém resposta
- Oferece um conjunto de vantagens como:
  - Balanceamento de carga, privacidade, ou segurança acrescida

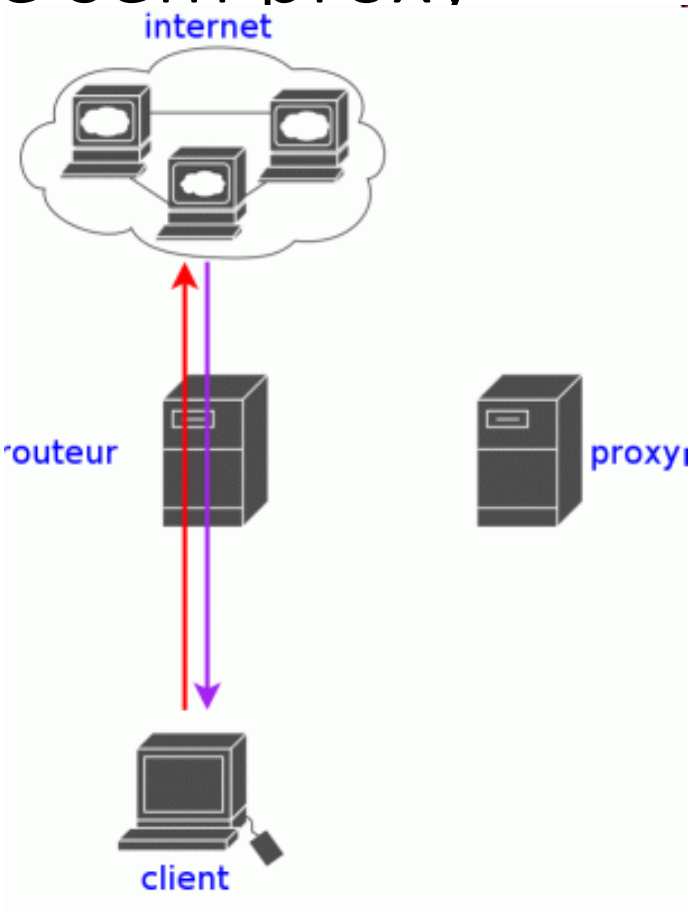


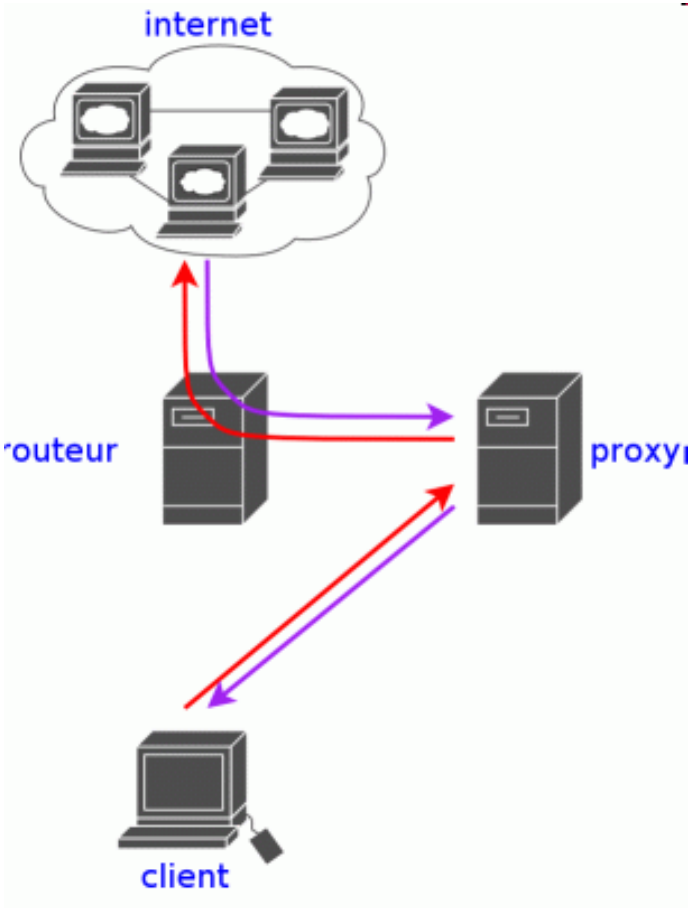
Cache server

- Pedidos são efetuados à proxy;
- Proxy pede ao exterior se não tiver.
- Faz cache da informação por algum tempo;
- Sempre que tiver informação em cach devolve-a sem pedir ao exterior;
-



