Фільтрація пакетів за допомогою iptables

Архітектура iptables

- Ключовими поняттями iptables є:
  - Правило - складається з критерію, дії і лічильника. Якщо пакет відповідає критерію, до нього застосовується дія, і він враховується лічильником. Критерію може і не бути - тоді неявно передбачається критерій «всі пакети». Вказувати дію теж не обов'язково - за відсутності дії правило буде працювати тільки як лічильник
  - Ланцюжок - упорядкована послідовність правил. Ланцюжки можна розділити на призначені для користувача і базові
  - Таблиця - сукупність базових і призначених для користувача ланцюжків, об'єднаних загальним функціональним призначенням

Правила iptables

- Правило складається з критерію, дії і лічильника
  - Критерій - логічний вираз, що аналізує властивості пакета і / або з'єднання і визначає, чи підпадає даний пакет під дію поточного правила
  - Дія - опис дії, яку треба виконати з пакетом і / або з'єднанням в тому випадку, якщо вони підпадають під критерій цього правила
  - Лічильник - компонент правила, що забезпечує облік кількості пакетів, які потрапили під критерій даного правила, лічильник також враховує сумарний обсяг таких пакетів в байтах

Ланцюжок iptables

- Базовий ланцюжок
  - Ланцюжок, що створюється за замовчуванням при ініціалізації таблиці
  - Кожен пакет, в залежності від того, чи призначений він самому вузлу, згенерований їм або є транзитними, повинен пройти визначений йому набір базових ланцюжків різних таблиць
  - Має «дії за замовчуванням» (default policy)
  - Імена базових ланцюжків завжди записуються в верхньому регістрі (PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING)
- Користувацький ланцюжок
  - Ланцюжок, створений користувачем
  - Може використовуватися тільки в межах своєї таблиці

Ланцюжки та таблиці iptables

PREROUTING	raw	mangle	nat	
INPUT		mangle		filter
FORWARD		mangle		filter
OUTPUT	raw	mangle	nat	filter
POSTROUTING		mangle	nat	

Принцип роботи

- Всі пакети пропускаються через визначені для них послідовності ланцюжків
- При проходженні пакетом ланцюжка, до нього послідовно застосовуються всі правила цього ланцюжка в порядку їх слідування
- Під застосуванням правила розуміється: по-перше, перевірка пакету на відповідність критерію, і по-друге, якщо пакет цьому критерію відповідає, застосування до нього зазначеної дії

Принцип роботи

- Дія - це може бути як елементарна операція (вбудована дія, наприклад, ACCEPT, MARK), так і перехід в одну з призначених для користувача ланцюжків
- Дії можуть бути як термінальними, тобто припиняють обробку пакета в рамках даного базового ланцюжка (наприклад, ACCEPT, REJECT), так і нетермінальнимі, тобто не переривають процесу обробки пакета (MARK, TOS)
- Якщо пакет пройшов через весь базовий ланцюжок і до нього так і не було застосовано жодної термінальної дії, до нього застосовується дія за замовчуванням для цього ланцюжка (обов'язково термінальна)

Утиліта iptables

- Створення та видалення призначених для користувача ланцюжків
- Установка дій за замовчуванням для базових ланцюжків
- Додавання і видалення правил
- Установка і обнулення лічильників пакетів і байт
- Перегляд ланцюжків і правил, а також значень лічильників
- Перевірка коректності завдання параметрів, що визначають роботу критеріїв і дій
- Вивід довідки щодо використання критеріїв (iptables -m критерій -h) і дій (iptables -j дія -h)

Додаткові утиліти iptables

- iptables-save використовується для збереження стану брандмауера у файл
- iptables-restore використовується для відновлення стану брандмауера з файлу
- Iptables-apply використовується для безпечної зміни налаштувань брандмауера при віддаленій роботі

