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

Laboratório de Redes e SO

Máquinas Virtuais - Continuação

O objetivo da aula de hoje é 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 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 8 disponível nas estações para servir de firewall para estação Windows 7 e o Windows 2012 utilizadas em outras aulas. Visualmente enxergando nosso laboratório ficará com a estrutura conforme a figura 1.

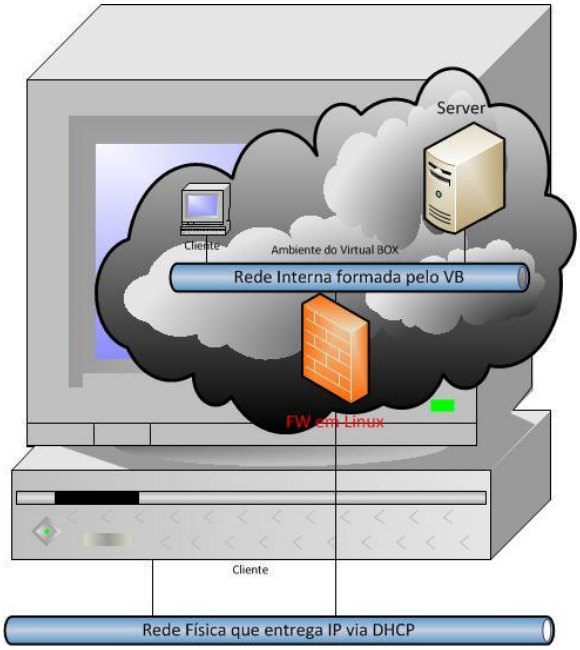

Figura 1. Topologia proposta para aula de configuração de Firewall

Vamos efetuar algumas alterações nas máquinas virtuais para não sobrecarregar a máquina física.

1. Altere a Memória alocada para o Windows 2012 para 2048 MB
2. Desabilite a placa de rede em modo NAT do Windows 2012 que ficará apenas com a placa em modo Rede Interna com o ip 192.168.5.1 (na verdade vc já deve ter feito isto na última aula quando habilitou o DHCP), aproveite para colocar como default gateway o ip que iremos colocar no Linux que é 192.168.5.254. Sua configuração deverá ficar da seguinte forma:

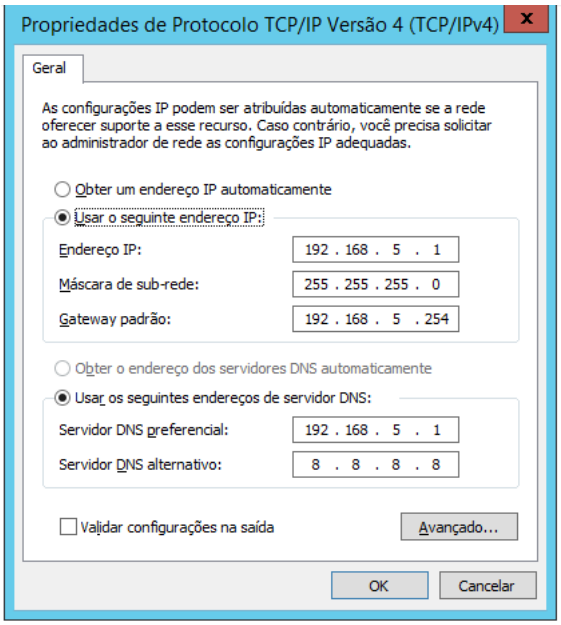

Figura 2. Configuração da Placa de Rede interna do Windows Server 2012

3. Deixe o Windows 7 com uma placa de rede em modo Rede Interna e certifique-se que ela esteja com ip na faixa 192.168.5.* obtido por DHCP ou configurado à mão.

a. Se o seu Windows 7 estiver com ip na mão basta vc fazer a alteração como foi feita no Windows Server 2012.
b. Se o seu Windows 7 estiver configurado para obter endereço automaticamente, você deverá alterar o servidor de DHCP no Windows Server. Vá em Ferramentas Administrativas e selecione o Serviço de DHCP. Em seguida escolha o escopo criado em seu laboratório, no exemplo abaixo a rede 192.168.5.0 em seguida o atributo Opções de Escopo, à direita algumas opções estarão à disposição entre elas a opção Roteador que uma vez selecionada vc deverá deixar com o valor 192.168.5.254.

