Instituto Federal de Santa Catarina – IFSC campus São José

Firewall

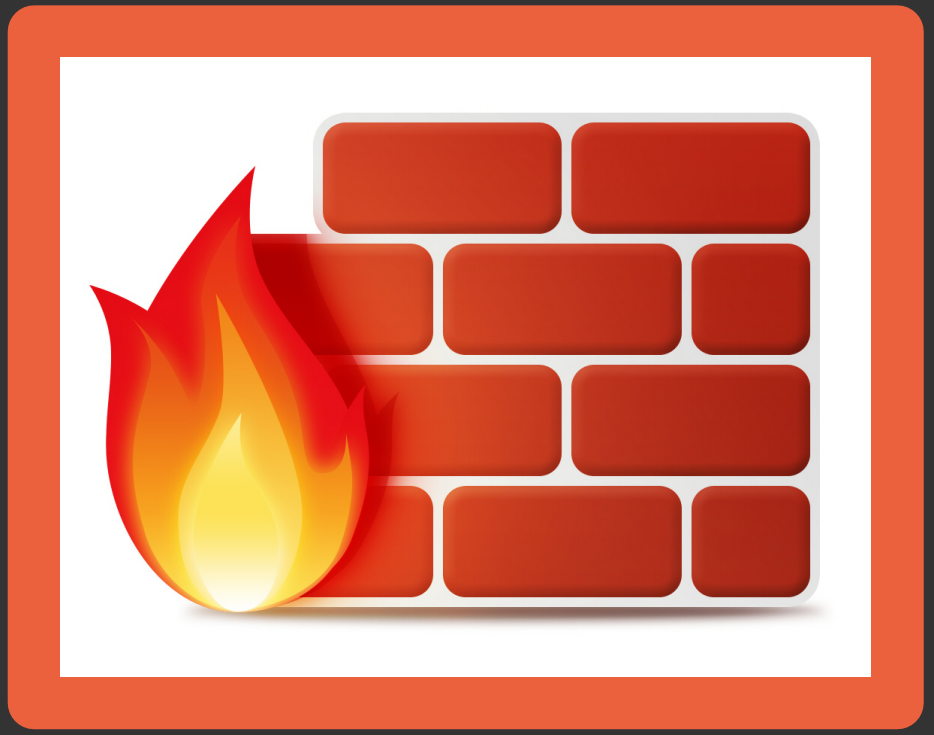
Turma: 6080822

Grupo: Bruna Leal
Eliakim F. Morais
Luísa Machado
Nikolas Weber
Matheus G. Bento

Definições

O Que é Firewall ?

É uma barreira inteligente entre duas redes que examina em tempo real o tráfego só permitindo a comunicação conforme as políticas pré-estabelecidas.



Tipos De Firewall

Nível de Aplicação

Analisam o conteúdo do pacote para decisões de filtragem e por isso são mais intrusivos e permitem um controle relacionado com o conteúdo do tráfego.

