www.redelegal.com

Transforme um Raspberry Pi em um roteador ethernet

Este tutorial irá guiá-lo através do processo de criação de seu Raspberry Pi como um roteador.

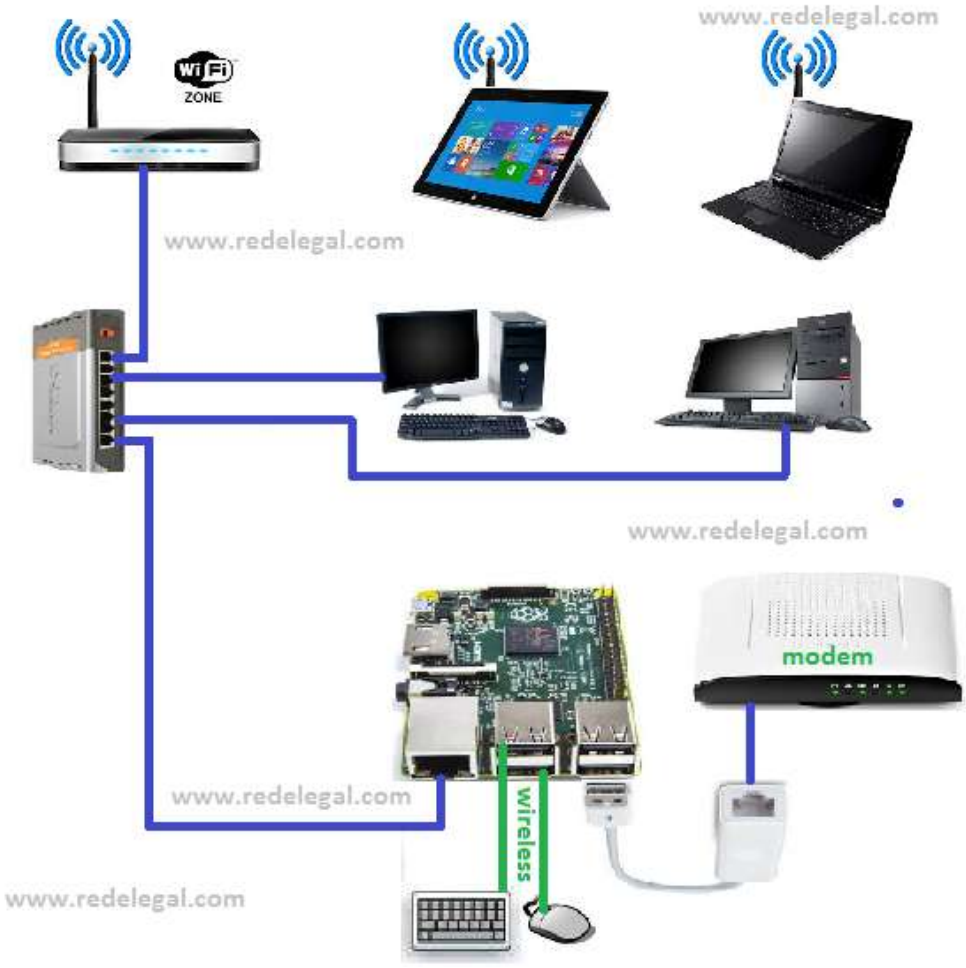
Tutorial feito com tentativas, erros, acertos e muita leitura de:

http://www.hardware.com.br/livros/servidores-linux/compartilhando-conexao.html

http://www.hardware.com.br/livros/servidores-linux/ativando-compartilhamento.html

https://www.digitalocean.com/community/tutorials/how-to-use-iproute2-tools-to-manage-network-configuration-on-a-linux-vps

http://raspberrypihq.com/how-to-turn-a-raspberry-pi-into-a-wifi-router/



Pré-requisitos e Equipamentos

Você vai precisar do seguinte:

Raspberry Pi (Pra teste foi usado um RPI 2)

Um SD Card de no minimo 2 gb com Raspbian Jessie-lite gravado

Aceso ao RPI via teclado e monitor (ou remotamente)

