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 Sistemas de Informação

Objetivos: Aplicar conceitos de criptografia e segurança de redes, criando um ambiente onde dois servidores Linux estabelecerão uma VPN para interligar duas redes locais com ip´s falsos.

VPN (Virtual Private Network)

- O que é?
  a. É a utilização de uma rede pública de comunicação de dados, normalmente a Internet, para trafegar dados privados, como por exemplo entre dois escritórios ou entre uma estação remota e a rede de origem do usuário.
- Objetivo.
  a. Economizar com a não contratação de links dedicados entre pontos remotos distantes e oferecer flexibilidade para interligar usuários que podem se conectar de qualquer ponto sem precisar aguardar a instalação de um link dedicado.
- Combina criptografia, autenticação e tunelamento
  a. Para tornar a comunicação segura pela Internet são necessários agrupar algumas funcionalidades aos pacotes, entre eles, garantir a identidade das pontas que estão se comunicando, garantir a integridade dos dados trafegados, em alguns casos também oferecer confidencialidade dos dados transmitidos.

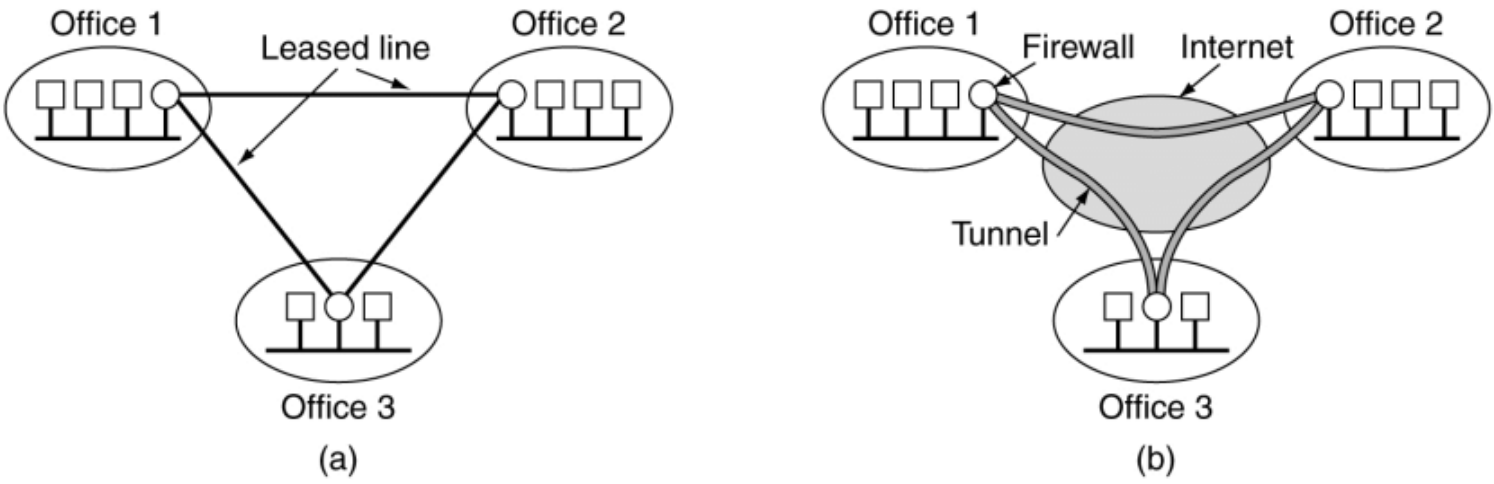

Figura 1. Exemplos de topologias sem e com a configuração e VPNs.

(a) rede privada particular (b) rede privada virtual

- O canal criado entre as pontas comunicantes pode ser **voluntário** (estabelecido pelo próprio usuário, por exemplo, quando um viajante estabelece uma conexão em um hotel com a Internet e depois abre uma conexão vpn utilizando este acesso) ou **compulsório** (o usuário não sabe que está passando por um túnel, por exemplo, quando o administrador da rede configura os roteadores ou firewalls da rede para estabelecer túneis entre os escritórios e o usuário não participa da configuração).

- O tunelamento e a criptografia garantem a segurança dos dados, mas não podem garantir tempos de resposta e taxas de transmissão, esta é uma desvantagem das VPNs quand comparados a serviços de links dedicados.

- Para se estabelecer túneis VPNs o administrador de rede deve considerar alguns requisitos básicos
    a. Autenticação de Usuários
        - Autenticar o usuário e permitir o acesso apenas de usuários autorizados.
        - Auditar qualquer tentativa de acesso, autorizado ou não.
    b. Gerenciamento de Endereços
        - Não divulgar os endereços internos da rede, utilizando endereços externos fictícios.
    c. Criptografia de Dados
        - Manter a privacidade dos dados na rede pública.

- O Nível de Segurança está diretamente relacionado ao algoritmo de criptografia escolhido e as chaves simétricas que devem permanecer em sigilo.

Protocolos de VPN

A criação de túneis VPNs pode se dar com o uso de diversos protocolos. Na verdade, pela pura definição do que é VPN, até uma conexão https pode ser considerada uma VPN, tendo em vista que a Internet é usada para tráfego de dados sensíveis nestes casos. Ou quando uma aplicação do tipo TeamViewer criptografa a comunicação entre as estações.