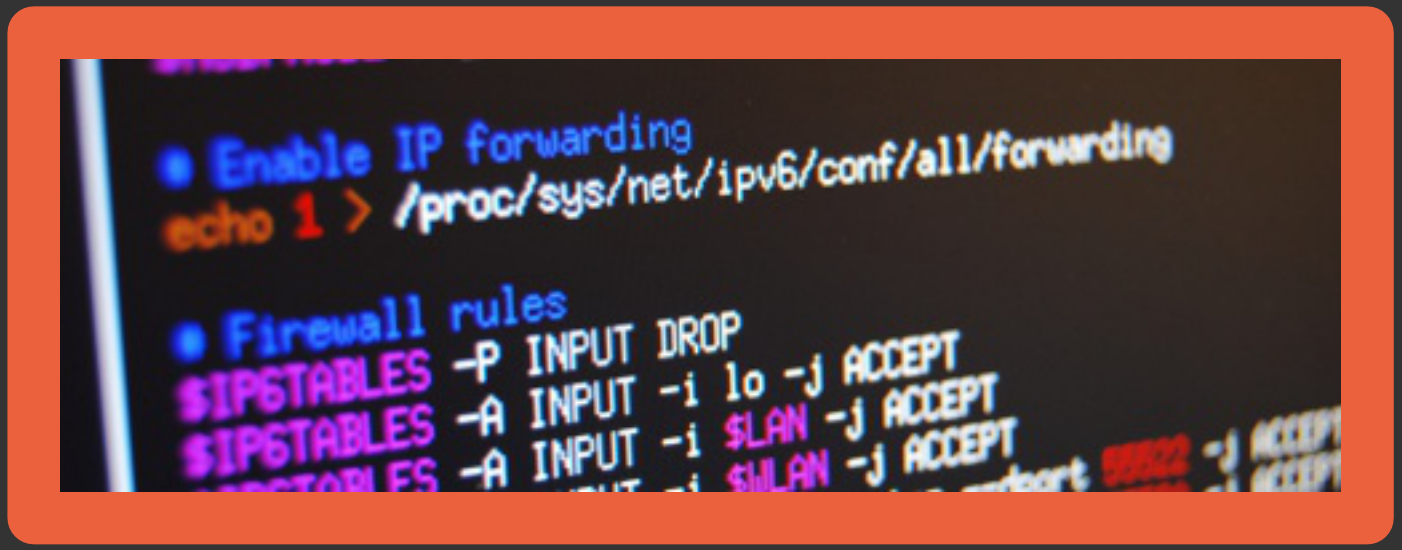
Nível de Pacotes

Toma as decisões baseadas nos parâmetros do pacote, como porta, endereço de origem e destino entre outros. O firewall então pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT).

IPTables

Iptables

O iptables suporta vários protocolos a na versão mais recente (ip6tables) suporta ao Ipv6.
Tem como vantagens uma configuração muito estável, fácil administração e confiabilidade.



Iptables: Caracteristicas

- Suporte aos protocolos TCP, UDP, ICMP
- Pode se especificar portas de endereço e de destino.
- Suporta módulos externos como FTP e IRC
- Suporta um número ilimitado de regras por CHAINS.
- Pode se criar regras de proteção contra ataques diversos
- Suporte para roteamento de pacotes e redirecionamento de portas.
- Suporta vários tipos de NAT, como o SNAT e DNAT e mascaramento.
- Pode priorizar tráfego para determinados tipos de pacotes.

Tabelas do IPTables

Filter

Está é a tabela padrão.

►INPUT: Consultado para dados que chegam ao host.
►OUTPUT: Consultado para dados que saem da host.
►FORWARD: Consultado para dados que são redirecionados para outra interface de rede ou outro host.

NAT

Usada para dados e gera outra conexão

►PREROUTING: Consultado quando os pacotes precisam ser modificados logo que chegam.
►OUTPUT: Consultado quando os pacotes gerados localmente precisam ser modificados antes de serem roteados.
►POSTROUTING: Consultado quando os pacotes precisam ser modificados após o tratamento de roteamento.

Mangle

Utilizada para alterações especiais de pacotes.

Contem em si uma versão de cada chain das tabelas *Filter* e *NAT* e são consultadas quando o pacote precisa ser alterado antes de ir para chain correspondente da outra tabela.

Politicas do IPTables

Politicas do IPTables

Basicamente o IPTABLES tem as seguintes políticas:

► DROP: Nega pacote e não manda um pacote de volta para o emitente.
► ACCEPT: Aceita o pacote.
► REJECT: Nega pacote e manda um pacote de volta do tipo host-unreachable (Host Inalcançável).

NAT

NAT

Serve para controlar a tradução de endereços dos hosts, A tradução de endereços tem inúmeras utilidades, uma delas é o Masquerading, redirecionamento de porta, proxy transparente, etc.

► SNAT: Aplicada quando queremos alterar o endereço de origem do pacote.

► DNAT: Aplicada quando desejamos alterar o endereço de destino do pacote.

Criando uma regra no IPTables

Criando a Regra

► Ativar o roteamento:

```
#echo  1 > /proc/sys/net/ipv4/ip_forward
```

► Verificar se a Distr. Linux está com o iptables ativo ou possui o modulo iptables:

```
#modprobe iptables
```

► Criar um script de firewall e dar permissão de execução:

```
#vim firewall.sh
#chmod +x firewall.sh
```

► Após inserir todas as regras rodar o script

```
#./firewall.sh
```

Instituto Federal de Santa Catarina – IFSC campus São José

Firewall

Turma: 6080822

Grupo: Bruna Leal
Eliakim F. Morais
Luísa Machado
Nikolas Weber
Matheus G. Bento