Дії в iptables

- Переходи
- Вбудовані дії
- Термінальні дії
- Нетермінальні дії

Переходи в iptables

- Для організації переходу пакета з поточного ланцюжка в інший (визначений користувачем), використовується дія -j ім'я_ланцюжка
  - У разі застосування в цьому ланцюжку до пакету дії RETURN, пакет повернеться в вихідний ланцюжок і продовжить його проходження починаючи з наступного правила (для базового ланцюжка до пакету відразу буде застосовано дію за замовчуванням)
- Дія безповоротного переходу -g ім'я_ланцюжка
  - В такому випадку, після проходження пакетом цього ланцюжка або при застосуванні в цьому ланцюжку до пакету дії RETURN, пакет повернеться до місця останнього переходу по -j
  - Якщо таких переходів не було, до пакету відразу буде застосовано дію за замовчуванням для базового ланцюжка

Вбудовані дії загального призначення

- ACCEPT, DROP і REJECT - базові операції фільтрації
- RETURN - забезпечує повернення з поточного ланцюжка
- LOG - записує інформацію про пакети в журнал ядра
- LOGMARK - спеціальна модель поведінки LOG заносить в лог інформацію, специфічну для системи conntrack
- ULOG - передає інформацію про оброблені пакети спеціальним демонам, таким, як ulogd, це дозволяє заносити інформацією про трафік в бази даних
- NFLOG - більш універсальний варіант ULOG, що забезпечує передачу інформації про пакет не безпосередньо в netlink-сокет (як це робить ULOG), а спеціальній підсистемі - logging backend
- NFQUEUE - багато в чому схожа на ULOG, але передає спеціальному демону не інформацію про пакет, а сам пакет, використовується для L7-фільтрації
- QUEUE - застаріла версія NFQUEUE, не має параметрів, оскільки працює тільки з чергою номер 0

