

Relatório do projeto Samba/Squid da disciplina de Segurança em Sistemas Operacionais e Redes de Computadores (SSORC)

Dupla: Italo César Sampaio Gomes Pinto / Francisco Ruan Frota Vieira
Docente: Juan Sebastian Toquica Arenas

Tema: Instalação e configuração de um sistema de proxy Squid para ambiente escolar de tempo integral, utilizando restrição de sites não convenientes e regramento na disponibilidade da internet.

Recursos utilizados no projeto Squid

Durante os testes foram utilizados:

1. Uma máquina virtual Debian Linux para hospedar o servidor squid.
2. Uma máquina virtual Ubuntu Linux para realizar os testes com o proxy do servidor squid configurado.
3. Uma máquina física Windows para realizar um teste fora da rede virtual e dar complemento aos testes.

As duas máquinas virtuais foram criadas dentro do software Oracle VirtualBox

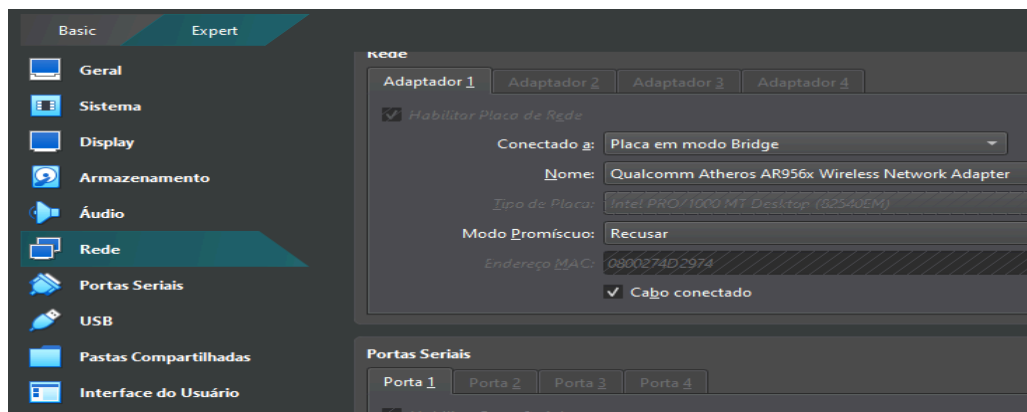
1ª Etapa: Criação das máquinas virtuais

Nesta etapa serão abordados os passos a serem seguidos até que o sistema de proxy Squid esteja pronto para edição.

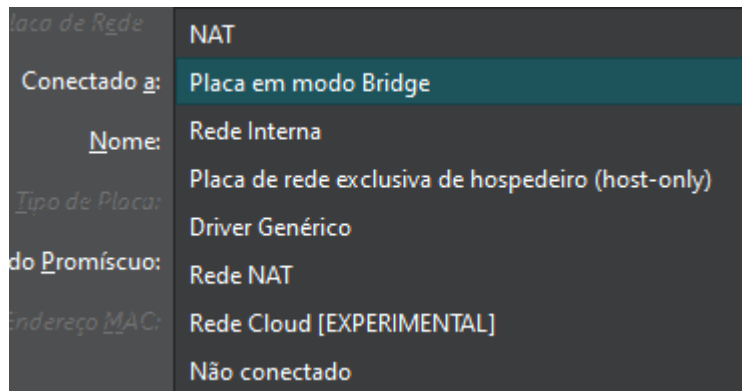
Em primeiro momento faz-se necessário uma máquina virtual para hospedar o servidor squid

Utilizei uma máquina virtual com Debian 12.9.0 com 4GB de RAM (4096 MB), 2 processadores e um armazenamento de 20GB

Mas antes de inicializar o sistema operacional, uma configuração deve ser alterada:



Na aba de Rede, deve ser alterado a conexão do Adaptador 1 para Modo Bridge:



Isso deve ser feito para que a máquina use da rede conectada ao computador, e não a conexão criada dentro da própria máquina, assim possibilitando a interação com o servidor Squid.

