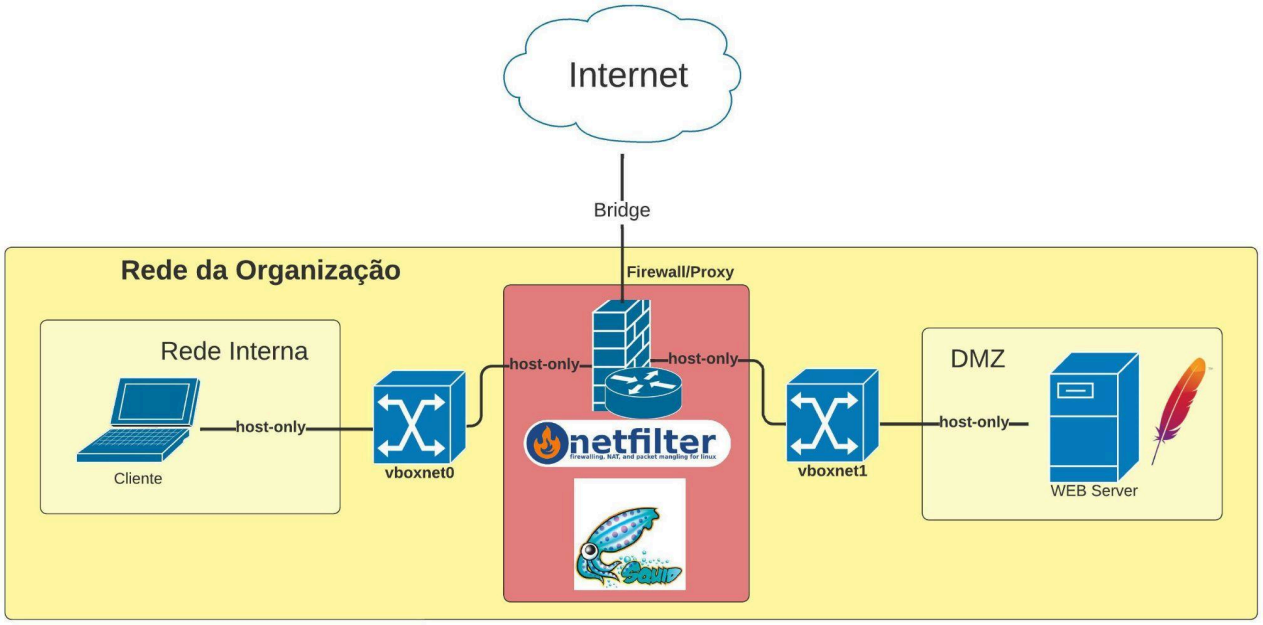
Laboratório de Segurança – VirtualBox



VM do firewall

#No VIRTUALBOX
#Adicionar Interface de rede
Arquivo → Host Network Manager
Clicar em criar

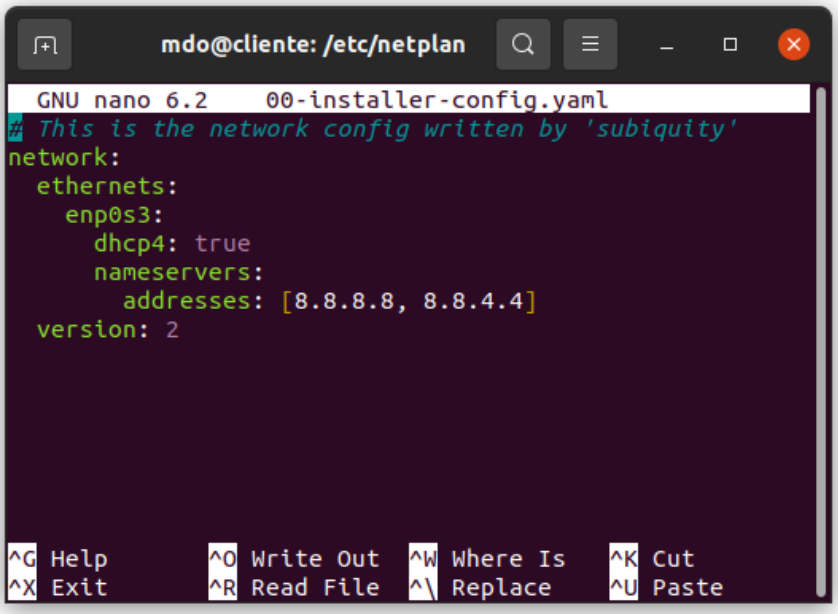
Configurar a Interface host-only (ex: enp0s8)
sudo ip link set <interface-host-only> up
sudo dhclient <interface-host-only>

