Manual de instalação e configuração do Squid no CentOS versão 6.10

O Squid Proxy é um servidor de proxy amplamente utilizado no Linux. Uma de suas principais características é a função de armazenamento em cache do conteúdo da Web acessado pelos usuários.

Cache é uma espécie de depósito de objetos da Internet, como arquivos e páginas completas. Ele é utilizado para facilitar o acesso aos conteúdos e entregá-los de forma segura ao solicitante já que armazena o conteúdo previamente acesso, dessa forma, consegue entregar requisições solicitadas sem a necessidade de buscá-lo novamente na internet.

Como instalar o Squid?

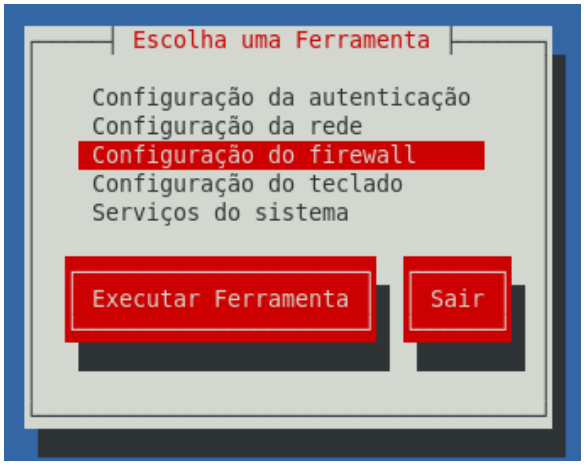
1 – Digite o seguinte comando (como usuário root):

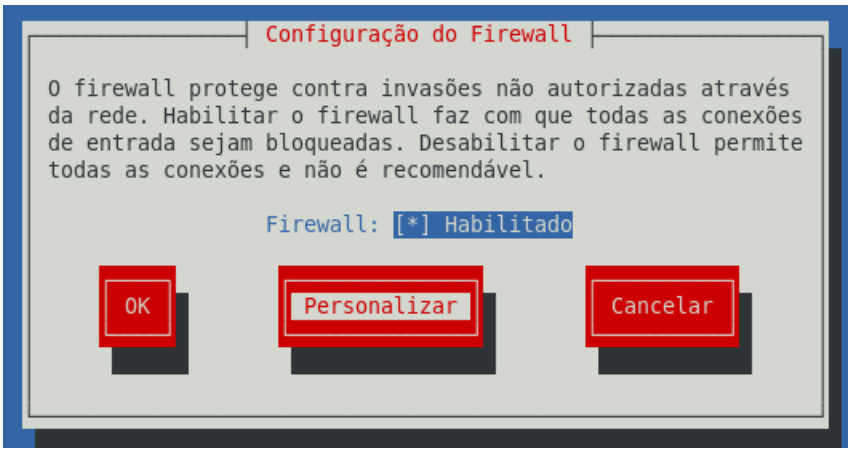
#yum install squid

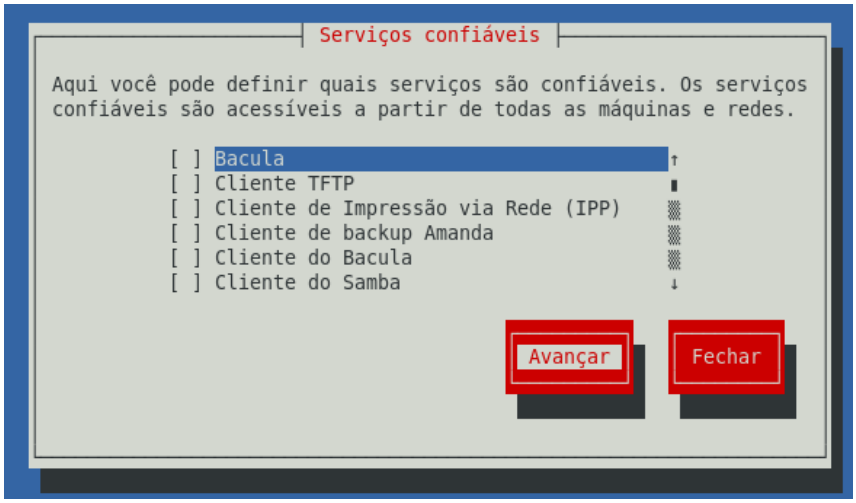
2 – Após instalar o Squid é necessário realizar a configuração do encaminhamento de portas através do firewall, para isso, digite o comando:

#setup

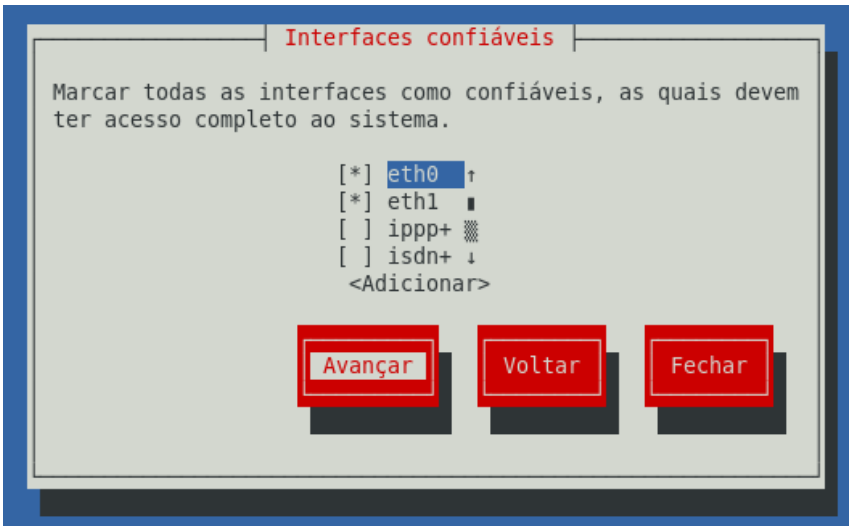
Agora siga as informações conforme as imagens abaixo:



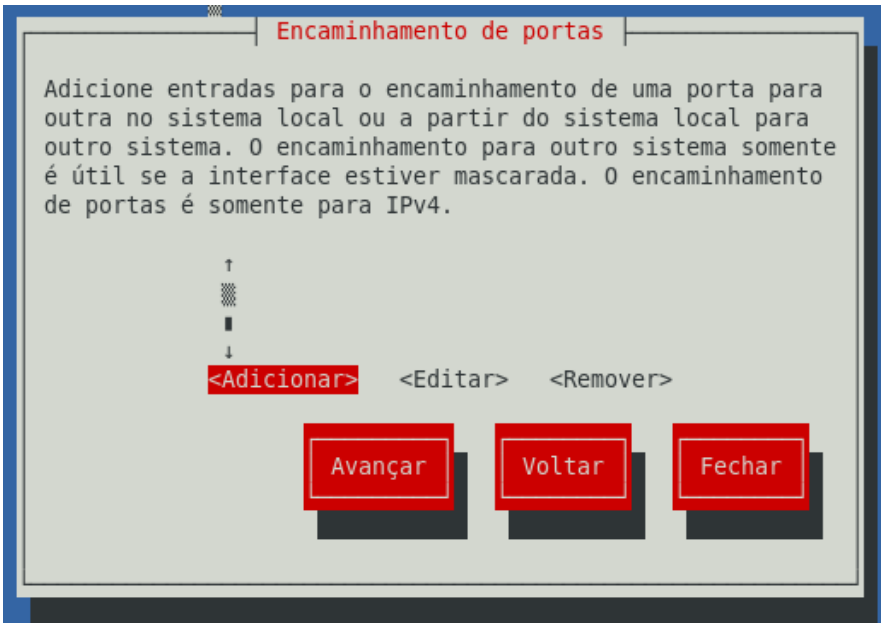

Configuração do Firewall
O firewall protege contra invasões não autorizadas através da rede. Habilitar o firewall faz com que todas as conexões de entrada sejam bloqueadas. Desabilitar o firewall permite todas as conexões e não é recomendável.
Firewall: [*] Habilitado
OK
Personalizar
Cancelar

