Exemplos

Regras para que a comunicação na porta 443 seja aceita no próprio servidor em que se encontra o iptables:

iptables -A INPUT -p tcp -dport 443 -j ACCEPT

Regras para que a comunicação na porta 80 seja rejeitada no próprio servidor em que se encontra o iptables:

iptables -A INPUT -p tcp -dport 80 -j REJECT

Em ambas as regras, possuímos:

-A para adicionar a regra na última linha da cadeia

-p para especificar o protocolo

-dport para definir a porta de destino

-j para escolher a ação a ser tomada pelo firewall

///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

Sobre a tabela FILTER

A tabela filter é utilizada para aceitar, rejeitar ou redirecionar pacotes, geralmente possui a maior quantidade de regras por se tratar da tabela em que armazena os bloqueios para redes externas, como internet.

Sobre a tabela NAT

Nessa tabela tem a função de controlar a tradução de endereços que atravessam o host linux.

Sobre a tabela Mangle

A tabela mangle contém regras de marcação de pacotes, possibilitando até mesmo aplicação de funcções referentes ao desempenho da rede e priorização de serviços.

Sobre a tabela RAW

Marca pacotes que não devem ser manipulados pelo sistema de rastreamento de conexões, basicamente é a primeira tabela na ordem de conexão de um pacote, e rejeitá-lo diretamente nessa tabela pode economizar processamento.

//////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

EX: Adicionar uma regra para bloquear tráfego de saída:

iptables -A OUTPUT -o eth0 -p udp --dport 53 -j DROP

Neste exemplo, estamos adicionando uma regra à cadeia de saída (OUTPUT) que bloqueia tráfego UDP na porta 53 (porta padrão do DNS) na interface de rede “eth0” (interface de rede de saída) e direcionando-o para a ação “DROP”, que descarta o pacote.

-A: Adiciona a regra à cadeia especificada.

-o: Especifica a interface de rede de saída para onde o tráfego está sendo enviado.

-p: Especifica o protocolo do pacote (neste caso, UDP).

--dport: Especifica a porta de destino do pacote.

-j: Indica a ação a ser tomada se a regra for correspondida (neste caso, DROP).

///////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

IDEIA PARA MOSTRAR COMO ESTÁ AS CONFIGURAÇÕES

1. Salvando as regras: Para salvar as regras do iptables, você precisa usar o comando iptables-save. Este comando exibe as regras do iptables em um formato legível por máquina, permitindo que você redirecione a saída para um arquivo.

Passo a passo:

Abra o terminal ou a linha de comando no seu sistema.

Use o comando iptables-save para exibir as regras atuais do iptables no seu terminal.

Redirecione a saída para um arquivo de texto. Por exemplo, para salvar as regras em um arquivo chamado regras-iptables.txt, você pode usar o seguinte comando:

iptables-save> regras-iptables.txt

/////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////

IDEIA PARA LISTAR AS CONFIGURAÇÕES E LISTA-LAS PARA ESCOLHER QUAL BACKUP FAZER (SALVAR AS REGRAS EM UM DIRETÓRIO SEGURO E, QUANDO FIZER A BUSCA NA APLICAÇÃO, ENTRAR NO MESMO E LISTAR AS CONFIGURAÇÕES)

2. Restaurando as regras: Após salvar as regras em um arquivo, você pode restaurá-las a qualquer momento usando o utilitário iptables-restore. Esse comando lerá o arquivo de texto contendo as regras salvas e as aplicará no iptables.

Passo a passo:

Verifique se você tem um arquivo contendo as regras salvas. No nosso exemplo, o arquivo é regras-iptables.txt.

Abra o terminal ou a linha de comando no seu sistema.

Use o comando iptables-restore e especifique o arquivo contendo as regras para restaurá-las:

iptables-restore< regras-iptables.txt

SITE: https://www.hostgator.com.br/blog/guia-iptables/

https://linux.die.net/man/8/iptables