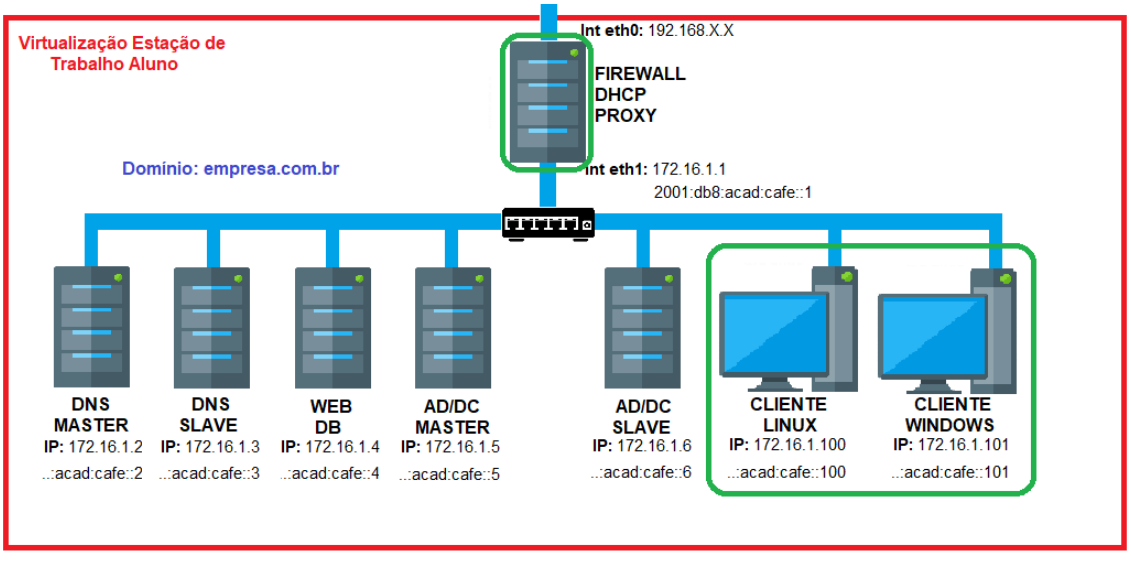
7. Implementação do serviço de Proxy

7.1 Introdução

O Squid é um proxy de armazenamento em cache para a Web que suporta os protocolos HTTP, HTTPS, FTP. Entre suas funções, desta-se a possessibilidade de redução da largura de banda e tempo de resposta mais rápidas, armazenando em cache e reutilizando páginas da Web acessadas com frequência. O Squid ainda possui suporte a ACLs (Listas de Controles de Acesso) para controle e filtro das conexões WEB realizadas pelos usuários da rede. O Squid está licenciado sob a GNU GPL e disponível para a maioria dos sistemas operacionais disponíveis, inclusive para o Windows.

Para este laboratório serão utilizadas as seguintes Máquinas Virtuais:

- Appl-Debian10-Firewall - Firewall, DHCP e Proxy
- Appl-Debian10-Client ou Appl-Windows7-Client - Realização de testes



7.2 Preparação do ambiente

Antes de iniciar a instalação e configuração do Servidor Proxy Squid, será necessário ajustar o script de firewall, acrescentando as linhas que liberam o INPUT e OUTPUT na porta 3128 (porta padrão do squid) no arquivo /etc/firewall/rules.

```
root@Firewall:/# vim /etc/firewall/rules
```

```
### Libera acesso ao Squid
iptables -A INPUT -p tcp --dport 3128 -j ACCEPT
```

Reinicie o serviço de firewall.

```
root@Firewall:/# service firewall restart
```

É importante destacar que na máquina que hospedará o serviço de proxy deverá estar ativada as regras básicas de compartilhamento da internet. Ou seja, o script de firewall deverá conter as seguintes linhas: (estas regras já foram ativadas na VM Firewall)

```
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

7.3 Instalação e configuração do Servidor Proxy Squid

Com as regras básicas aplicadas, agora será iniciada a instalação e configuração do servidor proxy. Para isso, inicialmente será intalado o softawre squid a partir dos repositórios oficiais do Debian.