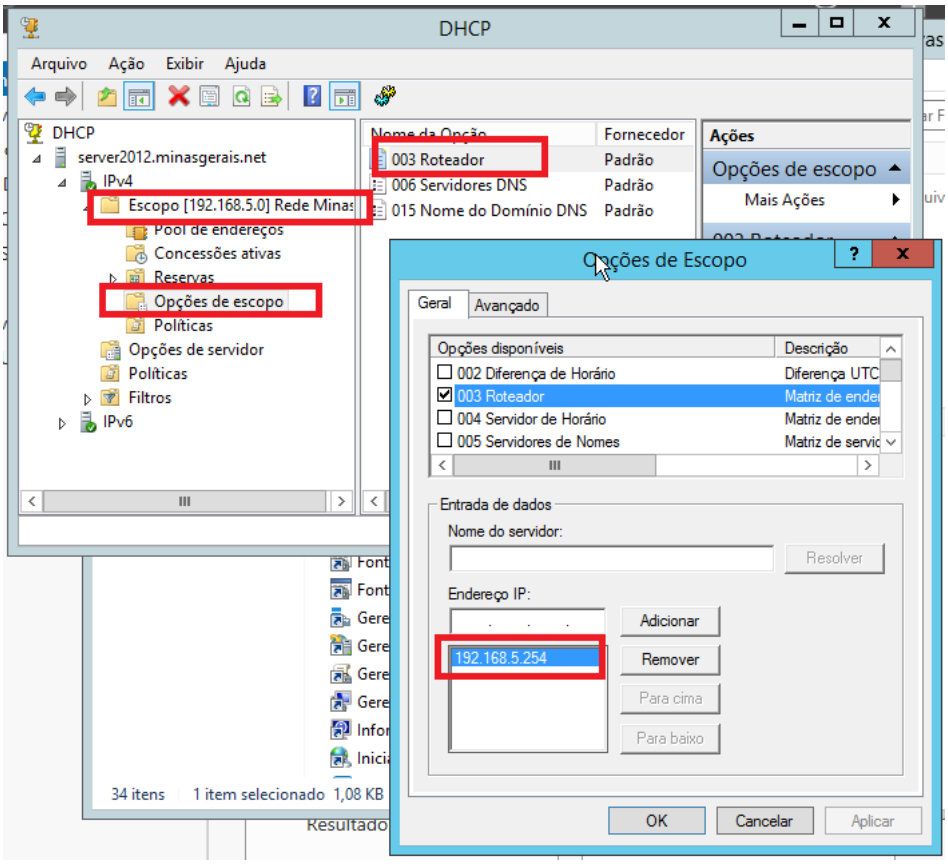

Figura 3. Alteração do Windows 2012 caso seu Windows 7 esteja cofigurado para obter endereço automaticamente.

Em seguida volte no Windows 7 para atualizar as configurações de Rede dando o comando no prompt do DOS ipconfig /release e depois ipconfig /renew.

4. Agora vamos configurar a Máquina Virtual do Linux. No menu Arquivo do Virtual Box, vamos importar o Debian.ova da pasta C:\VMs\ para o C:\Users\<seu usuários>\vms assim evitamos que alguém apague o que será alterado.
5. Se ao invés do *.ova eu tiver disponibilizado o Debian.vdi siga os seguintes passo.
    a. Crie uma nova máquina virtual Debian de 64 bits com 768 MB usando o Debian8.vdi copiado para usa pasta pessoal, conforme a sequência de imagens.