Fiz o mesmo com a máquina virtual Ubuntu, a única diferença foi a utilização de um sistema operacional Ubuntu 22.04.5 em vez do Debian.

Com as máquinas criadas e inicializadas ao clicar duas vezes no ícone, basta esperar todo o processo até elas estarem prontas para utilização e seguir para a próxima etapa

2ª Etapa: Preparação do ambiente para configuração Squid

Ao entrar pela primeira vez no linux, abri o terminal usando Ctrl + Alt + t e executei os seguintes comandos:

```
sudo apt update
sudo apt upgrade
sudo apt install squid -y
```

sudo apt update e **sudo apt upgrade** foram usados para atualizar o sistema, junto com **sudo apt install squid -y** para instalar o sistema squid, o **-y** foi apenas para aceitar todas as permissões que seriam pedidas durante a instalação

3ª Etapa: Configuração do proxy Squid

Quando instalado, fiz um backup do arquivo de configuração usando **sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bkp**

Logo após, criei dois arquivos .txt para o bloqueio dos sites e a escolha dos horários disponíveis

O primeiro arquivo criado foi “sites_bloqueados.txt” utilizando o comando **sudo nano /etc/squid/sites_bloqueados.txt** para bloquear os sites

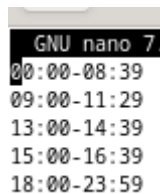
Ao ser criado, o arquivo de texto foi aberto e inseri os seguintes domínios:



```
GNU nano 7.2
facebook.com
.x.com
.tiktok.com
.instagram.com
.youtube.com
.steampowered.com
.epicgames.com
.riotgames.com
.discord.com
.chatgpt.com
```

Então fechei usando Ctrl + X, Y e Enter

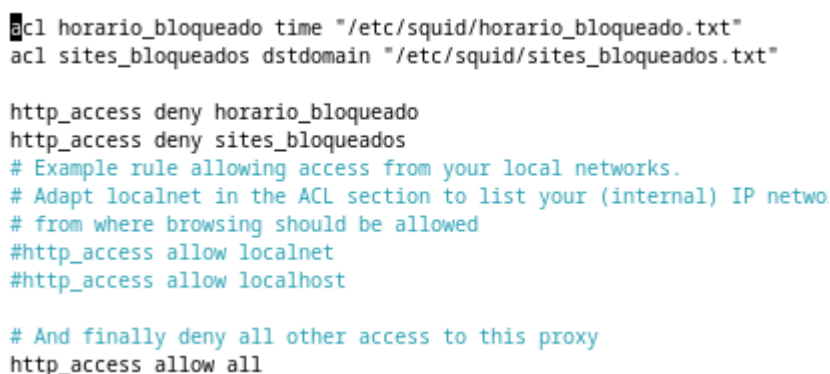
O segundo arquivo foi “horario_bloqueado.txt” utilizando o comando **sudo nano /etc/squid/horario_bloqueado.txt** para restringir os horários



```
GNU nano 7
00:00-08:39
09:00-11:29
13:00-14:39
15:00-16:39
18:00-23:59
```

Fechei e fui editar o arquivo squid.conf com o comando **sudo nano /etc/squid/squid.conf**

Como squid.conf aberto, pesquisei **INSERT YOUR OWN RULE** com o atalho Ctrl + W e inseri os comandos que iria usar para realizar os testes logo abaixo da linha **include /etc/squid/conf.d/*.conf**



```
acl horario_bloqueado time "/etc/squid/horario_bloqueado.txt"
acl sites_bloqueados dstdomain "/etc/squid/sites_bloqueados.txt"

http_access deny horario_bloqueado
http_access deny sites_bloqueados
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP netwo
# from where browsing should be allowed
#http_access allow localnet
#http_access allow localhost

# And finally deny all other access to this proxy
http_access allow all
```