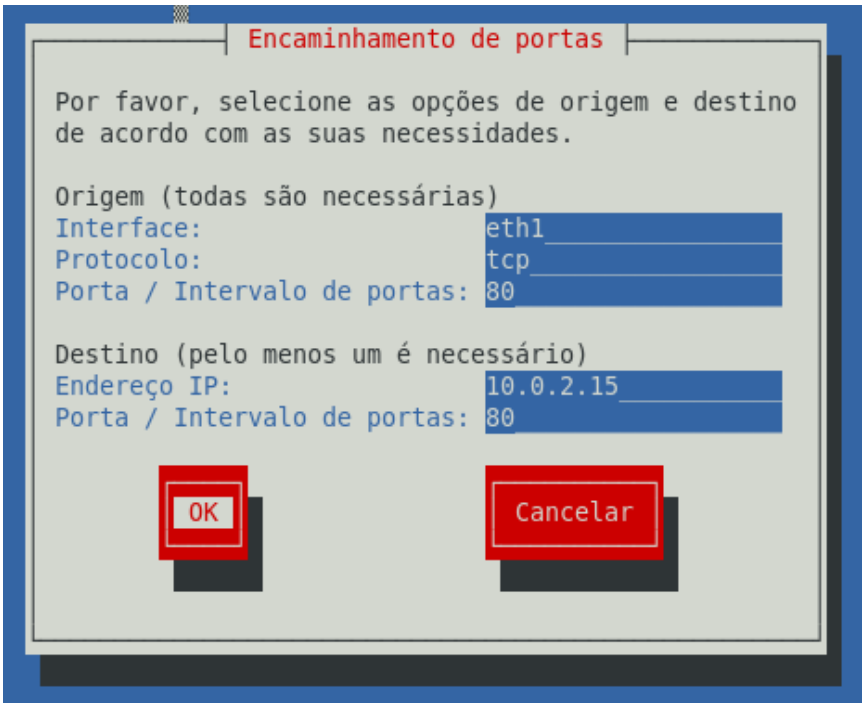

Serviços confiáveis
Aqui você pode definir quais serviços são confiáveis. Os serviços confiáveis são acessíveis a partir de todas as máquinas e redes.
[ ] Bacula
[ ] Cliente TFTP
[ ] Cliente de Impressão via Rede (IPP)
[ ] Cliente de backup Amanda
[ ] Cliente do Bacula
[ ] Cliente do Samba
Avançar
Fechar

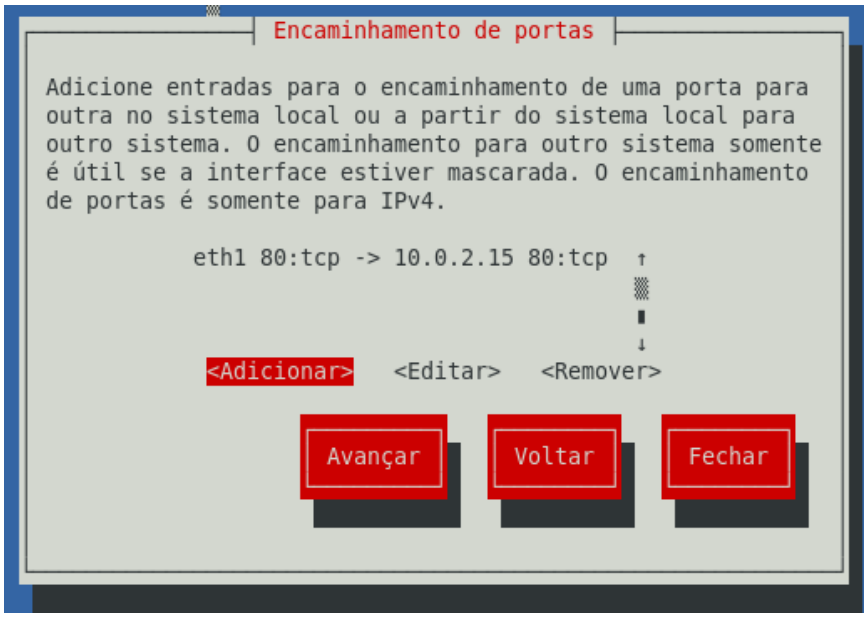

Outras portas
Incluir portar adicionais ou intervalos de portas, que precisam estar acessíveis para todas as máquinas ou redes.
<Adicionar>
<Editar>
<Remover>
Avançar
Voltar
Fechar

