Introdução

Esta é uma documentação para implementação de um firewall para aceitar somente os protocolos ICMP, HTTP/HTTPS e resoluções DNS, qualquer protocolo fora desses estabelecidos devem ser bloqueados.

Dependências

- net-tools (ping, host, ifconfig)
- w3m (command line web browser)
- iptables (Configuração de firewall e NAT)
- wondershare (limitador de banda)

De antemão instale todos os pacotes utilizando as linhas de comando:

```
$ sudo apt-get install net-tools
$ sudo apt-get install w3m
$ sudo apt-get install iptables
$ sudo apt-get install wondershare
```

Configuração do Firewall

Primeiramente execute os dois comandos para zerar/excluir qualquer regra das cadeias, sejam as criadas por um usuário ou em todas cadeias.

```
$ iptables -F
$ iptables -X
```

Agora verifique se as políticas de sua tabela (FILTER) está por padrão em ACCEPT, caso não esteja execute o comando para alterar o estado:

```
$ iptables --policy <chain> ACCEPT
```

Execute os comandos abaixo para liberar os pacotes do protocolo ICMP tanto no servidor quanto nos hosts da subrede.

```
iptables -A INPUT -p icmp -s 10.0.0.0/16 -j ACCEPT
iptables -A FORWARD -p icmp -s 10.0.0.0/16 -j ACCEPT
```

Feito isso, libera-se os pacotes HTTP e HTTPS, que utilizam as portas 80 e 443, respectivamente.

```
iptables -A FORWARD -p tcp --dport 80 -s 10.0.0.0/16 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 80 -s 10.0.0.0/16 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -s 10.0.0.0/16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 443 -s 10.0.0.0/16 -j ACCEPT
```

Agora, libere a resolução de DNS, para tanto, libera-se as portas 53 tanto no protocolo UDP quanto no TCP.

```
iptables -A FORWARD -p udp --dport 53 -s 10.0.0.0/16 -j ACCEPT
iptables -A FORWARD -p tcp --dport 53 -s 10.0.0.0/16 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 10.0.0.0/16 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -s 10.0.0.0/16 -j ACCEPT
```

Por fim, iremos rejeitar qualquer outro tipo de conexão tanto para o servidor (cadeia INPUT), quanto para os hosts (cadeia FORWARD)

```
iptables -A FORWARD -s 10.0.0.0/16 -j DROP
iptables -A INPUT  -s 10.0.0.0/16 -j DROP
```

Validações

ICMP

Para validar se os pacotes ICMP estão funcionando utilize o comando:

```
# Pingando o roteador
$ ping 10.0.0.1

# Pingando algum site externo
$ ping www.google.com
```

DNS

Para validar as resoluções de nomes, utiliza-se os comandos **host** ou **nslookup**:

```
$ host www.google.com
$ nslookup www.google.com
```

HTTP e HTTPS

Para validar o HTTP e HTTPS, pode-se utilizar um navegador por linha de comando (w3m) ou utilizar um browser de sua preferência. O tutorial irá mostrar através do w3m, para evitar qualquer proxy pré-configurado em algum browser como mozilla e chrome.

```
$ w3m www.google.com
```

Se tudo funcionar corretamente ele abrirá o socket e aprensentará uma tela do site escolhido em seu terminal.

Outros protocolos

Para verificar se o SSH está habilitado utiliza-se o comando a seguir, e espera-se que dê timeout, pois desabilitamos qualquer outro pacote que não fosse ICMP, HTTP e DNS.

```
$ ssh <user>@10.0.0.1
$ ssh <user>@10.0.0.X
```

Limitar banda

Para limitar a banda da subrede, utiliza-se o pacote **wondershaper**. Definiremos um limite de 1024 kbps tanto para upload quando download, basta utilizar o comando:

```
$ wondershaper <interface_rede> 1024 1024
```

Para testar a largura de banda entre no site Copel e verifique a velocidade de conexão.