Pontifícia Universidade Católica de Minas Gerais
Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Curso de Sistemas de Informação

Laboratório de Segurança de Redes de Computadores

Firewall

Aprendendo um pouco sobre Firewall

Agora vamos ambientá-lo com o iptables do Linux na distribuição do Debian. Apesar de existirem outras distribuições com interfaces mais amigáveis como a pfSense e a Endian o Debian é uma distribuição mais consolidada para servidores e versátil no que diz respeito a atualizações de pacotes.

O iptables é o aplicativo, assim como o ipfw, que assume a função de habilitar regras/políticas de controle de acesso à própria estação e o que trafega por ela, ou seja, é um software de firewall classificado como firewall de camada 4 (Filtro de Pacotes) já que suas políticas de acesso são definidas baseadas em portas ou ips de origem e destino. É possível recompilar o kernel e fazê-lo operar como firewall de camada 7, onde protocolos de aplicação podem ser validados, mas particularmente fiz testes que não se mostraram 100% eficazes. Quer saber mais sobre isto veja o link https://www.vivaolinux.com.br/artigo/Iptables-+-Layer7 , mas este não é o objetivo de nossa aula.

São três canais que devem ser controlados no iptables. O de INPUT que determina o que pode ou não entrar pelas interfaces de rede naquela estação, o de OUTPUT que determina o que pode sair pelas interfaces de rede daquela estação e por fim a de FORWARD que define o que pode passar de uma interface de rede para outra.

Para quem quiser se aprofundar nos conceitos de firewall com iptables recomendo o estudo das tabelas que são mantidas por este aplicativo e os conceitos de PRE e POST Routing.

O nosso laboratório terá por objetivo configurar uma imagem Debian 9 disponível nas estações para servir de firewall para estação Windows 7. Visualmente enxergando nosso laboratório ficará com a estrutura conforme a figura 1.

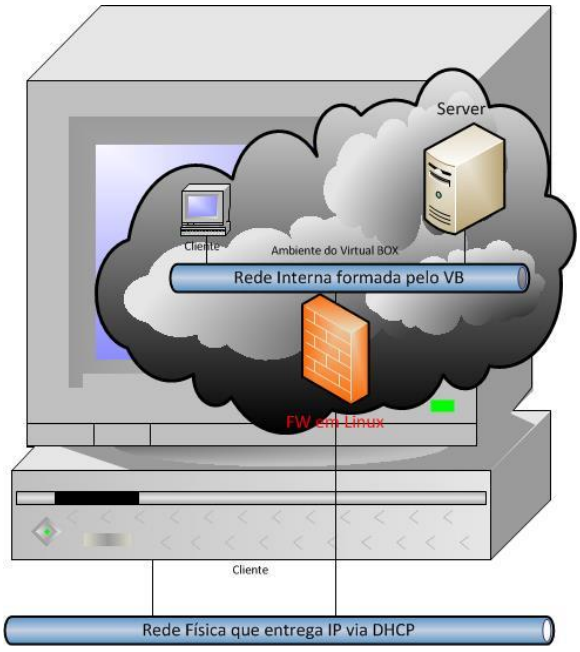


Figura 1. Topologia proposta para aula de configuração de Firewall

Como você está aproveitando o ".ova" disponível nas estações de laboratório vá ao menu Arquivo, opção Importar Appliance, em seguida selecione o arquivo Win7.ova que deve estar na pasta C:\VMs

