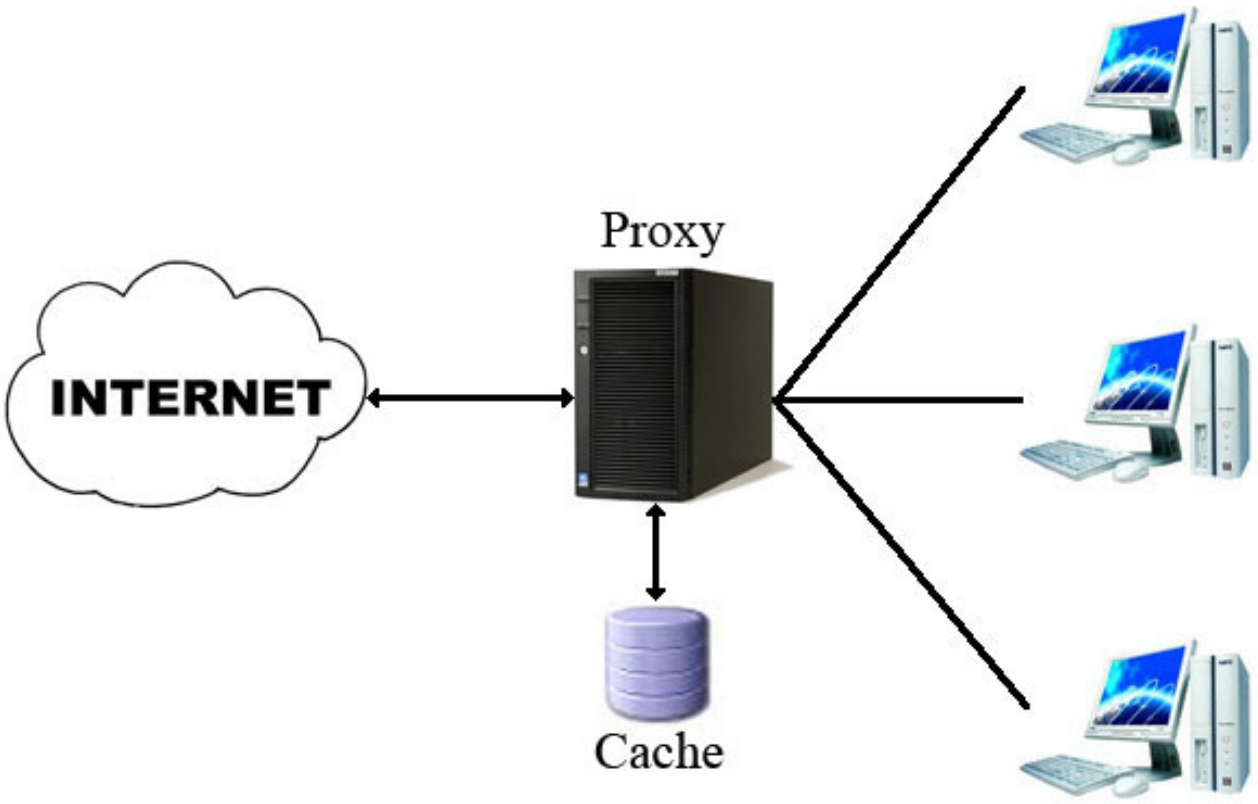
PROXY EM NÍVEL DE APLICATIVO

- Os servidores proxy foram desenvolvidos originalmente para colocar em cache as páginas Web que eram acessadas com frequência.
- Inicialmente o principal objetivo do proxy era eliminar os acessos redundantes (mesma página acessada diversas vezes, por pessoas diferentes, dentro de um mesmo local)

COMO FUNCIONAM OS PROXIES

- Os proxies funcionam ouvindo as solicitações por serviços oriundas de clientes internos e então enviando essas solicitações para a rede externa, como se o próprio proxy fosse o cliente de origem.
- Quando o servidor proxy recebe uma resposta vinda do servidor público, ele a retorna para o cliente original interno como se ele fosse o servidor público de origem da resposta.

