

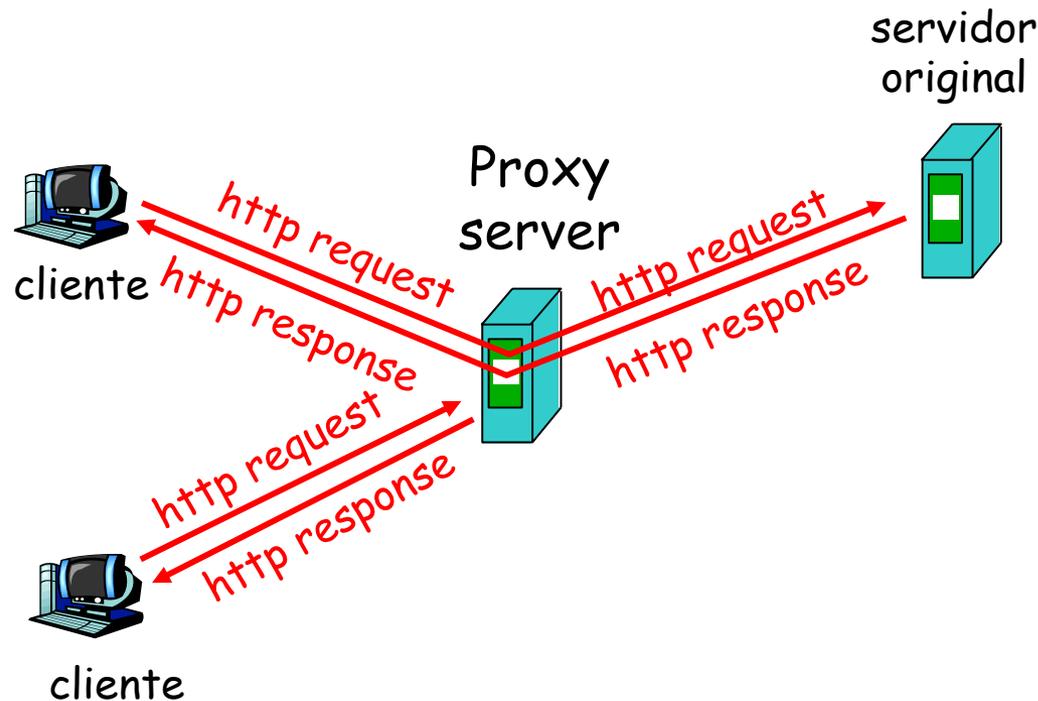
# Servidor Proxy



Prof. Dr. Márcio Andrey Teixeira  
Instituto Federal de São Paulo – Campus Catanduva  
Catanduva, SP  
Membro Sênior do IEEE  
[marcio.andrey@ifsp.edu.br](mailto:marcio.andrey@ifsp.edu.br)

