Основи на защитна стена iptables - Basic Firewall – iptables

Автор: Мартин Петров
Благодарение на: www.dhstudio.eu

След версия 2.4 на ядрото , GNU/Linux представи изцяло нова машина за обработка на пакети, наречена Netfilter. Инструментът, използвам за контролиране на Netfilter, *iptables*, е големият брат на по-старата команда *ipchains*, използвана в ядрата от версия 2.2. *iptables* прилага подредени "вериги" от правила за мрежовите пакети. Наборите от вериги съставят "таблици" и се използват за обратобка на определени видове трафик.

Например подразбиращата се таблица на iptables се нарича "*filter*". Веригите от правила в нея се използват за филтриране на пакетите на мрежовия трафик. Таблицата *filter* съдържа три подразбиращи се вериги. Всеки пакет, който се обработва от ядрото, се пропуска през точно една от тях. Правилата във веригата FORWARD се прилагат върху всички пакети, които пристигат на мрежовия интерфейс и трябва да се пренасочат към друг. Правилата във веригитите INPUT и OUTPUT се прилагат върху трафика, адресиран към или идващ от локалния хост, съответно. Тези три стандартни вериги обикновено са достатъчни за поставяне на защитна стена между ва мрежови интерфейса. Ако се налага, може да се дефинира собствена конфигурация за по- сложни сценарии.

Освен таблицата *filter*, *iptables* съдържа и таблиците "nat" и "mangle". Таблицата nat съдържа вериги правила за контрол на Network Address Translation (тук "nat" е името на таблицата на iptables, а "NAT" е името на схемата за превод на мрежови адреси).

Таблицата mangle съдържа вериги, които модифицират или променят съдържанието на мрежовите пакети извън контекста на NAT и филтрирането на пакети. Въпреки, че тя е много полезна за специални обработки на пакети, като например промяната на времето на живот на IP пакетите , тя обикновено не се използва в повечето производствени среди.

Всяко правило, което съставя верига, има клауза "target" (цел), която определя какво се прави с отговарящите й пакети. Когато някой пакет отговаря на дадено правило, съдбата му в повечето случаи е решена окончателно; не се използват допълнителни правила. Въпреки че много цели са дефинирани вътрешно в iptables, все пак се позволява като цел на правило да се подаде друга верига.

Целите, налични за използване в правилата на таблицата filter, са ACCEPT, DROP, REJECT, LOG, MIRROR, QUEUE, REDIRECT, RETURN и ULOG. Когато правилото води до използване на ACCEPT, на отговарящите пакети се позволява да продължат по пътя си. DROP и

REJECT отхвърлят пакетите. DROP го прави тихо, а REJECT връща ICMP съобщение за грешка. LOG дава прост начин за проследяване на пакетите, които отговарят на правилата, а ULOG предоставя по- разширени дневници.

REDIRECT отклонява пакетите към прокси, вместо да ги остави да продължат по пътя си. Тази функция може да се използва, за да се преара целия уеб трафик на сайта през уеб кеш, какъвто е Squid.

RETURN терминира дефинирани от потребителите правила и е аналогична на контракцията ретурн при извикване на подпроцедура.

Целта MIRROR разменя IP адресите на източника и дестинацията, преди да изпрати пакета.

QUEUE подава пакетите на локални потребителски програми чрез модул на ядрото.

Защитната стена на GNU/Linux обикновено се реализира като последователност от команди на *iptables* , намиращи се в rc стартов скрипт. Отделните команди на *iptables* обиковено имат един от следните формати:

```
iptables -F верига
iptables -P верига_цел
iptables -A верига -i интерфейс -j цел
```

Първият формат (-F) изчиства всички предишни правила от веригата. Вторият формат (-P) настройва подразбиращата се политика (или още цел) за веригата. Препоръчва се използването на *DROP* за подразбиращата се цел на веригата. Третият формат (-A) добавя текущата спецификация към веригата. Освен ако не се конкретизира таблица с аргумент **-t** , командите ще са прилагат към таблицата filter. Параметърът -i прилага правило към именуван интерфейс, а **-j** идентифицира целта. *iptables* приема и други клаузи, някои от които са изброени в следващата таблица № 3.1

Флагове за филтри на iptables Таблица 3.

Клауза	**Значение или възможни стойности**
-p протокол	Съответствие по протокол: tcp, udp или icmp
-s ip_на_източник	Съответсвие по хост или IP адрес на източник (приема се означението CIDR)
-d ip_наIдестинация	Съответсвие на хост или IP адрес на дестинация
--sport порт	Съответсвие по порт на източника
--dport порт	Съответсвие по порт на дестинацията
--icmp-type тип	Съответсвие по код за тип на *ICMP*
!	Отрицание на клауса
-t таблица	Указва таблицата, към която се отнася команда (подразбиращата е filter)