NETFILTER

O projeto netfilter é um projeto FOSS colaborativo conduzido pela comunidade que fornece software de filtragem de pacotes para a série de kernel Linux 2.4.x e posteriores. O projeto netfilter é comumente associado ao iptables e seu sucessor nftables.

O projeto netfilter permite filtragem de pacotes, tradução de endereço de rede [e porta] (NA[P]T), registro de pacotes, enfileiramento de pacotes de espaço de usuário e outras manipulações de pacotes.

Os hooks netfilter são uma estrutura dentro do kernel Linux que permite que os módulos do kernel registrem funções de retorno de chamada em diferentes locais da pilha de rede Linux. A função de retorno de chamada registrada é então chamada de volta para cada pacote que atravessa o respectivo hook dentro da pilha de rede Linux.

iptables é um software de firewall genérico que permite que você defina conjuntos de regras. Cada regra dentro de uma tabela IP consiste em um número de classificadores (correspondências iptables) e uma ação conectada (destino iptables).

Principais recursos

* filtragem de pacotes sem estado (IPv4 e IPv6)
* filtragem de pacotes com estado (IPv4 e IPv6)
* todos os tipos de tradução de endereços de rede e portas, por exemplo, NAT/NAPT (IPv4 e IPv6)
* infraestrutura flexível e extensível
* várias camadas de APIs para extensões de terceiros

O que é iptables?

iptables é o programa de linha de comando do espaço do usuário usado para configurar o conjunto de regras de filtragem de pacotes do Linux 2.4.x e posteriores. Ele é direcionado a administradores de sistema.

Como a Network Address Translation também é configurada a partir do conjunto de regras de filtragem de pacotes, o iptables também é usado para isso.

O pacote iptables também inclui ip6tables. O ip6tables é usado para configurar o filtro de pacotes IPv6.

Dependências

iptables requer um kernel que apresenta o filtro de pacotes ip\_tables. Isso inclui todas as versões do kernel 2.4.x e posteriores.

Principais recursos

* Construir firewalls de Internet baseados em filtragem de pacotes “stateless” e “stateful”
* Usar NAT e masquerading para compartilhamento de Internet com uma rede local
* Usar NAT para implementar proxies transparentes
* Realizar manipulação de pacotes adicional (mangling), como alterar bits no cabeçalho IP
* Monitorar o volume de tráfego de rede
* Realizar Encaminhamento de Portas (que é um tipo de DNAT)
* Balanceamento de carga de rede.

Árvore Git

A versão de desenvolvimento atual do iptables pode ser acessada em <https://git.netfilter.org/iptables/>.

**Como funciona o iptables**

O firewall iptables opera comparando o tráfego de rede que a máquina recebe com um conjunto de regras pré-especificadas, as quais definem as características que os pacotes devem possuir para corresponderem às regras, e as ações que serão tomadas para esses pacotes.

Podemos criar regras que verifiquem a correspondência de uma pacote com uma regra específica de várias formas, como por exemplo por tipo de protocolo, portas de origem ou destino, endereços IP de origem ou destino, interfaces em uso, tipos de mensagens, entre muitas outras.

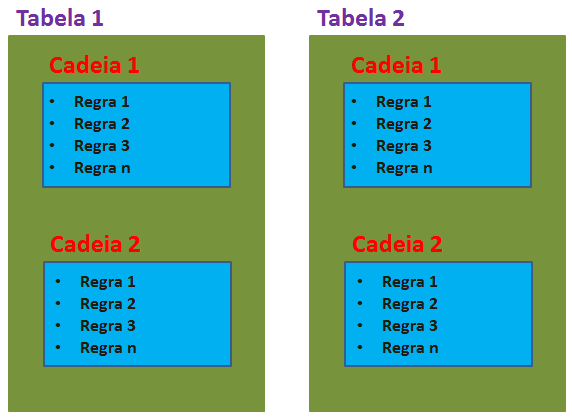
Quando ocorre uma correspondência entre um pacote e uma regra, uma ação será tomada, e a essa ação dá-se o nome de ***target***. O target (“objetivo”) pode determinar se um pacote será aceito ou descartado, movido para outra cadeia para processamento, logado, ou ainda outras opções.