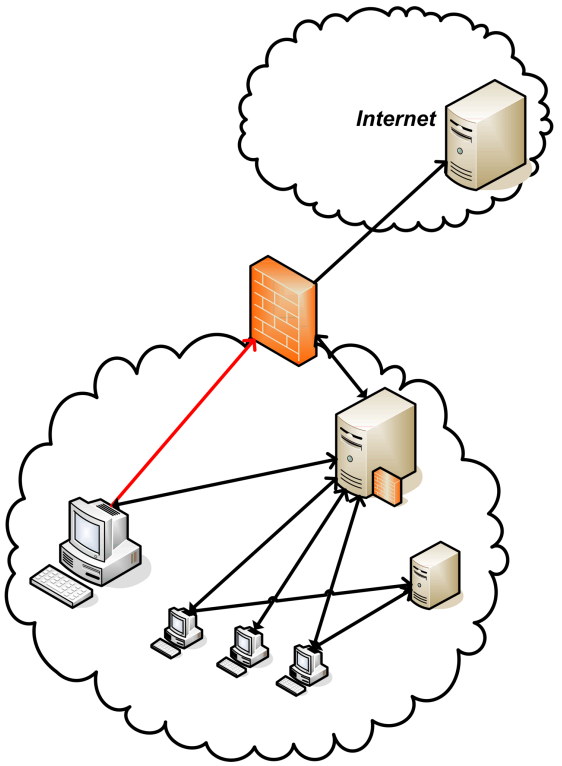
Com e sem proxy





Necessidade de integração

- Cliente tem que ser configurado para pedir à proxy
- Rede (firewall de rede) tem que proibir acesso direto
- Acesso ao interior é efetuado sem pedir à proxy.
- Eventualmente esquema de redirecção pode ser montado na firewall
  - Proxy transparente

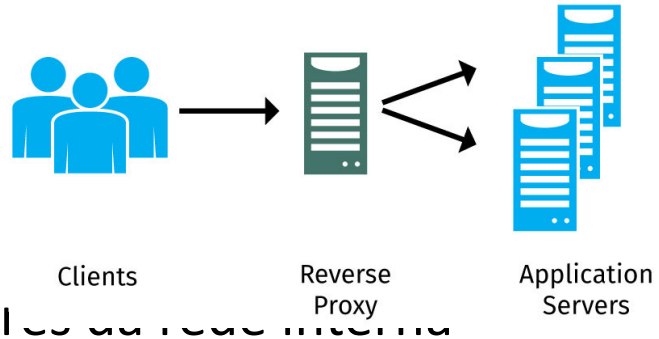


Reflecção

- Mas como é que as proxies se dão com HTTPS?

- E a utilização de HTTP está a ser abandonada....