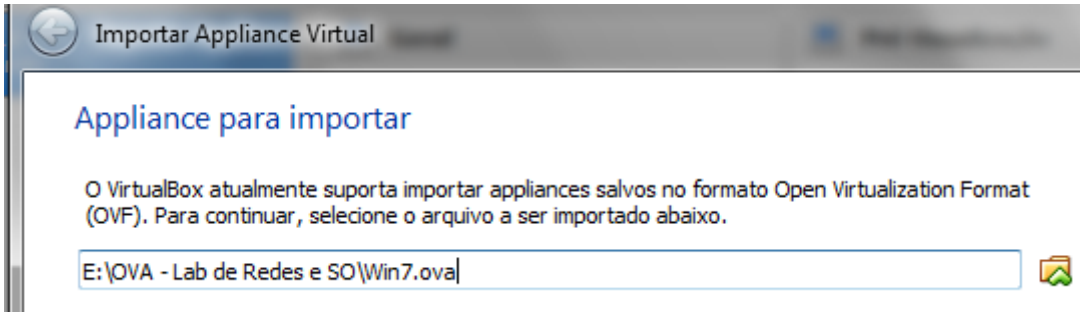
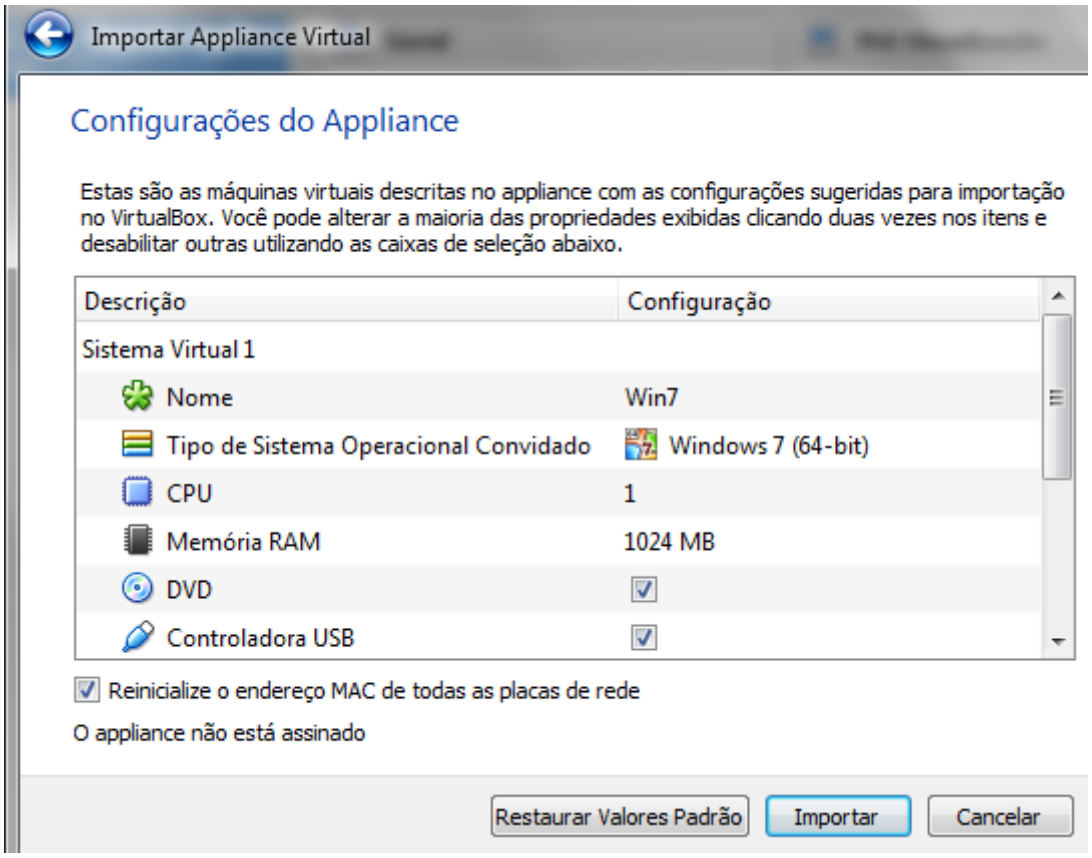


Figura 2. Selecionando uma imagem salva no disco

Marque a opção "Reinicialize o endereço MAC..." isto evitará termos problemas com várias máquinas clonadas do mesmo OVA.



Neste momento uma VM deverá aparecer no seu Virtual BOX.

Configurando a rede

Uma vez que o Sistema Operacional estiver instalado é necessário configurar a maneira como o dispositivo de rede irá se comportar. Cada um dos adaptadores da VM pode ser configurado separadamente nos seguintes modos.

- **Não conectado**. Neste modo, o Virtual Box considera que a placa de rede está presente, mas sem conexão. Como se não houvesse um cabo Ethernet conectado à placa.
- **Network Address Translation (NAT).** Se você quer navegar na WEB, fazer downloads de arquivos e ler e-mails na máquina virtual, este é o modo padrão.
- **Bridged networking**. Esta opção é para configurações de rede mais avançadas como simulação e execução de servidores na VM. Quando

habilitada, o Virtual Box conecta-se diretamente com a placa de rede instalada e troca pacotes diretamente com a rede.

