

# 1. Preparação do Ambiente

## 1.1 Introdução

Esta aula tem por objetivo a organização do ambiente que utilizaremos para executar os laboratórios práticos que serão disponibilizados no decorrer da disciplina de Administração de Sistemas Operacionais Não-Proprietários II. As máquinas virtuais estarão disponível no diretório “Prof. Ademir Dorneles” no compartilhamento “publico” da rede local da Faculdade SENAC e deverão conter as configurações descritas neste documento a fim de garantir o correto funcionamento dos laboratórios práticos.

O ambiente proposto consiste em:

- 01 (uma) máquina virtual com o sistema operacional GNU/Linux denominada (*Appl-Debian10-Firewall*) que servirá de plataforma para instalação dos serviços de Firewall, DHCP e Proxy. Essa VM obrigatoriamente deverá conter 02 (duas) interfaces de rede habilitadas, que terão a finalidade de isolar a Rede Virtual criada para execução dos Laboratórios da rede Local do SENAC
- Durante a disciplina outras máquinas virtuais com o sistema operacional GNU/Linux serão disponibilizadas, a fim de, servir de plataforma para os serviços de DNS (primário e secundário), WEB, Serviço de Diretórios (AD) e Controlador de Domínio (DC). Essas VMs deverão conter 01 (uma) interface de rede habilitada e farão parte da rede virtual isolada criada para execução dos laboratórios práticos.
- 01 (uma) máquina virtual com o sistema operacional GNU/Linux denominada ( *Appl-Debian10-Client*) com uma interface de rede habilitada, que será utilizada para testar o funcionamento dos serviços instalados; e
- 01 (uma) máquina virtual com o sistema operacional Microsoft Windows 7, com uma interface de rede habilitada, que também será utilizada para testar o funcionamento dos serviços instalados.

Orientações importantes:

#### Máquina Virtual Appl-Debian10-Firewall:

- Sempre que importar o appliance da máquina virtual Firewall, não esqueça de selecionar a opção “Reinicialize o endereço MAC de todas as placas de rede”.
- Esta máquina virtual deverá possuir duas interfaces de rede habilitadas, sendo a primeira em modo Bridge e a segunda em Modo Rede Interna.

#### Máquina Virtual Appl-Debian10-Client e Windows7:

- Esta máquina virtual deverá possuir uma interface de rede habilitada, sendo esta em Modo Rede Interna.

Caso tenha dúvida, é possível consultar uma explicação detalhada dos modos de funcionamento das interfaces de rede no VirtualBox acessando o [site oficial](#).

Na figura 1.1 é apresentado o escopo do ambiente para estudos.