ESQUEMA DE UM SERVIDOR PROXY



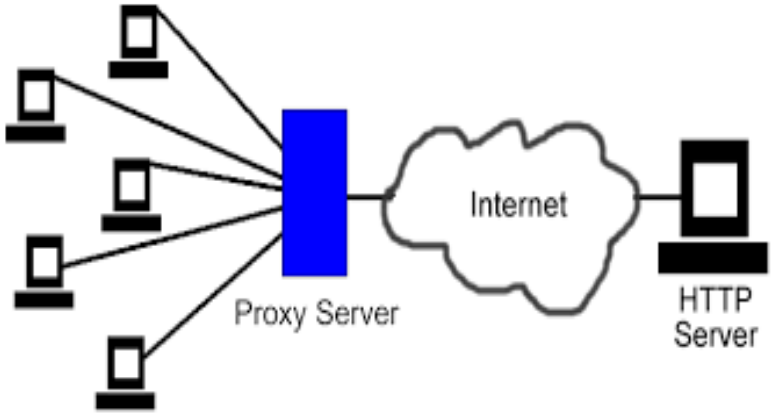
VANTAGENS RELATIVAS À SEGURANÇA DOS PROXIES

O servidor proxy oferece uma série de vantagens, como por exemplo:

- Os proxies ocultam os clientes privados de serem expostos externamente
- Os proxies podem bloquear URLs suspeitas ou consideradas perigosas
- Os proxies podem filtrar conteúdo suspeito ou perigoso como vírus e cavalos de Tróia antes de passá-los para o cliente

VANTAGENS RELATIVAS À SEGURANÇA DOS PROXIES

- Os proxies podem conferir a consistência do conteúdo retornado.
- Os proxies podem eliminar a necessidade de roteamento da camada de transporte entre redes
- Os proxies fornecem um único ponto de acesso, controle e monitoração