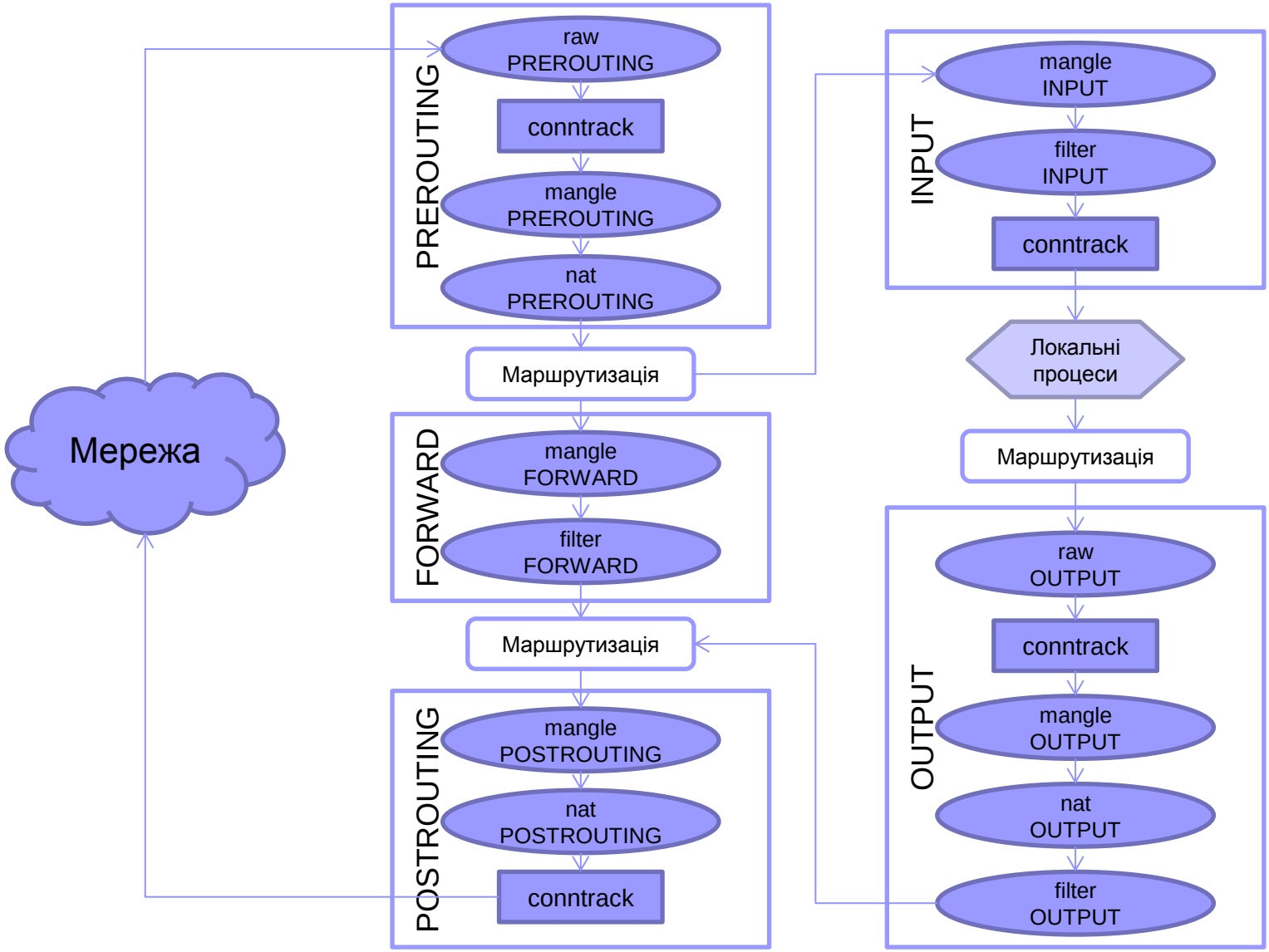
Термінальні дії

- Термінальними називаються дії, які переривають проходження пакета через поточний базовий ланцюжок
- Тобто якщо до пакету в рамках деякого правила було застосовано термінальну дію, він уже не перевіряється на відповідність усім наступним правилам в цьому ланцюжку (і в тих ланцюжках, з яких він був викликаний, якщо це ланцюжки користувача)
- Термінальними є всі дії, специфічні для таблиць filter і nat: ACCEPT, DROP, REJECT, NFQUEUE, QUEUE

Нетермінальні дії

- Нетермінальнимі є дії, які не переривають процес проходження пакета через ланцюжки
- Нетермінальнимі є дії, специфічні для таблиці mangle
- Приклади нетермінальних дій: LOG, ULOG і NFLOG

Шлях перевірки пакета в iptables



Таблиці iptables

- mangle
- nat
- filter
- security
- raw

Таблиця mangle

- Призначена для класифікації та маркування пакетів і з'єднань, а також модифікації заголовків пакетів (поля TTL і TOS)
- Таблиця mangle містить наступні ланцюжки:
  - PREROUTING - дозволяє модифікувати пакет до прийняття рішення про маршрутизації
  - INPUT - дозволяє модифікувати пакет, призначений самому вузлу
  - FORWARD - ланцюжок, що дозволяє модифікувати транзитні пакети
  - OUTPUT - дозволяє модифікувати пакети, які виходять від самого вузла
  - POSTROUTING - дає можливість модифікувати всі вихідні пакети, як згенеровані самим вузлом, так і транзитні

Дії в таблиці mangle

- TOS - змінює поле TOS пакета
- DSCP - змінює поле DSCP (клас DiffServ) в заголовку пакета
- TTL - змінює поле TTL пакета
- MARK - встановлює або змінює маркування пакета
- CONNMARK - встановлює або змінює маркування з'єднання
- CLASSIFY - встановлює CBQ-клас пакета для його подальшої обробки шейпером
- TCPMSS - встановлює максимальний розмір TCP-сегмента
- ECN - забезпечує обнулення ECN-бітів (прапори CWR і ECE) в TCP-заголовку
- TCPOPTSTRIP - виконує видалення заданих TCP-опцій з заголовка TCP
- TPROXY - реалізує механізм повністю прозорого проксінг

