УДК 004.724.4 (043.2)

О.Є. Соломяний

*Національний авіаційний університет*

МЕХАНІЗМ ВИЗНАЧЕННЯ СТАНУ В IPTABLES

Утиліта iptables використовується як інтерфейс управління роботою міжмережевого екрану (брандмауера) netfilter для ядер Linux, починаючи з версії 2.4. Стандартними цілями в правилах iptables є наступні:

<user-defined-chain> — визначена користувачем ціль в межах таблиці. Імена ланцюжків, визначених користувачем, повинні бути унікальні. Ця ціль передає пакет до вказаного ланцюжка.

ACCEPT – дозволяє проходження пакету до його місця призначення або до наступного ланцюжка.

DROP – відкидає пакет без відповіді його джерелу. Система, яка надіслала пакет, не отримує повідомлень про невдачу.

QUEUE – пакет вміщується у чергу для обробки додатком простору користувача (user-space).

RETURN – припиняє перевірку відповідності пакету правилам, що входять до поточного ланцюжка.

Окремою частиною iptables є механізм визначення стану (state machine). З погляду iptables, з’єднання може мати одне з 4-х базових станів: NEW, ESTABLISHED, RELATED i INVALID. Для управління проходженням пакетів, використовується критерій, що позначається як – state.

Ознака NEW повідомляє про те, що пакет є першим для даного з'єднання, тобто це перший пакет в даному з'єднанні, який побачив модуль. З'єднання отримує ознаку RELATED тоді, коли воно ініційоване з раніше встановленого з'єднання, що має ознаку ESTABLISHED. Ознака ESTABLISHED вказує на те, що це не перший пакет в з'єднанні. Схема встановлення стану ESTABLISHED достатньо проста. Єдина вимога, що пред'являється до з'єднання, полягає в тому, що для переходу в стан ESTABLISHED необхідно, щоб вузол мережі передав пакет і отримав на нього відповідь від іншого вузла. Після отримання відповіді стан з'єднання NEW або RELATED буде змінено на ESTABLISHED. Ознака INVALID говорить про те, що пакет не може бути ідентифікований і тому не може мати певного статусу.