Adaptador USB / Ethernet

Boot no RPI

Conecte o adaptador USB / Ethernet em uma das portas USB livres no RPI

Ligue o RPI

Após a inicialização e log-in use os comandos abaixo para ter certeza que o adaptador USB / Ethernet foi reconhecido

```
pi@raspberrypi:~$    sudo su
root@raspberrypi:/home/pi#    ifconfig
```
WWW.redelegal.com

Se a placa tiver sido reconhecida, você devera ter uma tela parecida com isso

```
root#raspberrpi:/home/pi#    ifconfig
eth0    Link  encap:Ethernet    HWaddr  b8:27:eb:xx:xx:xx
        inet addr:192.168.1.13   Bcast:192.168.1.15   Mask:255.255.255.240
        inet6 addr etc    etc    etc    etc

eth1    Link  encap:Ethernet    HWaddr  00:60:6e:xx:xx:xx
        inet6 addr  etc  etc    etc    etc

lo      Link  encap:local    Loopback
        inet addr:127.0.0.1   Mask:255.0.0.0
        inet6 addr etc    etc    etc    etc
```
www.redelegal.com.br

Eth0 = Rede onboard do RPI (Todos os numeros MAC das RPI 2 deverão começar com b8:27:eb).

Eth1 = Adaptador USB / Ethernet

Antes de iniciar a configuração da rede e muito importante:

1- Expandir a capacidade de armazenamento do SD Card

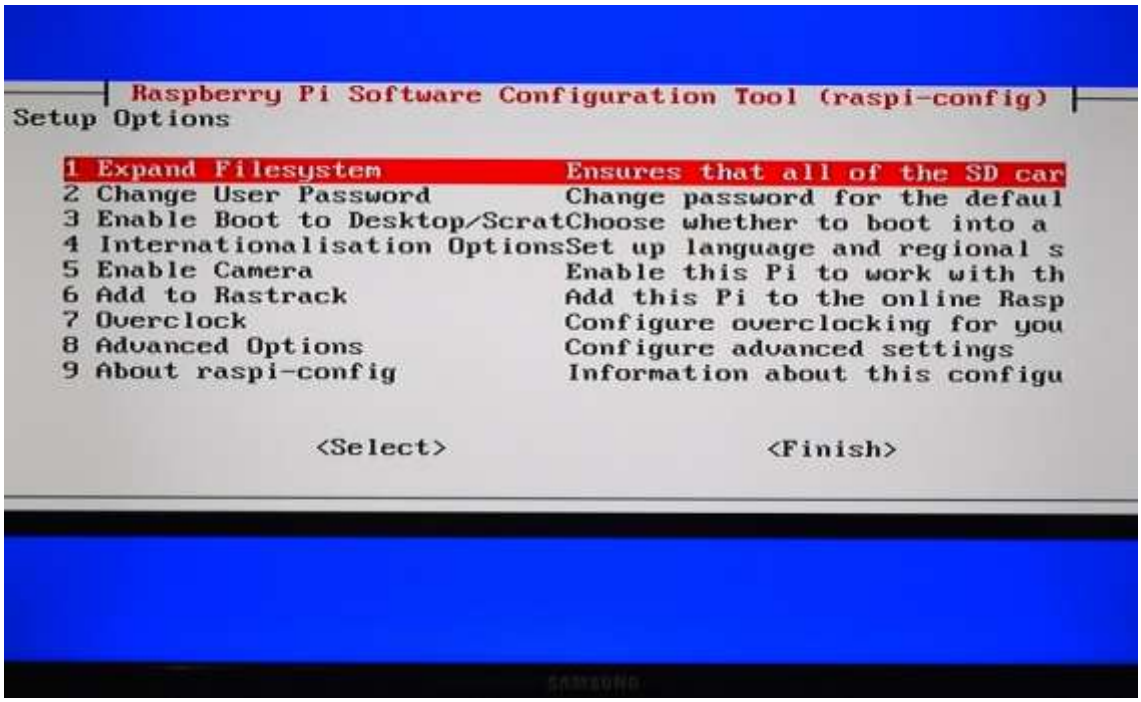
2- Configurar seu teclado(neste caso mostro como configurar para abnt2)

3- Mudar o idioma do sistema para Portugues BR.