No caso, adicionei as seguintes linhas:

acl horario_bloqueado time “/etc/squid/horario_bloqueado.txt”
acl sites_bloqueados dstdomain “/etc/squid/sites_bloqueados.txt”

http_access deny horario_bloqueado
http_access deny sites_bloqueados

http_access allow all

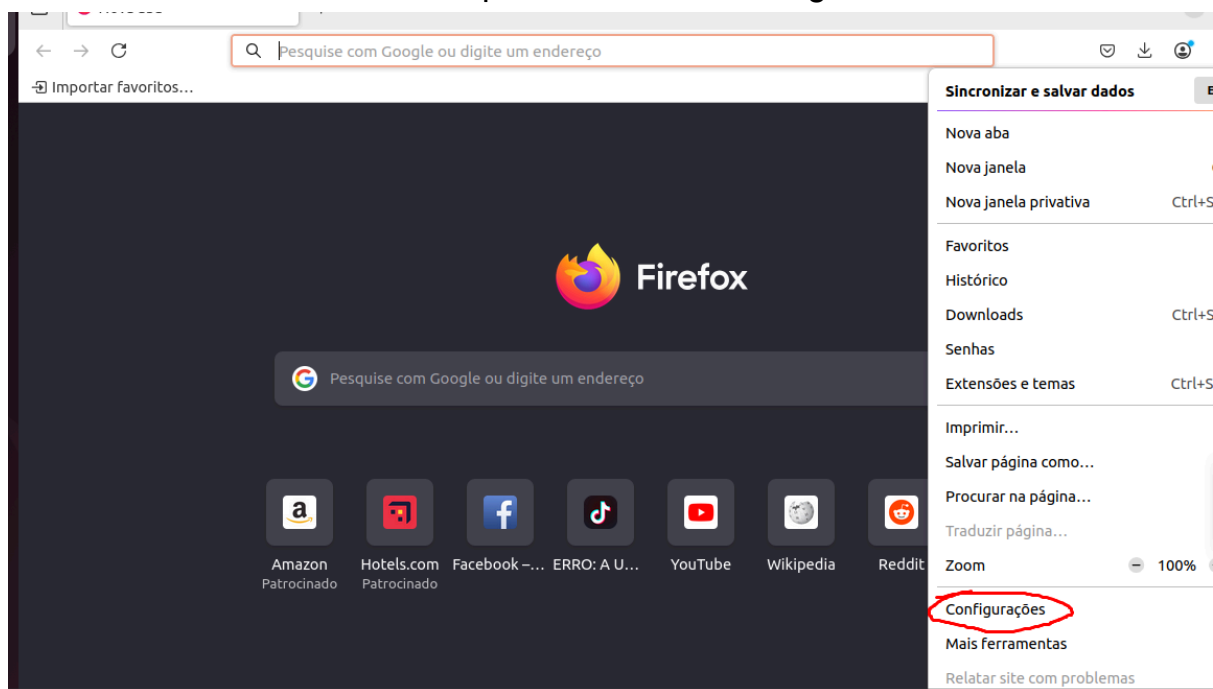
Os dois parâmetros acl que escrevi são para coletar os dados que coloquei nos arquivos e possibilitar a negação dos serviços dentro do proxy, sendo o acl com **time** para coletar os horários e o acl com **dstdomain** para coletar os domínios. O **http_access allow all** serve para aceitar qualquer serviço que não seja um domínio bloqueado e esteja dentro do horário para uso da internet

Fechei com Ctrl + X, Y e Enter, executei o comando **sudo squid -k parse** para verificar se há algum erro ao iniciar o servidor e reiniciei com o comando **sudo systemctl restart squid** para aplicar as alterações no squid.conf