Proxies inversas

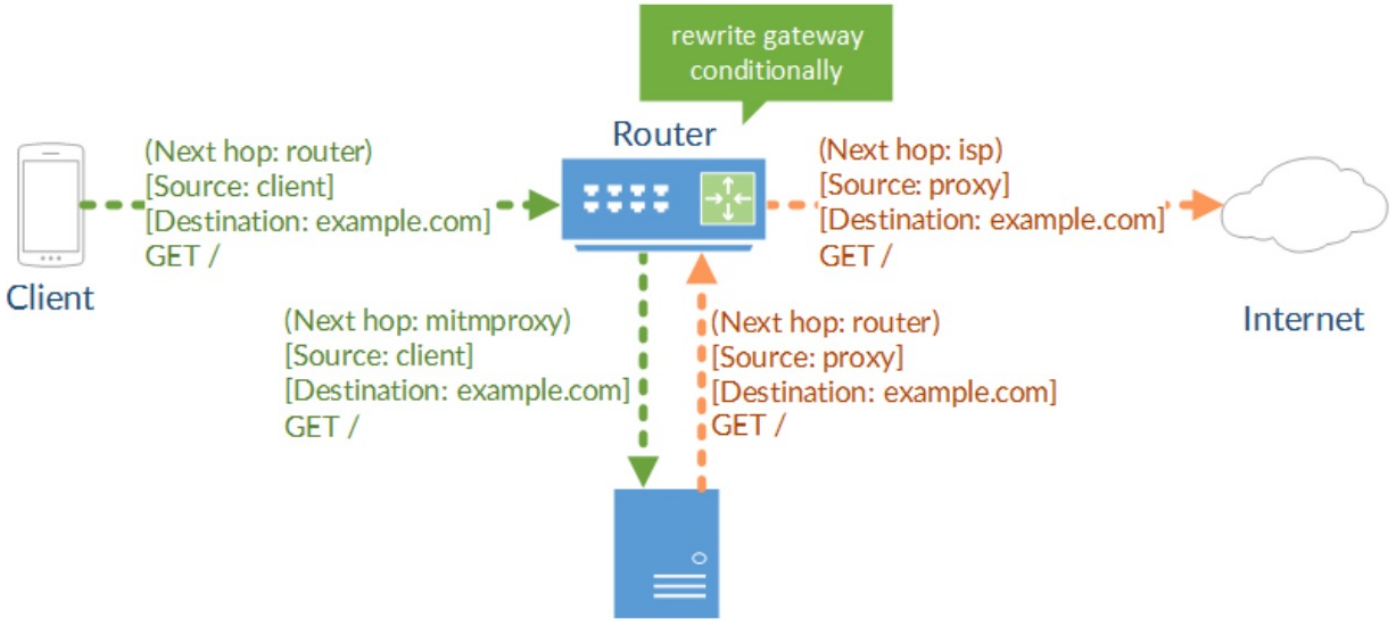


- Recebe pedidos da Internet e encaminha-os para servidores da rede interna
  - Clientes podem não conhecer recursos da rede interna
  - aparecem aos clientes como servidor vulgar
  - Resposta é devolvida como se viesse do servidor original
- Algumas razões para instalar reverse proxy servers:
  - Encryption/SSL acceleration: executa a criação de suporte Secure Sockets Layer (SSL) eventualmente usando hardware específico para o efeito, aliviando os servidores dessa carga.
  - Load balancing: o reverse proxy distribui os pedidos por vários servidores nesse caso reescreve os URL de cada página.
  - Serve/cache static content: o reverse proxy alivia os web servers fazendo cache de conteúdos estáticos como imagens e outros conteúdos gráficos estáticos.
  - Compression: o proxy server pode otimizar e comprimir o conteúdo para acelerar e diminuir o tempo de carga dos conteúdos
  - Segurança: fornece mais uma camada entre o servidor e o conteúdo

Transparent proxy

- Também conhecidas por intercepting proxy, inline proxy, ou forced proxy,
  - Intercepta comunicações sem requererem qualquer configuração do cliente
  - Clientes não precisam de ser configurados
  - Colocada entre clientes e Internet, e implementa funções de gateway ou router.
- Conceito definido na RFC 2616 (Hypertext Transfer Protocol—HTTP/1.1) :
  - "A 'transparent proxy' is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification". "A 'non-transparent proxy' is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering".

Transpatent proxy



Problemas associados

- Intercetar cria problemas à autenticação HTTP,
- Cria problemas às caches HTTP caches, existem pedidos e respostas que não podem ser armazenados (e.g. acesso ao email).
- Métodos de implementação:
  - Integrados em Router/firewall, eventualmente residentes na mesma máquina
  - Em rede que contenha firewall
    - Nesse caso requer que clientes sejam avisados do endereço e porto da proxy
    - Ou que firewall faça mangle dos pedidos – proxy transparente

- Métodos de deteção:
  - Comparação do endereço externo visto pelo servidor ou comparados pelos headers recebidos pelo server.
    - Utilização de serviço "What is my IP address"
  - Comparação da sequencia de hops (traceroute) para protocolos do como HTTP (port 80) e os que não são intermediados SMTP (port 25).[22]
  - Tentando aceder a um endereço que se saiba que não tem servidor web.
    - Proxy aceita ligação e vai tentar intermediar.
    - Quando descobre que não existe vai ter que dar erro e desligar a ligação
    - A situação nem deveria abrir o socket; se abriu há gato.

Configuração do SQUID

Configuração do Squid

- Configuração do squid em /etc/squid/squid.conf File

Access Control Lists

- # Add this to the bottom of the ACL section of squid.conf
- acl home_network src 192.168.1.0/24
- acl business_hours time M T W H F 9:00-17:00
- acl RestrictedHost src 192.168.1.23

- # Add this at the top of the http_access section of squid.conf
- http_access deny RestrictedHost
- http_access allow home_network business_hours

ACLs – acesso matinal

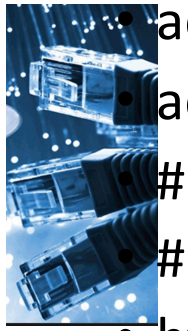
- #
- # Add this to the bottom of the ACL section of squid.conf
- #
- acl mornings time 08:00-12:00
- #
- # Add this at the top of the http_access section of squid.conf
- http_access allow mornings

Restringir alguns sites

- # File: /usr/local/etc/allowed-sites.squid
- www.openfree.org
- linuxhomenetworking.com
- # File: /usr/local/etc/restricted-sites.squid
- www.porn.com
- illegal.com

Restringir alguns sites a algumas horas

- # Add this to the bottom of the ACL section of squid.conf
- #
- acl home_network src 192.168.1.0/24
- acl business_hours time M T W H F 9:00-17:00
- acl GoodSites dstdomain "/usr/local/etc/allowed-sites.squid"
- acl BadSites dstdomain "/usr/local/etc/restricted-sites.squid"
- #
- # Add this at the top of the http_access section of squid.conf
- http_access deny BadSites
- http_access allow home_network business_hours GoodSites



Restricting Web Access By IP Address

- #
- # Add this to the bottom of the ACL section of squid.conf
- #
- acl home_network src 192.168.1.0/255.255.255.0
- #
- # Add this at the top of the http_access section of squid.conf
- #
- http_access allow home_network

E se os utilizadores não utilizam o proxy?

