



## Curso 452

# Linux Security Servers in Cloud

Versão 2015\_3.0

## Servidor Proxy – Parte I

---



4LINUX

2

### Cenário

A empresa Dexter Courier precisa ter um controle sobre os sites acessados, além disso manter um relatório sobre os mais acessados.

### Proposta de solução

A melhor solução é um Servidor Proxy com Sarg gerando relatórios.



## Aula 09

- 



[illegible]

# Servidor Proxy com Squid

---

## Introdução:

- As soluções Web Proxy foram desenvolvidas para contornar desperdício de banda nas empresas. Isso acontece quando várias máquinas acessam a mesma página;
- Quando um Proxy é implementado na rede o navegador das máquinas clientes, ao invés de consultar o site, consulta o "Web Proxy" previamente configurado, que armazena o conteúdo dos sites em um diretório num disco rígido.



5

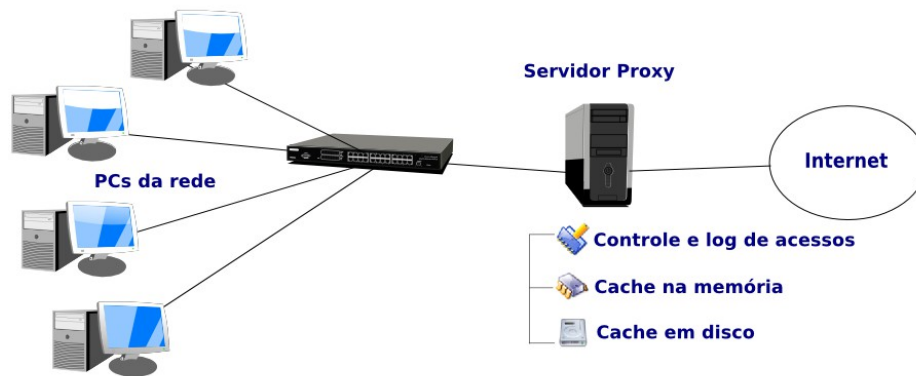
- As soluções Web Proxy foram desenvolvidas para contornar desperdício de banda nas empresas. Isso acontece quando várias máquinas acessam a mesma página;
- Quando um Proxy é implementado na rede o navegador das máquinas clientes, ao invés de consultar o site, consulta o "Web Proxy" previamente configurado, que armazena o conteúdo dos sites em um diretório num disco rígido.

5

## This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

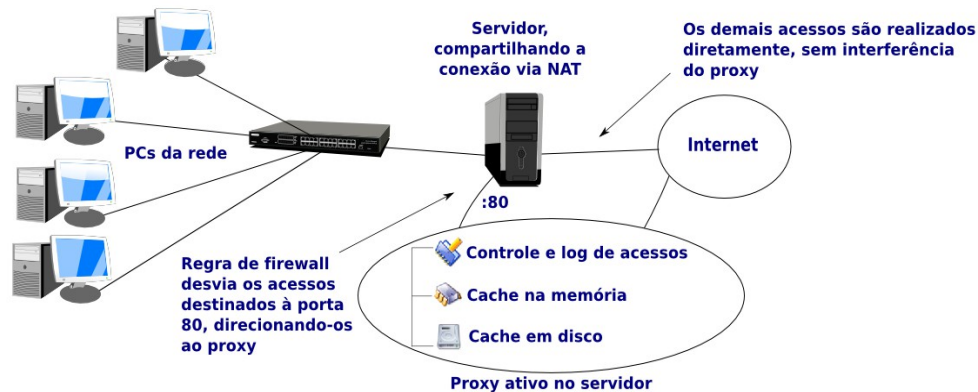
### Tipo de Proxy Manual:



**Proxy Manual** Com Proxy manual o usuário é obrigado a colocar no navegador o IP e PORTA do Proxy para poder navegar na internet.

## Servidor Proxy com Squid

### Tipo de Proxy Transparente:





**Proxy Manual** Com Proxy transparente cria-se uma regra de firewall para redirecionar tudo que vier na porta 80 e 443 para porta 3128 (Default do Squid).