Para expandir a capacidade de armazenamento do SD Card, no Prompt de comando digite

```
root@raspberrypi:/home/pi#  raspi-config
```
WWW.redelegal.com

Na tela a seguir escolha o item 1 e tecle “ Enter ”



Reinicie o sistema

Para configurar seu teclado para abnt2 basta editar o arquivo keyboard com o comando

```
root@raspberrypi:/home/pi#  Nano /etc/default/keyboard
```

para

XKBMODEL="abnt2"

XKBLAYOUT="br"

XKBVARIANT=""

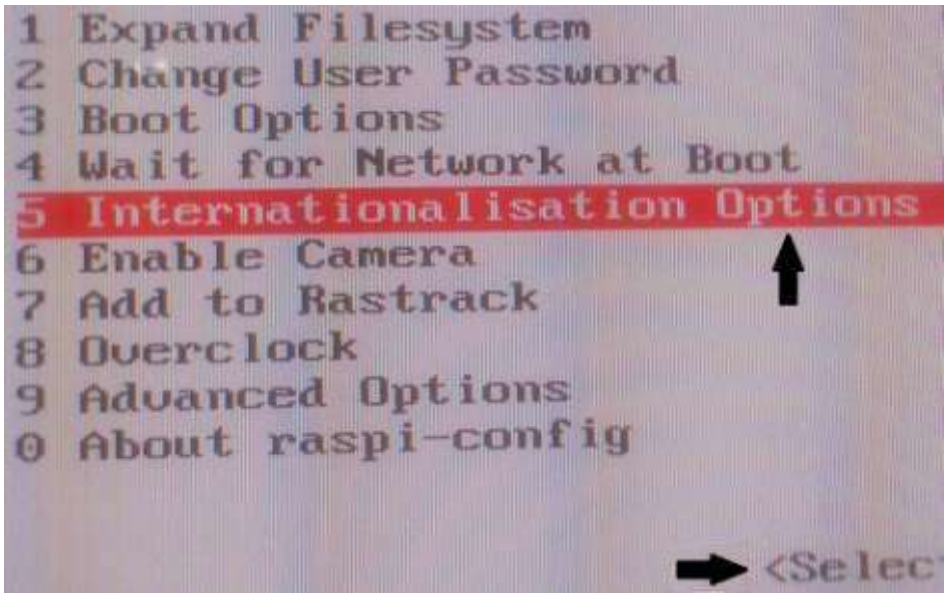
XKBOPTIONS="lv3:alt_switch,compose:rctrl"

Reiniciar o sistema

Para mudar o idioma do sistema para “português BR”