Forçam-se!

Making Your Squid Server Transparent To Users

- Utilização do squid como proxy sem que máquinas clientes tenham que ser informadas da sua existência.
- Firewall reencaminha o tráfego para o proxy.
- Configuração do squid:
- http_port 3128 transparent

Proxy transparente

- Até à versão 2.6
- httpd_accel_host virtual
- httpd_accel_port 80
- httpd_accel_with_proxy on
- httpd_accel_uses_host_header on

- A partir da versão 2.6
- http_port 3128 transparent

Proxy transparente: iptables

- iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 \
- -j REDIRECT --to-port 3128
- iptables -A INPUT -j ACCEPT -m state \
- --state NEW,ESTABLISHED,RELATED -i eth1 -p tcp --dport 3128
- iptables -A OUTPUT -j ACCEPT -m state \
- --state NEW,ESTABLISHED,RELATED -o eth0 -p tcp --dport 80
- iptables -A INPUT -j ACCEPT -m state \
- --state ESTABLISHED,RELATED -i eth0 -p tcp --sport 80
- iptables -A OUTPUT -j ACCEPT -m state \
- --state ESTABLISHED,RELATED -o eth1 -p tcp --sport 80

Squid Disk Usage

- Squid usa /var/spool/squid directory para arrumar a cache.
- Directório tende a acomular muita informação.
- Registo de utilização colocado em /var/log/squid/access.log
- que também cresce muito.
- Conteúdo periodicamente apagado.

Troubleshooting

- Squid faz log em:
- /var/log/squid/ directory
- O ficheiro squid.out guarda os erros de sistema da aplicação.
- Necessário ter cuidado com opções de filtragem esquecidas no ficheiro do configuração

- Apresentação não detalha todas as opções de configuração do squid. RFM!

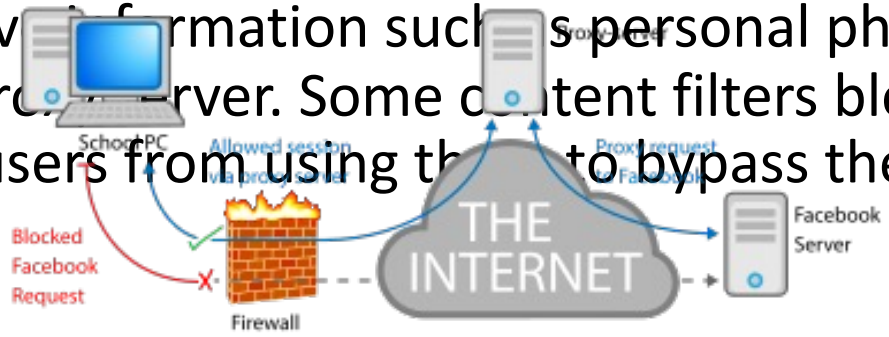
Reflecção

- Semelhanças entre proxies e network address translators
  - Conceito de proxy relaciona-se com camada acisa da pilha OSI (layer 7 application).
  - Network address translation (NAT) é semelhante a uma proxy que funciona na camada 3.
  - No NAT, configurar a gateway é suficiente.
  - O Cliente da proxu gera pedidos direccionados ao servidor, por isso precisa de ser configurado
    - Ou ser usado um proxy transparente

Reflecção

- Muitas redes bloqueiam o acesso a sites, por questões de segurança, trabalho, ou troas… Os utilizaodores contronam a proibição através de proxy servers comerciais de empresas que não conhecem, tipicamente estrangeiras.

- Sabendo que o tráfego passa a passer pelo servidor de proxy, há informações como fotos ou passwords que passam no servidor However, by connecting to proxy servers, they might be opening themselves up to danger by passing sensitiv[illegible]rmation such[illegible]s personal photos and passwords through the pro[illegible]rver. Some c[illegible]tent filters block proxy servers in order to keep users from using th[illegible] to bypass the filter.



Para continuarem a ler

- https://en.wikipedia.org/wiki/Darknet

E é tudo...

- Questões?
- Comentários?