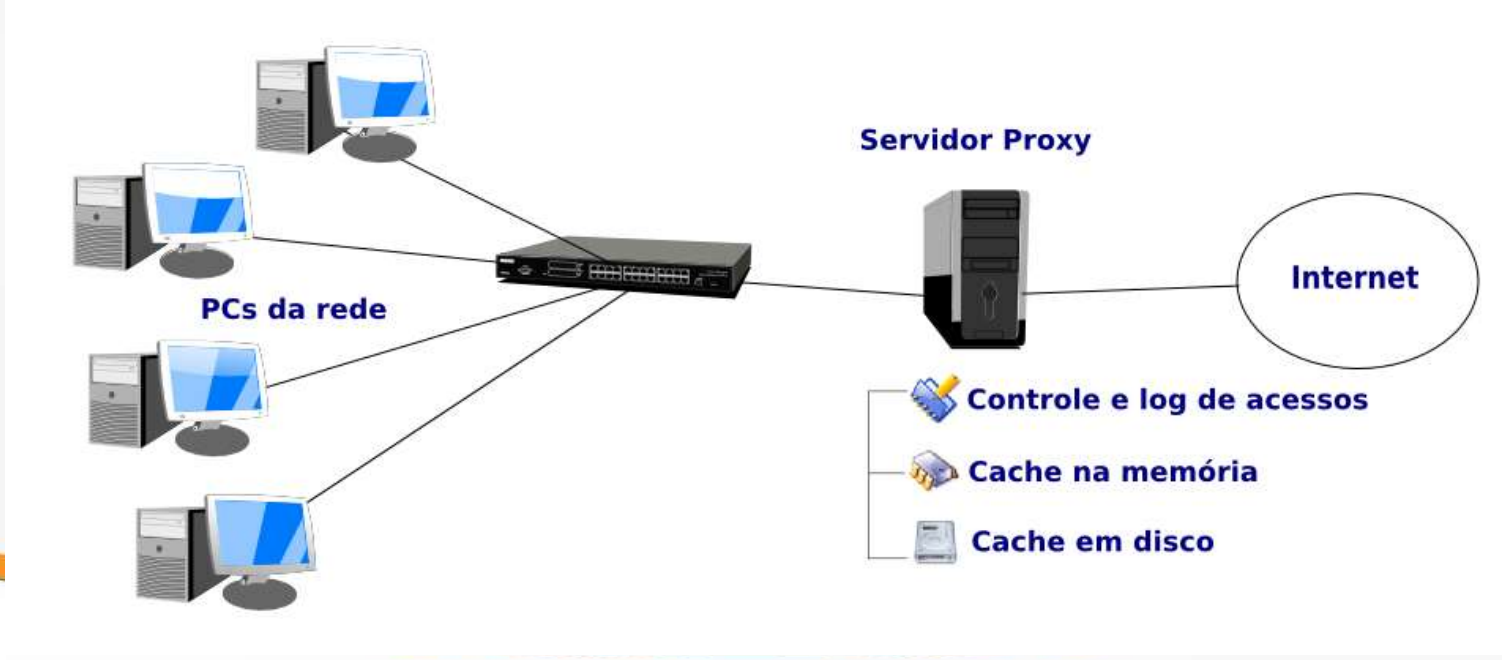
Debian server
Proxy Squid

Servidor Proxy

- O acesso a internet é praticamente obrigatório, em ambientes corporativo, tendo em vista o dinamismo que as novas tecnologias e recursos que podem trazer para este ambiente.
- Entretanto surgem vários problemas quanto a definição de como implementar esse acesso de computadores das **redes corporativas à internet de forma segura e eficiente**.
- No conjunto de medidas a serem tomadas para implementar esse acesso temos a utilização de **servidores proxy**.