# Servidor Proxy com Squid

---

## O que é um ACL?

- Access Control List ou Lista de Controle de Acesso (também conhecida pelo acrônimo ACL), como o próprio nome diz, é uma maneira de criar listas de acesso no Squid;
- É definida como uma lista que define quem tem permissão de acesso a certos serviços. Ou seja, para quem um servidor deve permitir ou negar determinada tarefa.



8

- Access Control List ou Lista de Controle de Acesso (também conhecida pelo acrônimo ACL), como o próprio nome diz, é uma maneira de criar listas de acesso no Squid;
- É definida como uma lista que define quem tem permissão de acesso a certos serviços. Ou seja, para quem um servidor deve permitir ou negar determinada tarefa.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.




# Servidor Proxy com Squid

---

## Tipos de ACL:

- **src** → Filtro por rede ou endereço IP;
- **time** → Filtro por hora e dia da semana;
- **urlpath\_regex** → Filtro de complemento de uma "url";
- **url\_regex** → Filtro de uma "string" na "url";
- **dstdomain** → Filtro de uma "url";
- **proxy\_auth** → Filtro por usuários autenticados;
- **arp** → Filtro por "MAC Address";
- **Maxconn** → Filtro por conexões;
- **Proto** → Filtro por protocolos;
- **port** → Filtro por porta.

 4LINUX

9

## This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.


# Servidor Proxy com Squid

---

## Regras das ACLs:

- **http\_access** → Permite ou nega acessos baseados nas ACLs pré definidas. É utilizado seguido de allow ou deny;
- Se a ACL for precedida de um ponto de exclamação significa que será a negação da ACL. As regras serão lidas na ordem em que aparecem;
- **Exemplos:**  

```
http_access allow DIRETOR  
http_access deny FACEBOOK !HORARIO_ALMOCO  
http_access deny EXTENSAO_PROIBIDA:
```

10

- **http\_access** → Permite ou nega acessos baseados nas ACLs pré definidas. É utilizado seguido de allow ou deny;
- Se a ACL for precedida de um ponto de exclamação significa que será a negação da ACL. As regras serão lidas na ordem em que aparecem;
- **Exemplos:**  

```
http_access allow DIRETOR  
http_access deny FACEBOOK !HORARIO_ALMOCO  
http_access deny EXTENSAO_PROIBIDA:
```

```
http_access allow DIRETOR
http_access deny FACEBOOK !HORARIO_ALMOCO
http_access deny EXTENSAO_PROIBIDA:
```

## This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Security**

## Liberando VPN no Firewall:

- Antes de implementar o squid libere a conexão VPN no arquivo de configuração do Firewall;
- Descomente a linha 16 no arquivo de configuração do firewall:

```
1# vim +16 /etc/firewall/rules
```

• • • •

DATACENTER="192.168.200.131"

VPN="10.0.0.X"

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Security**

## Liberando o Proxy e o OpenLDAP no Firewall:

- No arquivo de configuração do firewall, descomente da linha 95 até a linha 105:

```
1# vim +95 /etc/firewall/rules
```

- **Restarte o serviço do firewall:**

```
2# /etc/init.d/firewall restart
```

### Anotações:

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Security**

## Instalando o Squid:

```
1# apt-get install squid3 sarg
```

```
2# cd /etc/squid3
```

```
3# mv squid.conf squid.conf.dist
```

➤ Copie o arquivo de configuração do Squid:

```
4# cp /root/squid/squid.conf /etc/squid/
```

➤ Arquivos de configuração do Squid:

**/etc/squid3/squid.conf** → Arquivo de configuração

**/var/log/squid3/\*** → Arquivos de log do squid

**/var/spool/squid3** → Diretório que contém o cache do squid

### Anotações:

[illegible]

## Servidor Proxy com Squid

**Servidor: Security**

## Testando o Squid:

```
1# cd /etc/squid3
2# mkdir acls
3# cd acls/
4# echo "uol.com.br" > liberados1.txt
5# echo "terra.com.br" > liberados2.txt
6# echo "192.168.15.10" > financeiro.txt
7# echo "192.168.15.100" > vendas.txt
8# echo "playboy.com" > vip_bloqueados.txt
9# echo "192.168.15.200" > vip.txt
```

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Security**

## Implementando as ACLs no Squid:

- No arquivo de configuração do squid, descomente as acIs da linha 85 até a linha 97:

```
1# vim +85 /etc/squid3/squid.conf
```