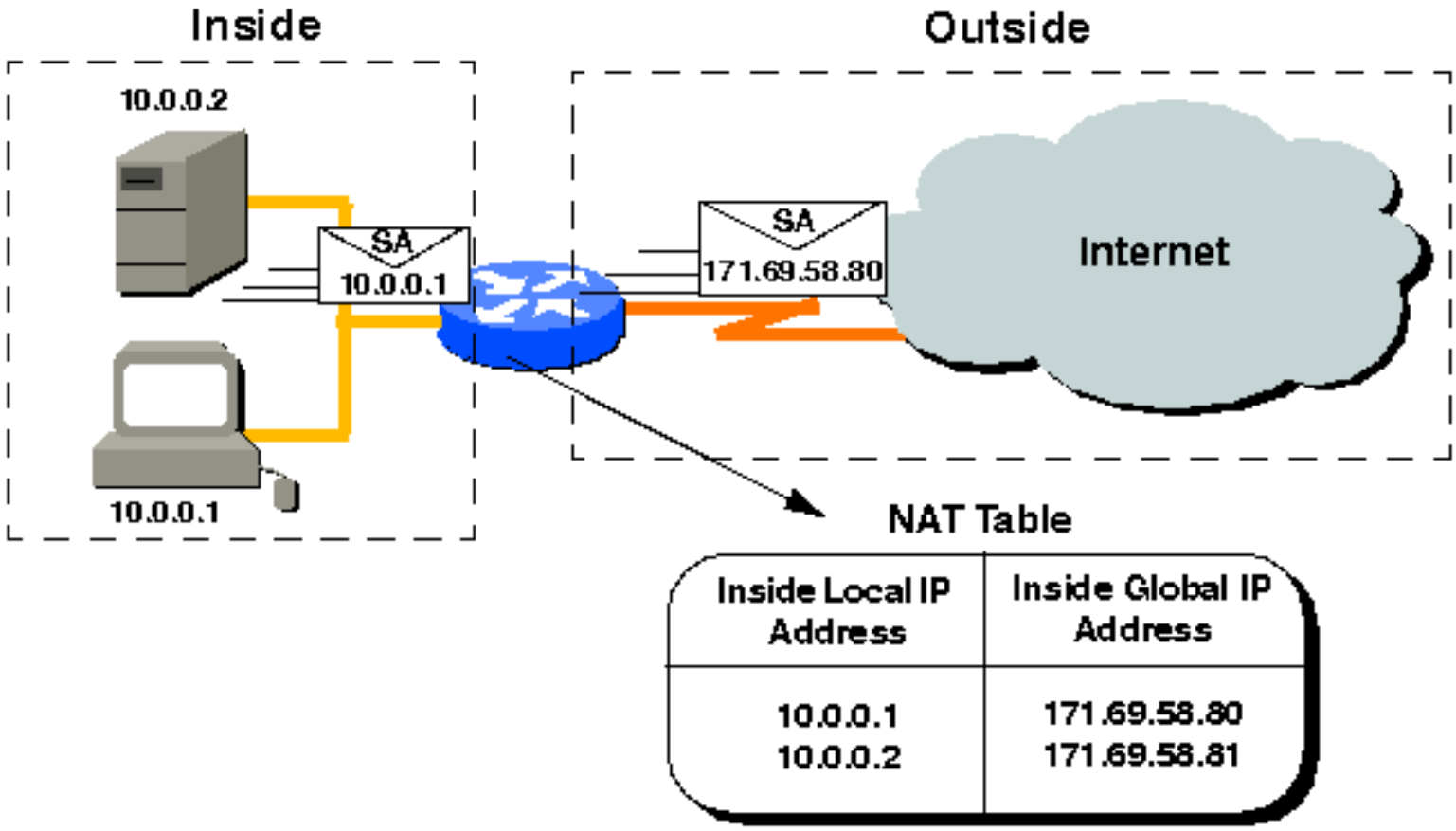
OCULTAMENTO DOS CLIENTES

- O recurso de segurança mais importante dos servidores proxy é o ocultamento dos clientes.
- Como no caso da NAT (Network Address Translation, conversão de endereços de rede), os servidores proxy podem fazer com que toda uma rede interna pareça ser uma única máquina vista da Internet porque somente uma única máquina passa as solicitações para a Internet.

Ocultamento dos clientes

- Como as NATs, os servidores proxy evitam que hosts conectem serviços a máquinas internas.
- No caso de servidores proxy, não existe nenhuma rota para os clientes porque os domínios de endereços das redes interna e externa podem ser incompatíveis e porque não existe roteamento da camada de transporte entre as duas redes.

NAT (Network Address Translation)



OCULTAMENTO DOS CLIENTES

- Outro aspecto do ocultamento de clientes é a multiplexação das conexões; um servidor proxy pode ser usado para compartilhar uma única conexão e endereço IP Internet em toda uma rede.

Bloqueio de URLs

- O bloqueio de URL permite aos administradores bloquear certos sites Web com base em seus URLs.
- Isso serve para impedir que os funcionários acessem sites Web não permitidos, sendo uma função facilmente implementada.
- Um problema desse método de bloqueio é a grande variedade de sites e a atualização constante da lista de endereços bloqueados.

FILTRAGEM DE CONTEÚDO

- O serviço proxy pode ser usado para pesquisar a informação útil em busca de conteúdo suspeito.
- O serviço proxy HTTP pode ser configurado para remover controles ActiveX, applets Java ou mesmo grandes imagens.
- O serviço proxy SMTP pode ser usado para remover anexos de e-mails com arquivos executáveis ou qualquer outro que possa representar riscos à segurança.

FILTRAGEM DE CONTEÚDO

- Os filtros também podem ser usados para verificar nas páginas Web a presença de certas palavras ou frases, que possam ser consideradas suspeitas ou não permitidas.

VERIFICAÇÃO DE CONSISTÊNCIA

- O teste de consistência refere-se à verificação do conteúdo de um protocolo para ter certeza de que há aderência ao mesmo.
- Ele garante que tipos de conteúdo especificamente mal formados não possam ser usados para explorar pontos fracos relativos à segurança na rede interna.

Bloqueio de rota

- Os pacotes de transporte não precisam ser encaminhados porque a solicitação é totalmente regenerada. Isso elimina ataques via camada de transporte como o roteamento de origem, a fragmentação e vários ataques do tipo recusa de serviço.
- O bloqueio de rota é uma das maiores vantagens do proxy, pois como nenhum pacote TCP/IP passa entre as redes interna e externa, muitos ataques são evitados.

Recursos de registro de ocorrência de alerta

- O proxy garante que todo conteúdo passe por um único ponto, fornecendo assim um ponto de controle central dos dados.
- Logs de registro de atividades e sites visitados podem ser obtidos através de prévia configuração.
- O recurso de alerta de alguns proxies podem avisar sobre ataques em andamento.

Desempenho dos proxies

Além da segurança, podem ofertar também melhorias no desempenho:

- Os proxies podem armazenar em cache os dados solicitados com mais frequência para melhorar o desempenho ao eliminar acessos redundantes.
- Os proxies podem equilibrar a carga dos serviços distribuindo-os por vários servidores internos.