# Web Caches (proxy server)

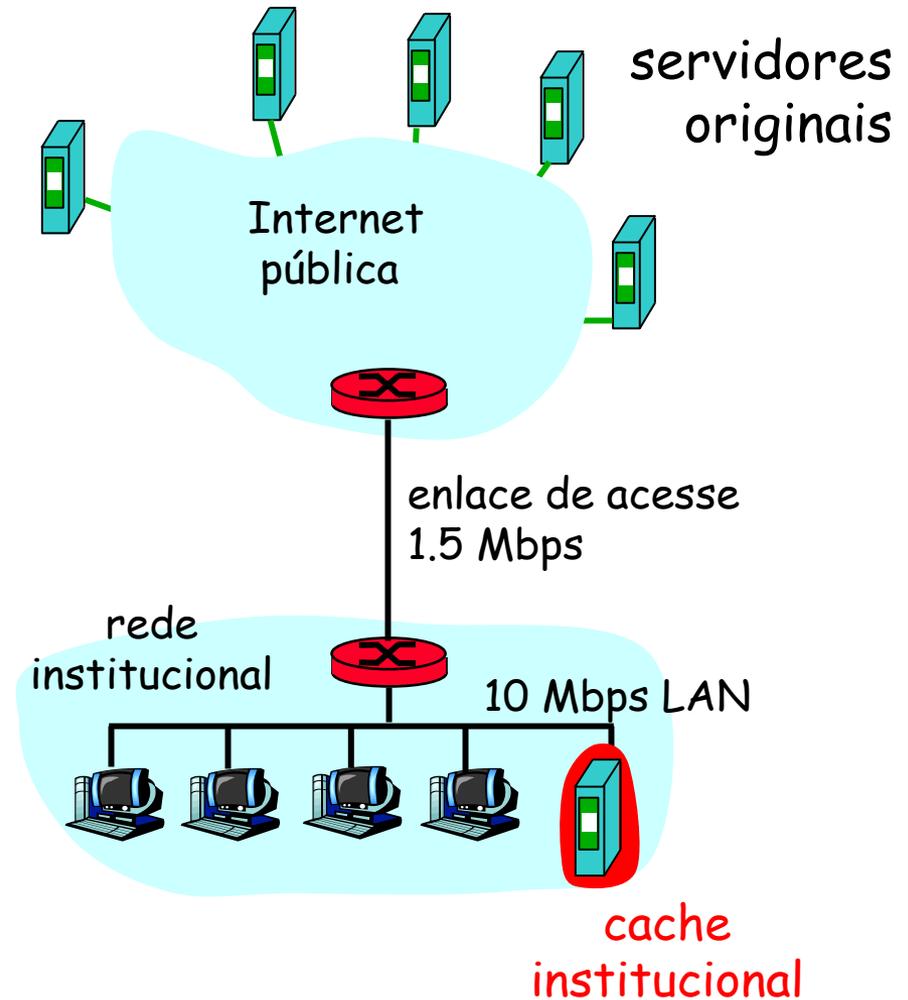
- **Objetivo:** atender o cliente sem envolver o servidor Web originador da informação
  - usuário configura o browser: acesso Web é feito através de um proxy
  - cliente envia todos os pedidos http para o web cache
    - se o objeto existe no web cache: web cache retorna o objeto
    - ou o web cache solicita objecto do servidor original, então envia o objeto ao cliente.



# Servidor Proxy

## Porque Web Caching?

- armazenamento está “perto” do cliente (ex., na mesma rede);
- menor tempo de resposta;
- reduz o tráfego para servidor distante
  - links externos podem ser caros e facilmente congestionáveis



# Servidor Proxy

## Configurando um servidor proxy (Web-Cache) com o Squid

O squid é um servidor proxy. Ele permite compartilhar a conexão entre vários micros, servindo com um intermediário entre eles e a internet.

Quando a internet é compartilhada, os micros passam a acessar a internet diretamente, sem restrições. O servidor de internet apenas repassa as requisições recebidas.

Com a utilização de um proxy, uma análise é feita em todo o tráfego de dados, verificando o que pode e o que não pode passar

# Servidor Proxy

Além disso, o proxy funciona com uma cache de páginas, no qual armazena informações já acessadas

Quando alguém acessa uma página que já foi carregada, o proxy envia os dados que guardou no cache, sem precisar acessar a mesma página repetidamente.

O Squid pode ser obtido em:

<http://www.squid-cache.org/>

# Servidor Proxy

## Instalação do squid

Para instalar o squid, execute o seguinte comando:

```
sudo apt-get install squid
```

O arquivo de configuração do squid está localizado em:  
`/etc/squid/squid.conf`

# Servidor Proxy

## Controle de acesso - ACL

O squid controla o acesso as páginas da internet através das chamadas ACL (*Access Control List*)

As ACLs permitem especificar endereços de origem e destino, domínios, horários, portas ou métodos de conexão ao *proxy*, que serão utilizados para negar, permitir ou negar acessos.