A seguir a lista dos principais protocolos utilizados para prover VPN e em qual camada que cada um se encontra, o que significa que as informações de cabeçalho e carga útil nas camadas superiores a que tem o protocol de tunelamento implementado estão de alguma forma sendo protegidos. Chamo atenção que pode ser de alguma forma, pois em alguns casos o objetivo pode ser oferecer só assinatura digital do conteúdo ou a assinatura mais a confidencialidade que são serviços diferentes.

- Tunelamento na Camada de Enlace:

- PPTP (*Point-to-Point Tunneling Protocol*) da Microsoft permite que o tráfego IP, IPX e NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas como a Internet.
- L2TP (*Layer 2 Tunneling Protocol*) da IETF (*Internet Engineering Task Force*) permite que o tráfego IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto tais como IP, X25, Frame Relay ou ATM.
- L2F (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.
- CIPE – Empilha tudo novamente dentro de um pacote UDP.

- Tunelamento na Camada de Rede
    a. IPsec (AH ou ESP, no modo túnel ou transporte)

- Tunelamento na Camada de Transporte
    a. SOCKS é usado para tráfego TCP através de um proxy.
    b. SOCKS com serviço de NAT
    c. SSL (Secure Socket Layer)
    d. SSH – abertura de uma sessão remota a um computador que irá trafegar como sendo seu proxy.

Conclusão

- VPNs são essenciais para a utilização da Internet como meio de transmissão de dados sensíveis
- A segurança de uma VPN vem dos algoritmos escolhidos e da segurança das senhas
- VPNs podem ser implementadas em hardware (roteadores) ou software (Windows Server , Linux, etc)
- O protocolo mais recomendado vai depender da situação, mas uma boa escolha é utilizar o IPSec que estará disponível nativamente no IPv6.

Atividade Prática (em dupla)

Cada membro da dupla deverá subir o Linux e o Windows 7 da aula anterior. O Linux deverá ter duas placas de rede, uma em modo Bridge (gere aleatório outro Endereço MAC – figura 3) e outra em modo de Rede Interna (figura 4), o cliente Windows deverá ter uma placa de rede em modo de Rede Interna. O cenário do laboratório ficará idêntico ao da figura 2.

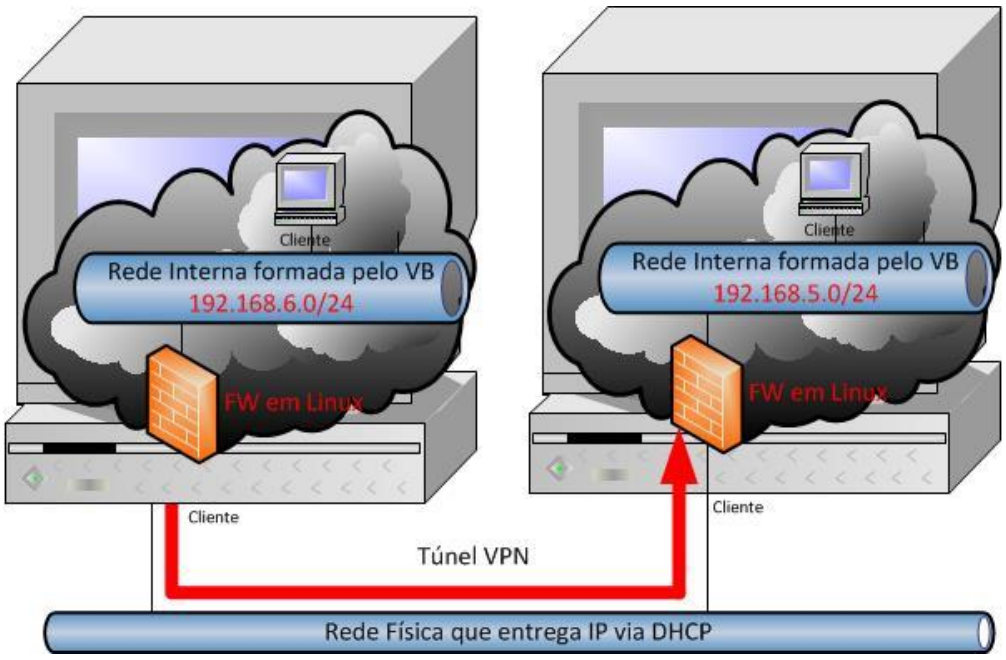

Figura 2. Cenário proposto para o Laboratório.