```
root@Firewall:/# apt-get update
root@Firewall:/# apt-get install squid
```

Por questões de segurança, o arquivo original de configuração do Squid deverá ser renomeado caso seja necessário realizar uma futura consulta ou restauração da configuração padrão.

```
root@Firewall:/# mv /etc/squid/squid.conf /etc/squid/squid.conf.old
```

Para configurar o squid, será criado um novo arquivo de configuração (em branco) onde serão adicionadas somente as linhas necessárias para o correto funcionamento do serviço de proxy.

```
root@Firewall:/# vim /etc/squid/squid.conf
```

Insira o seguinte conteúdo no arquivo:

```
### SQUID 4

visible_hostname proxy.empresax.com.br
http_port 3128

# Configuracoes do Cache
cache_mem 512 MB
maximum_object_size_in_memory 4096 KB
maximum_object_size 512 MB
minimum_object_size 0 KB
cache_swap_low 90
cache_swap_high 95
```

```
# Cache de FQDN
fqdncache_size 1024

# Define a % do uso do cache ##
cache_swap_low 90
cache_swap_high 95

# Define o local do CACHE
cache_dir ufs /var/spool/squid 1600 16 256

# Definições de logs
access_log /var/log/squid/access.log
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
# Controle de rotacao dos arquivos de log
logfile_rotate 10

# Pag de erro Squid
error_directory /usr/share/squid/errors/pt-br

# Contato pag de erro Squid
cache_mgr admin@empresax.com.br

#Manter as configuracoes Default
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern . 0 20% 4320

#Forca a resolucao em IPv4
#Caso sua rede não possua IPV6
dns v4 first on

#acl defaults (Safe ports)
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 21 # FTP
acl Safe_ports port 443 563 873 # https,News
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 901 # swat
acl Safe_ports port 1025-65535 # Portasaltas
acl CONNECT method CONNECT


## Listas de Controle de acesso

#Acesso Defaults
acl manager url_regex -i ^cache_object:// /squid-internal-mgr/
acl redelocal src 172.16.1.0/24
http_access allow redelocal

http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

# Regra default
http_access allow localhost
http_reply_access allow all
```

7.3.1 Testando as configurações

Após realizar as configurações, é hora de testar as regras que foram adicionadas carregando as novas configurações do Squid com os comandos:

```
root@Firewall:/# squid -k parse
root@Firewall:/# squid -k reconfigure
```

O comando "parse" processará todas as linhas do arquivo "squid.conf" retornando erro, caso encontre.

Já o comando reconfigure, realizará a leitura do novo arquivo e aplicará as regras ao Squid (este comando não deverá retornar nenhuma mensagem).

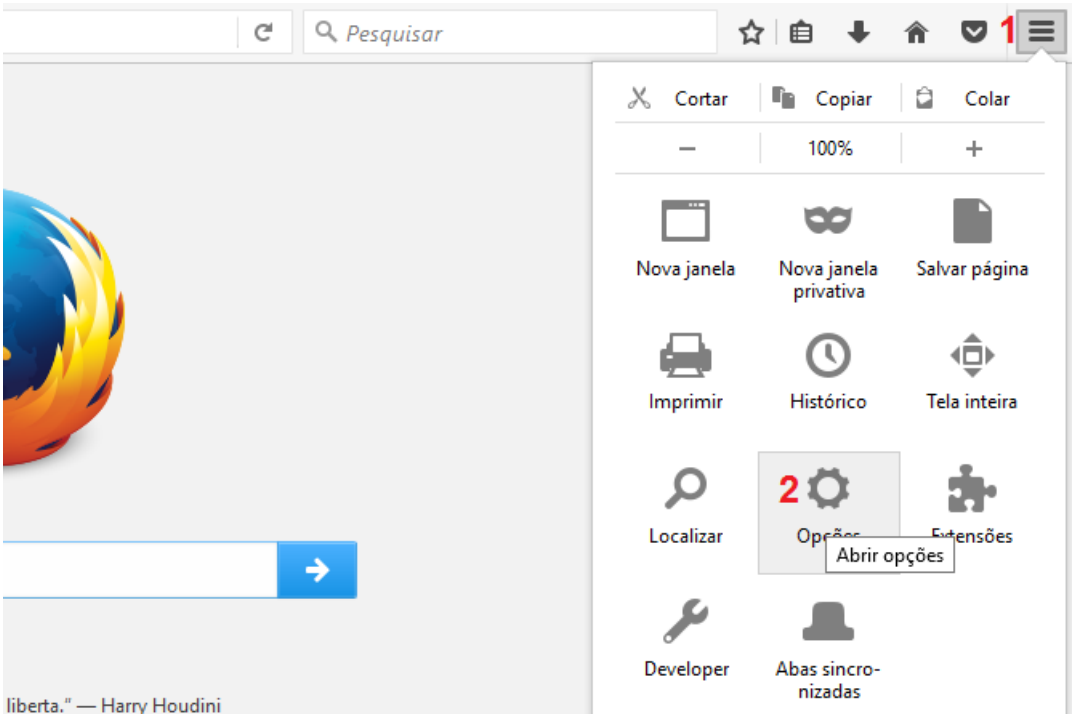
Não siga em frente caso os testes apresente erro. É prudente também, verificar o status do serviço, com o seguinte comando:

```
root@Firewall:/# systemctl status squid
```

Para realizar as atividades posteriores, será necessário confirmar o funcionamento do Proxy testando a navegação na Máquina Virtual Cliente, o tópico a seguir apresenta o passo-a-passo para configuração do Proxy no navegador Firefox da VM Debian10-Client.

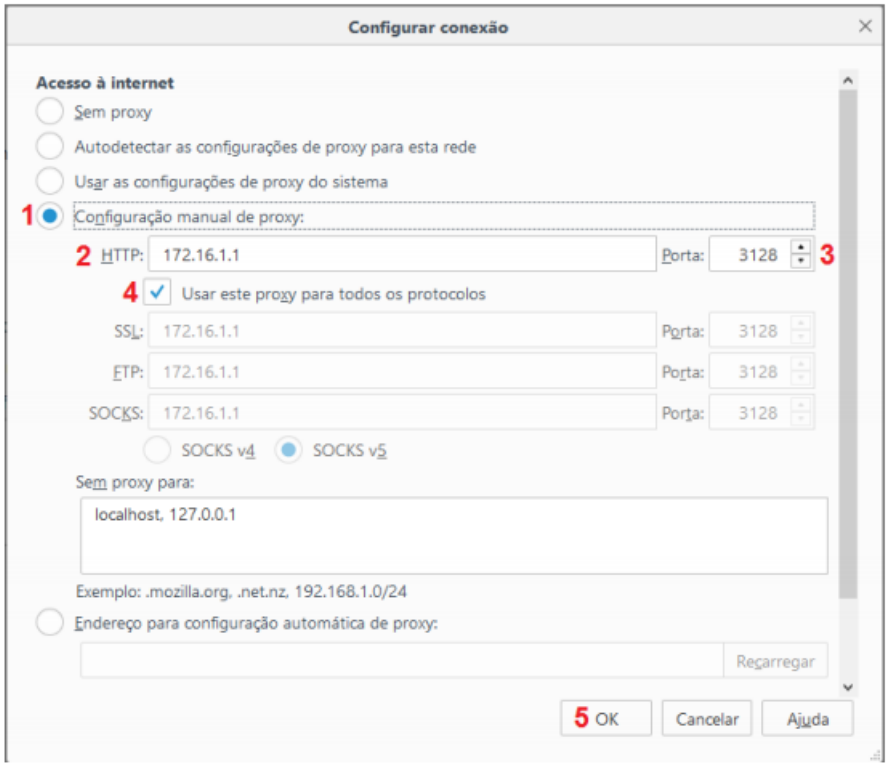
7.3.2 Configuração do proxy no navegador Firefox

Para testar o funcionamento do proxy, será realizado agora a configuração do navegador firefox da Máquina Virtual Cliente Linux. Para isso, clique no ícone configurações [1] e posteriormente em Opções [2], conforme apresentado na figura abaixo.



Na nova janela clique na opção Avançado [3], depois Rede [4] e por fim Configurar Conexão, conforme apresentado na figura 02.

Na aba “Configurar conexão”, ative a opção “Configuração manual de proxy”[1], preencha o campo HTTP com o endereço IP do servidor proxy [2] e porta 3128 [3], ative a opção “Usar este proxy para todos os protocolos”[4] e por fim clique em OK [5], conforme apresentado na figura 3.



7.4 Configuração de Listas de Controle de Acesso - ACL

Nesta seção, será configurada no Proxy Squid a utilização de Listas de Controle de Acesso (ACL) restringindo o acesso pelos seguintes elementos: endereço MAC, endereço IP, tempo, download por tipo de arquivo, domínios e palavras.

O Squid avalia as regras de acesso por procedência, ou seja, a primeira regra a qual a solicitação se adequar será a regra aplicada pelo servidor. Este comportamento faz com que todas as regras abaixo listadas devam anteceder a linha *http_access deny all* do arquivo de configuração.

Antes de iniciar a atividade, para melhor organização dos arquivos de controle de acesso, crie um diretório denominado *acls* dentro de */etc/squid/*.