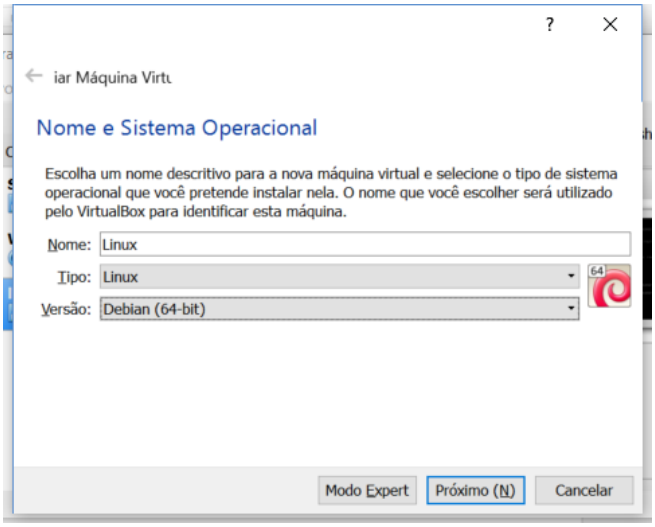

Figura 4. Seleção do Sistema Operacional do Linux debian

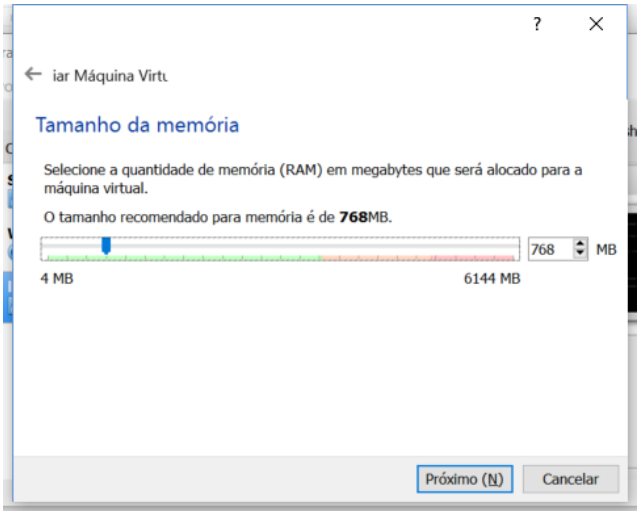

Figura 5. Determinando Quantidade de Memória para o servidor Linux

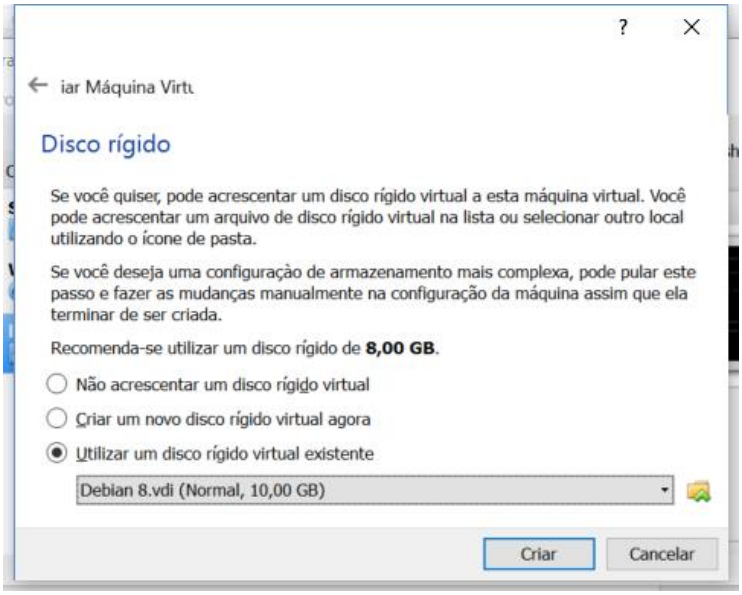

Figura 6. Selecionando o Arquivo de Imagem com a instalação da disitribuição do Debian 8.