- **Internal networking.** Esta opção pode ser usada para criar uma rede virtual em que as VMs podem enxergar umas às outras, mas não podem enxergar as aplicações da máquina física nem aplicações fora dela.
- **Host-only networking**. Esta opção pode ser usada para criar uma rede contendo o host e um conjunto de máquinas virtuais. As máquinas virtuais devem estar na mesma sub-rede IP da interface Host-Only adicionada na instalação do Virtual Box na máquina física

Para escolher a configuração da placa de rede, você deve clicar com o botão direito sobre a Máquina virtual desejada e escolher a opção Configurações. A tela da Figura 11 será apresentada e no item Rede a seleção pode ser feita.

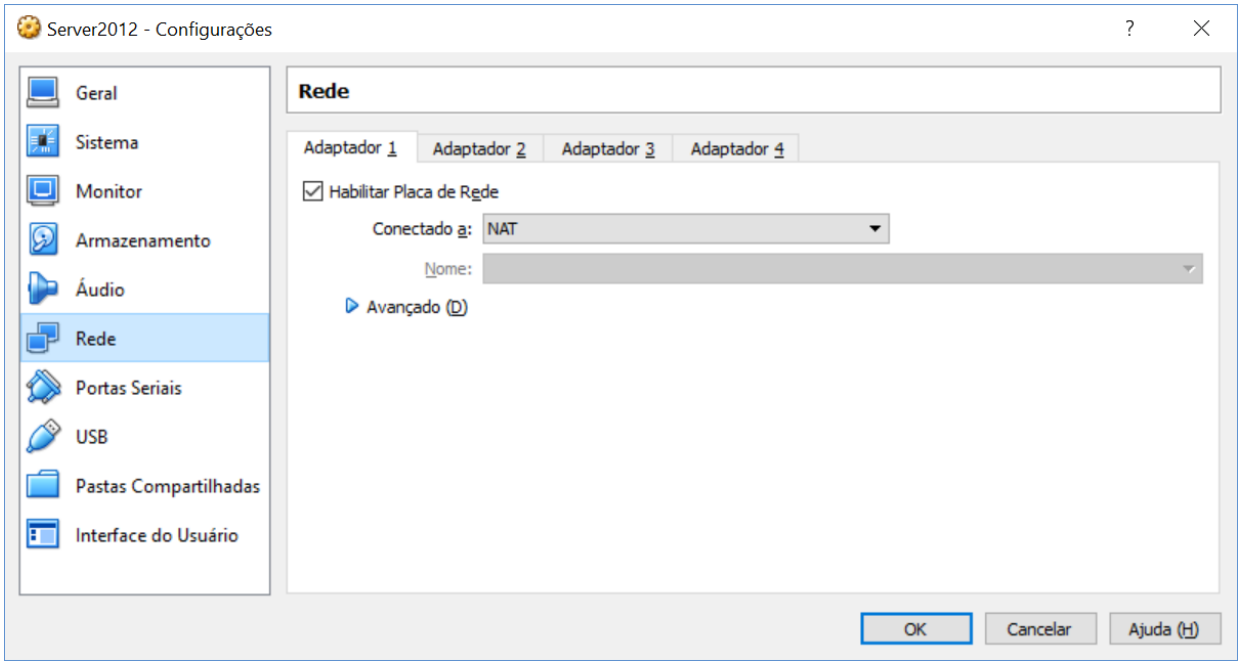


Figura 3. Configurando os recursos de uma máquina virtual

Atividades

1. Importe o cliente Windows 7 se vc ainda não o fez.
2. Quando as duas máquinas virtuais estiverem ativadas
3. Mude a placa de rede do Windows 7 para o modo “Rede Interna”. Configure a placa de rede do Windows 7 com o ip 192.168.5.2, gateway para 192.168.5.254, máscara 255.255.255.0, dns 8.8.8.8. (pode ser que eu já tenha deixado isto pronto).