Servidor Proxy

- Funciona como um intermediário entre os computadores da rede local com outras máquinas de fora dessa rede, como por exemplo na internet.
- Ele recebe as requisições para acesso externo dos hosts locais e as repassa a outros computadores fora da rede local, retornando as respostas aos computadores que as solicitaram.



Proxy com Squid

- O Squid é um dos **servidores proxy mais utilizados no mundo**, dado a sua robustez, segurança e recursos.

- Apesar dos poucos **protocolos que ele consegue trabalhar, no caso apenas o HTTP, HTTPS e FTP e gopher**, é ainda uma alternativa muito interessante, já que estes são os principais protocolos da internet, e além disso, muitos dos aplicativos que usam outros protocolos tem capacidade de usar o Squid através de um dos protocolos suportados por ele.

Proxy Squid

- Porque usar o Squid?

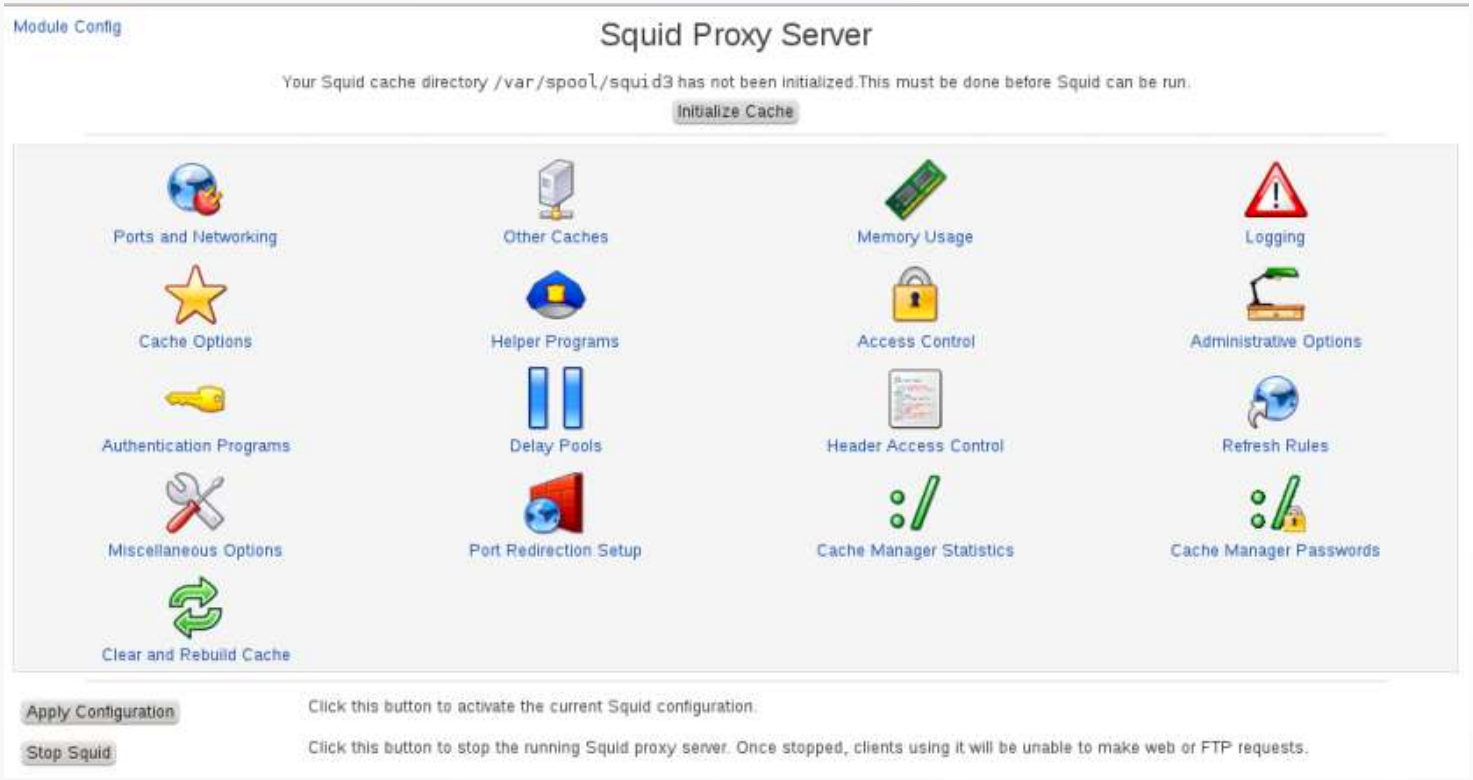
✓Cache

✓Autenticação

✓Registro de acessos

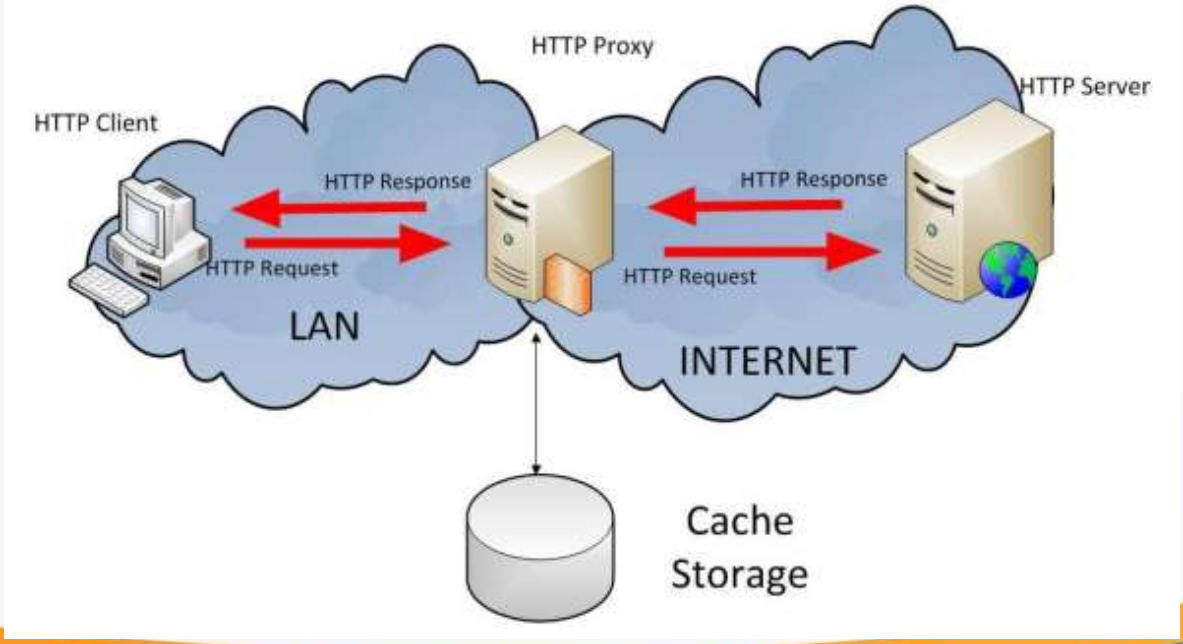
✓Controle centralizado

✓ Segurança



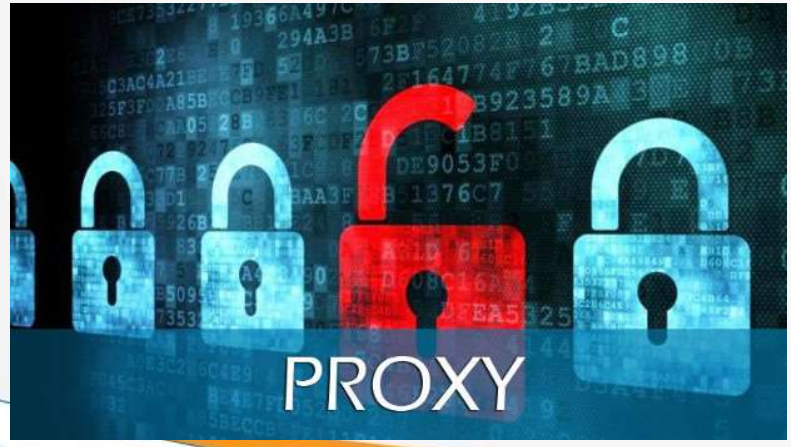
Proxy Squid - Cache

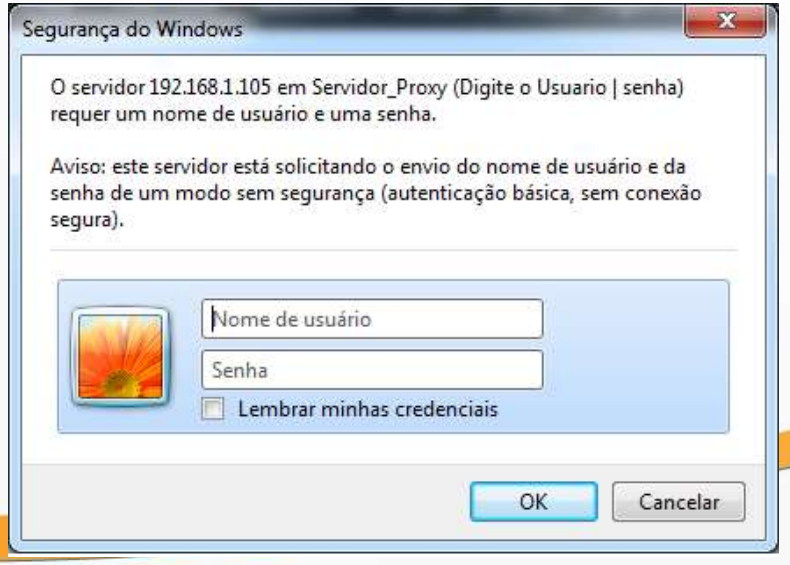
- Através desse recurso o Squid **armazena** em cache **o conteúdo acessado**, de forma que se algum host