6. Coloque duas placas de rede nesta máquina Linux, uma em modo Bridge (a primeira) e outra em modo Rede Interna.

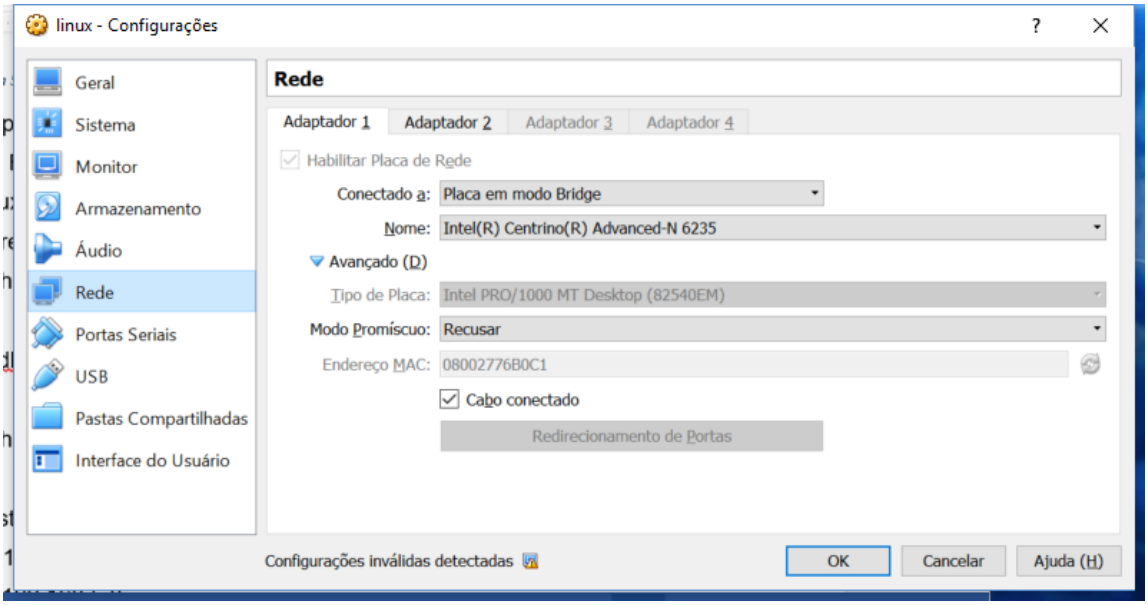

Figura 7. Configuração do Primeiro Adaptador de Rede do Servidor Linux.

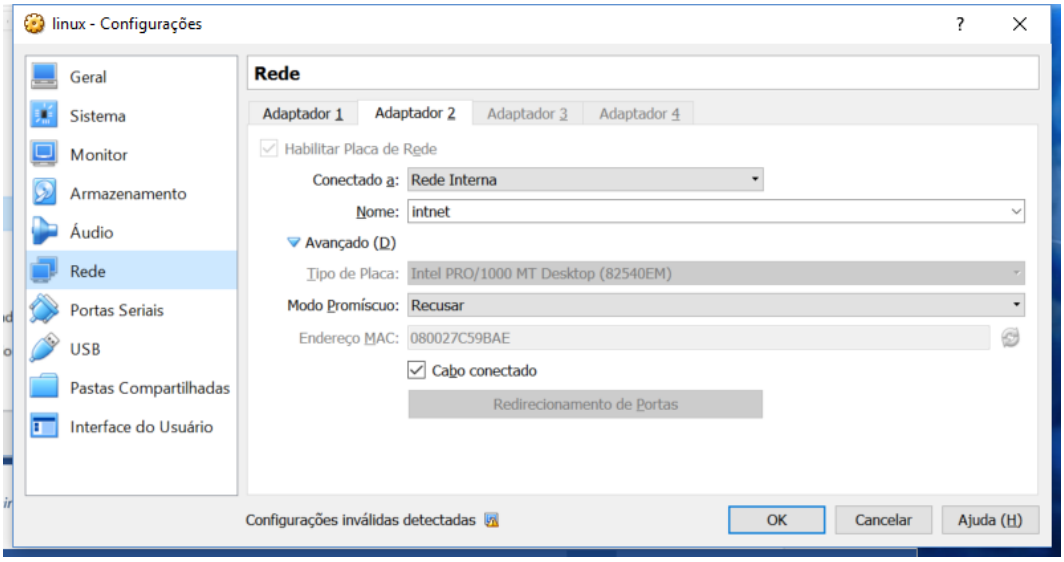

Figura 8. Configuração do segundo adaptador de rede do servidor Linux

7. 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 **password**.
8. Edite o arquivo /etc/network/interfaces

   auto lo

   iface lo inet loopback

   # a interface eth0 ficará com ip automático

   auto eth0

   iface eth0 inet dhcp

   # a interface eth1 ficará com a rede interna

   auto eth1

   iface eth1 inet static

address 192.168.5.254

network 192.168.5.0

broadcast 192.168.5.255

netmask 255.255.255.0

dns-nameservers 192.168.5.1

dns-nameservers 8.8.8.8

9. Depois de editado o arquivo /etc/network/interfaces reinicialize as interfaces de rede com o comando /etc/init.d/networking restart.
10. Dê o comando ipconfig eth0 e ifconfig eth1 você deverá ver algo parecido com o seguinte, perceba que a eth0 estará em uma faixa de ip de seu laboratório e a eth1 estará na faia de sua rede interna (192.168.5.254):

Figura 9. Informações da interfaces de rede do Linux depois de configurado as placas de rede.

