

SEG12 - Atividades - Semana 2

Francisco Marcelo, Marcelo Karam e Felipe Scarel

16-08-2018

Índice

Configuração preliminar das máquinas	1
1) Da divisão de grupos	1
2) Topologia geral de rede	2
3) Configuração do Virtualbox	3
4) Detalhamento das configurações de rede	4
3) Configuração da máquinas virtuais	4
4) Configuração de firewall e NAT	7

Configuração preliminar das máquinas

1) Da divisão de grupos

Neste curso, os alunos serão divididos em dois grupos: **A** e **B**. Ao longo da semana, iremos realizar algumas atividades que vão envolver a intercomunicação entre máquinas virtuais dos alunos de cada grupo; para que as configurações de rede de dois alunos envolvidos em uma mesma atividade não conflitem, iremos adotar uma nomenclatura de endereços para cada grupo, como se segue:

Tabela 1. Nomenclatura entre grupos

Grupo	Sufixo de endereço
A	1
B	2

O que isso significa, na prática? Em vários momentos, ao ler este material, você irá se deparar com endereços como 172.16.G.20 ou 10.1.G.10 — que evidentemente são inválidos. Nesse momento, substitua o número do seu grupo pela letra **G** no endereço. Se você for membro do grupo **B**, portanto, os endereços acima seriam 172.16.2.20 e 172.16.2.10.

2) Topologia geral de rede

A figura abaixo mostra a topologia de rede que será utilizada durante este curso. Nos tópicos que se seguem, iremos verificar que a importação de máquinas virtuais, configurações de rede e conectividade estão funcionais antes de prosseguir. As configurações específicas de cada máquina/interface serão detalhadas na seção a seguir.

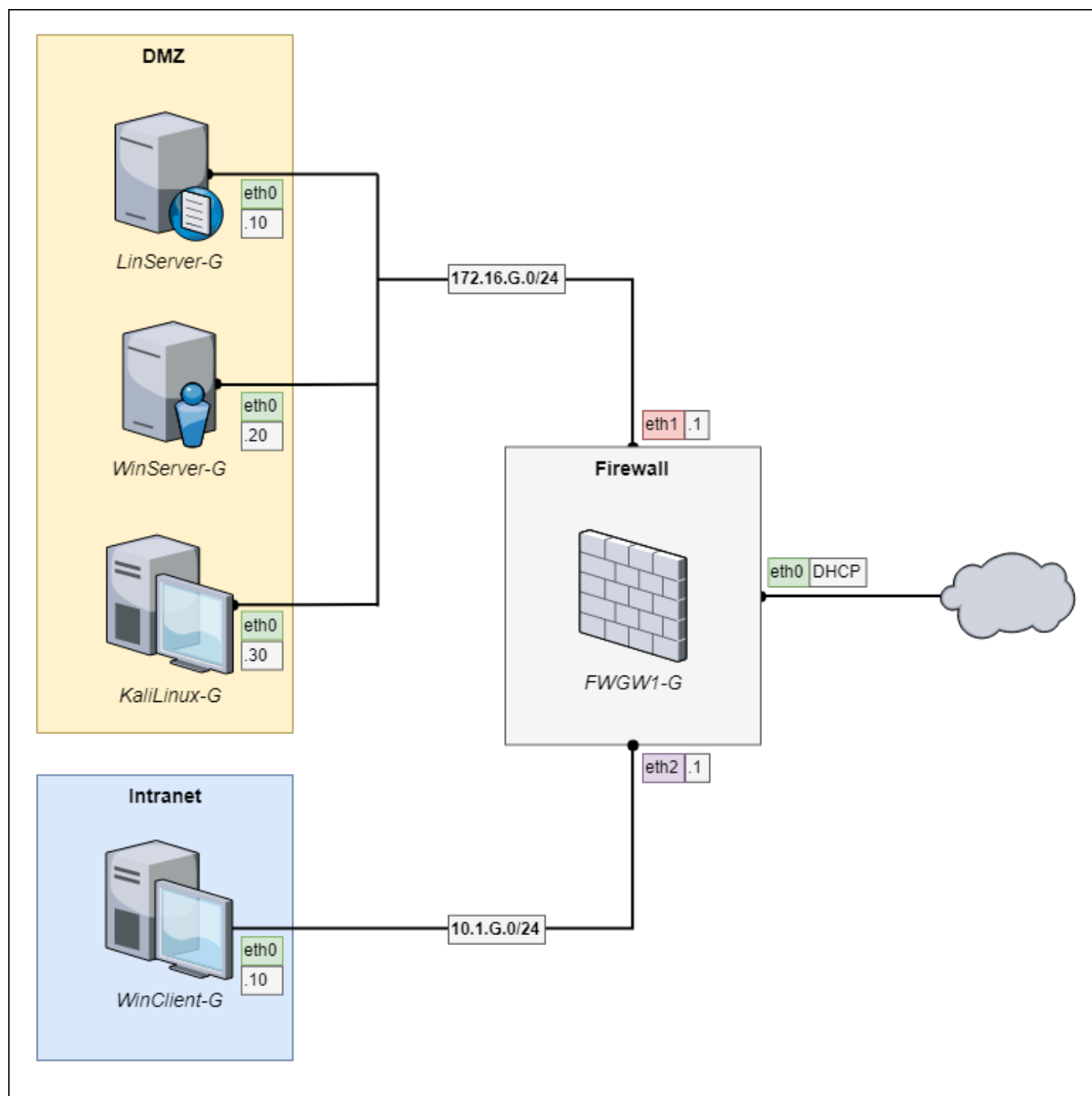


Figura 1: Topologia de rede do curso

3) Configuração do Virtualbox

1. Primeiramente, verifique se todas as máquinas virtuais foram importadas. Você deve ter cinco VMs, com as configurações que se seguem.