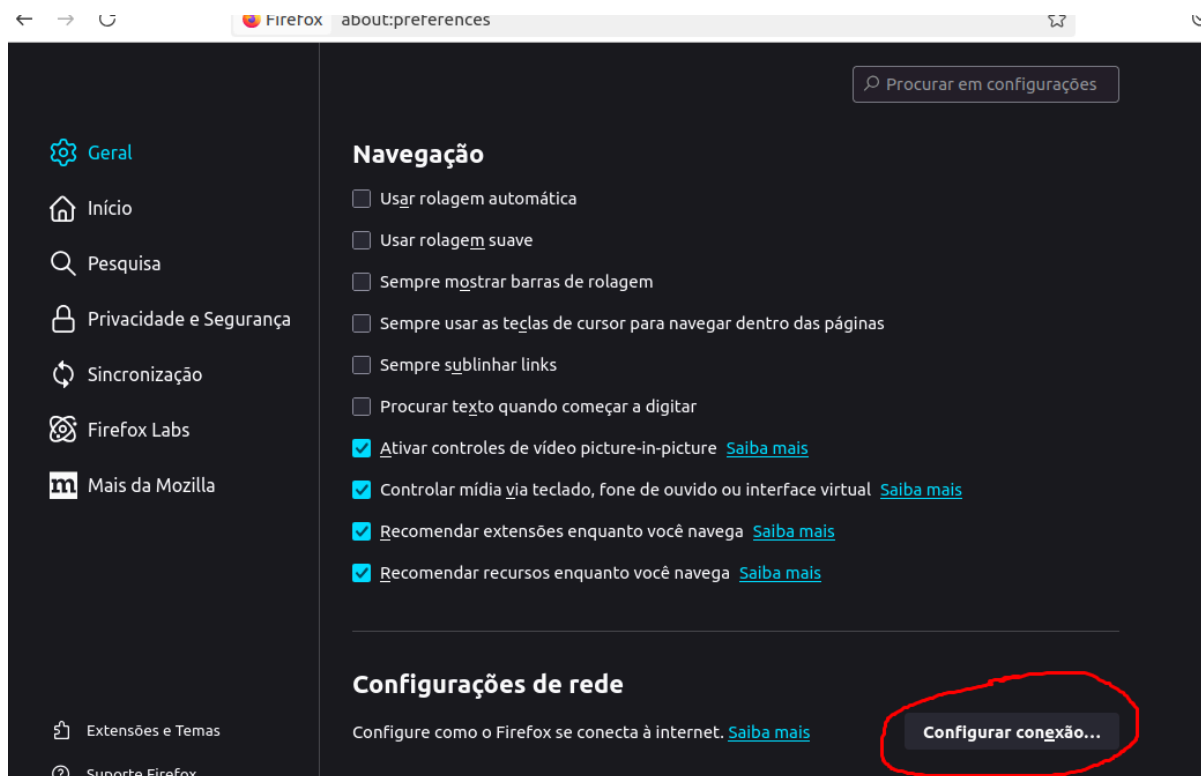
4ª Etapa: Configuração na outra máquina para testes

Com o servidor configurado, abri a máquina virtual Ubuntu e comecei a configuração no navegador para realizar os testes

Fui nas três barras no canto superior direito no navegador Firefox



Em Configurações, na aba Geral, desci até achar a opção Configurar conexão...



Voltei a máquina Debian para coletar o ip

```
debiansquiditalo@vbox:~$ ip a | grep inet
inet 127.0.0.1/8 scope host lo
inet6 ::1/128 scope host noprefixroute
inet 192.168.0.19/24 brd 192.168.0.255
inet6 2804:29b8:504e:bd9:3400:c733:837a
inet6 2804:29b8:504e:bd9:a00:27ff:fe4d:
...
inet6 fe80::a00:27ff:fe4d:2974/64 scope
```

No Firefox, selecionei a opção Configuração manual do proxy e coloquei o ip junto com a porta do servidor

Configuração de conexão

Configuração de proxy de acesso à internet

☐ Sem proxy

☐ Detectar automaticamente as configurações de proxy desta rede

☐ Usar as configurações de proxy do sistema

☒ Configuração manual de proxy

Proxy HTTP 192.168.0.19 Porta 3128

☒ Usar este proxy também em HTTPS

Proxy HTTPS 192.168.0.19 Porta 3128

Domínio SOCKS Porta 0

☐ SOCKS v4 ☒ SOCKS v5

☐ URL de configuração automática de proxy

Recarregar

Sem proxy para

Cancelar OK

Dei um OK e fui aos testes

5ª Etapa: Realização dos testes

Nas configurações que selecionei para o servidor, vou fazer 2 tipos de testes, com horários e com domínios