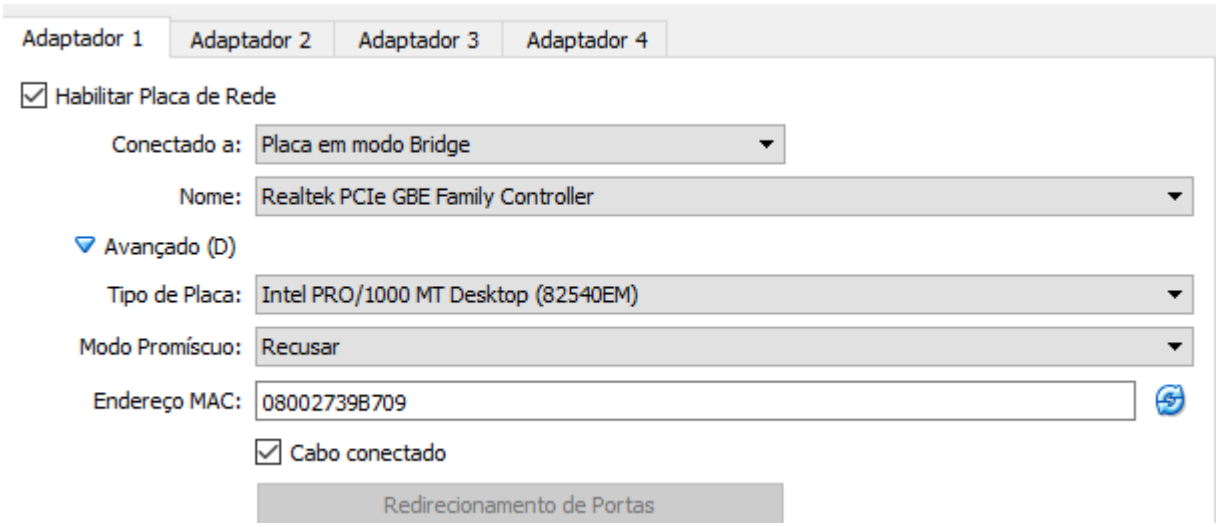

Figura 3. Configuração da Placa de Rede 1 do Linux

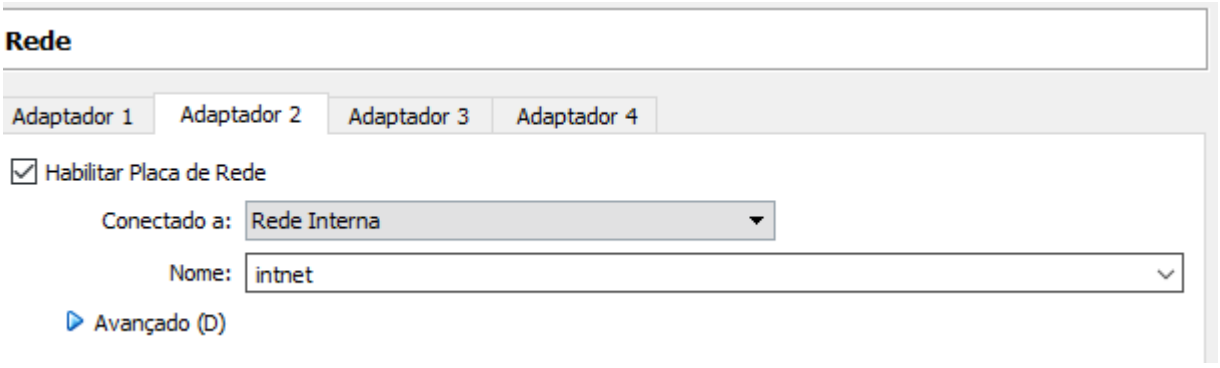

Figura 4. Configuração da segunda placa de rede

Na rede interna um aluno deverá deixar configurado a faixa de ip com a rede 192.168.5.0/24, como já havíamos feito nas outras aulas o outro aluno deve mudar esta faixa de endereço para 192.168.6.0/24.

Vamos proceder com estas configurações. Defina em sua dupla quem vai ficar com a faixa de ip 192.168.5.0/24 e quem vai ficar com a faixa 192.168.6.0/24. Suba a Máquina Virtual com Linux utilizada na aula de firewall.

Edite o arquivo /etc/network/interfaces e deixe um dos Linux com a configuração conforme a figura 5 e a outra deve ter os endereços 192.168.5 alterados para 192.168.6, mantenha o final 254 para os dois servidores. Depois de alterado dê o comando */etc/init.d/networking restart* e confira se o ip está adequado com o comando *ifconfig.* Se os novos endereços ainda não estiverem funcionando dê um comando reboot.