Desvantagens relativas a utilização dos proxies

Algumas desvantagens:

- Os proxies podem criar um ponto de falha único
- O software cliente precisa ser capaz de trabalhar com proxy
- Precisa existir um proxy para cada serviço
- O proxy não protege o sistema operacional base
- As configurações padrão são otimizadas para desempenho e não para segurança

Ponto de falha único

- Inerente a um ponto de controle único está um ponto de falha único. Se um hacker puder desativar o proxy, toda a organização será afetada.
- Proxies, roteadores e firewalls sofrem desse mesmo problema em algum grau. Nos roteadores o problema é facilmente corrigido simplesmente tendo-se mais de uma rota para a internet.

Ponto de falha único

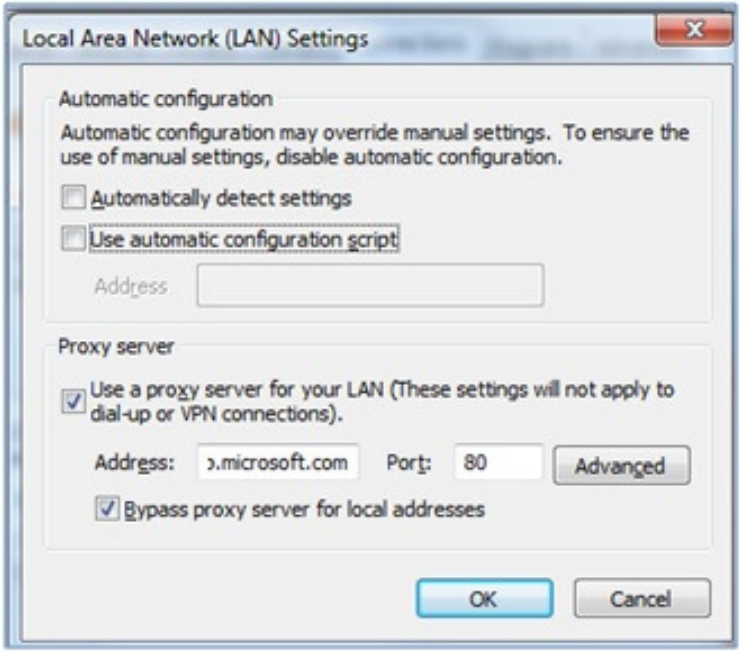
- Os firewalls são muito mais seguros que os proxies puros, porque eles incluem filtragem de pacotes de baixo nível para eliminar problemas causados por ataques do tipo de recusa de serviço.
- Os servidores proxy puros não incluem a funcionalidade de proteger a si próprios contra esses ataques, portanto são muito vulneráveis tanto à invasão quanto à recusa de serviço.

Ponto de falha único

- Um servidor proxy deve incluir os serviços de um filtro de pacote poderoso ou usar o mecanismo de filtragem de pacotes do sistema operacional.
- O filtro de pacote deve ser capaz de filtrar protocolos ICMP, IP, TCP e UDP.

Os clientes devem trabalhar com proxy

- Precisa existir um cliente com proxy habilitado para cada serviço com o qual se deseja trabalhar.
- Se o software cliente não suportar a configuração do proxy, o serviço proxy não poderá ser usado.



Um proxy para cada serviço

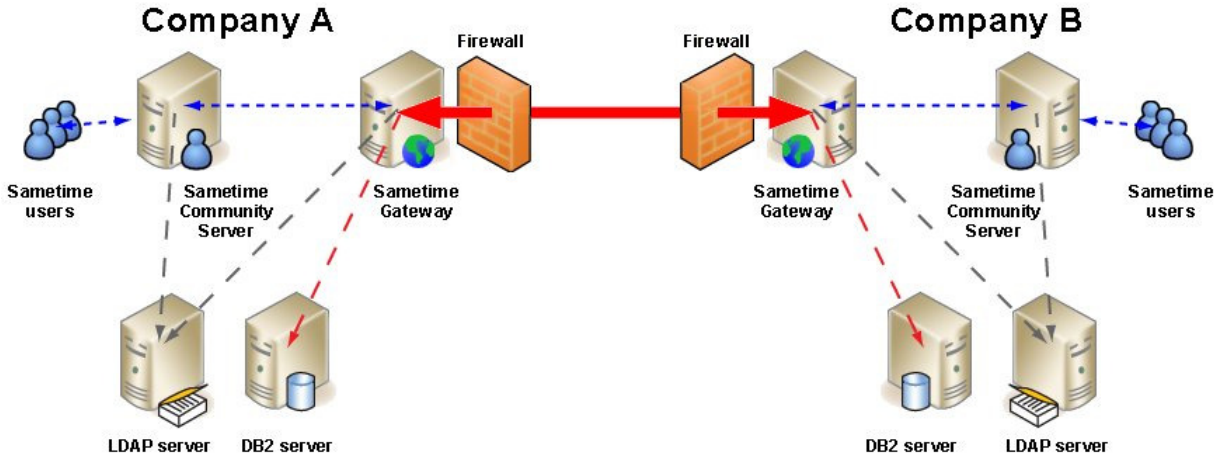
- Um serviço de proxy diferente é necessário para cada protocolo de serviço suportado.
- Os protocolos para os quais não existe um serviço proxy disponível não podem ser conectados.