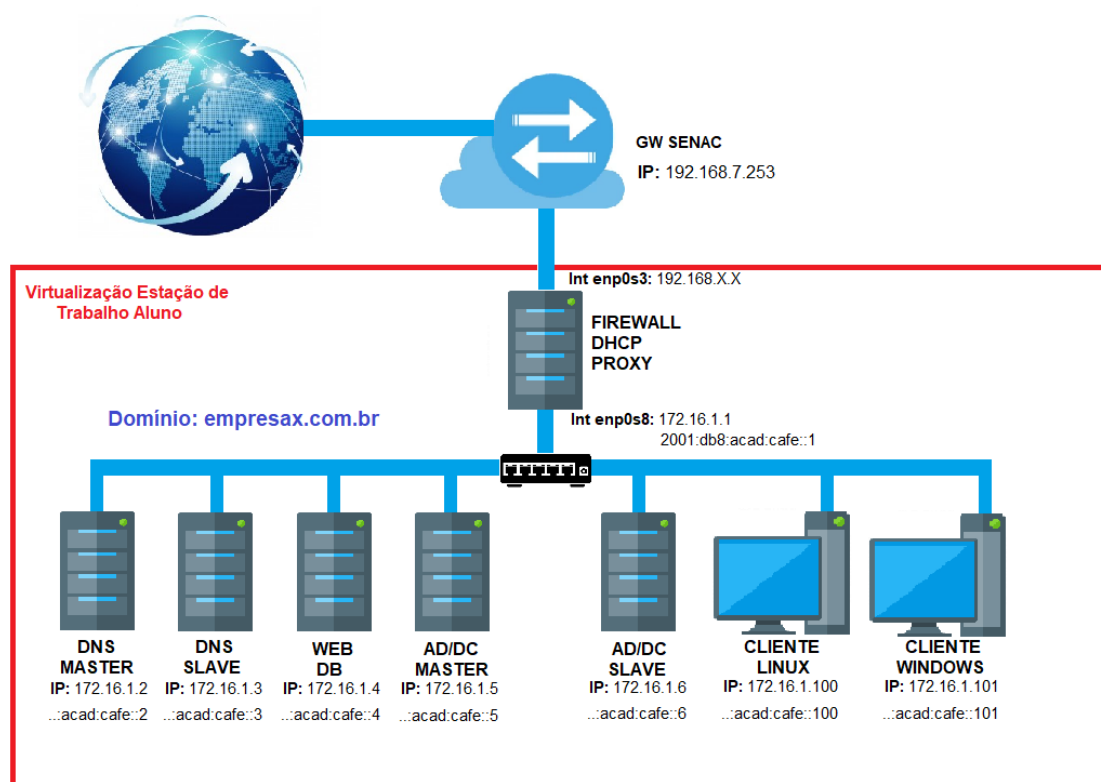


Figure 1.1: Escopo do ambiente de estudos

## 1.2 Configuração da VM Debian10 Firewall

### 1.2.1 Configuração da Interface de Rede

Primeiro será configurada a interface de rede da máquina virtual Debian-Firewall, para isso edite o arquivo `/etc/network/interfaces`:

```
root@Firewall:/# vim /etc/network/interfaces
```

E insira a seguinte configuração:

```
## Rede Externa - WAN (enp0s3)
    auto enp0s3
    iface enp0s3 inet static
    address 192.168.6.x
    netmask 21
    gateway 192.168.7.253

## Rede Interna – LAN (enp0s8)
    auto enp0s8
    iface enp0s8 inet static
    address 172.16.1.1
    netmask 24

## Rede Interna – LAN IPv6 (enp0s8)
    iface enp0s8 inet6 static
    address 2001:db8:acad:cafe::1
    netmask 64
```

Reinicie o serviço de rede:

```
root@Firewall:/# ifdown -a && ifup -a
```

O serviço de rede pode ser manipulado pelo script `networking`, porém a utilização deste script é obsoleto devido a possibilidade de não habilitar novamente alguma das interfaces.

```
root@Firewall:/# systemctl restart networking
```

Utilize a ferramenta `ping` para testar a conexão com a internet através do envio de pacotes ICMP:

```
root@Firewall:/# ping 8.8.8.8
```

### 1.2.2 Configuração do DNS VM Debian10-Firewall

Para configurar a resolução de nomes na máquina Debian-Firewall edite o arquivo `/etc/resolv.conf`:

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

E insira o seguinte conteúdo: (Utilize como DNS o IP do seu roteador ou algum público, como: 8.8.8.8)

```
nameserver 192.168.0.1
```

Utilize a ferramenta `ping` para testar a resolução de nomes através do envio de pacotes ICMP:

```
root@Client:/# ping www.senacrs.com.br
```

### 1.2.3 Configuração do NAT com iptables

Para ativar o nat na Máquina Virtual Debian-Firewall execute o seguinte comando:

```
root@Firewall:/# iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

**Obs.:** Este comando habilitará o NAT temporariamente, pois o comando ficará carregado na memória e ao reiniciar o sistema a configuração não será carregada. Portanto para fixar as configurações posteriormente iremos criar um *script* que além de aplicar regras de firewall, habilitará a função ao ser inserido sua execução na inicialização do sistema.

### 1.2.4 Ativação do ip\_forward no kernel do Linux

Nesta etapa ativaremos o *ip\_forward* para definir que o kernel irá encaminhar pacotes IP, para isso editaremos o arquivo */etc/sysctl.conf*:

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

Descomente a seguinte linha: *net.ipv4.ip\_forward=1*:

Execute *sysctl* com o opção *-p* para carregar as configurações de *sysctl* a partir do arquivo padrão */etc/sysctl.conf*:

```
root@Firewall:/# sysctl -p
```

**Obs.:** A configuração anterior substitui a necessidade de execução do comando abaixo para habilitar o encaminhamento de pacotes no sistema.