- Execute o comando abaixo para reler o arquivo squid.conf sem precisar reiniciar o squid:

```
2# squid -k reconfigure
```

- Execute o comando abaixo para criar a estrutura de cache do squid:

```
3# squid3 -z
```

### Anotações:

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Linux Interna**

## Configurando o Proxy no Browser:

- No navegador Firefox da máquina Linux Interna, siga as instruções abaixo para a configuração do Proxy:

```
1#  Editar  >  Preferências  >  Avançado  >  Rede  >  Configurar
Conexão
```

## Testando as ACLs:

- Utilize o comando `tailf` para acompanhar os logs do Squid:

```
2# tailf /var/log/squid3/cache.log
```

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



## Servidor Proxy com Squid

**Servidor: Security**

## Autenticação via LDAP:

Para liberação da autenticação via LDAP, no arquivo squid.conf descomente da linha 55 a 58:

```
1# vim +55 /etc/squid3/squid.conf
```

## Criação da ACL de Bloqueio:

Ainda no arquivo squid.conf crie a ACL de bloqueio:

```
acl AUTH proxy_auth REQUIRED
```

### Criação da regra de Acesso:

Coloque a seguinte linha como **PRIMEIRA** regra de acesso:

```
http_access deny !AUTH
```

## Recarregue as configurações do Squid e acesse as páginas:

```
2# squid -k reconfigure
```



17

### Anotações:

[illegible]

## Servidor Proxy com Squid

**Servidor: Security**

## Configurando o Sarg:

- Mova o arquivo de configuração `sarg.conf` para backup e em seguida baixe um novo `sarg.conf`:

```
1# cd /etc/sarg
```

```
2# mv sarg.conf sarg.conf.dist
```

```
3# cp /root/sarg/sarg.conf /etc/sarg
```

- Abra o arquivo `/etc/sarg/sarg-reports:`

```
4# vim /etc/sarg/sarg-reports
```

- Especifique aonde irá gerar os arquivos de logs do sarg alterando a seguinte entrada:

**HTMLOUT=/etc/sarg/reports**

## 4LINUX

18

**Anotações:**

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: Security**

### Script de Geração do Log do Sarg:

- Na instalação do sarg ele já configura suas rotinas de criação de logs no cron, conforme a agenda padrão dele:

```
1# ls -R /etc/cron.*
```

## Gerando o Relatório Manualmente:

- O tempo mínimo para a geração de relatório no sarg é de 1 dia, portanto será necessário alterar a data do sistema para amanhã.
- Após a alteração da data, gere o relatório manualmente:

```
2# /etc/cron.daily/sarg
```

### Anotações:

[illegible]

## Servidor Proxy com Squid

**Servidor: Security**

## Validando a Geração de Log do Sarg:

- Vamos verificar se os arquivos de log foram realmente criados:

```
1# cd /etc/sarg/reports
```

2# ls

```
3# ls /etc/sarg/reports/daily
```

## Enviando o relatório de log:

- Agora vamos enviar os relatórios para o Apache na DMZ, para conseguirmos visualizá-los via browser:

```
4# scp -r /etc/sarg/reports suporte@webserverinterno:
```



20

### Anotações:

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Servidor Proxy com Squid

**Servidor: WebServerInterno**

## Configurando o Novo VirtualHost:

- Acesse a máquina WebServer Interno para configurar um novo VirtualHost:

```
1# cp -a /home/suporte/reports /var/www/html
```

```
2# cd /etc/httpd/sites
```

```
3# cp /root/sarg/sarg.conf .
```

```
4# /etc/init.d/httpd restart
```

## Visualizando os Relatórios via Browser:

- Agora abra um browser na máquina DMZ e acesse o seguinte endereço:

```
5# sarg.dexter.com
```

### Anotações:

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

## Próximos Passos

---

Para que você tenha um melhor aproveitamento do curso, participe das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

**Mãos à obra!**

# 4LINUX

OPEN SOFTWARE SPECIALISTS



**ESPECIALISTA EM "JUNTAR AS PEÇAS" DO MUNDO OPEN SOURCE**

[WWW.4LINUX.COM.BR](http://WWW.4LINUX.COM.BR)