Continuação das Atividades

1. Coloque duas placas de rede nesta máquina Linux, uma em modo Bridge (a primeira) e outra em modo Rede Interna. Não deixe de gerar novos endereços de MAC. (isto pode já estar pronto)

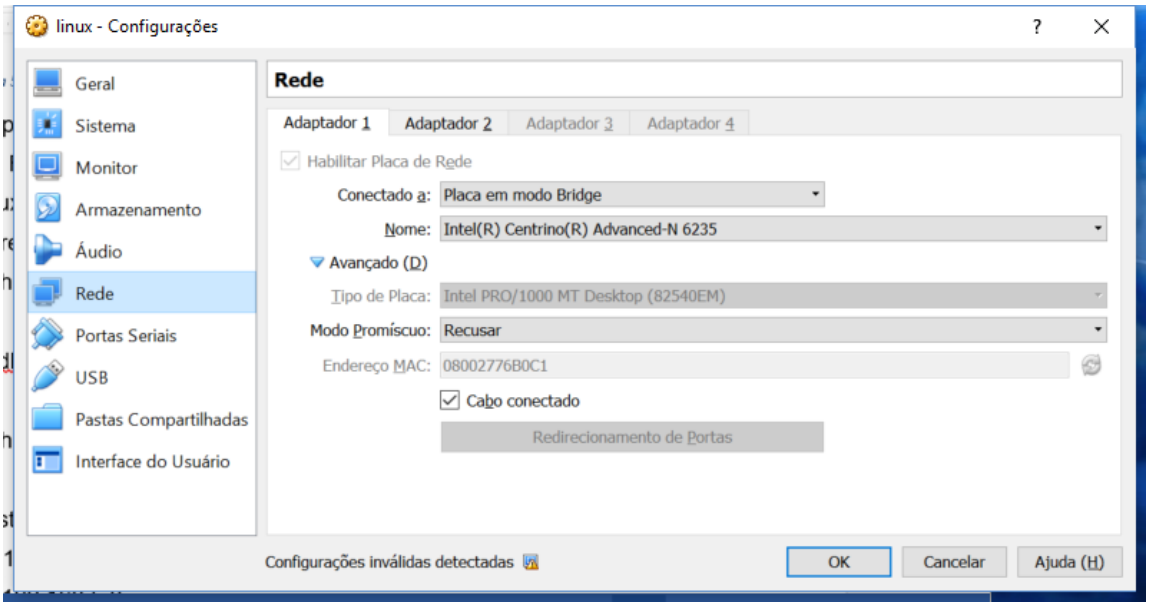


Figura 4. Configuração do Primeiro Adaptador de Rede do Servidor Linux.

