Script para inicializar o firewall e criar as regras para compartilhar a internet.

Abaixo vamos criar 10 regras básicas para o iptables, inclusive o compartilhamento da internet.

Fora os para abrir portas específicas. Não seria muito prático ficar digitando tudo isso cada vez que precisar reiniciar o micro. Para automatizar isso, basta colar todos os comandos dentro de um arquivo de texto e salvar dento das seguinte pasta. Você pode salvá-lo como por exemplo: /usr/local/bin/com o nome de meu_firewall

Criando o script de compartilhamento da internet em 3 passos

Parte 1 – criar o arquivo de configuração do firewall.

Para entrar na pasta

Digite: cd /usr/local/bin

Para criar o arquivo em branco

Digite: pico meu_firewall

As linhas de compartilhamento da conexão não conflitam com as regras de firewall que vimos anteriormente, você deve apenas ter o cuidado de colocá-las no inicio da seqüência. Neste caso nosso script completo ficaria assim:

```
#!/bin/sh

echo "Ativando o firewall"

# Carrega os módulos
modprobe iptables
modprobe iptable_nat

# Compartilha a conexão
modprobe iptable_nat
```

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
echo 1 > /proc/sys/net/ipv4/ip_forward

# protege contra pacotes danificados (usados em ataques DoS por exemplo) é:

iptables -A FORWARD -m unclean -j DROP

# Abre algumas portas (opcional)

iptables -A INPUT -p tcp --destination-port 22 -j ACCEPT
iptables -A INPUT -p tcp --destination-port 1021 -j ACCEPT
iptables -A INPUT -p tcp --destination-port 1080 -j ACCEPT

# Abre para a rede local, obs se vc estiver usando rede 192.168.0.1

iptables -A INPUT -p tcp --syn -s 192.168.0.0/255.255.255.0 -j ACCEPT

# Fecha o resto
iptables -A INPUT -p tcp --syn -j DROP
```

Se você quiser que o PC também não responda a pings, adicione a linha:

```
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

ctrl+o (salva)
ctrl+x (sai do editor)

Obs. O arquivo devera ser salvo dentro da pasta e caminho descrito:

/usr/local/bin/
Com o nome abaixo como descrito no inicio do script
meu_firewall

Parte 2 – Dar permissão de execução do arquivo de script.

Em seguida, dê permissão de execução para o arquivo
chmod +x /usr/local/bin/meu_firewall
Com isso o arquivo já tem premissão de execução.
Pata editar o arquivo para possíveis correções basta digitar:
pico /usr/local/bin/`meu_firewall`

Parte 3 – Usar um arquivo de inicialização do sistema para chamar o arquivo meu_firewall no boot.

Para tornar a inicialização realmente automática, você precisa apenas colocar o comando num dos arquivos de inicialização do sistema.

Lembre-ser vc precisa inserir o comando para executar o script quando o sistema iniciar.

Abra o arquivo **/** etc/rc.local e adicione a linha:

/usr/local/bin/meu_firewall

Digite: pico /etc/rc.local
Adicione a linha a abaixo antes do "exit 0"
/usr/local/bin/meu_firewall
Esse comando vai fazer com que o script seja executado junto com o boot.

No Debian e Kurumin você pode abrir o arquivo **/ etc/ init.d/ bootmisc.sh**

E adicionar a mesma linha:

/usr/local/bin/meu_firewall

Esse ultimo passo obriga o script a ser inicializado no boot.

Referencia: http://www.guiadohardware.net/artigos/firewall-iptables/

Pdf de apoio no site HTTP://profwilson.orgfree.com

Professor_wil@yahoo.com.br.