11. Confira o funcionamento das placas pingando o 8.8.8.8 (funcionando significa que a interface eth0 está ok) e o ip 192.168.5.1 (funcionado significa que sua interface eth1 está ok)
12. Vamos agora configurar o Firewall propriamente dito.
13. Vamos configurar o iptables. Neste momento são milhares de composições possíveis que são aceitas, vamos configurar algumas mais triviais. Criei um arquivo que vc vai transferir para 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 eth0 -j MASQUERADE
echo "Ativando mascaramento de IP ..............[ OK ]"
/sbin/iptables -A FORWARD -i eth0 -o eth1 -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 ]"
```

14. Para evitar a digitação completa de todo este texto nós vamos transferi-lo via ssh (obs.: tentei fazer com copy and paste, mas não funcionou). Primeiro vamos ter que habilitar o ssh para aceitar conexão via root.
15. Edite o arquivo /etc/ssh/sshd_config e procure a linha PermitRootLogin. Ela deve estar com o valor without-password troque para yes, ou seja, a linha deve ficar:

PermitRootLogin yes

16. Em seguida precisamos reiniciar o servidor de ssh com o comando /etc/init.d/ssh restart.
17. Vamos agora obter o Winscp Portable para conseguir transferir o arquivo. Você pode obtê-lo de https://winscp.net/eng/download.php.
18. Ao executar o WinSCP você deverá informar o IP da interface eth0 do seu Linux, ou seja, aquela que está em modo Bridge. No meu exemplo 10.254.254.111.