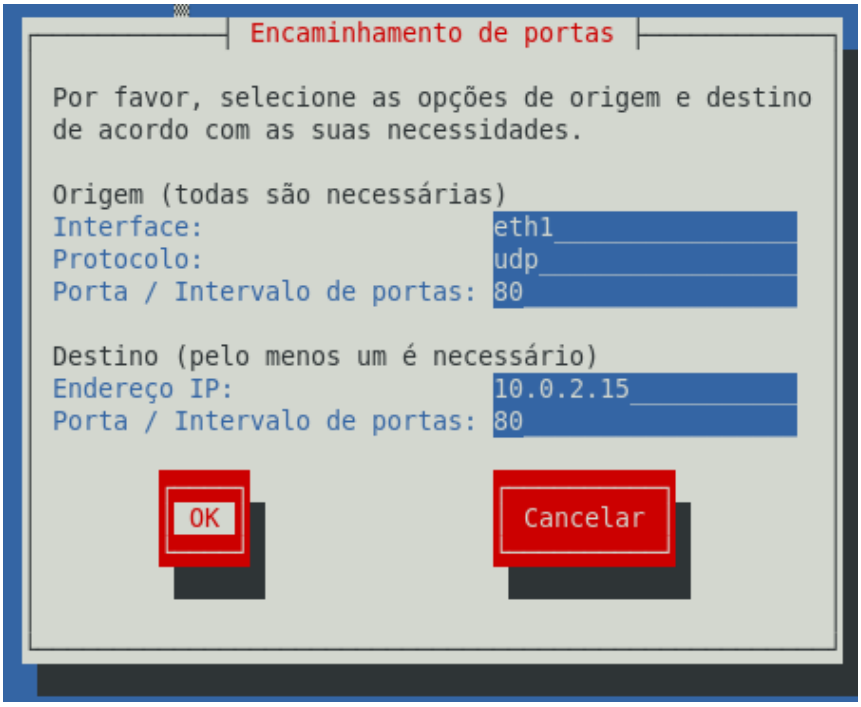

Interfaces confiáveis
Marcar todas as interfaces como confiáveis, as quais devem ter acesso completo ao sistema.
[*] eth0
[*] eth1
[ ] ippp+
[ ] isdn+
<Adicionar>
Avançar
Voltar
Fechar

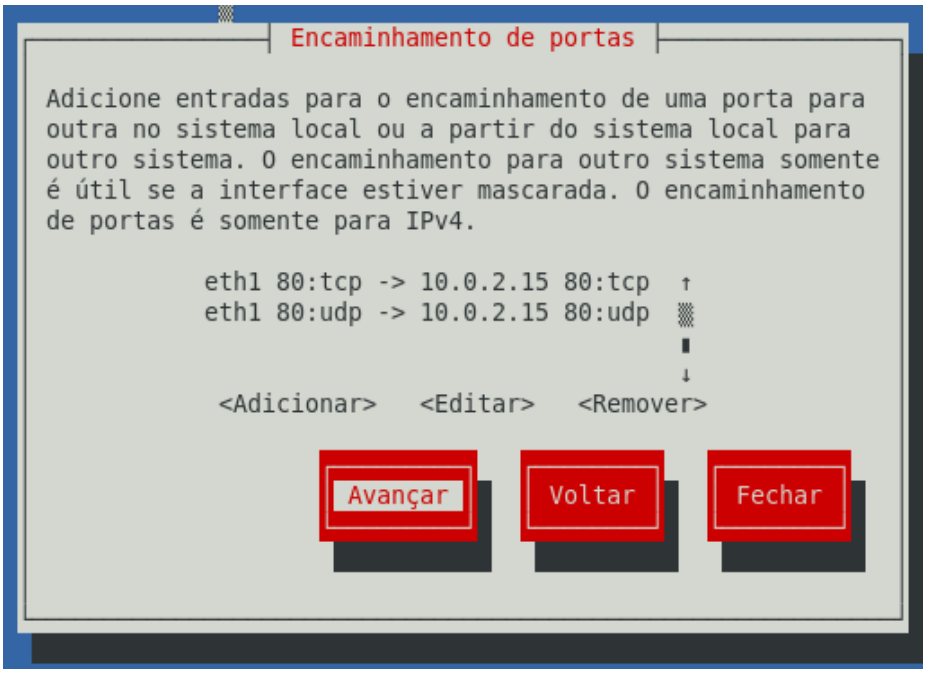

Mascarar
Selecione as interfaces para o uso de máscaras.
[*] eth0
[*] eth1
[ ] ippp+
[ ] isdn+
<Adicionar>
Avançar
Voltar
Fechar


Encaminhamento de portas
Adicione entradas para o encaminhamento de uma porta para outra no sistema local ou a partir do sistema local para outro sistema. O encaminhamento para outro sistema somente é útil se a interface estiver mascarada. O encaminhamento de portas é somente para IPv4.
<Adicionar>
<Editar>
<Remover>
Avançar
Voltar
Fechar