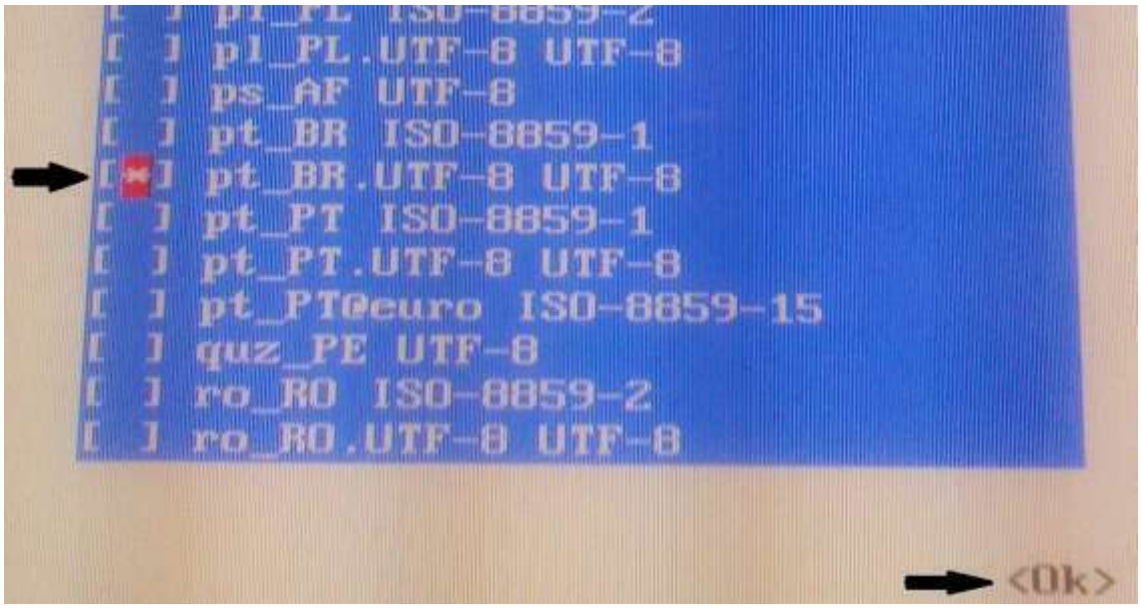
No prompt de comando digite

Selecione a opção numero 5 **(Internationalisation options)**



Selecione a opção numero 1 **(Change Locale)**

Selecione a opção **“ pt_BR.UTF-8 UTF-8 “**



Depois de tudo instalado, reinicie o sistema.

Configuração da rede

Você deve editar o arquivo “interfaces”, para abri-lo com o nano use este comando:

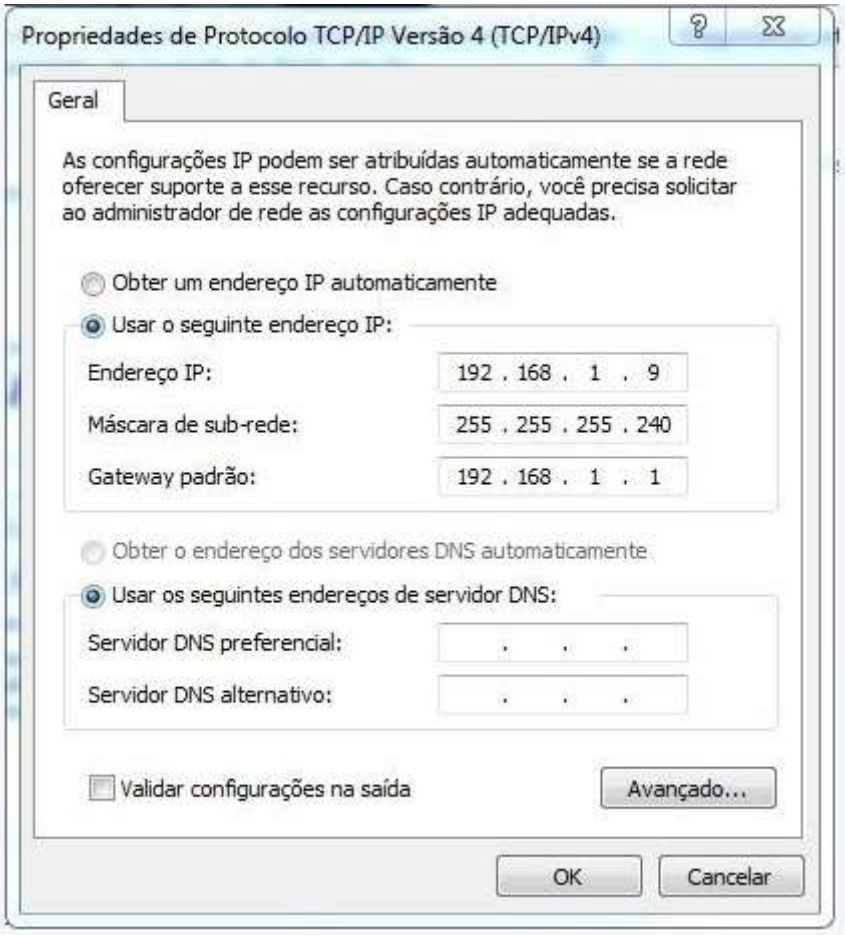
```
nano /etc/network/interfaces                    www.redelegal.com
```

Abaixo esta como ficou o meu arquivo

Salve o arquivo e reinicie o RPI.