Encaminhar pacotes (firewall)
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
Verrificar se o encaminhamento foi habilitado (ip_forward = 1)
cat /proc/sys/net/ipv4/ip_forward

Configurar o NAT para masquerade
sudo iptables -t nat -A POSTROUTING -o **<interface-bridge-firewall>** -j MASQUERADE

VM do Cliente

configurar o DNS
cd /etc/netplan
sudo pico 00-installer-config.yaml



sudo netplan apply
resolvectl status | grep "DNS Server" -A2

Configurar o gateway padrão
sudo ip route add default via **<ip-do-firewall-host-only-enp0s8>**
você pode testar o ping para alguma máquina externa
ping 8.8.8.8

SQUID - VM do FIREWALL

Configurar NAT para redirecionamento (proxy transparent)
sudo iptables -t nat -A PREROUTING -i enp0s8 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3129
sudo iptables -t nat -A PREROUTING -i enp0s8 -p tcp -m tcp --dport 433 -j REDIRECT --to-ports 3130

#Instalar o Squid
sudo apt-get update
sudo apt-get install squid

cd /etc/squid/
#Fazer o backup do arquivo de configuracao
sudo cp ./squid.conf ./squid.conf.original

#Configurar o squid
sudo pico squid.conf

Squid normally listens to port 3128
http_port 3128
http_port 3129 intercept
http_port 3130 intercept

#
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
include /etc/squid/conf.d/*.conf

acl localnet src 192.168.56.0/24

acl blockuece url_regex uece
http_access deny localnet blockuece

acl blockufc url_regex ufc
http_access deny localnet blockufc

http_access allow localnet

And finally deny all other access to this proxy
http_access deny all

#squid recarregar o arquivo de configuracoes
sudo invoke-rc.d squid reload

#verificar se o arquivo de configuracao possui erros
squid -k parse

#reiniciar o squid
sudo invoke-rc.d squid restart

#encerrar o squid
sudo invoke-rc.d squid stop

sudo invoke-rc.d squid status

#Adicionar rede privada DMZ
Arquivo → Host Network Manager
Clicar em criar
#Lembrar de habilitar a nova vboxnet criada

#Clonar a VM Cliente para criar a VM webserver
#Lembrar de criar novos endereços MAC na opção “política de endereço MAC”
#Fazer o **Clone Linkado** ao invés do **Clone Completo**

#Com a VM **webserver** iniciada, faça:
#Atualizar o hostname da VM criada
sudo hostnamectl set-hostname webserver

#configurar o gateway padrão
sudo ip route add default via **<ip-do-firewall-host-only>**

#você pode testar o ping para alguma máquina externa
ping 8.8.8.8

#instalar o apache
sudo apt-get install apache2

#verificar o status do apache
sudo systemctl status apache2

#testar localmente
wget localhost

#VM do Firewall
#configurar a nova interface host-only nas configs de rede do virtualbox
#escolher a nova rede privada criada (ex: vboxnet1)

#Provavelmente essa nova interface não estará configurada
#Configurar a Interface host-only (ex: enp0s9)
sudo ip link set <interface-host-only> up
sudo dhclient <interface-host-only>

#DNAT - **VM do Firewall**
#Redirecionar o tráfego WEB destinado ao firewall ao ***webserver*** da organização na DMZ

sudo iptables -t nat -A PREROUTING -d <ip-do-firewall-bridge> -p tcp -m tcp --dport 80 -j DNAT --to-destination <ip-do-webserver>:80

#Testar no browser do host real
http://<ip-do-firewall-bridge>