Um dos horários estabelecidos para bloqueio de internet foi de 00:00-08:39 e 09:00-11:29

Vamos ver se os horários estão funcionando corretamente

Como a máquina Debian é a hospedeira do servidor Squid, este deve ser o relógio a ser modificado

Mar 6 07:00

Date & Time

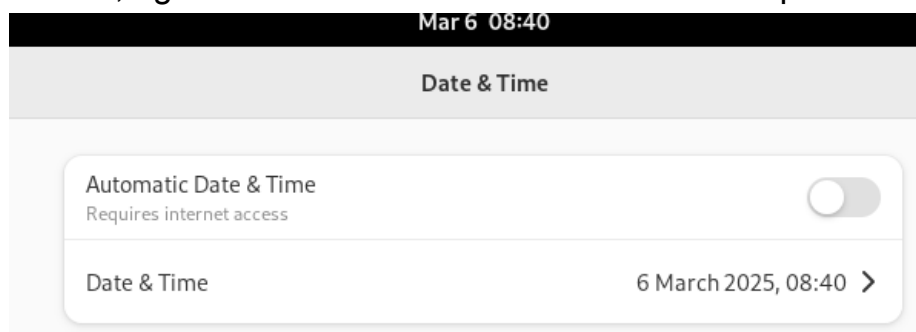
Automatic Date & Time Requires internet access

Date & Time 6 March 2025, 07:00 >

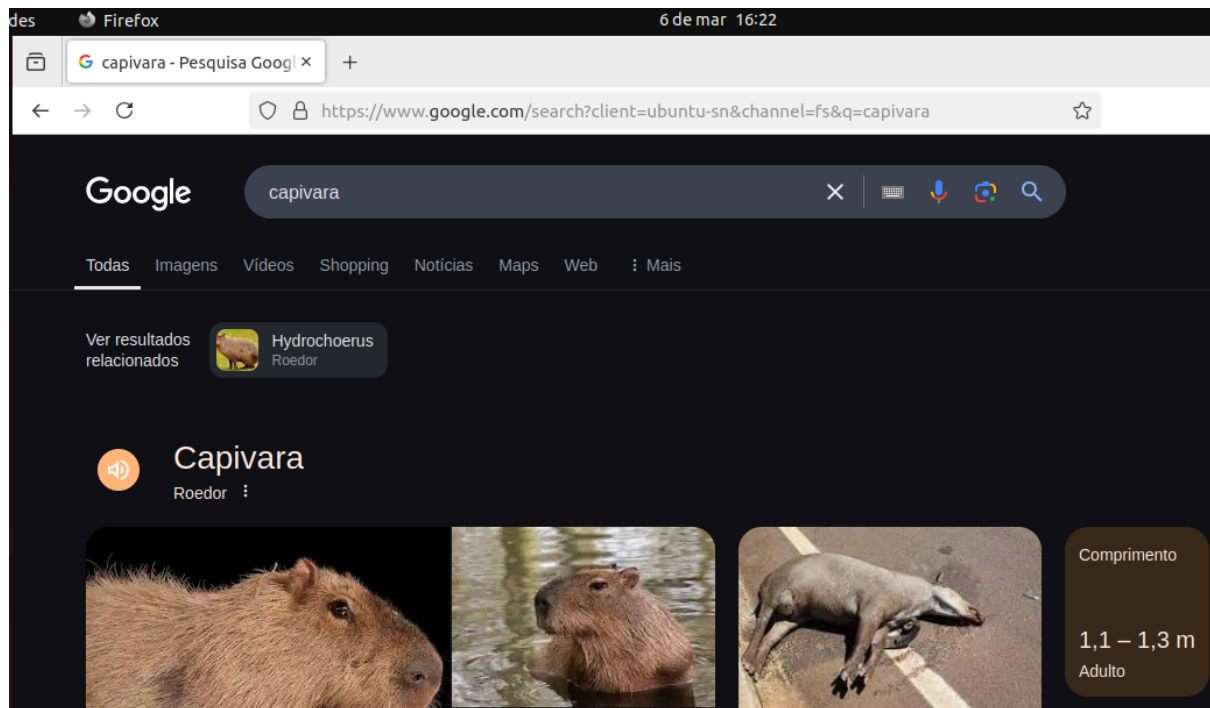
Coloquei 07:00, vamos ver se o Firefox permite