```
root@Firewall:/# echo 1 > /proc/sys/net/ipv4/ip_forward
```

### 1.2.5 Configurando o gerenciador de pacotes APT

Para utilizarmos o gerenciador de pacotes APT (Advanced Package Tool) para realizarmos as instalações dos serviços, pacotes, bibliotecas e dependência em geral, faz-se necessário a configuração dos repositórios que serão utilizados para download. Para isso editaremos o arquivo */etc/apt/sources.list*:

```
root@Firewall:/# vim /etc/apt/sources.list
```

Utilizaremos os repositórios oficiais do Debian 10, para isso configure seu arquivo conforme apresentado na figura 2:

```
deb http://deb.debian.org/debian/ buster main
deb-src http://deb.debian.org/debian/ buster main

deb http://security.debian.org/debian-security buster/updates main
deb-src http://security.debian.org/debian-security buster/updates main

deb http://deb.debian.org/debian/ buster-updates main
deb-src http://deb.debian.org/debian/ buster-updates main
```

Após a configuração do arquivo, atualize a lista de pacotes disponíveis nos repositórios com o comando *apt update*:

```
root@Firewall:/# apt update
```

**Obs.:** Caso o APT tente atualizar utilizando IPv6 é possível forçar o gerenciador a utilizar o IPv4, para isso faça o seguinte procedimento:

Crie um arquivo denominado *99-force-ipv4* dentro do diretório “/etc/apt/apt.conf.d/”:

```
root@Firewall:/# vim /etc/apt/apt.conf.d/99force-ipv4
```

E insira o seguinte conteúdo:

```
Acquire::ForceIPv4 "true";
```

Após executar este procedimento, tente novamente atualizar o APT:

```
root@Firewall:/# apt update
```

## 1.3 Configuração da VM Debian10 Client

### 1.3.1 Configuração da Interface de Rede

Configure a interface de rede da máquina virtual Debian10-Client, para isso edite o arquivo */etc/network/interfaces*:

```
root@Client:/# vim /etc/network/interfaces
```

E insira a seguinte configuração:

```
# IPv4
auto enp0s3
iface enp0s3 inet static
address 172.16.1.100
netmask 24
gateway 172.16.1.1

# IPv6
iface enp0s3 inet6 static
address 2001:db8:acad:cafe::a
netmask 64
```

Reinicie o serviço de rede:

```
root@Client:/# ifdown -a && ifup -a
```

O serviço de rede pode ser manipulado pelo script *networking*, porem a utilização deste script é obsoleto devido a possibilidade de não habilitar novamente alguma das interfaces.

```
root@Client:/# systemctl restart networking
```

Utilize a ferramenta *ping* para testar a conexão com a máquina Debian-Firewall através do envio de pacotes ICMP:

```
root@Client:/# ping 172.16.1.1  
root@Client:/# ping6 2001:db8:acad:cafe::a
```

Utilize a ferramenta *ping* para testar a conexão com a internet através do envio de pacotes ICMP:

```
root@Client:/# ping 8.8.8.8
```

### 1.3.2 Configuração do DNS VM Debian-Client

Para configurar a resolução de nomes na máquina Debian-Client edite o arquivo */etc/resolv.conf*:

```
root@Client:/# vim /etc/resolv.conf
```

E insira o seguinte conteúdo: (Utilize como DNS o IP do seu roteador ou algum público, como: 8.8.8.8)

```
nameserver 192.168.0.1
```

Utilize a ferramenta *ping* para testar a resolução de nomes através do envio de pacotes ICMP:

```
root@Client:/# ping www.senacrs.com.br
```