

Introdução

Um Firewall é um dispositivo de segurança de rede que monitora e filtra o tráfego de rede de entrada e saída com base nas políticas de segurança estabelecidas anteriormente por uma organização. Basicamente, um firewall é essencialmente a barreira que fica entre uma rede interna privada e a Internet pública. O objetivo principal de um firewall é permitir a entrada de tráfego não ameaçador e impedir a entrada de tráfego perigoso.

Firewalls são importantes para as redes cabeadas, porém existem algumas opções que também podem ser acatadas para melhorar a segurança, como por exemplo, realizar um mapeamento e auditoria sobre a rede para levantar as possíveis ameaças, utilização de VLANs para separar o tráfego, o que também aumenta a performance, utilizar filtros de endereçamento MAC que vão realizar uma primeira autenticação na rede com fio, uso da autenticação 802.1x que também aplica autenticação e criptografia, utilização de VPNs para também implementar criptografia.

Já para as redes sem fio, é importante que haja também um gerenciamento dos dispositivos conectados, para que não hajam dispositivos maliciosos na rede que sejam capazes de interferir, realizar a segmentação de acesso a rede, para que existam barreiras de acesso a informações, utilizar um sistema de prevenção de intrusões – WIPS, o qual realiza a monitorização das ondas de rádio, procurando e alertando para pontos de acesso não autorizados ou atividades nocivas

Os iptables são firewalls muito potentes, os quais permitem a manipulação e configuração dos pacotes na camada de rede ou transporte. Ele é estruturado em tabelas e cadeias, sendo as tabelas responsáveis por receber as regras e as cadeias responsáveis por aplicar ações relacionadas a estas regras

Nele existem 3 tipos de tabelas:

- **Filter:** As regras contidas na tabela de filtro determinam se um pacote é aceito, portanto, estamos falando sobre a tabela iptables básica, e suas regras podem ser gerais. Existem três cadeias nesta camada: INPUT, OUTPUT e FORWARD. Estas por sua vez podem aplicar 4 ações: REJECT, ACCEPT, DROP e LOG
- **NAT:** responsável por traduzir os endereços que passam pelo roteador. Possui também três cadeias: PREROUTING, POSTROUTING e OUTPUT e suas ações são SNAT, o qual realiza a troca dos endereços IP de origem, DNAT, altera os endereços de IP de destino, MASQUERADE, mascara o IP e REDIRECT, que redireciona o pacote.

- Mangles: Tem a função de especificar ações especiais que devem ser aplicadas ao tráfego que passa pela cadeia. Nesse caso, tais operações ocorrem antes do filtro e da cadeia NAT.

Os pacotes são modificados utilizando o comando `iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE`, o qual troca os IP's internos pelos IP's externos quando os pacotes estão quase sendo enviados para a rede, para que assim o retorno seja efetuado, e realiza a troca novamente quando a resposta é devolvida, fazendo com que se pareça que não existe um servidor intermediando toda esta operação.

Atividade:

Nesta atividade foi reproduzido um cenário de uma livraria a qual possui a seguinte topologia de rede

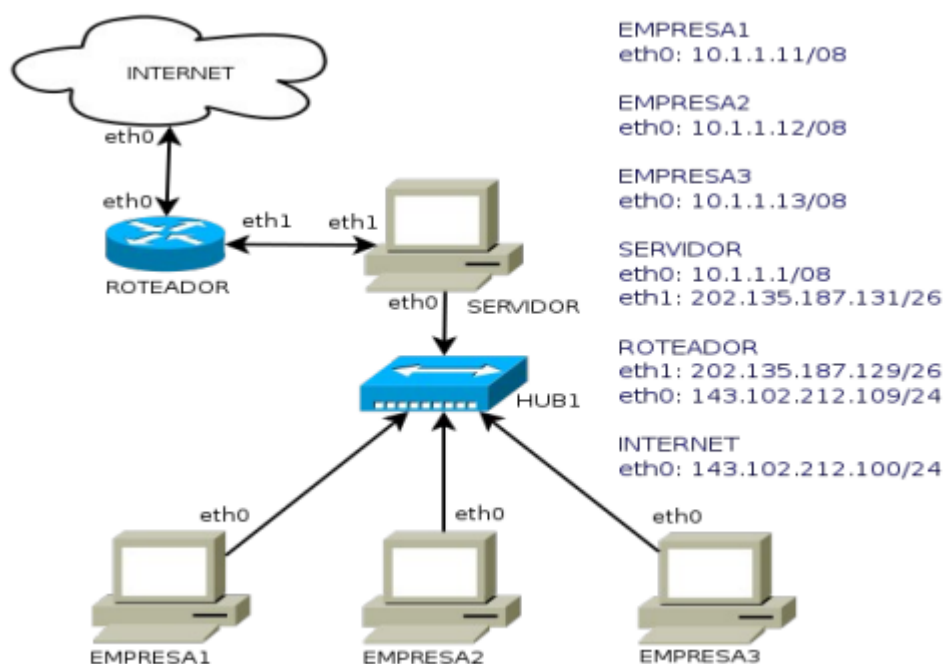


Figura 1 - Topologia

A partir disso, utilizando o software Kathara para gerar a topologia, são gerados os terminais contendo o Roteador, Servidor, Empresa 1, 2 e 3 e Internet. Assim são gerados os seguintes testes:

Realizar um comando `ping` da Internet para o Servidor, o que acontece com sucesso como é possível ver na Figura 2.

```
root@internet: /  
root@internet: /# ping 202.135.187.131  
PING 202.135.187.131 (202.135.187.131) 56(84) bytes of data:  
64 bytes from 202.135.187.131: icmp_seq=1 ttl=63 time=0.187 ms  
64 bytes from 202.135.187.131: icmp_seq=2 ttl=63 time=0.057 ms  
64 bytes from 202.135.187.131: icmp_seq=3 ttl=63 time=0.057 ms  
64 bytes from 202.135.187.131: icmp_seq=4 ttl=63 time=0.059 ms  
64 bytes from 202.135.187.131: icmp_seq=5 ttl=63 time=0.060 ms  
64 bytes from 202.135.187.131: icmp_seq=6 ttl=63 time=0.058 ms  
64 bytes from 202.135.187.131: icmp_seq=7 ttl=63 time=0.058 ms  
^C  
--- 202.135.187.131 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6208ms  
rtt min/avg/max/mdev = 0.057/0.076/0.187/0.046 ms  
root@internet: /#
```

Figura 2 - Ping Internet para Servidor

Realizar um comando ping da Internet para a Empresa 2, o que resulta em um erro de 100% de perda de pacotes, pois esta não pode ser alcançada.

```
root@internet: /  
root@internet: /# ping 10.1.1.12  
PING 10.1.1.12 (10.1.1.12) 56(84) bytes of data:  
From 143.102.212.109 icmp_seq=1 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=2 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=3 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=4 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=5 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=6 Destination Net Unreachable  
From 143.102.212.109 icmp_seq=7 Destination Net Unreachable  
^C  
--- 10.1.1.12 ping statistics ---  
7 packets transmitted, 0 received, +7 errors, 100% packet loss, time 6250ms  
root@internet: /#
```

Figura 3 - Ping Internet para Empresa2

O proximo é realizar um ping entre Servidor e Internet, o que também ocorre sucesso.

```
root@servidor: /  
root@servidor: /# ping 143.102.212.100  
PING 143.102.212.100 (143.102.212.100) 56(84) bytes of data.  
64 bytes from 143.102.212.100: icmp_seq=1 ttl=63 time=0.173 ms  
64 bytes from 143.102.212.100: icmp_seq=2 ttl=63 time=0.071 ms  
64 bytes from 143.102.212.100: icmp_seq=3 ttl=63 time=0.067 ms  
64 bytes from 143.102.212.100: icmp_seq=4 ttl=63 time=0.058 ms  
64 bytes from 143.102.212.100: icmp_seq=5 ttl=63 time=0.059 ms  
64 bytes from 143.102.212.100: icmp_seq=6 ttl=63 time=0.077 ms  
64 bytes from 143.102.212.100: icmp_seq=7 ttl=63 time=0.064 ms  
64 bytes from 143.102.212.100: icmp_seq=8 ttl=63 time=0.059 ms  
AC  
--- 143.102.212.100 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7252ms  
rtt min/avg/max/mdev = 0.058/0.078/0.173/0.037 ms  
root@servidor: /#
```

Figura 4 - Ping Servidor para Internet

Por fim é realizado um ping entre Empresa1 e Internet, o que resulta em erro, pois não há como alcançá-la.

```
root@empresal: /  
root@empresal: /# ping 143.102.212.100  
PING 143.102.212.100 (143.102.212.100) 56(84) bytes of data.  
AC  
--- 143.102.212.100 ping statistics ---  
29 packets transmitted, 0 received, 100% packet loss, time 29121ms  
root@empresal: /# ping 143.102.212.100  
PING 143.102.212.100 (143.102.212.100) 56(84) bytes of data.  
AC  
--- 143.102.212.100 ping statistics ---  
31 packets transmitted, 0 received, 100% packet loss, time 31168ms  
root@empresal: /#
```

Figura 5 - Ping Empresa1 para Internet

O próximo passo é configurar o iptables, como na Figura 6

```
root@servidor: /  
root@servidor: /# iptables -F  
root@servidor: /# iptables -F -t nat  
root@servidor: /# iptables -F -t mangle  
root@servidor: /# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE  
root@servidor: /#
```

Figura 6 - Configuração do iptables no Servidor

Com isto configurado, o que antes na figura 5 não era possível, agora se torna possível de receber os pacotes, como na figura 7.

```
root@empresal: /  
root@empresal: /# ping 143.102.212.100  
PING 143.102.212.100 (143.102.212.100) 56(84) bytes of data:  
64 bytes from 143.102.212.100: icmp_seq=1 ttl=62 time=0.245 ms  
64 bytes from 143.102.212.100: icmp_seq=2 ttl=62 time=0.110 ms  
64 bytes from 143.102.212.100: icmp_seq=3 ttl=62 time=0.533 ms  
64 bytes from 143.102.212.100: icmp_seq=4 ttl=62 time=0.116 ms  
64 bytes from 143.102.212.100: icmp_seq=5 ttl=62 time=0.091 ms  
64 bytes from 143.102.212.100: icmp_seq=6 ttl=62 time=0.091 ms  
^C  
--- 143.102.212.100 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5234ms  
rtt min/avg/max/mdev = 0.091/0.197/0.533/0.159 ms  
root@empresal: /#
```

Figura 7 - Recebimento dos pacotes de Empresa1 para Internet

Bibliografia

<https://e-tinet.com/linux/tabelas-do-iptables-firewall-linux/>

<https://convexnet.com.br/seguranca-em-roteadores-dicas-para-se-proteger-e-ter-um-a-rede-segura/>

<https://ostec.blog/geral/dicas-seguranca-rede-wireless-corporativa/>

<https://www.kathara.org/>