E como esperado, o servidor recusou a conexão
Pode ver como na máquina Ubuntu de teste o horário está diferente do
Debian, agora vamos alterar o horário e realizar o próximo teste



Dessa vez coloquei 08:40



E assim como foi configurado, a conexão foi estabelecida com sucesso, permitindo a pesquisa normalmente

Para último teste, vamos ver os domínios que escolhi

Vou testar com 3 deles: **.tiktok.com** **.facebook.com** **.discord.com**

E segue as prints, respectivamente





O servidor proxy está recusando conexões

O Firefox está configurado para usar um servidor proxy que está recusando conexões.

Código de erro: 403 Forbidden

- Verifique se as configurações de proxy estão corretas.
- Entre em contato com um administrador de rede para verificar se o servidor proxy está funcionando.

Tentar novamente



O servidor proxy está recusando conexões

O Firefox está configurado para usar um servidor proxy que está recusando conexões.

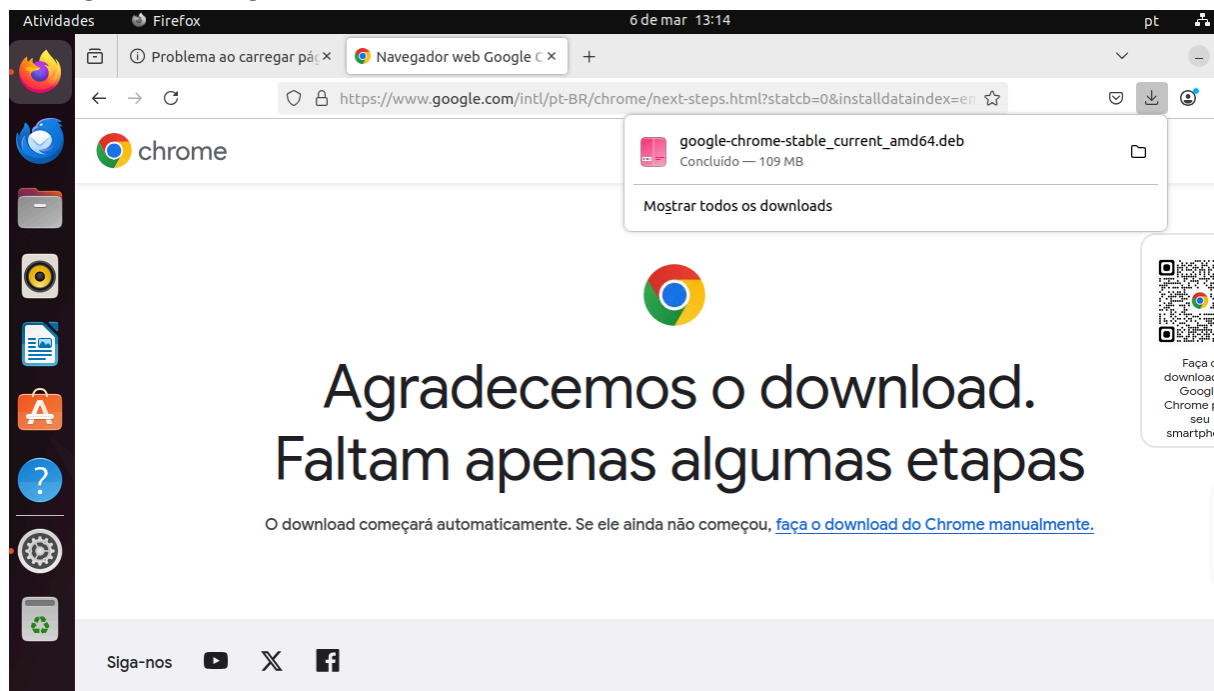
Código de erro: 403 Forbidden

- Verifique se as configurações de proxy estão corretas.
- Entre em contato com um administrador de rede para verificar se o servidor proxy está funcionando.