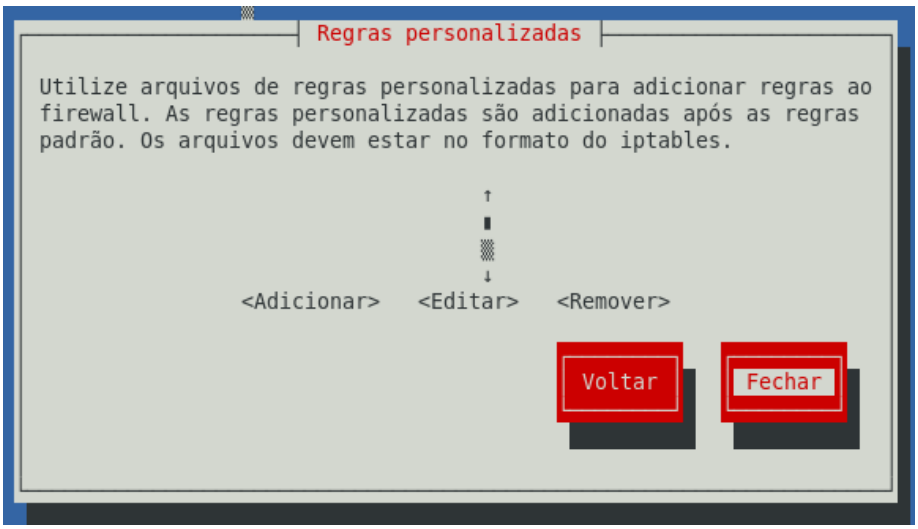

Encaminhamento de portas
Por favor, selecione as opções de origem e destino de acordo com as suas necessidades.
Origem (todas são necessárias)
Interface: eth1
Protocolo: tcp
Porta / Intervalo de portas: 80
Destino (pelo menos um é necessário)
Endereço IP: 10.0.2.15
Porta / Intervalo de portas: 80
OK
Cancelar

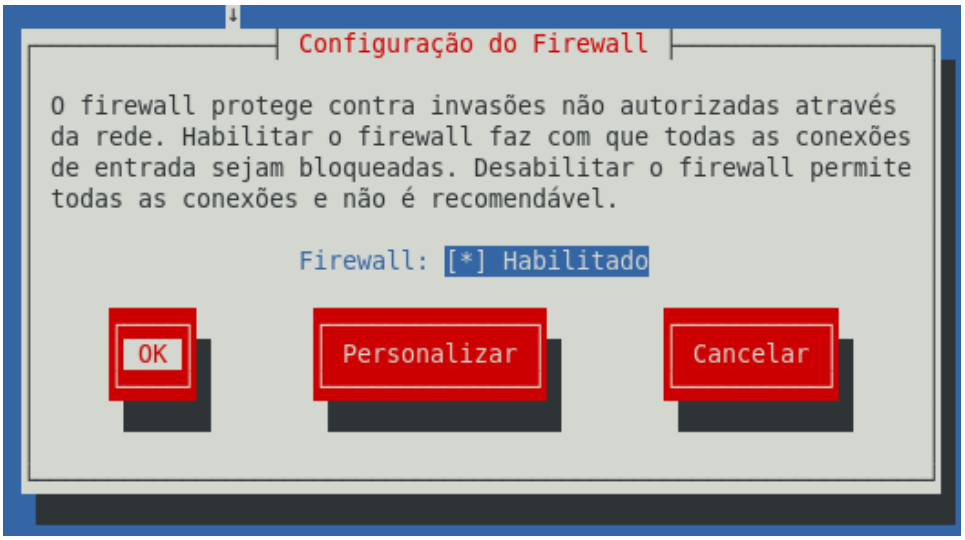

Encaminhamento de portas
Adicione entradas para o encaminhamento de uma porta para outra no sistema local ou a partir do sistema local para outro sistema. O encaminhamento para outro sistema somente é útil se a interface estiver mascarada. O encaminhamento de portas é somente para IPv4.
eth1 80:tcp -> 10.0.2.15 80:tcp
<Adicionar>
<Editar>
<Remover>
Avançar
Voltar
Fechar