CONFIGURAÇÕES PADRONIZADAS

- Muitos pacotes de software de servidor proxy sofrem devido a configuração padrão mal feitas que podem causar sérios problemas de segurança.

PROXY CRIA UM GARGALO NA REDE

- Como ocorre com os firewalls e os roteadores, uma única conexão do servidor proxy à Internet pode criar um gargalo se não for atualizada apropriadamente conforme o número de usuários da rede aumenta.



Melhores práticas para proxy

- O proxy é útil para diversos e diferentes propósitos e, por essa razão, a segurança frequentemente é deixada para trás dando-se mais atenção ao desempenho ou à multiplexação das conexões.

USE UM FIREWALL REAL

- Uma dica muito importante é usar a funcionalidade de proxy em um firewall ou colocar um firewall na frente do servidor proxy para protegê-lo.

Desativar o roteamento

- Se o proxy for usado como medida de segurança contra ataques na rede, certifique-se de desativar o roteamento por meio do proxy.
- Se o roteamento do proxy for permitido, este poderá endereçar diretamente qualquer cliente da rede, fato que é uma grande falha de segurança.

PROTEGER O SISTEMA OPERACIONAL

- A segurança do sistema operacional base é crucial para o uso eficaz do proxy como dispositivo de segurança.
- Se os hackers puderem explorar o servidor no qual executa o proxy, eles poderão reconfigurar a segurança do proxy para contorná-lo completamente.
- Use permissões de segurança com base nos usuários, filtragens de portas e protocolos em nível de S.O. para ter certeza de que o proxy esteja atendendo somente aos protocolos desejados.

DESATIVE O ACESSO EXTERNO

- Nunca permita que os clientes da rede externa usem o proxy através do servidor.
- Permitir acesso externo ao proxy do servidor torna possível aos hackers explorar o servidor proxy para ocultar suas conexões via IP e fazer com que pareçam vir do servidor proxy como a origem dos ataques perpetuados por eles.

DESATIVE SERVIÇOS EM EXCESSO

- Não deixe todos os serviços públicos na mesma máquina que o servidor proxy.
- Se um serviço como o FTP ou SMTP permitir que um hacker acesse o servidor proxy, ele poderá desativar a proteção fornecida pelo servidor proxy e ter acesso à rede.

Atividades de pesquisa

- Pesquisar sobre os principais proxies existentes no mercado, tanto Windows quanto Linux, suas principais funcionalidades, vantagens e desvantagens.
- Entregar na forma de um relatório.
- Pode ser feito em dupla.

Referências bibliográficas

STREBE, Matthew; PERKINS, Charles. **Firewalls**. Tradução: Lavio Pareschi; Revisão técnica: Alvaro Rodrigues Antunes. São Paulo: MAKRON Books, 2002

Squid
Proxy/Cache

Proxy / Cache

- Proxy
  - um agente que tem autorização para agir em nome de outro.
- Cache
  - local “disfarçado” para se preservar e esconder provisões (dados) que são inconvenientes para se transportar

O que é o *Squid* ?

- Agente que aceita solicitações de clientes (browsers) e as repassa aos servidores apropriados.
- Armazena uma cópia num cache de disco local
- Seu benefício só é sentido se o mesmo dado é requisitado várias vezes.