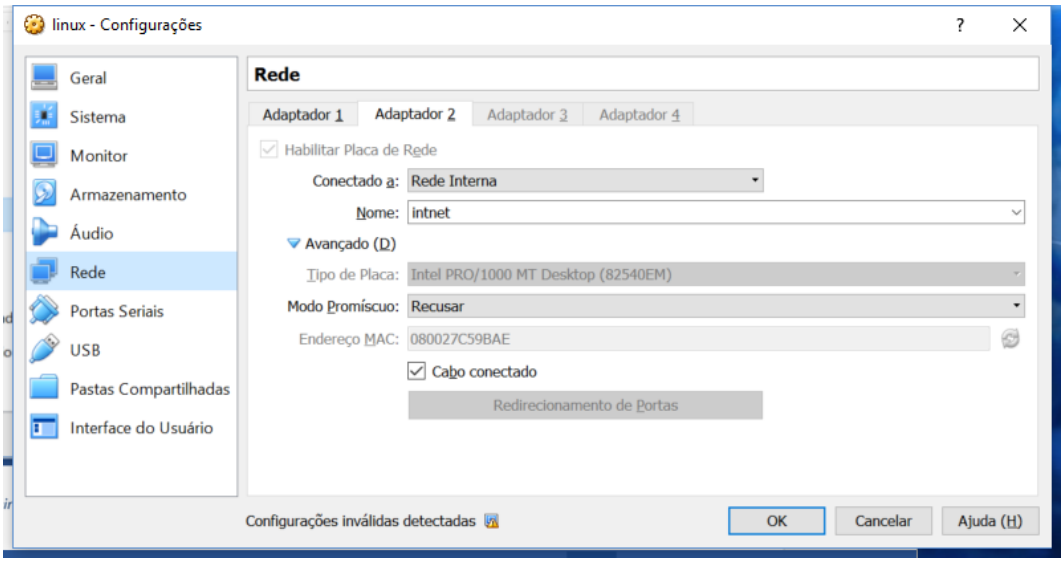


Figura 5. Configuração do segundo adaptador de rede do servidor Linux

2. Inicialize o Linux e vamos configurar as placas de rede em /etc/network/interfaces, use o editor de sua preferência. A senha do root é **labssi**.
3. Abra o terminal se o Linux estiver com ambiente gráfico. Clique em Aplicativos no canto superior direito e em seguida procure o “terminal”, dê o comando “su” para mudar para root.
4. Edite o arquivo /etc/network/interfaces (OBS.: até a versão 8 do Debian as interfaces tinham nome de eth0, eth1, etc. Nesta nova distribuição mudaram para enp…, para saber quais foram carregadas em seu linux dê o comando “ip a”) (Pode ser que já esteja pronto). Use o vim para editar arquivos.

```
auto lo
iface lo inet loopback

# a interface enp0s3 ficará com ip automático
allow-hotplug enp0s3
auto enp0s3
iface enp0s3 inet dhcp

# a interface eth1 ficará com a rede interna
allow-hotplug enp0s8
auto enp0s8
```

iface enp0s8 inet static

address 192.168.5.254

network 192.168.5.0

broadcast 192.168.5.255

netmask 255.255.255.0

dns-nameservers 8.8.8.8

5. Depois de editado o arquivo /etc/network/interfaces reinicialize as interfaces de rede com o comando /etc/init.d/networking restart. Se não funcionar, reboot a máquina.
6. Dê o comando ipconfig enp0s3 e ifconfig enp0s8 você deverá ver algo parecido com o seguinte, perceba que a enp0s3 estará em uma faixa de ip de seu laboratório e a enp0s8 estará na faia de sua rede interna (192.168.5.254):