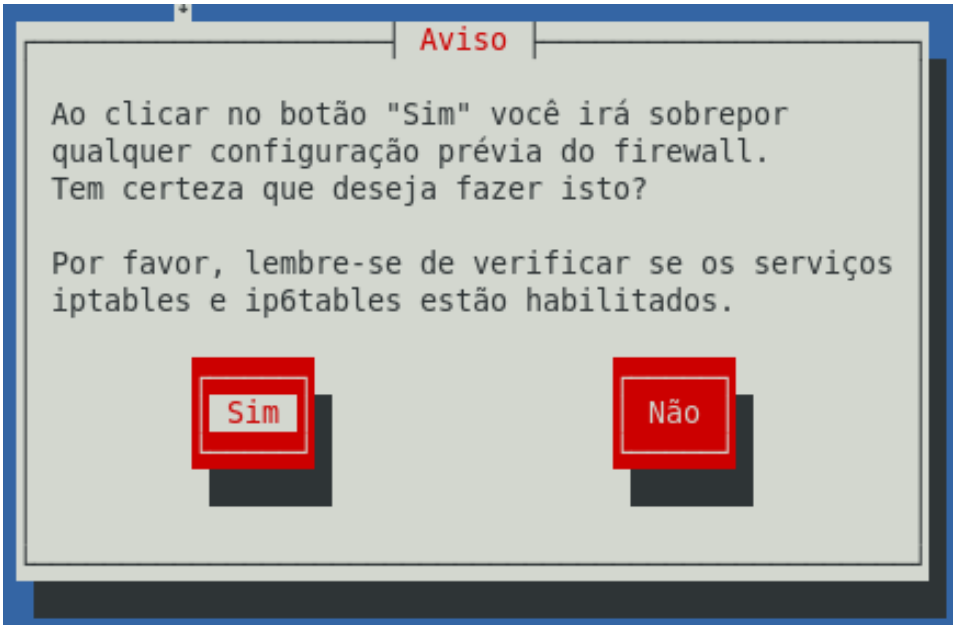

Encaminhamento de portas
Por favor, selecione as opções de origem e destino de acordo com as suas necessidades.
Origem (todas são necessárias)
Interface: eth1
Protocolo: udp
Porta / Intervalo de portas: 80
Destino (pelo menos um é necessário)
Endereço IP: 10.0.2.15
Porta / Intervalo de portas: 80
OK
Cancelar

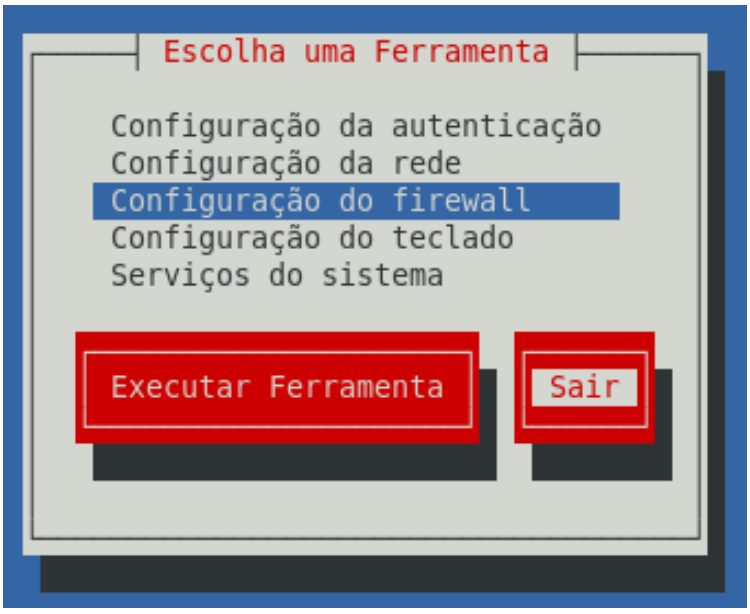

Encaminhamento de portas
Adicione entradas para o encaminhamento de uma porta para outra no sistema local ou a partir do sistema local para outro sistema. O encaminhamento para outro sistema somente é útil se a interface estiver mascarada. O encaminhamento de portas é somente para IPv4.
eth1 80:tcp -> 10.0.2.15 80:tcp
eth1 80:udp -> 10.0.2.15 80:udp
<Adicionar>
<Editar>
<Remover>
Avançar
Voltar
Fechar


Filtro ICMP
Marque na lista os tipos de ICMP que devem ser rejeitados. Todos os outros tipos são permitidos para passar pelo firewall. O padrão é não haver limitações.
[ ] Requisição de eco (ping)
[ ] Resposta de eco (pong)
[ ] Destino inacessível
[ ] Problema de parâmetro
Avançar
Voltar
Fechar


Regras personalizadas
Utilize arquivos de regras personalizadas para adicionar regras ao firewall. As regras personalizadas são adicionadas após as regras padrão. Os arquivos devem estar no formato do iptables.
<Adicionar>
<Editar>
<Remover>
Voltar
Fechar


Configuração do Firewall
O firewall protege contra invasões não autorizadas através da rede. Habilitar o firewall faz com que todas as conexões de entrada sejam bloqueadas. Desabilitar o firewall permite todas as conexões e não é recomendável.
Firewall: [*] Habilitado
OK
Personalizar
Cancelar


Aviso
Ao clicar no botão "Sim" você irá sobrepor qualquer configuração prévia do firewall.
Tem certeza que deseja fazer isto?
Por favor, lembre-se de verificar se os serviços iptables e ip6tables estão habilitados.
Sim
Não


Escolha uma Ferramenta
Configuração da autenticação
Configuração da rede
Configuração do firewall
Configuração do teclado
Serviços do sistema
Executar Ferramenta
Sair