Squid

- É um programa proxy **HTTP** que faz cache (*caching proxy*), pois armazena os dados visitados
- Quais dados?
  - páginas HTML, sons, imagens (Objetos)
- Faz filtragem, mas não pode ser considerado como um sistema *firewall*.

Squid - Protocolos

- Desde que as requisições sejam enviadas por clientes via HTTP, Squid suporta (além de HTTP, obviamente):
  - FTP
  - *Gopher*
  - SSL (Secure Socket Layer)

Comunicação inter-cache

- Caches Squid “conversam” via UDP através dos protocolos:
  - HTTP: recuperar cópias de objetos de outros caches
  - ICP: *Internet Cache Protocol*. Tenta descobrir se um determinado objeto está em um determinado cache.
  - SNMP: Simple Network Management Protocol
  - *Cache Digest*. Recupera tabela de índices de objetos de outros caches.

Comunicação inter-cache

- Por que?
  - Base de usuário. Quanto maior a ‘user base’, maior a ‘hit rate’ (taxa de acerto). Grandes bases são possíveis se os caches cooperam
  - Redução de carga local
  - Espaço em disco. Cache usam muito (muito) disco...

Instalação

- Requisitos de hardware (em ordem decrescente de importância)
  - Disk Random Seek Time
  - Memória RAM
  - Throughput de disco sustentável
  - Poder de CPU

Quantidade de Disco

- Suponha um cache pessoal, com 1GB disco
- Navegação diária: 10 MB dados
  - 100 dias para encher o cache

  ⇒ taxa de entrada influencia quantidade de disco a alocar
- Decida a quantidade de disco segundo a quantidade de dados que vai passar pelo cache por dia.

Quantidade de Disco

- Seja uma linha de 1 Mbs. ->125000 bytes/s
- todos clientes acessando cache -> usaríamos disco na taxa de 125k por segundo -> 450 Mbytes por hora.
- Supondo maior parte do tráfego diário (8 hs)-> 3,6 GB por dia. Isso para 100% uso
- Vamos estimar, então, 2 GB Squid Cache, para cachear DIARIAMENTE os dados !

RAM

- Para otimizar busca, Squid utiliza memória para guardar tabelas do tipo Look-up.
- Cada objeto no disco consome cerca de 75 bytes de índice em RAM
- Média de um objeto na Internet 13 Kbytes. Supondo 1 GB cache -> 80000 objetos -> requerem 6 MB RAM.
- Um cache razoável (8 GB) requer 48 MB RAM !

Setup do Sistema

- Criar usuário e grupo squid
- Permissão de diretórios
  - ...../squid/bin; ../squi
    .../squid/logs; .....
- Executando ‘squid -
  (../squid/cache). Dev
  pode falhar.
- Faça isso manualmente

mkdir /usr/local/squid/cache
chown squid:squidadm .../cache
chmod770 .../cache

Para o impaciente ...

Editar /etc/passwd: squid:x:1004:103:Squid Proxy:/:

Editar /etc/group: squid:x:103:

cd /usr/local/squid

chown root:squid -R etc/ ; chmod 775 -R etc/

chown squid:squid -R var/ ; chmod 770 -R var/

./sbin/squid -z (cria o diretorio de cache em ./var/cache)

Configuração

- /usr/local/squid/etc/squid.conf

- porta http: http_port 3128
- local de cache: **cache_dir /usr/local/squid/cache/ 100 16 256**
  - 100 MB de cache; 16 diretórios, cada qual com 256 sub-diretórios

Configuração

- Usuários e grupos

  cache_effective_user squid *
  cache_effective_group squid *

- Lista de controle de Acesso
  - importante configurar
  - Lembre-se: por *default*, tudo é negado !!!!