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

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
```

Figura 5. Arquivo /etc/network/interfaces

No caso das estações clientes confirme se a placa de rede está em modo de Rede Interna, coloque a máquina para rodar, vá à configuração de rede e deixe uma com o endereço 192.168.5.2 e a outra com 192.168.6.2 o default gateways deve ser o final 254 o dns pode ser o final 254. Veja na figura 6 a configuração de uma das estações.

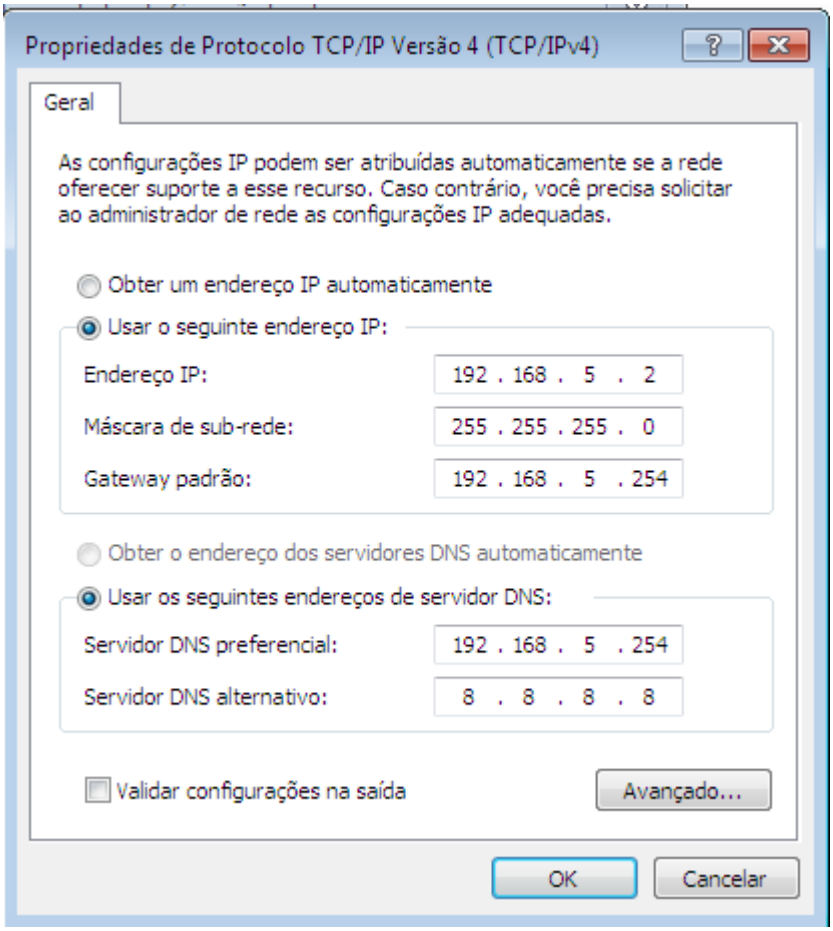

Figura 6. Configuração de uma das estações Cliente Windows.

Certifique-se que as configurações estão funcionando pingando do Windows para o servidor Linux do seu ambiente virtual, ou seja, um aluno deverá pingar o 192.168.5.254 e o outro o 192.168.6.254. Não avance enquanto isto não estiver funcionando.

Instalando pacotes

Poderíamos agora configurar na mão os arquivos de configuração do servidor, criar as chaves, os certificados, etc, mas por restrições de tempo vamos usar os entregues pelo professor. Se vc quiser ver como isto seria feito acesse o link How to setup na OpenVPN Server on debian 8.

Se vocês ainda não tiverem o WinScp vamos puxá-lo no endereço https://winscp.net/download/winscp577.zip, pois a partir de agora cada um vai trabalhar em seu servidor, mas vendo o que o outro está fazendo. Veja se ele já não está na pasta c:\vms.

Descubra o endereço da interface enp0s3 dos dois Linux, quem estiver com a rede 192.168.5.0/24 irá configurar o servidor Linux para ser o servidor da VPN e logicamente o da rede 192.168.6.0/24 irá configura para ser o cliente da VPN.

Configurando o Server VPN.