Таблиця nat

- Призначена для операцій stateful-перетворення мережних адрес і портів пакетів
- Таблиця nat містить такі ланцюжки
  - PREROUTING - в цей ланцюжок пакети потрапляють до прийняття рішення про маршрутизації, саме на даному етапі потрібно проводити операції прокидання (DNAT, REDIRECT, NETMAP)
  - OUTPUT - через цей ланцюжок проходять пакети, згенеровані процесами самого вузла
  - POSTROUTING - через цей ланцюжок проходять всі вихідні пакети, тому саме в ній доцільно проводити операції маскарадінг (SNAT і MASQUERADE)

Дії в таблиці nat

- MASQUERADE - підміняє адресу джерела для вихідних пакетів адресою того інтерфейсу, з якого вони виходять, тобто здійснює маскарадінг
- SNAT (Source Network Address Translation) - працює аналогічно MASQUERADE, але дозволяє вказати адресу «зовнішнього» інтерфейсу (опція --to-source)
- DNAT (Destination Network Address Translation) - підміняє адресу призначення для вхідних пакетів, дозволяючи «прокидати» адреси або окремі порти всередину локальної мережі
- REDIRECT - підміняє номер порту в TCP- або UDP-пакеті, а також підміняє адресу призначення на свій власний
- SAME - в залежності від ланцюжка (PREROUTING або POSTROUTING) може працювати як DNAT або SNAT
- NETMAP - дозволяє «прокинути» цілу мережу
- MIRROR - Міняє місцями адресу джерела і призначення і висилає пакет назад

Таблиця filter

- Призначена для фільтрації трафіку, тобто дозволяє або забороняє проходження пакетів і з'єднань
- Таблиця filter містить наступні ланцюжки:
  - INPUT - цей ланцюжок обробляє трафік, що надходить безпосередньо самому вузлу
  - FORWARD - дозволяє фільтрувати транзитний трафік
  - OUTPUT - цей ланцюжок дозволяє фільтрувати трафік, що виходить від самого вузла

Дії таблиці filter

- ACCEPT - дозволити проходження пакету
- REJECT - заблокувати пакет і повідомити його джерело про відмову (за замовчуванням про відмову повідомляється відправкою відповідного ICMP-пакета: icmp-port-unreachable)
- DROP - заблокувати пакет, не повідомляючи джерело про відмову
- STEAL - аналогічно DROP, але в разі використання в ланцюжку OUTPUT при блокуванні вихідного пакета не повідомляє про помилку процес, який намагався відправити цей пакет
- TARPIT - «підвісити» TCP-з'єднання, використовується при боротьбі з DoS-атаками
- DELUDE - створити видимість відкритого TCP-порту, на SYN-пакети відповідає пакетами SYN / ACK, на всі інші пакети відповідає RST
- CHAOS - для кожного нового TCP-з'єднання випадково вибрати одну з двох дій: перша з них - REJECT, друга, в залежності від обраної опції, або TARPIT, або DELUDE

Таблиця security

- Призначена для зміни маркування безпеки (міток SELinux) пакетів і з'єднань
- Таблиця security містить такі ланцюжки:
  - INPUT - цей ланцюжок обробляє трафік, що надходить безпосередньо самому вузлу
  - FORWARD - через цей ланцюжок проходить транзитний трафік
  - OUTPUT - цей ланцюжок дозволяє обробляти трафік, що виходить від самого вузла
- Оскільки як ця таблиця з'явилася відносно недавно, її рідко можна побачити на схемах проходження пакетів iptables