Tabela 2. VMs disponíveis no Virtualbox

Nome VM	Memória
FWGW1-G	2048 MB
LinServer-G	2048 MB
WinServer-G	2048 MB
KaliLinux-G	2048 MB
WinClient-G	2048 MB

Se a quantidade de RAM de alguma das máquinas for inferior aos valores estipulados, ajuste-a.

2. Agora, configure as redes do Virtualbox. Acesso o menu *File > Host Network Manager* e crie as seguintes redes:

Tabela 3. Redes host-only no Virtualbox

Rede	Endereço IPv4	Máscara de rede	Servidor DHCP
Virtualbox Host-Only Ethernet Adapter	172.16.G.254	255.255.255.0	Desabilitado
Virtualbox Host-Only Ethernet Adapter #2	10.1.G.254	255.255.255.0	Desabilitado

3. Finalmente, configure as interfaces de rede de cada máquinas virtual. Para cada VM, acesse *Settings > Network* e faça as configurações que se seguem:

Tabela 4. Interfaces de rede das máquinas virtuais

VM Nome	Interface	Conectado a	Nome da rede
FWGW1-G	Adapter 1	Bridged Adapter	Placa de rede física do <i>host</i>
	Adapter 2	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
	Adapter 3	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2
LinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinServer-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
KaliLinux-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter
WinClient-G	Adapter 1	Host-only Adapter	Virtualbox Host-Only Ethernet Adapter #2

4) Detalhamento das configurações de rede

As configurações de rede realizadas internamente em cada máquina virtual foram apresentados de forma sucinta na figura 1. Iremos detalhar as configurações logo abaixo:

Tabela 5. Configurações de rede de cada VM

VM Nome	Interface	Modo	Endereço	Gateway	Servidores DNS
FWGW1-G	eth0	Estático	DHCP	Automático	Automático
	eth1	Estático	172.16.G.1/24	n/a	n/a
	eth2	Estático	10.1.G.1/24	n/a	n/a
LinServer-G	eth0	Estático	172.16.G.10/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinServer-G	eth0	Estático	172.16.G.20/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
KaliLinux-G	eth0	Estático	172.16.G.30/24	172.16.G.1	8.8.8.8 ; 8.8.4.4
WinClient-G	eth0	Estático	10.1.G.10/24	10.1.G.1	8.8.8.8 ; 8.8.4.4

3) Configuração da máquinas virtuais

Agora, vamos configurar a rede de cada máquina virtual de acordo com as especificações da topologia de rede apresentada no começo deste capítulo.

1. Primeiramente, ligue a máquina *Server_Linux* e faça login como usuário **root** e senha **rnpesr**. A seguir, edite o arquivo **/etc/network/interfaces** como se segue, reinicie a rede e verifique o funcionamento:

```
# hostname
servidor

# whoami
root

# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0 eth1 eth2

iface eth0 inet dhcp

iface eth1 inet static
    address 192.168.0.10
    netmask 255.255.255.0

iface eth2 inet static
    address 172.16.0.10
    netmask 255.255.255.0

# systemctl restart networking

# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.0.204/24 brd 10.0.0.255 scope global eth0
    inet 192.168.0.10/24 brd 192.168.0.255 scope global eth1
    inet 172.16.0.10/24 brd 172.16.0.255 scope global eth2
```

2. Faça o mesmo para a máquina *Client_Linux*:

```
# hostname
cliente

# whoami
root

# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.0.20
    netmask 255.255.255.0
    gateway 192.168.0.10

# systemctl restart networking

# ip a s | grep '^ *inet '
    inet 127.0.0.1/8 scope host lo
    inet 192.168.0.20/24 brd 192.168.0.255 scope global eth0
```


3. Na máquina *Win7-padrao*, verifique que a configuração IPv4 da interface de rede está ajustada para obter endereço IP e servidor DNS automaticamente, como mostra a imagem a seguir:

4) Configuração de firewall e NAT

O passo final é garantir que as máquinas *Client_Linux* e *Win7-padrao* consigam acessar a internet através da máquina *Server_Linux*, que está atuando como um firewall/roteador na topologia de rede do curso.

1. Na máquina *Server_Linux*, verifique que o firewall de host está limpo e permitindo qualquer tipo de conexão:

```
# hostname
servidor

# iptables -L -vn
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

# iptables -L -vn -t nat
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source                   destination
```

2. A seguir, habilite o repasse de pacotes entre interfaces descomentando a linha `net.ipv4.ip_forward=1` no arquivo `/etc/sysctl.conf`. A seguir, execute `# sysctl -p`:

```
# sed -i 's/^#\(\net.ipv4.ip_forward\)\1/' /etc/sysctl.conf

# grep 'net.ipv4.ip_forward' /etc/sysctl.conf
net.ipv4.ip_forward=1

# sysctl -p
net.ipv4.ip_forward = 1
```

3. Finalmente, habilite IP *masquerading* no firewall através do comando `# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`:

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# iptables -L POSTROUTING -vn -t nat
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source        destination
  0     0 MASQUERADE  all  --  *       eth0     0.0.0.0/0     0.0.0.0/0
```

4. Acesse a máquina *Client_Linux* e faça um teste de conectividade. Você deve conseguir *ping* com um *host* da internet, como **8.8.8.8**, por exemplo:

```
$ ping -c3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=32.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=33.2 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 31.982/32.482/33.291/0.595 ms
```

5. Torne permanente a configuração de *masquerading* na máquina *Server_Linux* editando o arquivo `/etc/rc.local` e adicionando a linha `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE` antes da linha `exit 0` ao final do arquivo.

```
# cat /etc/rc.local | grep -v '^# \| ^#\$ \| ^$'
#!/bin/sh -e
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
exit 0
```