Use o Winscp para transferir os arquivos chave.key, server.conf e openvpn2 para a pasta /etc/openvpn, lembre-se de na hora de fazer o upload use o modo texto (veja figura 10), aproveite para jogar o arquivo regras para a pasta /etc. O arquivo regras será o mesmo para os dois servidores.

Ao executar o WinSCP você deverá informar o IP da interface enp0s3 do seu Linux, ou seja, aquela que está em modo Bridge. No meu exemplo 10.254.254.111.

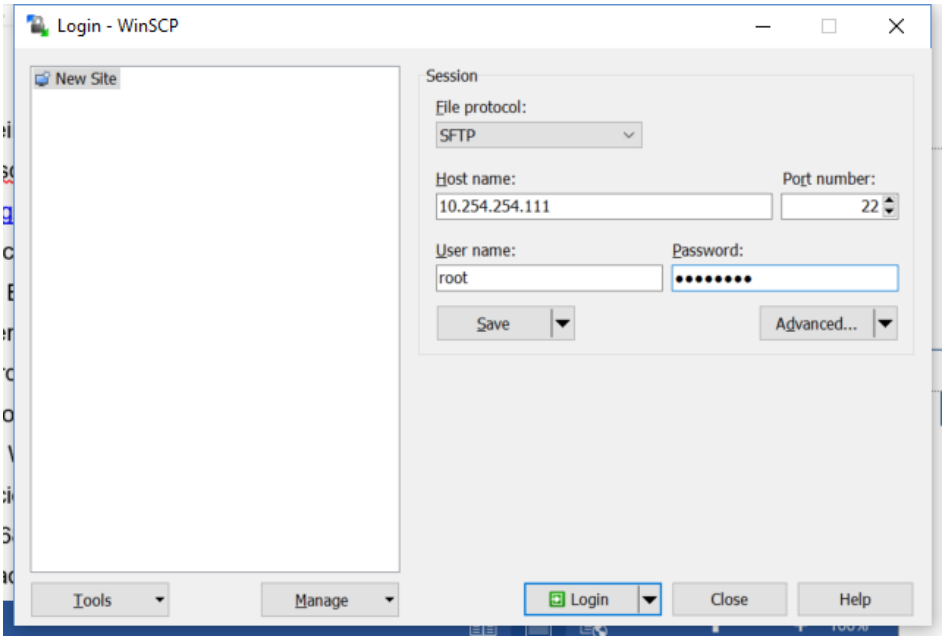

Figura 8. Tela de configuração do Aplicativo WINSCP.

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

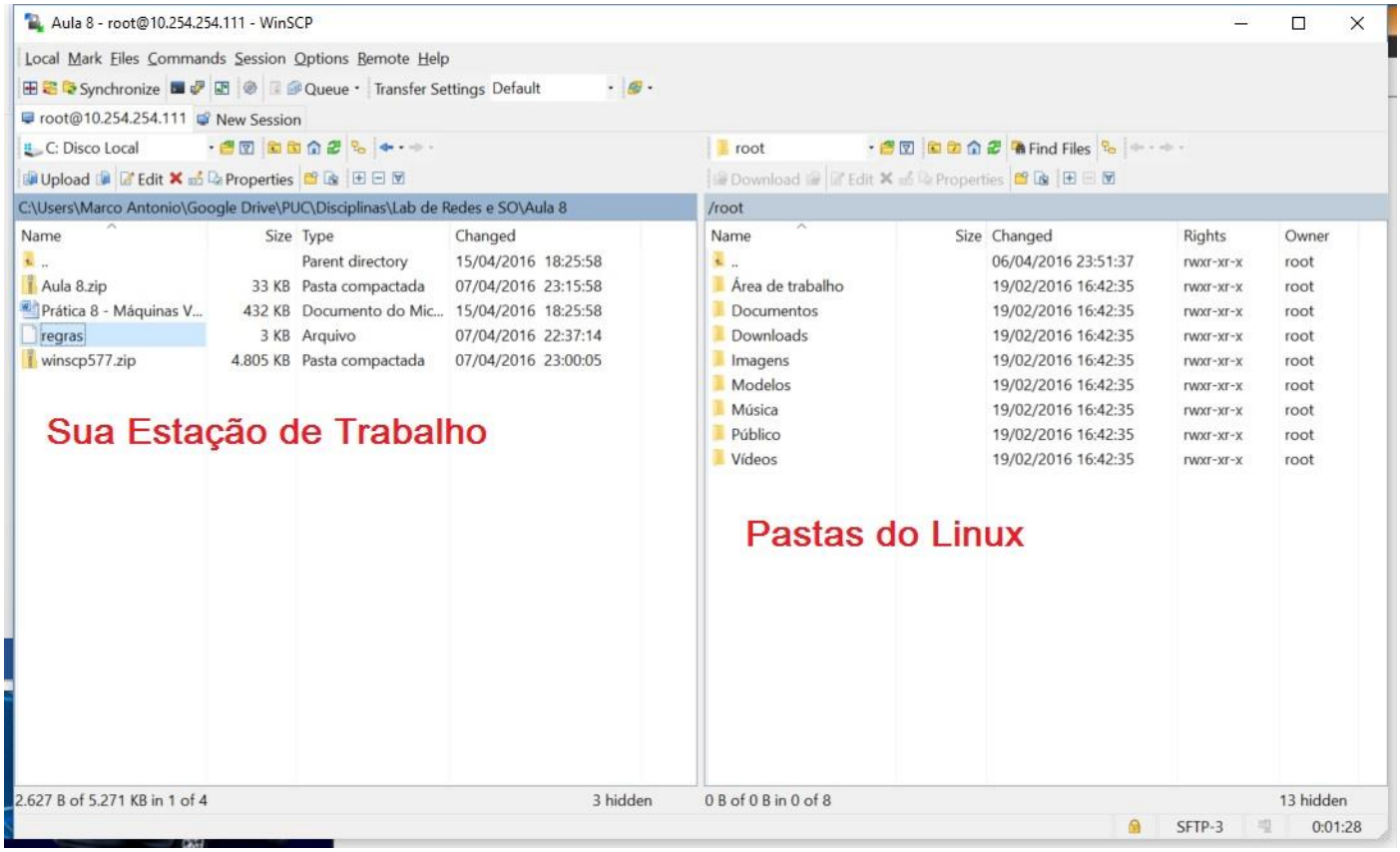

Figura 9. Interface de transferência do Winscp

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!

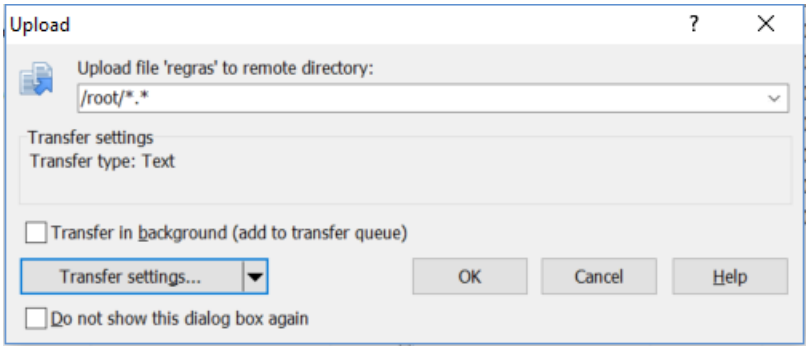

Figura 10. Alterando o modo de transferência do arquivo de binário para texto.

Mova o arquivo **server.conf, chave.key e openvpn2** para a pasta /etc/openvpn do mesmo modo.

Entendendo a função de cada arquivo.

O *chave.key* foi gerada com um comando do tipo build-key-server que baseado em alguns dados fornecidos gerou a chave simétrica de criptografia. Em nosso caso

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
aa4f5e52dce3e5d7d6bc2665a21deaf9
2031c389a35f7856e532693fb5b381cc
6715ba5b8eb3279d704d77b79d30601c
1b6263a5e5ad8d4321fea107ce16e336
f9739902c02503262d5031e499399e01
f6f88236e31171020a8d312ba89807ce
a70b618e88e1d5f3133198b14413771b
c893c1971c43bdfde408d6af3524459b
b76a5c66b5655f490995b50c9d0f5436
63457af1fb39f6980b4a4d36c1392a1a
239c8ca0de458ef0bca5d5be3e290769
2b6019e6909124931445bfcb8032e324
50dca616d478e9227a0aef3260dd5210
95d450f075acb6e2102b29f515f4d689
d9b395fce136031641673e49cc3e95cf
74092b141832e30fabfc159682c995f5
-----END OpenVPN Static key V1-----
```