fizer novamente uma requisição ao mesmo conteúdo, que já se encontra armazenado, ele recebe diretamente do cache, sem a necessidade de efetuar uma nova busca dos dados na internet, gerando maior rapidez ao acesso à internet.



Proxy Squid - Autenticação

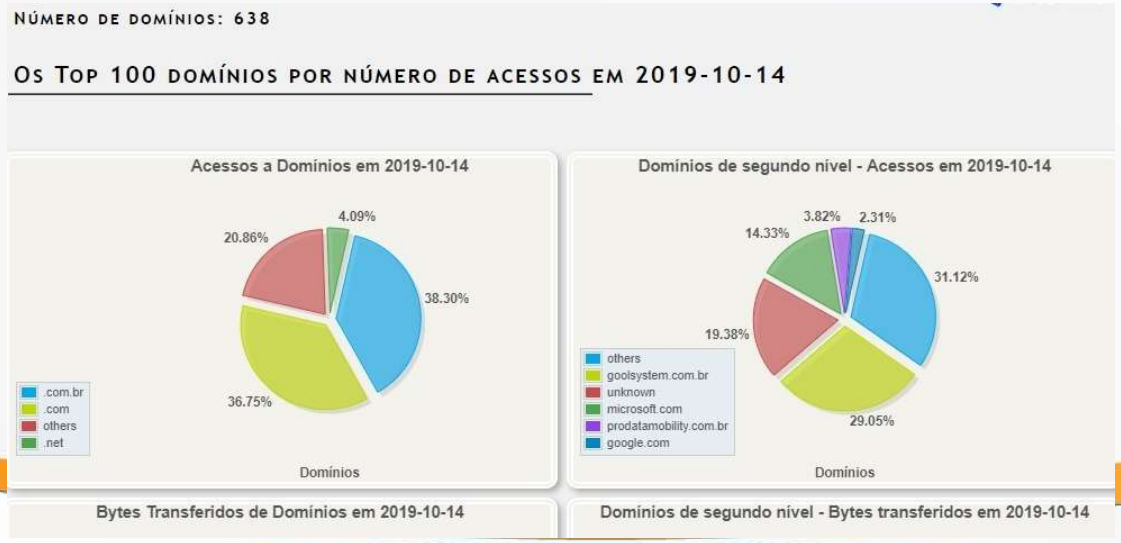
- Podemos **restringir o acesso ao servidor proxy com o uso da autenticação de usuários**, de forma que seja melhorada a segurança, já que somente usuários autorizados poderão acessar a internet. Este recurso é bastante flexível e pode ser implementado de várias maneiras, como uso do protocolo LDAP, SMB e etc.