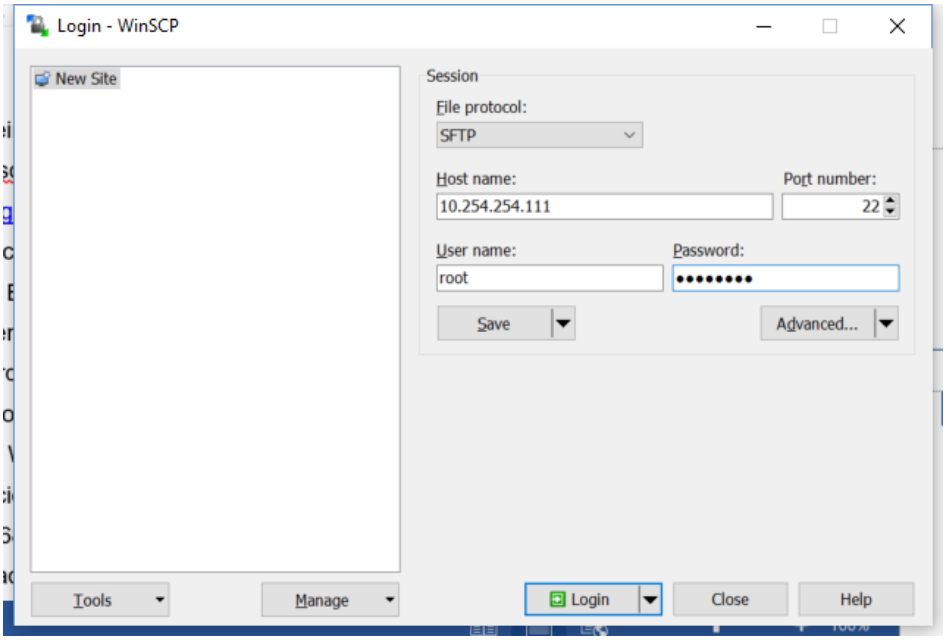

Figura 10. Tela de configuração do Aplicativo WINSCP.

19. Uma vez Conectado à esquerda você tem o explorer de sua estação de trabalho física e à direita as pastas de trabalho do Linux.

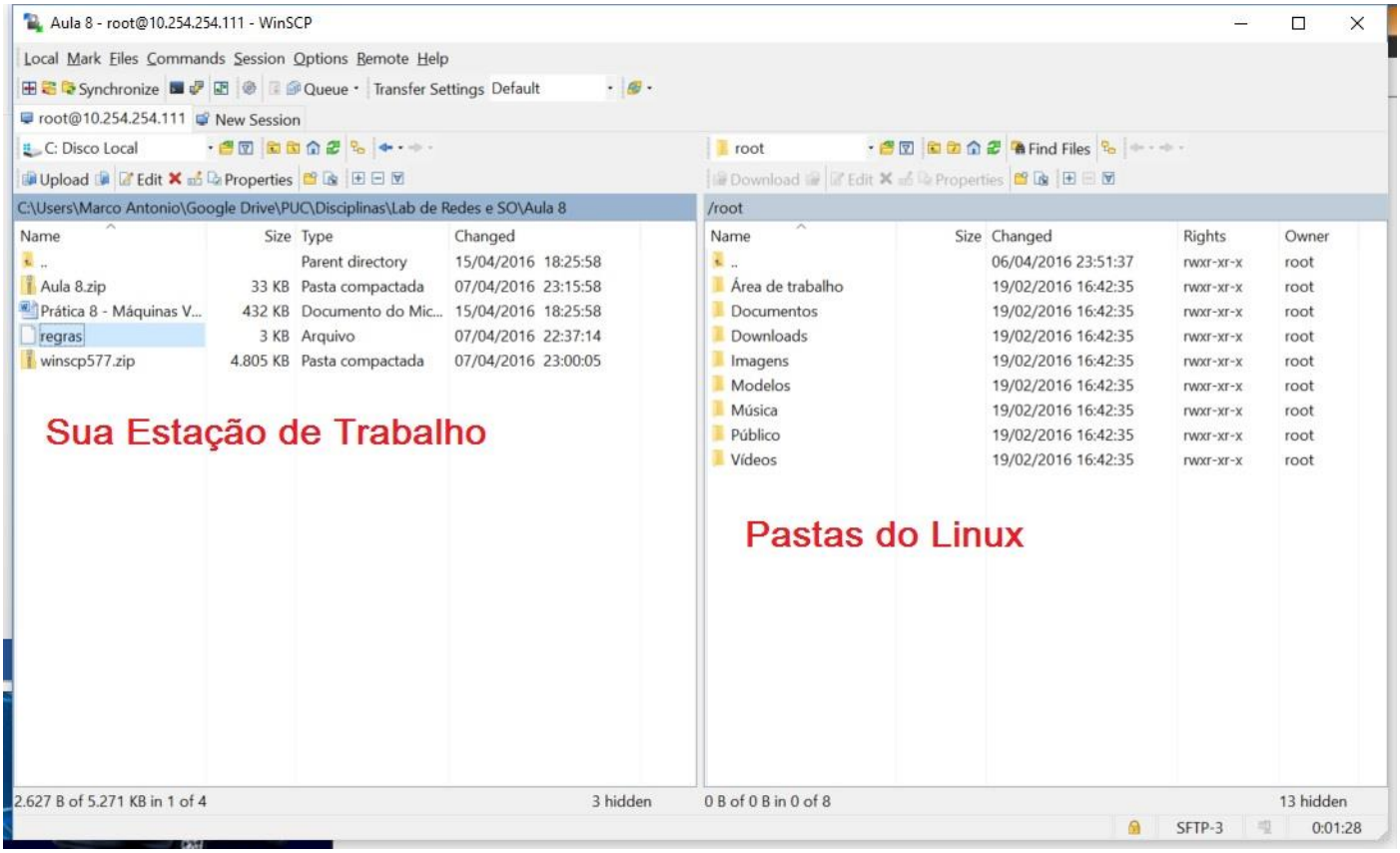

Figura 11. Interface de transferência do Winscp

20. Selecione a pasta em seu computador onde está localizado o arquivo regras disponibilizado junto com este roteiro. No lado do Linux navegue até a pasta /etc. Clique no arquivo **regras** e em seguida Upload. Irá aparecer a tela seguinte. É MUITO IMPORTANTE QUE VOCÊ CLIQUE EM TRANSFER SETTINGS E ESCOLHA A OPÇÃO TEXT!

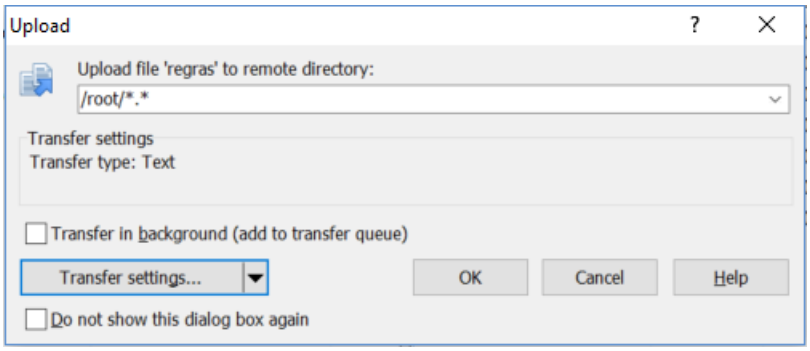

Figura 12. Alterando o modo de transferência do arquivo de binário para texto.

21. Pronto o arquivo está agora no Linux. Mude as permissões do arquivo para 755 com o comando chmod 755 /etc/regras
22. Deixe um ping 8.8.8.8 –t rodando no Windows 7, ele não deverá funcionar enquanto nossas regras de firewall estiverem habilitadas.
23. Execute o arquivo script com o comado /etc/regras. Mágica seu ping deve ter começado a funcionar e suas estações Windows devem navegar também.
24. Vamos 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 servidor Windows dentro da rede. É claro que outra máquina da rede também poderá fazer o acesso.

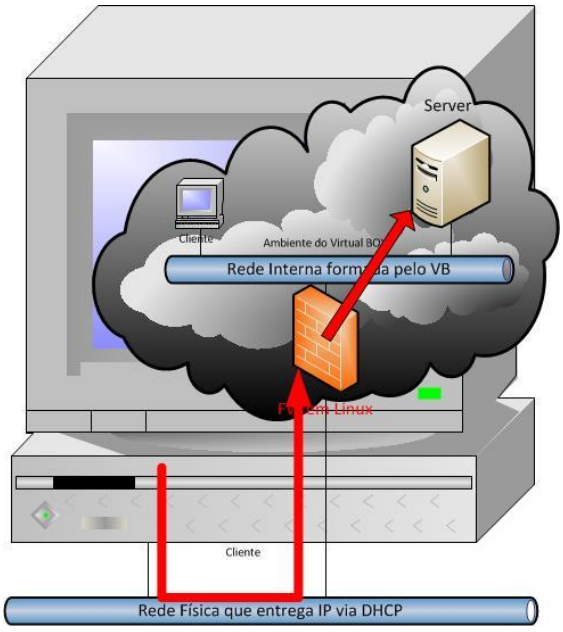

Figura 13. COnceito de redirecionamento de Porta