Configure manualmente as configurações de rede de outra maquina.

(Exemplo das configurações de rede de micro com Windows 7)

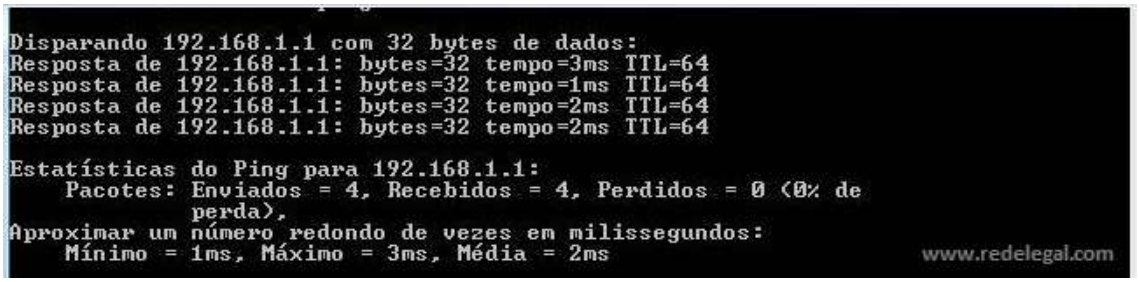


www.redelegal.com

Nessa outra maquina use o comando “ping” para confirmar que as maquinas estão se comunicando.

Ping 192.168.1.1 www.redelegal.com

Se tudo estiver correto você terá essa imagem



(Essa maquina esta ligada a rede do RPI pelo roteador WIFi)

Instale o software do roteador

Para que seu Raspberry Pi2 possa funcionar como roteador você vai precisar instalar o seguinte software

isc-dhcp-server

isc-dhcp-server é um servidor DHCP. Um servidor DHCP é responsável pela atribuição de endereços de computadores e dispositivos de conexão.

Para instalar o software DHCP execute os seguintes comandos:

```
Pi#  apt-get update
Pi#  apt-get  install  isc-dhcp-server          www.redelegal.com
```

Depois de instalado, estamos prontos para configurar o software.

Configurando o ISC-DHCP-Server

Para configurar o servidor DHCP, abrir o arquivo ”dhcpd.conf” em /etc/dhcp no seu editor de texto favorito. Você pode abri-lo com o nano usando este comando:

```
PI# Nano  /etc/dhcp/dhcpd.conf                www.redelegal.com
```

Este arquivo esta com muitos comentários (frases que começam com uma tralha (#)) e alguns comandos, encontrei varios tutoriais em inglês e portugues, achei muito confuso e por isso resolvi apagar tudo e deixar somente o que achei necessario, ficou assim

```
authoritative;

subnet 192.168.1.0 netmask 255.255.255.240 {
range 192.168.1.1 192.168.1.14;
option routers 192.168.1.1;
default-lease-time 600;
max-lease-time 7200;
option domain-name "raspberry-pi2";
option domain-name-servers 1  9.39.2  0.2,1  7.  4.1  6.1;
}
 host reserva1 {
    hardware ethernet 00:00:00:00:00:01;
    fixed-address 192.168.1.2;
}
 host reserva2 {
    hardware ethernet 00:00:00:00:00:02;
    fixed-address 192.168.1.3;
}
 host hp_cabo {
    hardware ethernet 00:1b:38:3a:c2:7c;
    fixed-address 192.168.1.4;
}
 host srv2 {
    hardware ethernet 00:60:67:78:f8:d5;
    fixed-address 192.168.1.5;
}
 host hp_wire {
    hardware ethernet 00:1d:e0:67:7e:8d;
    fixed-address 192.168.1.6;
}
 host impre_hp {
    hardware ethernet 9c:b6:54:d7:b8:98;
    fixed-address 192.168.1.7;
}
 host tablet {
    hardware ethernet 58:3f:54:fc:45:09;
    fixed-address 192.168.1.8;
}
 host len_wire {
    hardware ethernet 9c:b7:0d:0f:1f:78;
    fixed-address 192.168.1.9;
}
 host len_cabo {
    hardware ethernet dc:0e:a1:be:51:fb;
    fixed-address 192.168.1.10;
}
 host reserva3 {
    hardware ethernet 00:00:00:00:00:03;
    fixed-address 192.168.1.11;
}
 host reserva4 {
    hardware ethernet 00:00:00:00:00:04;
    fixed-address 192.168.1.12;
}
 host reserva5 {
    hardware ethernet 00:00:00:00:00:05;
    fixed-address 192.168.1.13;
}
 host reserva6 {
    hardware ethernet 00:00:00:00:00:06;
    fixed-address 192.168.1.14;
}
```