Proxy Squid – Registro de Acessos

- Os **acessos são registrados em arquivos de log**, podendo esses serem utilizados para as mais diversas finalidades, que vão desde a análise de performance do servidor, até a geração de relatórios detalhados dos acessos à internet.
- Existem vários softwares analisadores de logs do Squid capazes de gerar relatórios tão bons, que por si já justificariam o uso do Squid.



Proxy Squid – Controle Centralizado

- Com o uso do proxy temos a facilidade de um único ponto **centralizador do acesso à internet**, o que torna a gerência da rede mais fácil e eficiente.
- Uma única máquina é capaz de prover acesso à várias outras.

Proxy Squid - Segurança

- Como apenas o proxy está diretamente ligado à internet”, temos apenas uma (ou mesmo poucas, caso tenhamos mais de um servidor proxy) máquina potencialmente vulnerável.
- Desta forma fica mais fácil concentrar esforços na melhoria da segurança de apenas um ponto na rede.

Instalação do Squid no Debian Server

```
# apt-get update
# apt-get install squid
```

- Visualizando o status do squid

```
# systemctl status squid
# systemctl start squid
# systemctl stop squid
```

- Leia, renomeie e crie um novo arquivo de configuração do squid.

```
# cat /etc/squid/squid.conf
# mv /etc/squid/squid.conf /etc/squid/squid.conf.bkp
# touch /etc/squid/squid.conf
```

- Edite o novo arquivo “#vim /etc/squid/squid.conf” conforme a imagem.

```
http_port 3128
visible_hostname Squid-Server
cache_mem 8 MB
cache_dir ufs /var/log/squid/ 100 16 256
cache_access_log /var/log/squid/access.log
cache_store_log /var/log/squid/store.log
cache_log /var/log/squid/cache.log
cache_mgr seu-email4@gmail.com
acl localhost src 127.0.0.0
acl redelocal1 src 192.168.0.0/24
acl bloqueio url_regex -i '/etc/squid/bloqueio.txt'
http_access deny bloqueio
http_access allow localhost
http_access allow redelocal1
http_access deny all
```

Criando diretórios no Squid

- Criar pastas de acordo com squid.conf depois mudar o proprietário e o grupo dos arquivos squid.

