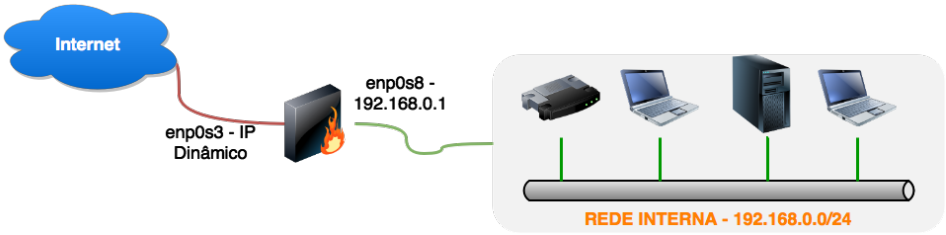
Campus: Palmares
Curso: Redes de Computadores
Disciplina: Segurança em Redes de Computadores

Prática IPTABLES – Montando um Firewall Linux usando IPTABLES para permitir o acesso dos usuários a Internet

O ambiente virtual será composto dos seguintes elementos:

- 01 VM Linux rodando UBUNTU Linux
- 01 VM Windows 7, 8 ou 10

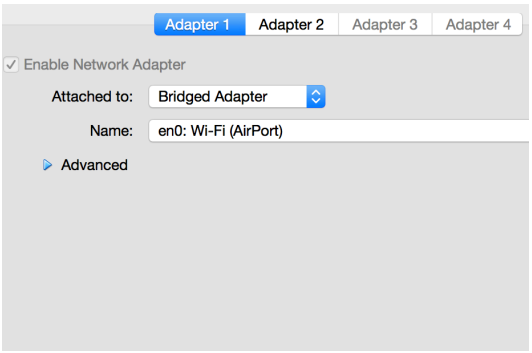


PREPARANDO VIRTUALBOX

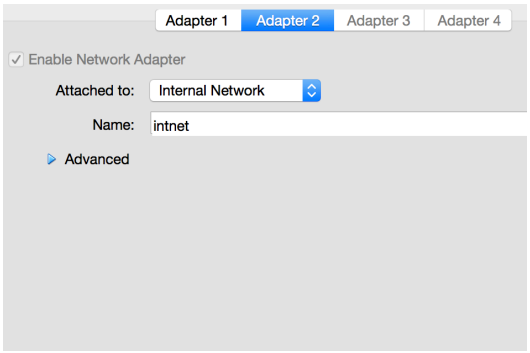
1. Você deverá inicialmente realizar os ajustes nas interfaces de rede de ambas as VMs, seguindo o padrão abaixo. Adapter 1 (Bridged Adapter) e Adapter 2 (Internal Network).

VM LINUX

Adapter 1

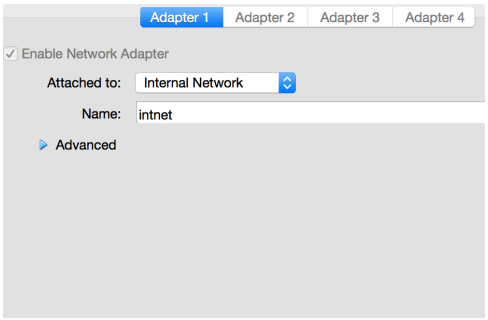


Adapter 2



VM Win

Adapter 1



PREPARANDO O FIREWALL

1. Depois de inicializada a VM, verifique as interfaces. Identifique a numeração das interfaces. Na nossa VM a numeração foi enp0s3 para a interface *Bridged* e enp0s8 para a interface *Internal Network*. No seu caso essa numeração pode variar e você deverá considerar as suas durante a atividade.

```
# ifconfig -a
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:88:24:8b
          inet addr:192.168.2.15  Bcast:192.168.2.255  Mask:255.255.255.0
....
enp0s8    Link encap:Ethernet  HWaddr 08:00:27:2d:b8:24
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
....
```

2. Configure os IPs das interfaces *Bridged* e *Internal*, editando o arquivo abaixo, e adicionando o conteúdo informado, configurando a interface enp0s3 com DHCP e a enp0s8 com IP estático (192.168.0.1). O DNS deverá ser configurado automaticamente no momento que você recebe o IP automático da interface *bridged*.

```
# nano /etc/network/interfaces
auto enp0s3
iface eth0 inet dhcp


auto enp0s8
iface eth0 inet static
   address 192.168.0.151
   netmask 255.255.255.0

# service networking restart
```

3. Habilite no Kernel o *forward* de pacotes entre as interfaces:

```
# vi /etc/sysctl.conf
net.ipv4.ip_forward=1
```

4. Instalando e habilitando o servidor DHCP na interface *Internal* do Firewall, de modo que os clientes da rede interna possam receber IPs dinâmicos. O arquivo de configuração poderá ser baixado do Github.

```
# apt-get install udhcpd
# cd /etc
# rm -f udhcpd.conf
# wget https://raw.githubusercontent.com/hutger/PMR-SRC-SCRIPTS/master/udhcpd.conf

# service udhcpd restart
```

5. Verifique se existem regras adicionadas na tabela FILTER e NAT

```
# iptables -L
# iptables -t nat -L
```

6. Se houverem regras adicionadas (o que provavelmente não terão), apague-as:

```
# iptables -F
# iptables -t nat -F
```

7. Alterando a *Policy* padrão para DROP, para as *chains* INPUT e FORWARD:

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
```

8. Permitindo conexões ESTABLISHED e RELATED:

```
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

9. Permitindo acesso SSH ao Firewall a partir da rede *Internal*:

```
# iptables -A INPUT -i enp0s8 -s 192.168.0.0/24 -p tcp --dport 22 -
j ACCEPT
```

10. Permitindo que os hosts da rede *Internal* acessem os serviços HTTP, HTTPS e DNS externamente.

```
# iptables -A FORWARD -i enp0s8 -s 192.168.0.0/24 -p tcp -m multiport
--dports 80,443 -j ACCEPT
# iptables -A FORWARD -i enp0s8 -s 192.168.0.0/24 -p udp -m multiport
--dports 53 -j ACCEPT
```

11. É importante lembrar que o endereço da rede *Internal* é privado e não pode ser roteado na Internet. Desse modo, é necessário mascará-lo de modo que os pacotes possam trafegar externamente. Assim, utilizamos recurso de NAT para esse fim.

```
# iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -j MASQUERADE -o enp0s3
```

12. De modo a podermos realizar testes de conectividade, é interessante habilitar o protocolo ICMP, para que internamente os usuários possam realizar testes:

```
# iptables -A INPUT -i enp0s8 -s 192.168.0.0/24 -p icmp -j ACCEPT
# iptables -A FORWARD -i enp0s8 -s 192.168.0.0/24 -p icmp -j ACCEPT
```

13. Permitindo acesso externo ao serviço de SSH a partir de um host da Rede Interna:

```
# iptables -A FORWARD -i enp0s8 -s 192.168.0.10 -p tcp --dport 22 -j ACCEPT
```

14. Negando o acesso a um site especifico. Ex. ao site do UOL:

```
# iptables -I FORWARD 1 -i enp0s8 -s 192.168.0.0/24 -d www.uol.com.br -p tcp --dport 80 -j ACCEPT
```

15. Salvando as regras para uso futuro:

```
# iptables-save > /root/firewall.save
```

16. Carregando regras salvas:

```
# iptables-restore < /root/firewall.save
```

Para acesso às regras em formato de script: Clique Aqui (https://raw.githubusercontent.com/hutger/PMR-SRC-SCRIPTS/master/firewall_lan.sh)