* Obs: pode usar UID e GID default: **nobody**

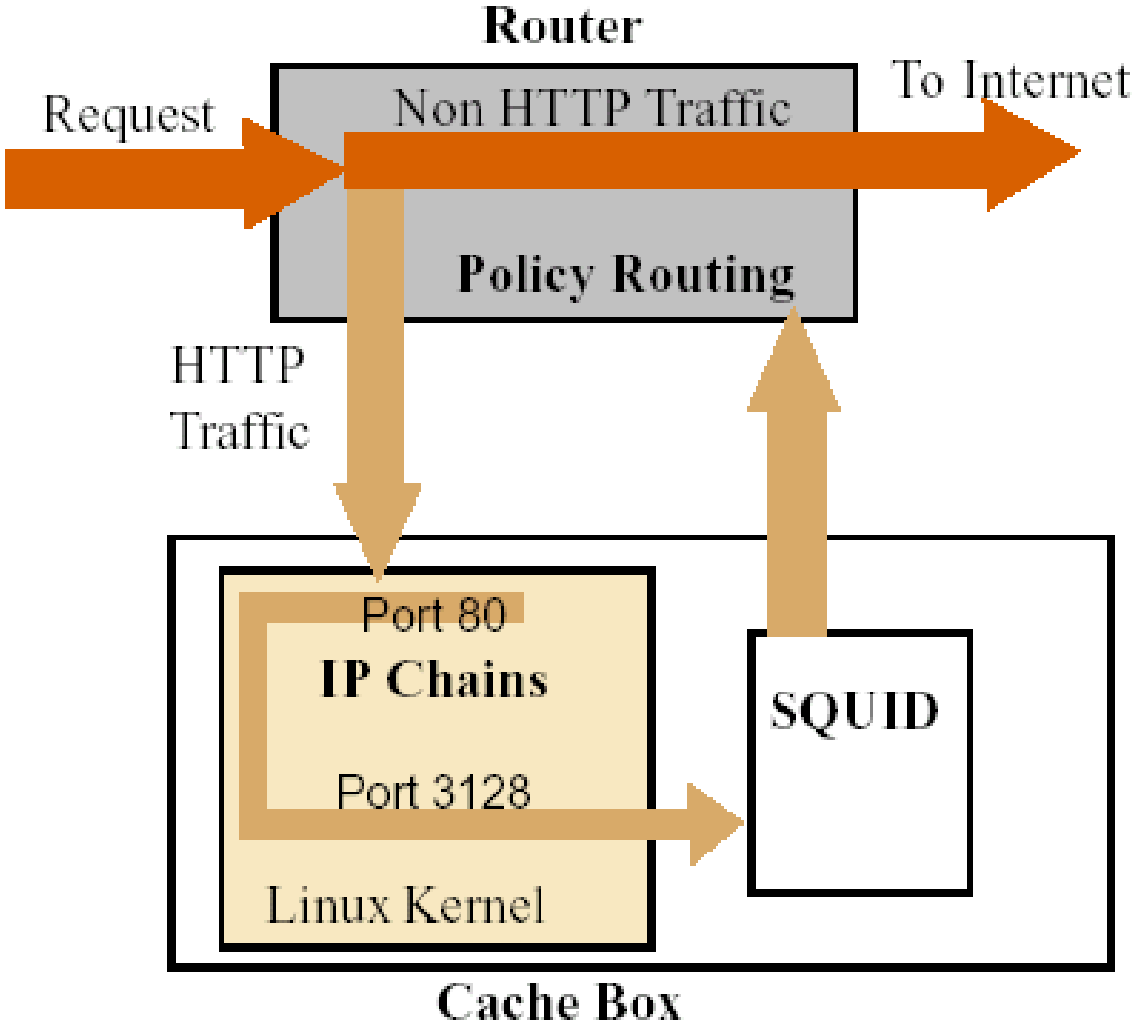
Proxy Transparente

- Clientes não precisam configurar o browser
- Squid se encarrega de interceptar os pacotes e colocá-los no cache.
- Setup é transparente, mas sua utilização não o é.
  - Há mascaramento de IPs. O IP origem do pacote será mudado !