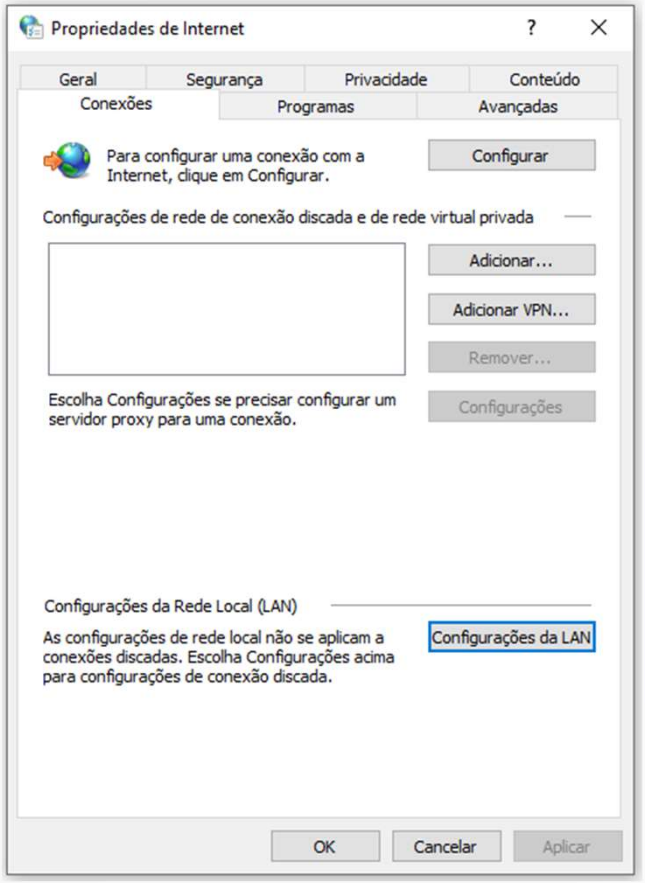
```
# mkdir /var/cache/squid/
# touch /var/log/squid/store.log
# touch /etc/squid/bloqueio.txt
# echo facebook >> /etc/squid/bloqueio.txt
# chown proxy:proxy /etc/squid/bloqueio.txt
# chown proxy:proxy /var/log/squid/ -R
# chown proxy:proxy /var/cache/squid/ -R
```

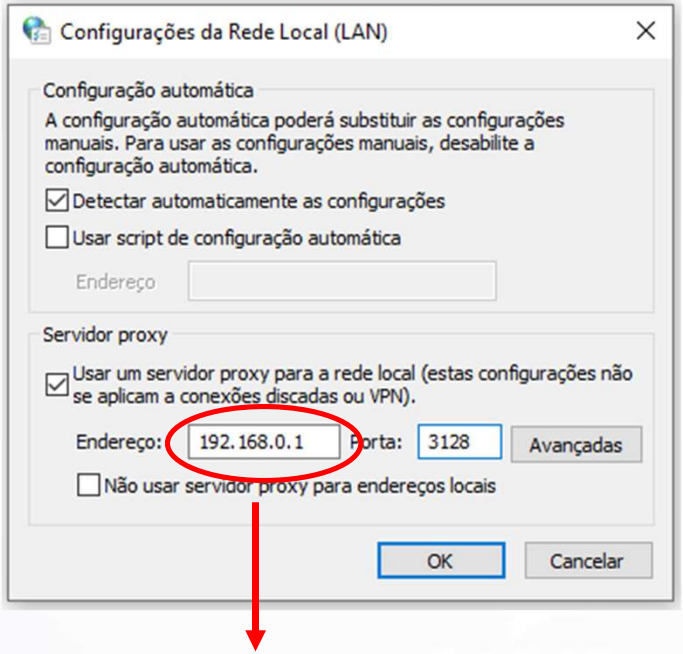
- Obs.: Os arquivos "access.log" e "cache.log" não precisam ser criados, pois já existem.
- Reiniciando o squid para aplicar as alterações, verificando o status.

```
# systemctl restart squid
# systemctl status squid
```