3 – Agora vamos editar o arquivo de configuração do Squid, vá até /etc/squid e abra o arquivo de configuração:

#vi squid.conf

Escreva as linhas abaixo:

```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
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 CONNECT method CONNECT

acl proibidos url_regex -i "/etc/squid/proibidos"

http_access deny proibidos
```

Salve e saia do arquivo

Agora vamos criar o arquivo proibidos, esse arquivo contém as palavras que serão filtradas pelo Squid

#vi proibidos

Deixe o conteúdo como na imagem:

```
uol
facebook
yahoo
~
~
~
~
~
~
~
```

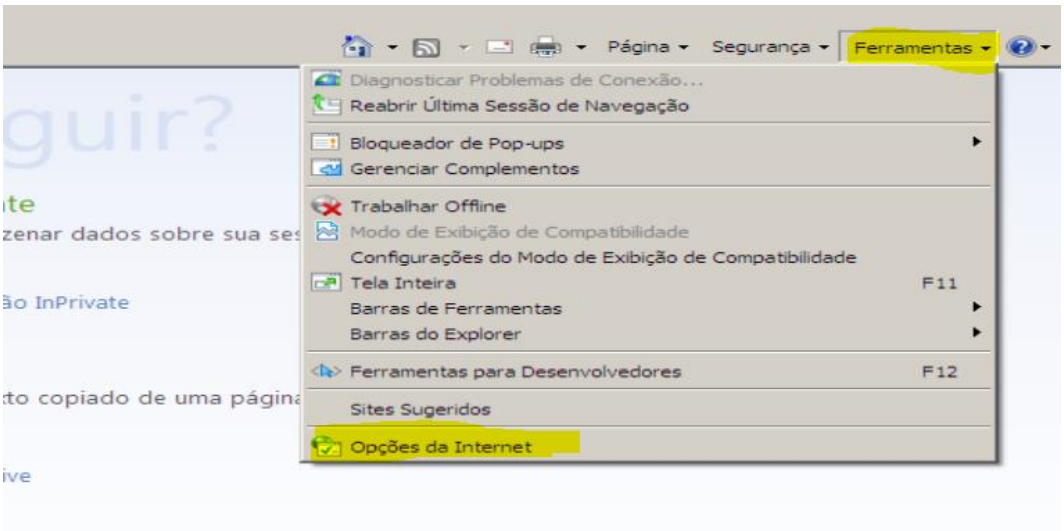
Salve e saia do arquivo

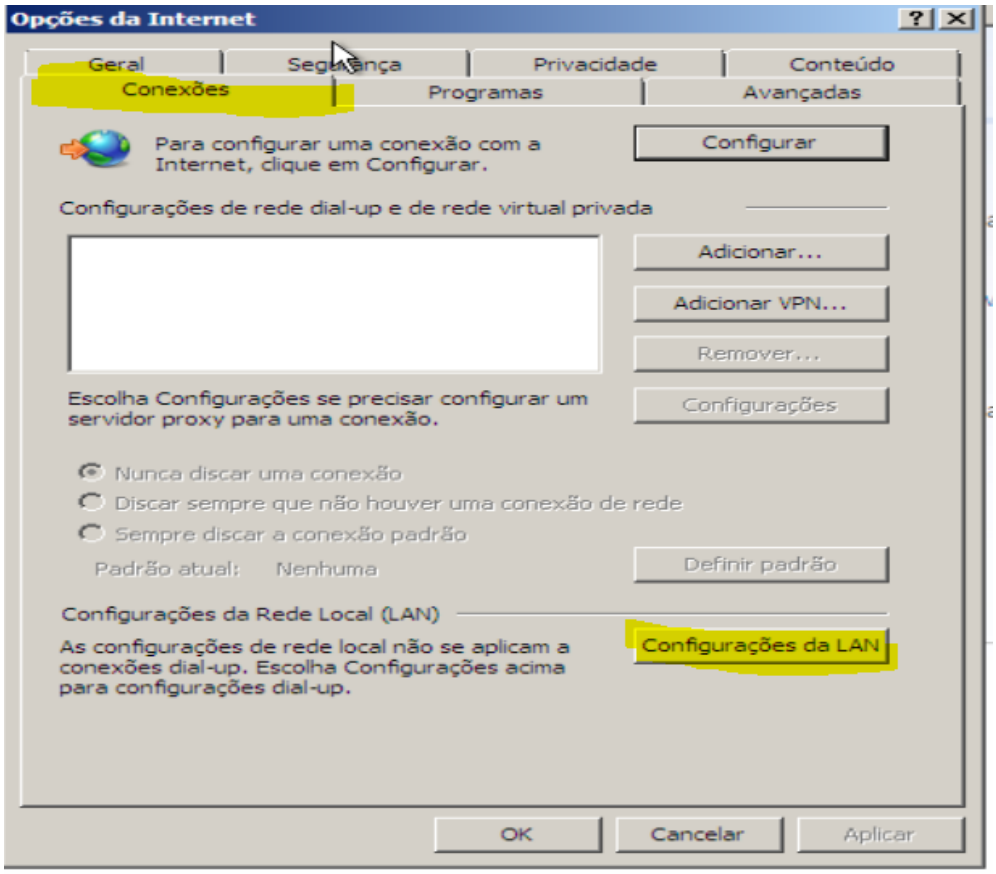