25. Primeiro vamos reconfigurar o servidor WEB de nosso Windows Server 2012. Parando o site www.pucminas.net que havíamos criado e deixando apenas o Default Site no ar. O aspecto da configuração deve ser parecido com a imagem a seguir.

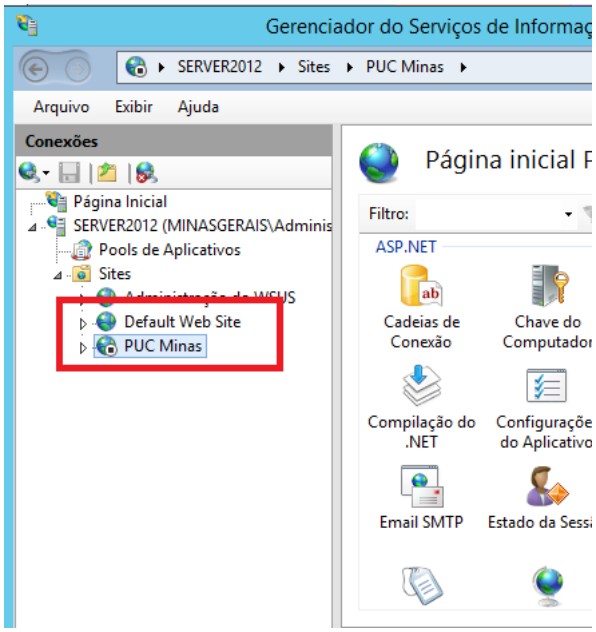

Figura 14. Aspectos do gerenciador do IIS após a reconfiguração dos sites.

26. Pelo navegador de seu Windows 7 acesse o endereço 192.168.5.1, este procedimento é apenas para confirmarmos que seu servidor web está funcionado. De aparecer uma página padrão da Microsoft.

27. De sua estação física abra o navegador e coloque o ip da interface eth0 do Linux que já usamos antes para o Winscp, no meu exemplo, 10.254.254.111. Você não deverá acessar nada.
28. Vamos configurar o iptables para redirecionar a porta 80 do Linux para o Servidor WEB que configuramos no Windows 2012 com as regras a seguir. Pode dar o comando no prompt mesmo.

```
iptables -t nat -A PREROUTING -p tcp --dport  80 -i eth0 -j DNAT --to 192.168.5.1:80
iptables –A FORWARD –d 192.168.5.1/32 –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 eth0 (nossa placa de bridge com a rede física) e redirecione (DNAT) para a máquinas interna 192.168.5.1 (nosso Windows Server). 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 192.168.5.1 está sendo autorizado.

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

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