O arquivo server.conf indica como o servidor irá se comportar em termos de portas que serão abertas (UDP 1190), interface que será criada (tun0), ips das interfaces (o servidor ficará com 192.168.10.1 e o cliente com 192.168.10.2), algoritmo de criptografia (DES), tipo de cifra (CBC), chave simétrica que será usada, rota que deverá subir para outra rede (route 192.168.6.0 255.255.255.0), arquivos de log, etc.

```
dev tun0
ifconfig 192.168.10.1 192.168.10.2
proto udp
port 1190
secret /etc/openvpn/chave.key
cipher DES-EDE3-CBC
persist-key
float
verb 3
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
persist-tun
persist-key
route 192.168.6.0 255.255.255.0
```

Por fim, o arquivo openvpn2 que é um script para subir o serviço, se vc preferir pode substituir o /etc/init.d/openvpn por este arquivo. Abaixo um trecho onde pode ser vista a sintaxe do comando.

.....

```
case "$1" in
start)
       /usr/sbin/openvpn --writepid /var/run/openvpn.0.pid --script-security
3 system -daemon ovpn --cd /etc/openvpn --config /etc/openvpn/server.conf &
  ;;
stop)
  if test -z "$2" ; then
    for PIDFILE in `ls /var/run/openvpn.*.pid 2> /dev/null`; do
      NAME=`echo $PIDFILE | cut -c18-`
      NAME=${NAME%%.pid}
      stop_vpn
    done
  else
    while shift ; do
      [ -z "$1" ] && break
      if test -e /var/run/openvpn.$1.pid ; then
```

.....

Mude a permissão do arquivo /etc/openvpn/openvpn2 com o comando *chmod 755 /etc/openvpn/openvpn2,* rode o script com o comando */etc/openvpn/openvpn2 start* e em seguida dê o comando *ifconfig*, você deve ver uma interface nova, a tun0.

Dê um ping para 192.168.10.2 que é o ip do túnel da outra ponta, se seu colega já configurou o outro lado você deve ter resposta, caso contrário vá ajuda-lo!!!!

Configurando o Cliente VPN

Use o Winscp para transferir os arquivos chave.key, cliente.ovpn e openvpn2-cliente para a pasta /etc/openvpn, lembre-se de na hora de fazer o upload use o modo texto (veja figura 13), aproveite para jogar o arquivo regras para a pasta /etc. O arquivo regras será o mesmo para os dois servidores.

> 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.

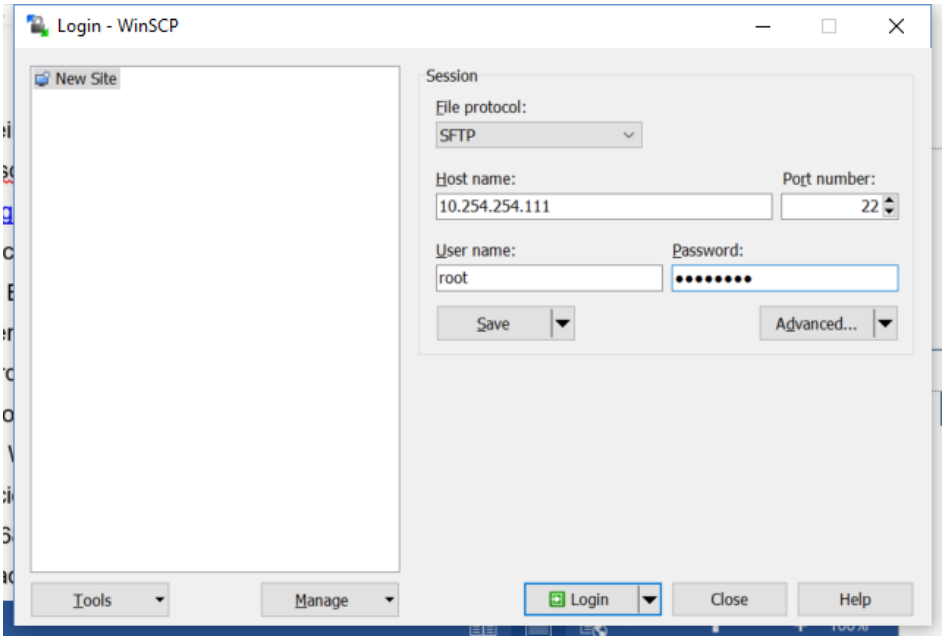

Figura 11. Tela de configuração do Aplicativo WINSCP.

