INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança de Redes

Aula extra - Squid

Filipe Raulino
filipe.raulino@ifrn.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Instalação

Instalando o Squid :

```
# yum install squid
```

Iniciando o serviço:

```
# /etc/init.d/squid start
```

Arquivos/Diretórios:

/etc/squid/squid.conf – É o principal arquivo de configuração do Squid, aqui são configuradas as regras do proxy.

/var/spool/squid – Diretório de cache utilizado pelo Squid.

/var/log/squid – Diretório de arquivos de log do squid.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Configuração Squid.conf

- **http_port 3128**
  - Define a porta em que o Squid irá receber requisições, por padrão 3128.

- **visible_hostname meuproxy.com.br**
  - Nome do host a ser exibido nas mensagens de erro. Sem ela o squid não inicializa.

- **cache_mem 64 MB**
  - Quantidade de memória

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Configuração Squid.conf

- **access_log /var/log/squid/access.log squid**
  - Especifica o diretório de log dos acessos dos clientes.
- **cache_log /var/log/squid/cache.log**
  - Especifica o diretório de log do comportamento do cache.
- **cache_dir ufs /var/spool/squid 100 16 256**
    - Especifica o diretório de cache e os paramentos abaixo:
      - 100 - Espaço em MB;
      - 16 - Quantidade de diretórios que serão criados
      - 256 - Quantidade de subdiretórios dentro dos 16 principais.
- **# squid -z**
  - Comando para criar os diretórios de cache.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

ACLs

- **ACL (Access Control List) -** Criam objetos como: hosts, urls, horários, portas, etc…

- Formato:
  - acl nome_acl tipo [“arquivo” | string]

Exemplo:

acl rede_local src 192.168.1.0/255.255.255.0

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tipos de ACL

- **src:** Utilizada para especificar um determinado host ou rede de origem.

```
acl rede_local src 192.168.1.0/255.255.255.0
```

- **dst:** Utilizada para especificar um determinado host ou rede de destino.

```
acl rede_local dst 10.68.1.1/255.255.255.255
```

- **dstdomain:** Utilizado para especificar um determinado domínio de destino.

```
acl hotmail dstdomain .hotmail.com
```

- **port:** Porta usada pelo site.

```
acl Safe_ports port 80
```

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tipos de ACL

- **url_regex:** Procura por expressão em toda a URL.

```
acl palavras_proibidas url_regex -i "/etc/squid/palavras_proibidas"
```

- **dstdomain_regex:** Procura por expressão no domínio.

```
acl sites_proibidos dstdomain_regex -i "/etc/squid/sites_proibidos"
```

- **time:** Hora e dia da semana. Especifica um determinado horário.

```
acl horario_comercial time MTWHF 08:00-18:00
```

S	domingo
M	segunda-feira
T	terça-feira
W	quarta-feira
H	quinta-feira
F	sexta-feira
A	sábado

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Controle de acesso

- O controle de acesso e realizado pelo rótulo **http_access**
- Formato:
  - http_access [allow|deny] nome_da_acl

Exemplo:

acl rede_local src 192.168.1.0/255.255.255.0
http_access allow rede_local

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Testando o Squid

- Salve o arquivo original em outro arquivo:
  - `#mv /etc/squid/squid.conf /etc/squid/squid.conf.orig`

- As quatro linhas abaixo são suficientes para que o squid funcione:

```
http_port 3128
visible_hostname debian

acl all src 0.0.0.0/0.0.0.0
http_access allow all
```

- Configure o seu browser e teste o acesso.

Configuração Básica

```
http_port 3128
visible_hostname gdh

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 21 80 443 563 70 210 280 488 59 777 901 1025-65535
acl purge method PURGE
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

acl redelocal src 192.168.1.0/24

http_access allow localhost http_access allow redelocal
http_access deny all
```

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Configuração de cache

```
cache_mem 64 MB
maximum_object_size_in_memory 64 KB
maximum_object_size 512 MB
minimum_object_size 0 KB
cache_swap_low 90
cache_swap_high 95
cache_dir ufs /var/spool/squid 2048 16 256
cache_access_log /var/log/squid/access.log
refresh_pattern ^ftp: 15 20% 2280
refresh_pattern ^gopher: 15 0% 2280
refresh_pattern . 15 20% 2280
```

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Restrições de Acesso

```
acl rede_local src 192.168.0.0/24
acl palavras_bloqueadas url_regex -i "/etc/squid/palavras_bloqueadas.txt "
acl sites_bloqueados url_regex -i "/etc/squid/ sites_bloqueados.txt "
acl redes_sociais url_regex -i "/etc/squid/redes_sociais.txt"
acl liberados src "/etc/squid/ips_liberados.txt "
acl porno url_regex -i "/etc/squid/sites_porno.txt "
acl formato_arquivo url_regex -i "/etc/squid/formato_arquivo.txt"
acl horario_almoco time 12:00-13:00

http_access allow liberados
http_access allow redes_sociais  horario_almoco
http_access deny redes_sociais
http_access deny sites_bloqueados
http_access deny palavras_bloqueadas
http_access deny porno
http_access deny formato_arquivo
http_access allow rede_local
```

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Proxy transparente

- Redirecionamento
  - `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128`
- squid.conf
  - `http_port 3128 transparent`