Agora vamos reiniciar o serviço

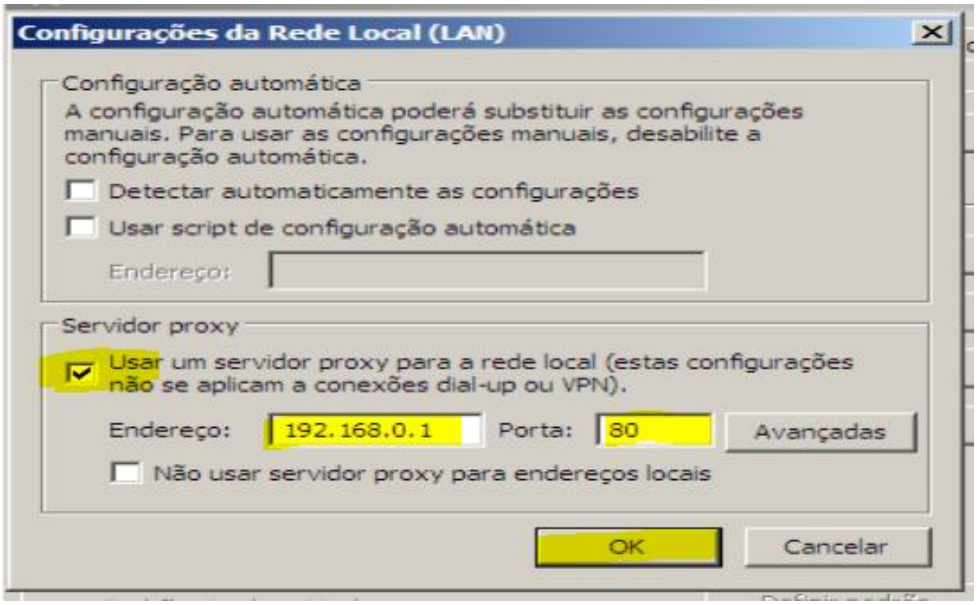
#service squid restart

```
[root@localhost squid]# service squid restart
Parando o squid: .................                         [  OK  ]
Iniciando o squid: .                                      [  OK  ]
[root@localhost squid]#
```

Agora vá até a máquina virtual cliente (Windows) e abra o navegador:

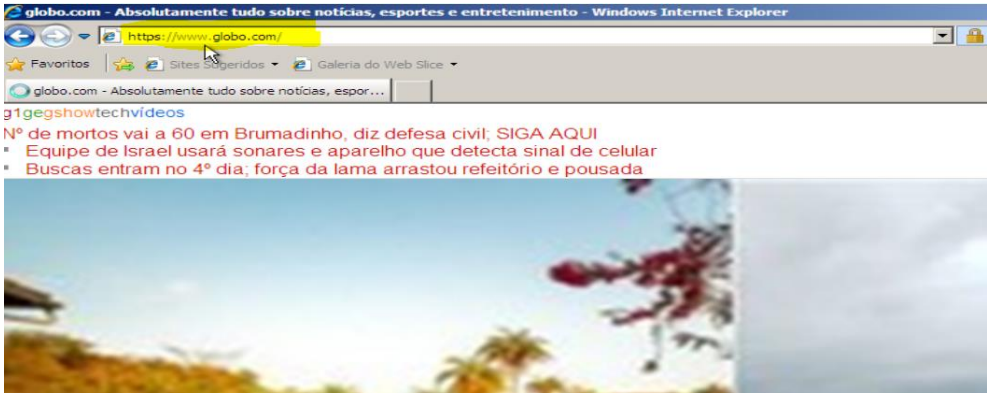






Agora realize os testes de navegação, todos os sites que estão dentro do arquivo proibidos não devem ser acessados, de mesma oposta, os sites que não estão no arquivo devem ser acessados normalmente.

Esse não está na lista de proibidos



Esse está na lista de proibidos