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

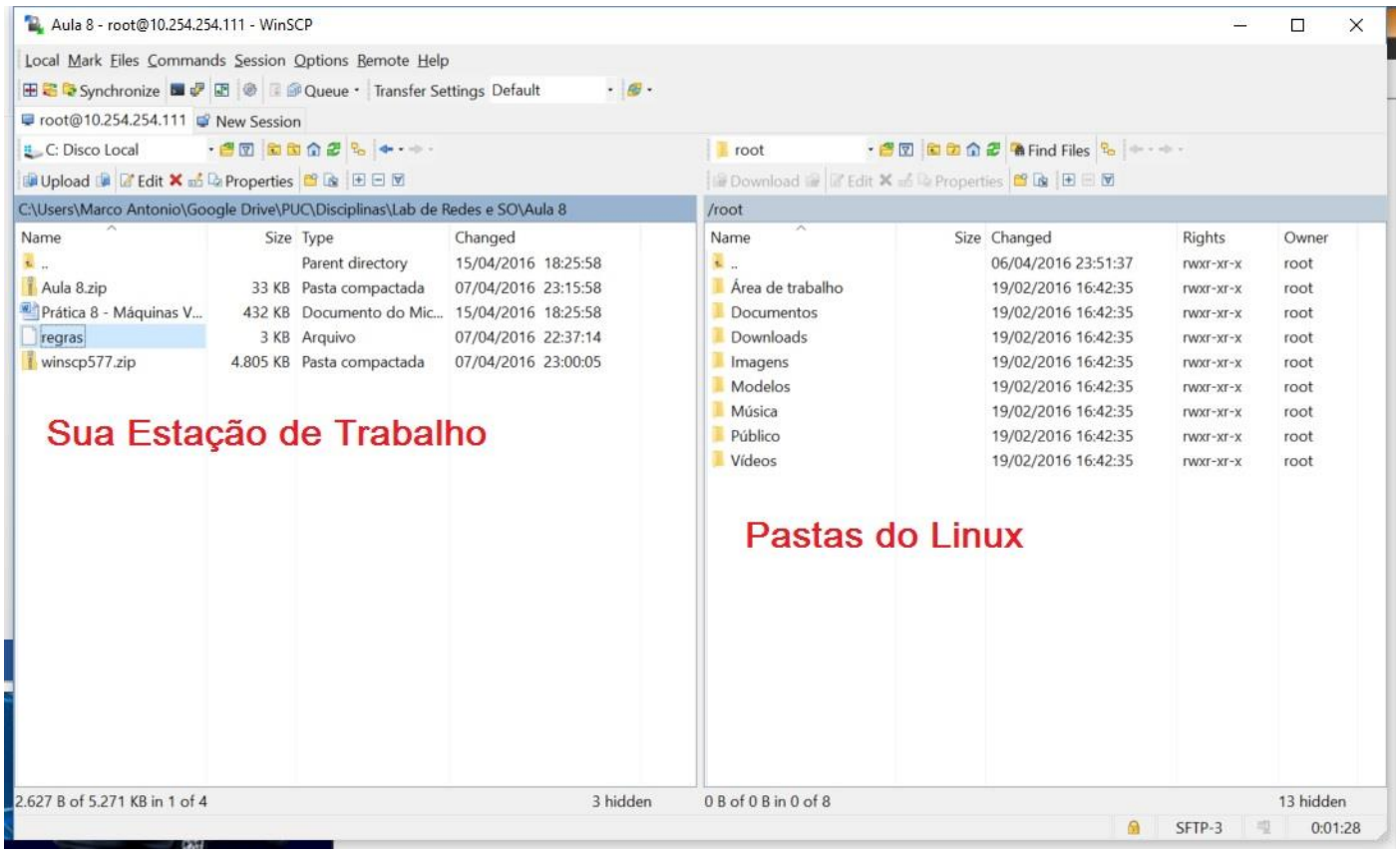

Figura 12. Interface de transferência do Winscp

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!

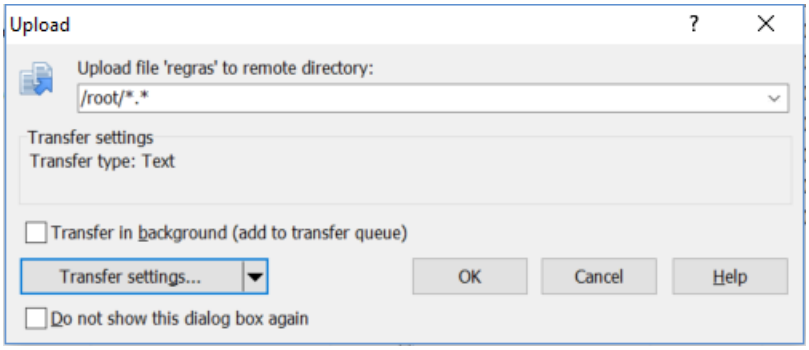

Figura 13. Alterando o modo de transferência do arquivo de binário para texto.

Mova o arquivo **cliente.ovpn, chave.key e openvpn2-cliente** para a pasta /etc/openvpn do mesmo modo.

Entendendo a função de cada arquivo.