```
root@Firewall:/# mkdir /etc/squid/acls
```

7.4.1 Restringir o acesso à internet para determinados endereços MAC

Para restringir o acesso à internet através do endereço MAC da interface de rede de uma estação de trabalho, inicialmente será criado o arquivo */etc/squid/acls/mac_bloqueados*, este arquivo será responsável por armazenar a lista com todos os endereços MAC que não poderão acessar o serviço.

```
root@Firewall:/# touch /etc/squid/acls/mac_bloqueados
```

Agora será editado o arquivo de configuração do Squid, para criarmos a ACL que será responsável pela restrição de acesso através de endereços MAC.

```
root@Firewall:/# vim /etc/squid/squid.conf
```

Insira as seguintes linhas no arquivo de configuração do Squid, logo após o comentário "##Listas de Controle de acesso".

```
#Restringe estação pelo MAC
acl mac arp "/etc/squid/acls/mac_bloqueados"
http_access deny mac
```

Para testar a configuração, insira no arquivo */etc/squid/acls/mac_bloqueados* o endereço MAC da interface de rede da estação cliente Windows ou Linux e efetue um reload no serviço Squid.

```
root@Firewall:/# systemctl reload squid
root@Firewall:/# systemctl status squid
```

Aspectos importantes:

1. O arquivo não pode ficar vazio, pois o serviço falhará na inicialização;
2. Em caso de bloqueio de mais de um endereço MAC, esses deverão ser adicionados um em cada linha.
3. As páginas de ERROS podem ser personalizadas no seguinte diretório: /usr/share/squid/errors/pt-br

Teste o acesso a internet através da VM cliente. Se o bloqueio foi aplicado corretamente, será carregada para o usuário a página de Acesso negado ao proxy.

Para realizar a próxima atividade, modifique o endereço MAC inserido no arquivo mac_bloqueados, ou comente as linhas referentes a restrição no arquivo *squid.conf*.

7.4.2 Restringir o acesso à internet para determinado endereço IP

Para restringir o acesso à internet através do endereço IP da interface de rede de uma estação de trabalho, criaremos o arquivo */etc/squid/acls/ip_bloqueados*, esse arquivo será responsável por armazenar a lista com todos os endereços IP que não poderão acessar o serviço.

```
root@Firewall:/# touch /etc/squid/acls/ip_bloqueados
```

Agora edite o arquivo de configuração do Squid, para inserir as linhas referentes a ACL que será responsável pela restrição de acesso através de endereços IP.