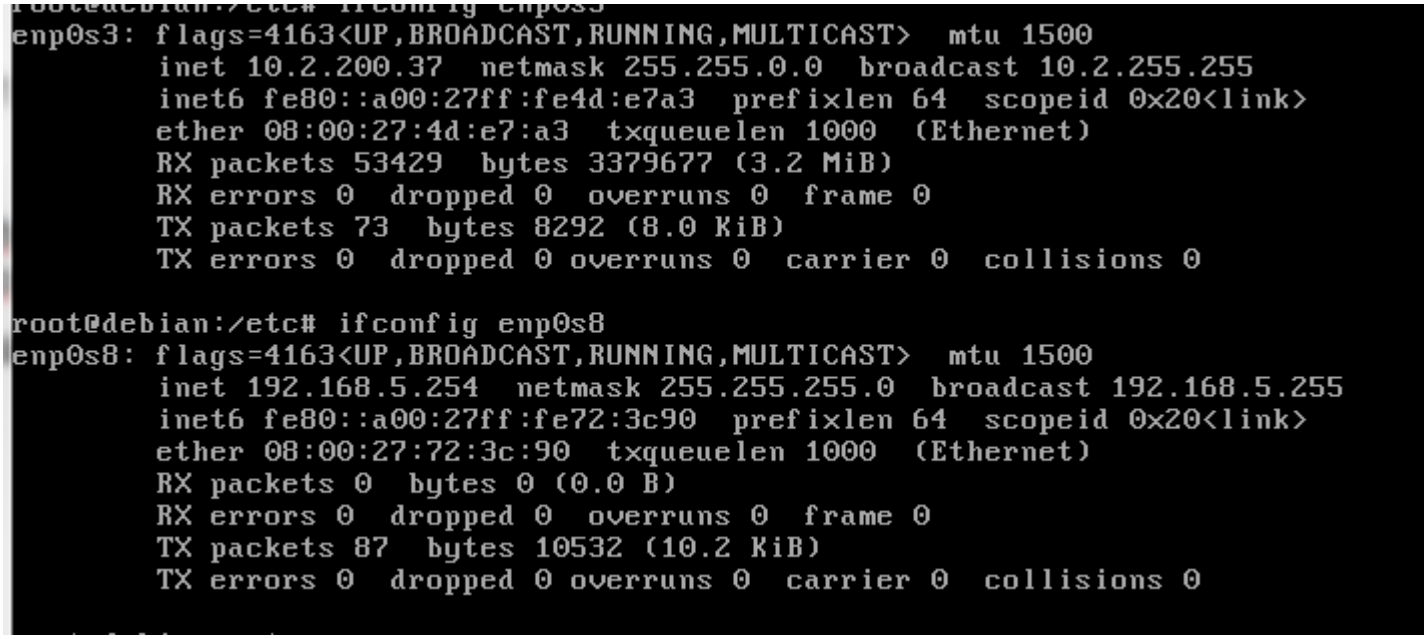


Figura 6. Informações da interfaces de rede do Linux depois de configurado as placas de rede.

7. Confira o funcionamento das placas pingando o 8.8.8.8 (funcionando significa que a interface enp0s3 está ok) e o ip 192.168.5.2 (funcionado significa que sua interface enp0s8 está ok)
8. Vamos agora configurar o Firewall propriamente dito.
9. Vamos configurar o iptables. Neste momento são milhares de composições possíveis que são aceitas, vamos configurar algumas mais triviais. Criei um arquivo que vc já deve encontrar no /etc do seu Linux, ele está todo comentado, estude-o antes de passar para o próximo passo. As últimas 10 linhas são as mais interessantes.

```
#!/bin/bash
echo "================================================"
echo "| ::  SETANDO A CONFIGURACAO DO IPTABLES   :: |"
echo "================================================"

### Passo 1: Limpando as regras ###
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD
echo "Limpando todas as regras .................[ OK ]"

# Definindo a Politica Default das Cadeias
/sbin/iptables -P INPUT ACCEPT
/sbin/iptables -P FORWARD DROP
/sbin/iptables -P OUTPUT ACCEPT
echo "Setando as regras padrao .................[ OK ]"


### Passo 2: Habilitando o trafego IP entre as placas de rede ###
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "Setando ip_foward ........................[ OK ]"

# Protecao contra ataques de syn flood (inicio da conexao TCP).
Tenta conter ataques de DoS.
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
echo "Setando protecao anti_synflood ...........[ OK ]"
# Protecao contra port scanners ocultos
/sbin/iptables -A INPUT -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m
limit --limit 1/s -j ACCEPT
# Bloqueio de ping vindos de quaisquer outros destinhos
#/sbin/iptables -A INPUT -s 0.0.0.0/0 -p icmp -j DROP
```

```
### Passo 3: Carregando os modulos do iptables ###
modprobe ip_tables
modprobe iptable_filter
modprobe iptable_mangle
modprobe iptable_nat
modprobe ipt_MASQUERADE
modprobe ip_nat_ftp
modprobe ip_conntrack_ftp
modprobe ip_conntrack_irc
echo "Carregando modulos do iptables ...........[ OK ]"
### Passo 4: Agora, vamos definir o que pode passar e o que nao ###
################################
# Cadeia de Reenvio (FORWARD).
# Primeiro, ativar o mascaramento (nat).
/sbin/iptables -t nat -F POSTROUTING
/sbin/iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
echo "Ativando mascaramento de IP ..............[ OK ]"
/sbin/iptables -A FORWARD -i enp0s3 -o enp0s8 -m state --state
ESTABLISHED,RELATED -j ACCEPT

#   libero as portas 22, 53, 80 e 443 que veja do ip 192.168.5.*
/sbin/iptables -A FORWARD -S 192.168.5.0/24 -p tcp --dport 80 -j
ACCEPT

#/sbin/iptables -A FORWARD -s 192.168.5.0/24 -d 0.0.0.0/0:22 -j
ACCEPT
#/sbin/iptables -A FORWARD -s 192.168.5.0/24 -d 0.0.0.0/0:53 -j
ACCEPT
#/sbin/iptables -A FORWARD -s 192.168.5.0/24 --dport 80 -j ACCEPT
#/sbin/iptables -A FORWARD -s 192.168.5.0/24 --dport 443 -j ACCEPT
#libero icmp para fora
/sbin/iptables -A FORWARD -p icmp -s 192.168.5.0/24 -d 0.0.0.0/0 -j
ACCEPT
echo "Setando regras para FORWARD ..............[ OK ]"
echo "Firewall configurado com sucesso .........[ OK ]"
```

10. Deixe um ping 8.8.8.8 –t rodando no Windows 7, ele não deverá funcionar enquanto nossas regras de firewall estiverem habilitadas.
11. Execute o arquivo script com o comado /etc/regras. Mágica seu ping deve ter começado a funcionar e suas estações Windows devem navegar também.