Proxy Transparente

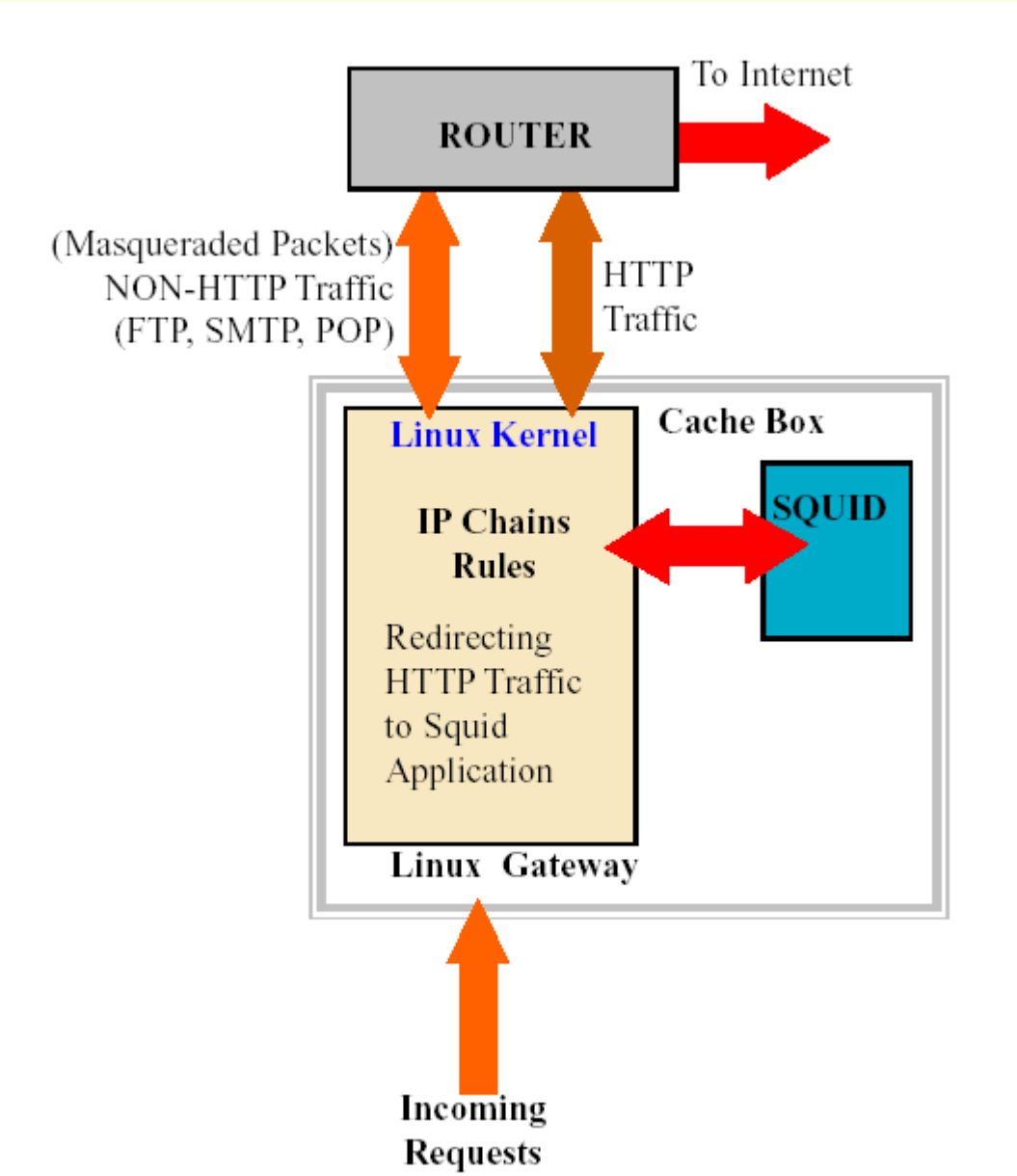
- Tipo de setup em que o squid roda na máquina que também é o gateway primário (uma possível configuração)
- É preciso:
  - configurar Kernel para transparência: redirecionar conexões porta 80 para squid
  - configurar squid (veja documentação)

Roteador que direciona tráfego IP para servidor proxy SQUID



Transparent Caching - Policy based routing

SQUID como um gateway



Configuração básica

- Redirecionamento da porta
  - iptables -t nat -A PREROUTING -p TCP --dport 80 -j REDIRECT --to-port 3128
- Modo transparente
  - httpd_accel_host **virtual**
  - httpd_accel_port **80**
  - httpd_accel_with_proxy **on**
  - httpd_accel_uses_host_header **on**

O Modo ‘Acelerado’

Accelerator mode

- Squid rodar na porta 80 !
  - Formato de requisições proxy muito semelhantes às HTTPs
    - Web Server pode agir como web cache.
- Suponha que um sítio use IIS como solução Web (http **e** proxy ambos na porta 80), mas quer colocar squid para melhorar desempenho do serviço de proxy ???

O Modo ‘Acelerado’

- Squid pode aceita requisições no formato servidor web (trilha+nome do arquivo, não inclui o endereço do host) e repassá-las a outros servidores (apache, IIS).
- Squid aceita solicitações na porta 80 e repassa para o servidor Web na porta 81 (por exemplo)
- Isso é o que chamamos de modo acelerado.