Tentar novamente

E como é possível observar, os domínios estão nas URLs e o proxy barra a conexão com os sites

Para finalizar os testes na máquina virtual, irei fazer o download do navegador Google Chrome e fazer o mesmo teste



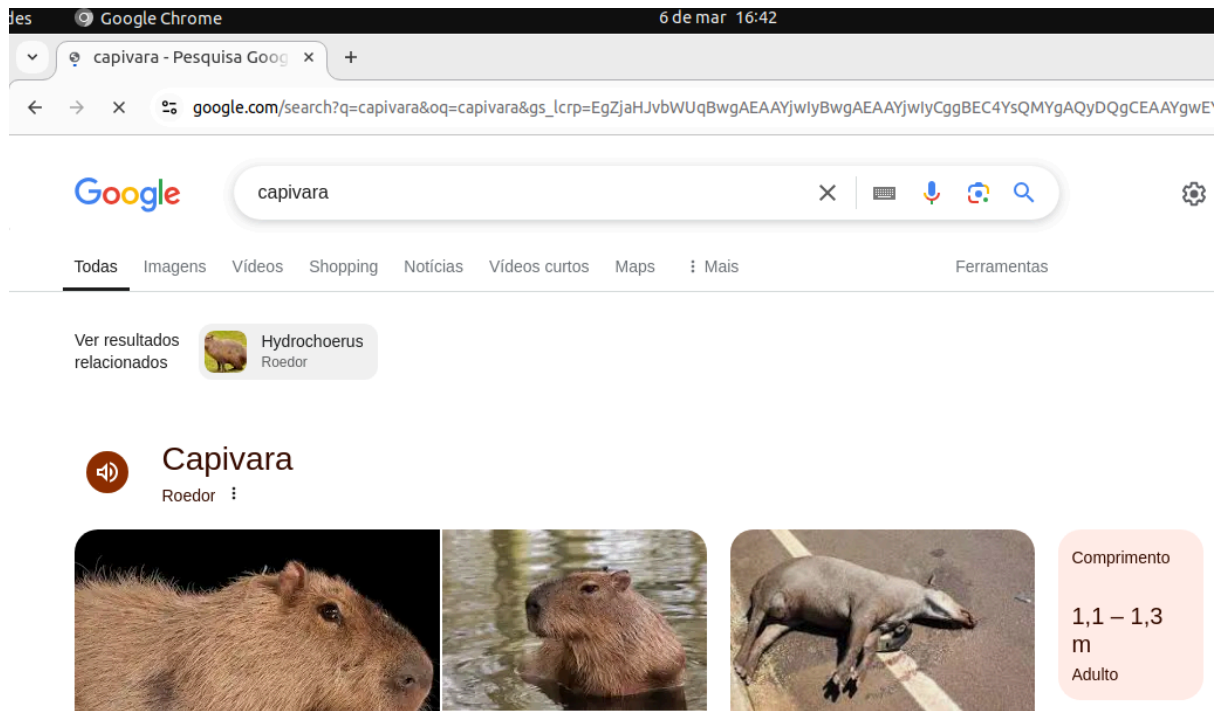
Como pode ver, o download foi bem sucedido

Abri o navegador, fui até três pontos no canto superior direito, Configurações > Sistema. No caso, o Chrome altera o proxy de acordo com o configurado na máquina, e não diretamente no navegador como foi no Firefox

Então vamos até as Configurações do Ubuntu, Rede > Proxy de rede



Ao abrir, selecionei a caixa **Manual** e preenchi os espaços com o ip



A conexão estabelecida com sucesso dentro do horário permitido



Não é possível acessar esse site

A página <https://discord.com/> pode estar temporariamente indisponível ou pode ter sido movida permanentemente para um novo endereço da Web.