(Option domain-name-servers foi modificado)

Por usar um router WiFi ligado ao switch resolvi ocupar os 14 endereços possíveis na minha rede para evitar uso indevido (não da 100% de segurança mais dificulta bastante para o usuário comum ne?)

Próximo arquivo para editar é / etc / default / isc-dhcp-server, você pode abri-lo com o nano usando este comando:

```
nano /etc/default/isc-dhcp-server                    www.redelegal.com
```

Coloque na ultima linha do arquivo

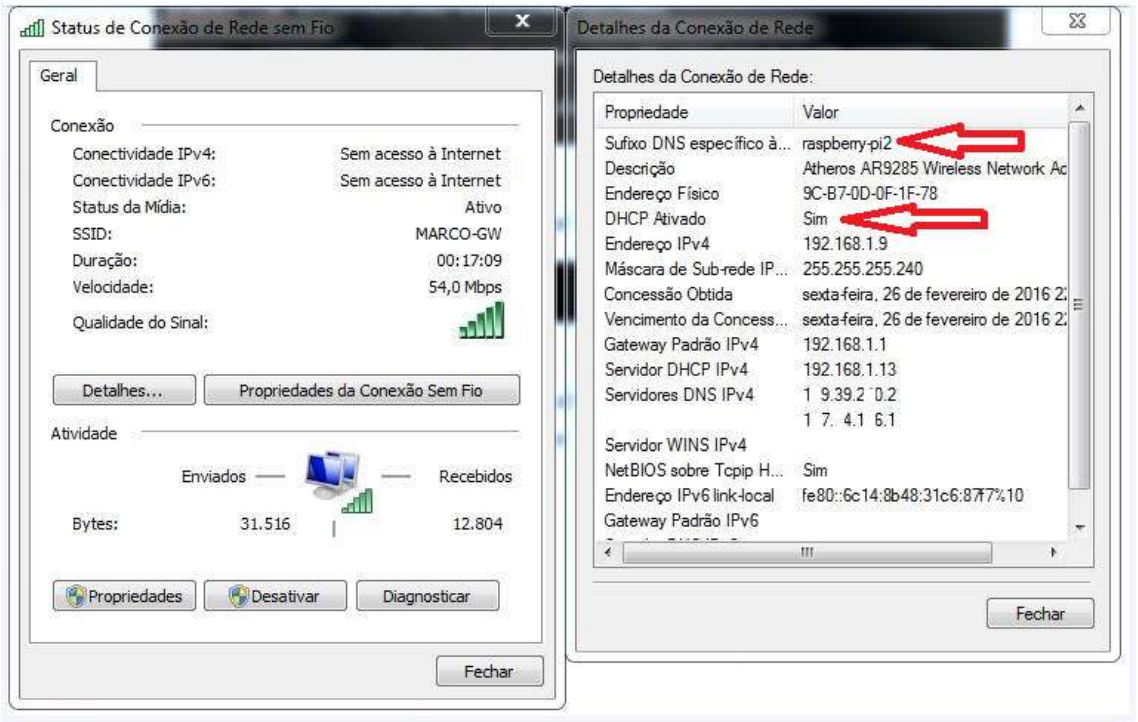
```
INTERFACES="eth0"                                    www.redelegal.com
```