Sintaxe de uma ACL:

```
acl [nome_da_acl] [tipo_da_acl] {argumentos}
```

Exemplos:

```
acl minharede src 192.168.10.1/24
```

```
httpd_access allow minharede
```

# Servidor Proxy

## Configuração Básica

Para que o squid funcione, as seguintes linhas devem ser inseridas/descomentada no do arquivo de configuração:

```
http_port 3128
```

```
visible_hostname marcio-VirtualBox
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl rede_local src 192.168.10.0/24
```

```
http_access allow rede_local
```

```
http_access deny all
```

# Servidor Proxy

## Bloqueando palavras por domínio

Uma forma fácil de bloquear sites no Squid é criar uma lista de palavras, um arquivo texto, onde você adiciona palavras e domínios que serão bloqueados pelo squid.

Bloquear um determinado domínio, como por exemplo, “facebook.com”, não gera muitos problemas, mas deve-se tomar cuidado ao bloquear palavras específicas, pois o squid irá bloquear qualquer página que conter essa palavra em questão.

Se bloquear a palavra “sexo”, por exemplo, qualquer site ou artigo que conter a palavra sexo será bloqueado.

Ao bloquear por palavras, é necessário ser específico, bloqueando apenas “jargões” e expressões que normalmente se encontra no site que se quer bloquear.

# Servidor Proxy

## Exemplos

```
acl bloqueados dstdomain www.globo.com  
http_access deny bloqueados
```

```
acl proibidos dstdom_regex "/etc/squid/proibidos"  
http_access deny proibidos
```

# Servidor Proxy

## Exemplos

```
acl palavras_bloqueadas url_regex -i "/etc/squid/palavras_bloqueadas.txt"
```

```
http_access deny palavras_bloqueadas
```

# Servidor Proxy

## Exemplos

```
http_port 3128
```

```
visible_hostname marcio-VirtualBox
```

```
acl all src 0.0.0.0/0.0.0.0
```

```
acl SSL_ports port 443 563
```

```
acl Safe_ports port 21 80 443 563 70 80
```

```
acl purge method PURGE
```

```
acl CONNECT method CONNECT
```

```
acl rede_local src 192.168.10.0/24
```

```
#acl bloqueados dstdomain www.globo.com
```

```
#http_access deny bloqueados
```

```
#acl proibidos dstdom_regex "/etc/squid/proibidos"
```

```
#http_access deny proibidos
```

# Servidor Proxy

## Exemplos (cont.)

```
acl palavras_bloqueadas url_regex -i "/etc/squid/palavras_bloqueadas.txt"  
http_access deny palavras_bloqueadas
```

```
http_access deny !Safe_ports  
http_access deny CONNECT !SSL_ports
```

```
http_access allow rede_local
```

```
http_access deny all
```



**Prof. Dr. Marcio Andrey Teixeira**

**[marcio.andrey@ifsp.edu.br](mailto:marcio.andrey@ifsp.edu.br)**

**<http://marcioandrey.pro.br>**

# Bibliografia

SILVA, G. M.. Segurança em sistemas Linux. 1. ed. Rio de Janeiro: Ciência Moderna, 2008. 240p.

THOMPSON, M. A.. Windows Server 2012: fundamentos. 1. ed. São Paulo: Érica, 2012. 232p.

VIANA, E. R. C.. Virtualização de servidores Linux para redes corporativas: guia prático. 1.

ed. Rio de Janeiro: Ciência Moderna, 2008. 342p.

6 - BIBLIOGRAFIA COMPLEMENTAR:

KUROSE, J. F.; ROSS, K. W.. Computer networking: a top-down approach. 6. ed. AddisonWesley, 2012. 864p.

SCHRODER, C.. Redes Linux: livro de receitas. 1. ed. Rio de Janeiro: Alta Books, 2006. 569p.