```
root@Firewall:/# vim /etc/squid/squid.conf
```

Insira as seguintes linhas no arquivo de configuração do Squid, logo após as linhas que restringem o acesso por endereço MAC.

```
#Restringe estação pelo IP
acl negaip src "/etc/squid/acls/ip_bloqueados"
http_access deny negaip
```

Para testar a configuração, insira no arquivo */etc/squid/acls/ip_bloqueados* o endereço IP da interface de rede da estação cliente Windows ou Linux e efetue um reload no serviço Squid.

```
root@Firewall:/# systemctl reload squid
root@Firewall:/# systemctl status squid
```

Teste o acesso a internet através da VM cliente.

Aspectos importantes:

1. O arquivo não pode ficar vazio, pois o serviço falhará na inicialização;
2. Em caso de bloqueio de mais de um endereço IP, esses deverão ser adicionados um em cada linha.

Para realizar a próxima atividade, modifique o endereço IP inserido no arquivo ip_bloqueados, ou comente as linhas referentes a restrição no arquivo *squid.conf*.

7.4.3 Restringir o acesso à internet por tempo

Para restringir o acesso à internet por tempo pré determinado, edite o arquivo de configuração do Squid e crie a ACL que será responsável por essa restrição.

```
root@Firewall:/# vim /etc/squid/squid.conf
```

Insira as seguintes linhas no arquivo de configuração do Squid, logo após as linhas que restringem o acesso por endereço IP.

```
#Limitar horário de acesso
acl horario1 time MTWHF 00:00-06:00
acl horario2 time MTWHF 12:00-14:00
http_access deny horario1
http_access deny horario2
```

Efetue um reload no serviço Squid.

```
root@Firewall:/# systemctl reload squid
root@Firewall:/# systemctl status squid
```

Teste a conexão na máquina virtual cliente, o acesso não deverá ser bloqueado, pois o bloqueio está programado para o período de 00h até 06h e 12h até 14h.

Para testar se o bloqueio está funcional, modifique o horário do servidor.

```
root@Firewall:/# date -s 13:00:00
```

Faça o teste de conexão com a internet a partir da máquina virtual cliente. Agora o bloqueio deve ter sido efetivado.

Aspectos importantes: Para realizar a próxima atividade, modifique o horário do servidor para a hora atual.

7.4.4 Restringir acesso a sites por listas de palavras e domínios

Inicialmente será criada a restrição por lista de palavras. Para isso, será criado o arquivo /etc/squid /acls/palavras_bloqueadas.

```
root@server:/# vim /etc/squid/acls/palavras_bloqueadas
```

Nesse arquivo adicionaremos uma lista de palavras que não poderão ser utilizadas nas URL's acessadas. Insira a seguinte lista para teste.

facebook
youtube
instagram
snapchat

Agora será criado o arquivo /etc/squid/acls/url_bloqueados que irá conter uma lista com todos os endereços de sites que não poderão ser acessados.

```
root@Firewall:/# vim /etc/squid/acls/url_bloqueados
```

Nesse arquivo, adicione a lista de endereços de sites que não poderão ser acessados. Insira a seguinte lista para teste.

br.pinterest.com
www.twitter.com/
batepapo.uol.com.br
musica.uol.com.br

Para efetivar as restrições por palavras e endereços de sites, será criada as ACLs no arquivo de configuração do Squid.

```
root@server:/# vim /etc/squid/squid.conf
```

Insira as seguintes linhas no arquivo de configuração do Squid, logo após as linhas que restringem o download por tipo de extensão.

```
#Negar pesquisa ou acesso por palavras
acl negapalavra url_regex "/etc/squid/acls/palavras_bloqueadas"
http_access deny negapalavra

#Negar acesso a determinadas paginas
acl negaurl dstdomain "/etc/squid /acls/url_bloqueados"
http_access deny negaurl
```

Efetue um reload no serviço Squid.

```
root@Firewall:/# systemctl reload squid
root@Firewall:/# systemctl status squid
```

Teste na máquina cliente o acesso aos sites bloqueados e endereços que contenham as palavras definidas no arquivo de bloqueio.