Дії таблиці security

- SECMARK - встановлює для пакета контекст безпеки SELinux (єдина допустима опція --selctx)
- CONNSECMARK - дозволяє скопіювати контекст безпеки SELinux з окремого пакета на з'єднання в цілому (опція --save) і навпаки (опція --restore)

Таблиця raw

- Призначена для виконання дій з пакетами до їх обробки системою conntrack
- В даній таблиці не будуть спрацьовувати критерії, яким для коректної роботи необхідний conntrack
- Ланцюжки
  - PREROUTING - в цей ланцюжок пакети потрапляють раніше, ніж в будь-який інший з ланцюжків iptables, і до обробки їх системою conntrack
  - OUTPUT - аналогічно для пакетів, згенерованих самим вузлом

Дії таблиці raw

- NOTRACK - дозволяє запобігти обробку пакетів системою conntrack (застосовувати її варто не до всіх пакетів поспіль, а тільки до тих, для яких така обробка не потрібна і навіть шкідлива. Наприклад, до пакетів, до яких згодом застосовується дія TARPIT)
- CT - дозволяє задати різні настройки conntrack, відповідно до яких буде оброблятися з'єднання, відкрите даними пакетом
- RAWDNAT - дозволяє виконувати «проброс» адрес і портів «сирим» методом - без використання системи conntrack, тобто без урахування станів з'єднань

Критерії

- Критерій - це логічний вираз, що визначає, чи відповідає пакет або з'єднання даному конкретному правилу
- В одному правилі можна вказати кілька критеріїв
- Для того, щоб пакет був оброблений правилом, повинні виконуватися всі критерії, тобто критерії неявно об'єднуються логічним І
- Критерії і параметри критеріїв можна інвертувати, поставивши перед ними знак оклику (інверсія змінює зміст критерію або його параметра на протилежний)

Універсальні критерії

- -p, --protocol протокол
  - Дозволяє вказати протокол транспортного рівня, найбільш часто вживаються tcp, udp, icmp і all
- -s, --src, --source адреса [/маска] [, адреса [/маска] ...]
  - Визначає адресу відправника, в якості адреси може виступати IP-адреса (можливо з маскою), ім'я вузла з /etc/hosts, або доменне ім'я
- -d, --dst, --destination адреса [/маска] [, адреса [/маска] ...]
  - Визначає адресу одержувача

Універсальні критерії

- -i, --in-interface ім'я_інтерфейсу
  - Визначає вхідний мережний інтерфейс.
  - Якщо вказане ім'я інтерфейсу, яке закінчується знаком «+» (наприклад, eth+), то критерію відповідають все інтерфейси, чиї назви починаються на вказане ім'я
- -o, --out-interface ім'я_інтерфейсу
  - Визначає вихідний мережний інтерфейс, синтаксис аналогічний -i

Критерії, специфічні для протоколів

- --sport, --source-port порт [:порт]
  - Дозволяє вказати вихідний порт (або їх діапазон)
- --dport, --destination-port порт [:порт]
  - Дозволяє вказати порт призначення (або їх діапазон)
- --tcp-flags маска встановлені_прапори
  - Дозволяє вказати список встановлених і знятих TCP-прапорів
- --syn
  - Дозволяє фільтрувати TCP SYN-пакети

Критерії, специфічні для протоколів

- --tcp-option номер
  - Дозволяє перевірити, чи встановлена в заголовку TCP-пакету відповідна опція
- --chunk-types {all | any | only} тип_секції [:прапори] [,тип_секції[:прапори]...]
  - Дозволяє аналізувати набір секцій (chunks), що входять до складу SCTP-пакета
- --dccp-types маска
  - Дозволяє вказати тип DCCP-пакета

Критерії, специфічні для протоколів

- -f, --fragment
  - Перевірка фрагментації: критерію відповідають тільки фрагменти пакета, починаючи з другого фрагмента
- addrtype - дозволяє перевірити тип адреси джерела і / або призначення з точки зору підсистеми маршрутизації
- ecn - дозволяє перевіряти значення бітів ECN в заголовках TCP і IPv4
- realm - перевірка області маршрутизації (realm) пакета