ERR_TUNNEL_CONNECTION_FAILED

E o site **discord.com** não está disponível, como esperado

Agora vamos partir para os testes na máquina física Windows, utilizando um Windows 10

Fui em Configurações > Rede e Internet > Proxy, desci a página e coloquei as entradas

Usar um servidor proxy

☒ Ativado

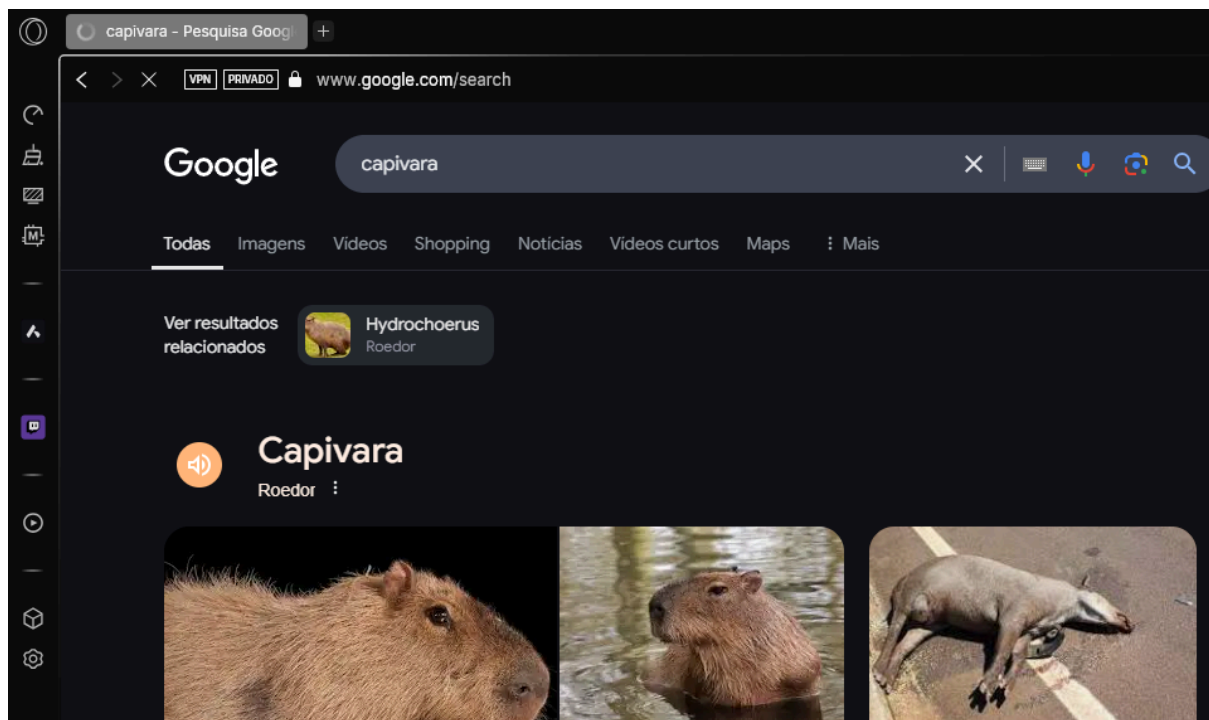
Endereço Porta

Use o servidor proxy, exceto para os endereços que comecem com as entradas a seguir. Use ponto e vírgula (;) para separar as entradas.

☐ Não usar o servidor proxy para endereços locais (intranet)

Salvar

Como os navegadores Firefox e Chrome já foram testados, irei usar o Opera desta vez



A pesquisa funcionando sem problema



Realizei o teste com o site **.steampowered.com**, e está bloqueado como esperado

6ª Etapa: Conclusões

Após todos os processos presentes neste relatório, o proxy Squid demonstrou muito potencial para o manuseio de uma rede.

Seja para monitoramento ou controle de acesso, acredito que com os conhecimentos aqui adquiridos, é possível uma configuração real para máquinas dentro de algum meio, seja empresarial ou acadêmico.

Além da capacidade de alteração, pois em meu código, basta alguém com a permissão para alterar o código e poderá retirar ou inserir novos sites e horários para configurar o proxy de acordo com a necessidade desejada.