Salvar o arquivo, sair e reiniciar o RPI

Digite o comando abaixo para iniciar o servidor DHCP

```
service isc-dhcp-server start                        www.redelegal.com
```

Se tudo estiver correto o **prompt** vai reaparecer, nenhuma mensagem vai aparecer, como tira teima, se estiver usando o Windows 7 verifique o **STATUS** das configurações de rede.



(Servidores DNS IPv4 modificados)

Terminando . . .

Ativando o compartilhamento

Depois de tudo preparado, ativar o compartilhamento é bastante simples

No Linux, o compartilhamento é feito no Iptables, para ativar o compartilhamento são necessários três comandos:

```
modprobe iptable_nat
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Este comando compartilha a conexão proveniente da

placa da internet com a placa de rede no RPI, por isso não é necessário

especificar a placa de rede local.

O primeiro comando ativa o módulo do Iptables responsável por oferecer suporte ao roteamento de pacotes via NAT.

O segundo ativa o módulo responsável pelo encaminhamento de pacotes, utilizado pelo módulo iptable_nat.

O terceiro cria uma regra de roteamento, que orienta o servidor a direcionar para a internet todos os pacotes (recebidos dos clientes) que se destinarem a endereços que não façam parte da rede local.

A partir daí, o servidor passa a ser o gateway da rede.

É importante proteger o servidor de ataques da Internet usando um firewall.

Devemos ativar um firewall de bloqueio usando mais alguns comandos do Iptables, complementando os três comandos anteriores:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --syn -j DROP
```

O primeiro comando faz com que o seu servidor deixe de responder a pings.

Os dois comandos seguintes protegem contra IP spoofing (uma técnica usada em diversos tipos de ataques, onde o atacante envia pacotes usando um endereço IP falso como remetente, tentando assim

obter acesso a PCs da rede interna) e contra pacotes inválidos, que são comumente utilizados em ataques DoS e ataques de buffer overflow.

As duas linhas seguintes autorizam pacotes provenientes da interface de loopback (lo), juntamente com pacotes provenientes da rede local. Como pode ver, a sintaxe das regras do Iptables segue um padrão lógico, onde você especifica uma determinada condição e diz o que o firewall deve fazer com os pacotes que se enquadrarem nela.

No caso da regra que autoriza os pacotes da rede local (iptables -A INPUT -i eth0 -j ACCEPT) usamos os parâmetros "-A INPUT" (pacotes de entrada) e "-i eth0" (recebidos na interface eth0), seguidos da regra "-j ACCEPT", que diz que os pacotes devem ser aceitos sem checagem adicional

A linha "iptables -A INPUT -p tcp --dport 22 -j ACCEPT" abre a porta 22, usada pelo SSH para conexões externas, permitindo que você possa administrar o servidor remotamente. Você pode abrir mais portas

simplesmente adicionando mais linhas, com as portas desejadas. Concluindo, temos a linha "iptables -A INPUT -p tcp --syn -j DROP", que faz o trabalho pesado, bloqueando tentativas de conexão provenientes da Internet.

Depois de testar o compartilhamento, falta fazer com que os comandos sejam executados durante o boot, tornando a configuração permanente. A forma mais simples de fazer isso é colocar os comandos no arquivo "/etc/rc.local", um script próprio para a tarefa, que está disponível tanto em distribuições derivadas do Debian quanto em distribuições da linhagem do Red Hat. Um exemplo de arquivo completo, incluindo os comandos para ativar o firewall seria:

```
#!/bin/sh
# /etc/rc.local
modprobe iptable_nat
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
echo 1 > /proc/sys/net/ipv4/conf/default/rp_filter
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -p tcp --syn -j DROP
```

Esta receita é genérica, deve funcionar em qualquer distribuição.