Configurando cliente para usar o proxy

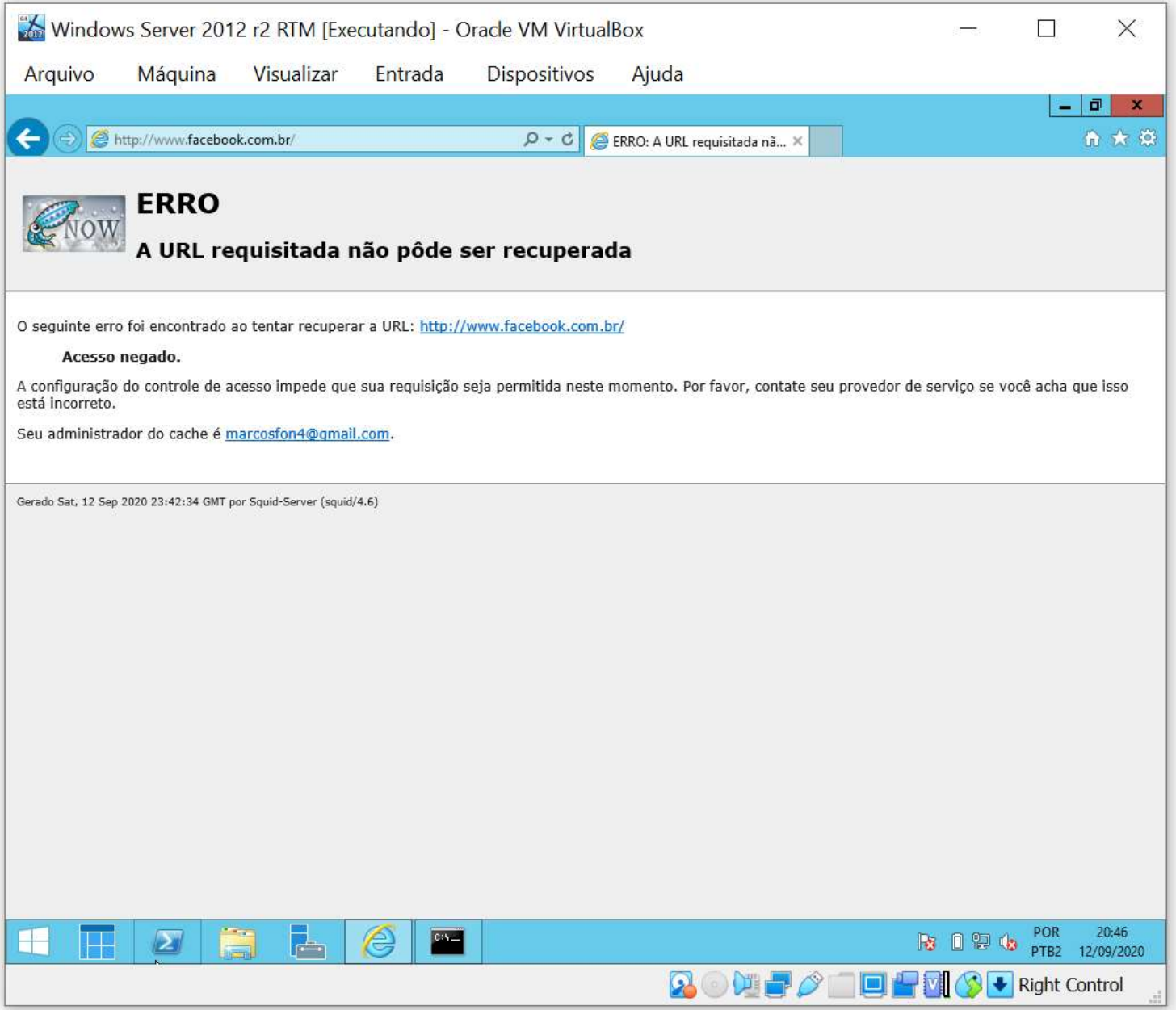
1. Painel de controle
2. Rede e Internet
3. Opções da Internet





O endereço deve ser o IP do seu Servidor Squid

- Squid bloqueando o Facebook



Verificando os Logs via CLI

- # tail -f /var/log/squid/access.log
- # tail -f /var/log/squid/access.log | grep facebook

- o comando **tail** lista a parte final do conteúdo de um arquivo;

- o parâmetro **-f** permanece com o arquivo aberto mostrando as atualizações.

- **| grep** é um filtro de pesquisa no resultado de um comando, ou seja, se você quiser ver quem está acessando o facebook.