Psicodélico!!!! Agora vc já pode sair vendendo esta solução por aí.

12. Quer incrementar a funcionalidade de nosso firewall. O objetivo agora é fazer o que chamamos de redirecionamento de Portas da Rede Externa para Interna, conforme o ilustrado na figura 13. No exemplo sua máquina

física vai tentar acessar o Linux que deverá reencaminhar a consulta para o Windows 7 dentro da rede. É claro que outra máquina da rede também poderá fazer o acesso.

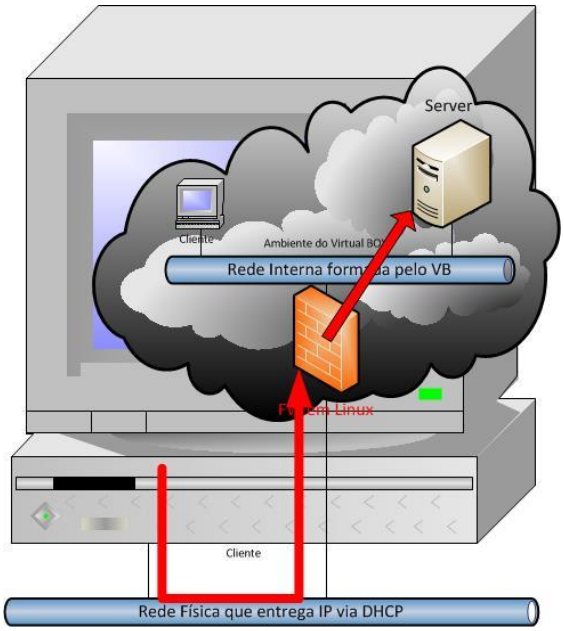


Figura 7. COnceito de redirecionamento de Porta

13. Instale o Xamp em seu Windows 7 para ele ter um servidor WEB disponível. (pode ser que já esteja instalado na imagem que passei.)
14. Pelo navegador de seu Windows 7 acesse o endereço 192.168.5.2, este procedimento é apenas para confirmarmos que seu servidor web está funcionado. Deve aparecer uma página padrão da Microsoft.
15. De sua estação física abra o navegador e coloque o ip da interface enp0s3 do Linux no meu exemplo, http://10.254.254.111. Você não deverá acessar nada.
16. Vamos configurar o iptables para redirecionar a porta 80 do Linux para o Servidor WEB que configuramos no Windows 7 com as regras a seguir. Pode dar o comando no prompt mesmo.

```
iptables -t nat -A PREROUTING -p tcp --dport  80 -i enp0s3 -j DNAT --to
192.168.5.2:80
iptables –A FORWARD –d 192.168.5.2/32 –j ACCEPT
```

A primeira linha pode ser lida da seguinte forma. Antes de se processar o roteamento (PREROUTING) pegue os pacotes que chegarem a porta 80 da placa de rede enp0s3 (nossa placa de bridge com a rede física) e redirecione (DNAT) para a máquinas interna 192.168.5.2 (nosso Windows 7). Isto que estamos fazendo é o chamado Redirecionamento de porta, que pode também ser feito nos modens de nossas bandas largas domésticas. A segunda linha indica que tudo que será encaminhado para a máquina 192.168.5.2 está sendo autorizado.

17. Tente acessar novamente de sua estação física o endereço de seu Linux, no meu exemplo http://10.254.254.111. Se não funcionou vc grita “Ô Fessor!!!!”, mas antes teste algumas coisas. Vc colocou default gateway no Windows 7 192.168.5.254? Vc pinga o 192.168.5.254 do Windows, vc pinga 8.8.8.8 do Server? Restart o serviço do Xamp, vai se virando que vc não deve ser quadrado..... até o professor chegar.