O *chave.key* foi gerada com um comando do tipo build-key-server que baseado em alguns dados fornecidos gerou a chave simétrica de criptografia. Em nosso caso

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
aa4f5e52dce3e5d7d6bc2665a21deaf9
2031c389a35f7856e532693fb5b381cc
6715ba5b8eb3279d704d77b79d30601c
1b6263a5e5ad8d4321fea107ce16e336
f9739902c02503262d5031e499399e01
f6f88236e31171020a8d312ba89807ce
a70b618e88e1d5f3133198b14413771b
c893c1971c43bdfde408d6af3524459b
b76a5c66b5655f490995b50c9d0f5436
63457af1fb39f6980b4a4d36c1392a1a
239c8ca0de458ef0bca5d5be3e290769
2b6019e6909124931445bfcb8032e324
50dca616d478e9227a0aef3260dd5210
95d450f075acb6e2102b29f515f4d689
d9b395fce136031641673e49cc3e95cf
74092b141832e30fabfc159682c995f5
```

```
-----END OpenVPN Static key V1-----
```

O arquivo cliente.ovpn indica em qual endereço remoto o cliente deverá abrir o túnel, em qual interface (tun0) , com quais ips das interfaces (o servidor ficará com 192.168.10.1 e o cliente com 192.168.10.2), algoritmo de criptografia (DES), tipo de cifra (CBC), chave simétrica que será usada, rota que deverá subir para outra rede (route 192.168.5.0 255.255.255.0), etc. Mude o endereço remote eu está com 10.2.200.5 para o ip do seu parceiro de atividade!!!

```
remote 10.2.200.5
dev tun0
ifconfig 192.168.10.2 192.168.10.1
secret chave.key
proto udp
port 1190
cipher DES-EDE3-CBC
ping 15
verb 4
persist-tun
persist-key
route 192.168.5.0 255.255.255.0
```

Por fim, o arquivo openvpn2-cliente que é um script para subir o serviço, se vc preferir pode substituir o /etc/init.d/openvpn por este arquivo. Abaixo um trecho onde pode ser vista a sintaxe do comando.

.....

```
case "$1" in
start)
       /usr/sbin/openvpn --writepid /var/run/openvpn.0.pid --script-security
3 system -daemon ovpn --cd /etc/openvpn --config /etc/openvpn/cliente.ovpn &
  ;;
stop)
  if test -z "$2" ; then
    for PIDFILE in `ls /var/run/openvpn.*.pid 2> /dev/null`; do
      NAME=`echo $PIDFILE | cut -c18-`
```

.....

Mude a permissão do arquivo /etc/openvpn/openvpn2-cliente com o comando *chmod 755 /etc/openvpn/openvpn2-cliente,* rode o script com o comando */etc/openvpn/openvpn2-cliente start* e em seguida dê o comando *ifconfig*, você deve ver uma interface nova, a tun0.

Dê um ping para 192.168.10.1 que é o ip do túnel da outra ponta, se seu colega já configurou o outro lado você deve ter resposta, caso contrário vá ajuda-lo!!!!

Recado para a dupla – Não avancem enquanto não conseguirem pingar as interfaces 192.168.10.1 ou 2.

Agora entre no Windows que está com o ip 192.168.6.2 tente pingar o 192.168.5.2 que é o outro Windows que está em uma rede “remota” (no computador do lado). Não vai funcionar.

Você consegue dizer o porquê?
Sim os Linux não estão configurados para redirecionar pacotes de uma interface (enp0s3) para outra (tun0) mesmo havendo a rota que vc pode verificar com o comando *route*.

Deixe o *ping 192.168.5.2 –t* rodando na estação 6.2, ele não deve estar respondendo ainda.

Agora nos dois servidores vcs devem alterar a permissão do arquivo regras que já fizemos o upload antes com o comando *chmod 755 /etc/regras* e em seguida rodar o script com o comando */etc/regras start*.

Entenda partes do arquivo de regras do firewall

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

......
#ativando o mascaramento - NAT para os pacotes que passarem pelo tun0
/sbin/iptables -t nat -A POSTROUTING -o tun0 -j MASQUERADE
echo "Ativando mascaramento de IP ..............[ OK ]"

.......
# liberando alguns encaminhamentos não importando a origem ou destino
/sbin/iptables -A FORWARD -p icmp -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
/sbin/iptables -A FORWARD -p udp --dport 53 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 80 -j ACCEPT
/sbin/iptables -A FORWARD -p tcp --dport 443 -j ACCEPT


Importante, perceba que quando eu der um ping da 6.2 para 5.2, ao apssar
pelo firewall ele vai fazer NAT do IP 5.2 para 192.168.10.2. Logo o
192.168.5.2 não saberá da existência da 6.2
```

E aí seu ping está funcionado agora?

Atividades extras.

1. Instale o Wireshark no seu Windows 7, no endereço https://www.wireshark.org/download.html (sua estação deve estar sem internet, coloque a placa de rede em modo bridge e altere as configurações da placa de rede para obter endereço automaticamente). Retorne as configurações para rede interna depois de fazer o download.
2. Dê o ping novamente para o outro lado e capture os pacotes de comunicação entre as estações clientes Windows. Qual é o ip de origem dos pacotes?
3. Tente fazer mudanças de tal forma que o endereço de origem que chegue ao destino seja o real da máquina, ou seja se a 5.2 está pingando a 6.2, o ip que deve aparecer no wireshark são estes.
4. Tente descobrir qual é o protocolo de vpn que está sendo usado pelo Openvpn, para isto vc terá que capturar o tráfego entre as interfaces 192.168.10.1 e 10.2.