A arquitetura do iptables agrupa o processamento dos pacotes de rede em tabelas por função (filtro de pacotes, tradução de endereços de rede e outras formas de configuração de pacotes), cada qual possui cadeias (chains) de regras de processamento. As regras consistem em correspondências (*matches*) usadas para determinar a quais pacotes cada regra será aplicada, e objetivos (*targets*), que determinam o que será feito com os pacotes que correspondam às regras.

**Tabelas**

O iptables organiza suas regras em uma estrutura que contém **tabelas** e **cadeias**. As tabelas são um agrupamento de cadeias em um nível mais alto, e determinam grosso modo o escopo das regras que serão criadas. O iptables possui diversas tabelas ou listas de regras:

* **filter** – Tabela padrão para manipular pacotes de rede, usada para configurar políticas para o tráfego uqe entra, atravessa ou sai do computador.
* **nat** – Usada para alterar pacotes que criam uma nova conexão, e para redirecionar conexões para NAT.
* **mangle** – Usada para tipos específicos de alteração de pacotes, como a modificação de opções do cabeçalho IP de um pacote.
* **raw** – Marca pacotes que não devem ser manipulados pelo sistema de rastreamento de conexões.



A estrutura geral de uma regra é a seguinte:

**iptables subcomando chain parâmetro\_1 valor\_1 parâmetro\_n valor\_n ação**

Os subcomandos principais que podem ser usados podem ser vistos no quadro a seguir:

|  |
| --- |
| **-A** anexa a regra no final da cadeia especificada  **-F** apaga todas as regras na cadeia especificada  **-L** lista todas as regras da cadeia  **-N** cria uma nova cadeia com o nome desejado  **-P** configura a regra padrão da cadeia  **-D** apaga uma regra em uma posição na cadeia  **-X** exclui uma cadeia vazia  **-I** insere uma regra em uma posição na cadeia |

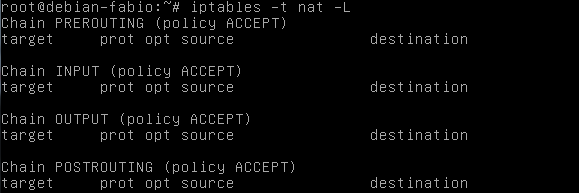
Já as ações (targets) possíveis estão listadas na tabela a seguir:

|  |
| --- |
| *Ações embutidas no iptables:*  **ACCEPT** – O pacote é permitido  **DROP** – Descartar o pacote  **QUEUE** – Enviar o pacote ao userspace (código fora do kernel)  **RETURN** – Descontinuar o processamento do pacote e aplicar a regra padrão a ele.  *Ações adicionais:*  **REJECT** – Descarta o pacote e envia feedback ao remetente.  **DNAT** – reescreve endereço de destino (NAT)  **SNAT** – reescreve endereço de origem (NAT)  **LOG** – coloca no log informações sobre o pacote |

Com relação aos parâmetros, existem dezenas deles para que possamos criar regras dos mais variados tipos. Na tabela a seguir listamos alguns dos parâmetros mais comuns:

| **Parâmetro** | **Significado** |
| --- | --- |
| -t tabela | Especificar a tabela (filter é a padrão) |
| -j ação | Realiza a ação especificada |
| -p protocolo | Especifica o protocolo (icmp, tcp, udp, all) |
| -s IP | IP de origem do pacote |
| -d IP | IP de destino do pacote |
| -i interface | Nome da interface de rede de entrada do pacote |
| -o interface | Nome da interface de rede de saída do pacote |
| –sport portas | Portas de origem |
| –dport portas | Portas de destino |
| –syn | Identifica nova requisição de conexão |
| –icmp-type | tipo de mensagem ICMP |

Uso iptables



Os campos mostrados na saída do comando de listagem de regras são os seguintes:

* target – Ação a ser realizada no pacote
* prot – Protocolo especificado
* opt – Opções especiais da regra
* source – Endereço IP de origem do pacote
* destination – Endereço IP de destino do pacote.
* num – Exibido com a opção –line-numbers. Mostra o número da regra dentro da cadeia.