Критерії, специфічні для протоколів

- --ttl - забезпечує перевірку поля TTL в заголовку пакета
- --icmp-type тип - забезпечує перевірку типу ICMP-пакета
- --ahspi значення [:значення] - дозволяє вказати значення (або діапазон значень) SPI (Security Parameter Index)
- --espspi значення [:значення] - дозволяє вказати значення (або діапазон значень) SPI (Security Parameter Index)

Критерії стану з'єднання

- --ctstate маска
  - Маска містить список можливих станів з'єднання, пакет задовольняє критерію, якщо з'єднання, по якому він проходить, знаходиться в одному з перерахованих станів
- Можливі стани:
  - NEW - з'єднання не відкрито, тобто пакет є першим в з'єднанні
  - ESTABLISHED - пакет належить до вже встановленого з'єднання, зазвичай такі пакети приймаються без додаткової фільтрації, як і в випадку з RELATED
  - RELATED - пакет відкриває нове з'єднання, логічно пов'язане з уже встановленими, наприклад, відкриття каналу даних в пасивному режимі FTP

Критерії стану з'єднання

- Можливі стани:
  - INVALID - пакет за змістом повинен належати вже встановленому з'єднанню (наприклад, ICMP-повідомлення port-unreachable), однак таке з'єднання в системі не зареєстровано (зазвичай до таких пакетів застосовують дію DROP)
  - UNTRACKED - відстеження стану з'єднання для даного пакета було відключено (зазвичай воно відключається за допомогою дії NOTRACK в таблиці raw)
  - DNAT - показує, що до даного з'єднання застосована операція підміни адреси призначення
  - SNAT - показує, що до даного з'єднання застосована операція підміни адреси джерела

Критерії стану з'єднання

- --ctstatus маска
- Застосовується для визначення статусу з'єднання в системі conntrack
- Можливі статуси:
  - EXPECTED - це з'єднання очікувалося системою conntrack за результатами аналізу інших з'єднань, наприклад, після того, як клієнт і сервер через керуюче FTP-з'єднання узгодять номер порту для з'єднання даних в пасивному режимі, система conntrack на сервері чекатиме вхідні повідомлення на цей порт
  - CONFIRMED - підтверджене з'єднання (такий статус надається з'єднанню після того, як ініціатор почав передачу пакетів)
  - SEEN_REPLY - з'єднання, за яким надійшла відповідь, тобто має місце передача даних в обох напрямках (підтримка даного стану з'явилася порівняно недавно)
  - ASSURED - з'єднання можна вважати повністю встановленим (цей статус надається з'єднанню після передачі певної кількості даних)
  - NONE - немає статусу (з'єднання не відповідає жодному з перерахованих критеріїв)

Критерії стану з'єднання

- --ctproto протокол
  - Протокол транспортного рівня, визначений системою conntrack
- --ctdir {ORIGINAL | REPLY}
  - Дозволяє вказати напрямок проходження пакетів
- --ctorigsrc адресу [/маска], --ctorigdst адресу [/маска], --ctreplsrc адресу [/маска], --ctrepldst адресу [/маска]
  - Дозволяє визначати адреси джерела (src) і призначення (dst) при передачі даних від ініціатора до сервера (orig) і навпаки (repl)

Критерії стану з'єднання

- --ctorigsrcport порт, --ctorigdstport порт, --ctreplsrcport порт, --ctrepldstport порт
  - Дозволяє визначати порти джерела (src) і призначення (dst) при передачі даних від ініціатора до сервера (orig) і навпаки (repl) для протоколів транспортного рівня
- --ctexpire мін_час [:макс_час]
  - Дозволяє вказати в якості критерію час, що залишився до завершення тайм-ауту для даного з'єднання