Engineer

Брандмауер

набір правил, що вирішує, який трафік пройде

Що це таке

Брандмауер — це фільтр на шляху мережевого трафіку, який звіряє кожен пакет або з'єднання зі списком правил, а тоді пропускає його, відкидає або повертає відмову. Він буває програмою на тому самому комп'ютері, який захищає, окремим пристроєм між двома мережами або сервісом, який хмарний провайдер ставить перед віртуальною машиною. В IT-розмові частіше чути «фаєрвол», у нормативних документах — «міжмережевий екран», адміністратори Linux кажуть просто «пакетний фільтр», а хмарні провайдери називають свої фаєрволи, наприклад, security group. Брандмауерів зазвичай кілька, шарами: один у провайдера, другий на самому сервері.

Настанова NIST SP 800-41 Rev. 1 від вересня 2009 року поділяє їх за тим, скільки трафіку вони читають. Пакетний фільтр дивиться на адреси, протокол і номери портів, по одному пакету за раз. Брандмауер зі станом (stateful) ще й пам'ятає з'єднання, тож відповідь на запит, який сервер надіслав сам, проходить без окремого правила. Шлюз-посередник прикладного рівня (application-proxy gateway) завершує з'єднання і читає протокол усередині нього. Брандмауер на рівні хоста працює на тому сервері чи ноутбуці, який охороняє, і знає, якій програмі належить сокет.

На сервері з Linux фільтрацію виконує підсистема netfilter у ядрі. nftables, що з'явився в ядрі з версії 3.13, замінює старіші інструменти iptables, а оболонки на кшталт ufw пишуть правила за тих, хто волів би описати намір, а не будувати ланцюжки. Хоч би що їх писало, модель однакова: упорядкований список, який читають згори, і перше правило, що збіглося, вирішує, що станеться з пакетом.

Брандмауер часто плутають із сусідніми інструментами. Брандмауер вебзастосунків (WAF) читає HTTP-запити й блокує в них шаблони атак, тоді як мережевий фаєрвол тримається адрес і портів. Інструмент, що блокує адреси за підозрілу поведінку, читає журнали й додає проти них тимчасові правила, тож працює поверх брандмауера. VPN вирішує, хто взагалі перебуває в мережі. Кожен відповідає на своє запитання, а список правил лишається основою під усіма ними.

Застосуйте поняття до рішення

Застосуйте «Що таке брандмауер?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Кожна служба, що слухає на публічній адресі, — це двері, а брандмауер — опис того, які двері існують. Рішення, яке ухвалює команда, має три частини: де живе брандмауер, що він дозволяє за замовчуванням і хто має право його змінювати.

Брандмауер провайдера зупиняє трафік ще до машини, працює далі, навіть якщо хтось отримав root на сервері, і не забирає в сервера жодного циклу процесора. Його правила живуть у консолі чи API, поза власною конфігурацією сервера, тож вони розходяться з дійсністю, якщо їх не описати кодом. Брандмауер на хості переїжджає разом із машиною, може обмежити частоту з’єднань до одного порту, і його можна перевірити із самої машини, але скомпрометований root здатен його переписати — так само, як і програми, що керують власними правилами. Тримати обидва — звична й розумна практика, а ціна — два списки, які треба вести синхронно: кожен відкритий чи закритий порт означає зміну у двох місцях.

Друга частина — поведінка за замовчуванням. NIST радить відхиляти весь трафік, який явно не дозволено, і щодо вхідного трафіку з цим погоджуються майже всі. Фільтрація вихідного трафіку — місце, де компроміс стає

відчутним: вона обмежує, куди може дістатися зламана служба, але й зупиняє оновлення пакетів, поновлення сертифікатів і моніторинг, доки кожне призначення не отримає своє правило.

Третя частина — відповідальність. Брандмауер у режимі заборони за замовчуванням правильний рівно настільки, наскільки правильний список портів, який хтось задекларував, тож найціннішим є саме цей список: у системі контролю версій і звірений із живими правилами. Саме програмне забезпечення безкоштовне в усіх поширених дистрибутивах Linux, а платити доводиться увагою, потрібною, щоб декларація лишалася правдивою. І брандмауер — це друга лінія. Службу, що слухає лише на адресі loopback, ззовні не досягти, хоч би що казали правила, і це надійніша гарантія, ніж забороняльне правило перед службою, яка слухає на всіх адресах.

Як це виглядає на практиці

Три фрагменти інфраструктурної роботи компанії показують брандмауер із трьох боків: як його перевіряють, коли його створюють і що може його обійти.

На одному сервері обмеження частоти для порту SSH рік простояло у списку правил, і жоден пакет до нього не дійшов, бо ширше дозвільне правило вище спрацьовувало першим. Інструменти статусу весь рік показували це обмеження, і слушно: воно існувало. Перевірки переписали так, щоб вони читали позицію правил, а не лише їхню наявність: тепер вони звіряють порядок у нумерованому переліку та в ланцюжку, яким ядро фільтрує насправді, із задуманим. Кожен порт отримує одне правило, і кожне правило називає протокол; SSH має обмеження частоти й окремого дозволу не має. П’ять публічних портів оголошено разом і перевіряють як набір, тож відкритий порт, якого в оголошенні немає, робить перевірку червоною, а звіт безпеки перелічує правила в тому порядку, в якому їх зустрічають пакети, з приміткою, як цей порядок читати.

Перший сервер зібрали руками, і брандмауер він отримав лише потім, тож був проміжок часу, коли свіжа машина була досяжна з інтернету. Для другого сервера в іншого провайдера брандмауер створює окремий плей ще до появи машини, тож нова машина зустрічає інтернет уже з правилами на місці. У того провайдера спершу ставлять теги, бо брандмауерові, що націлюється на теги, потрібно, щоб вони вже існували. Брандмауер кожного провайдера описано прямо через його REST API звичайним HTTP-завданням.

У сухому прогоні це завдання не виконується, тож зміни репетирують на самому плеї брандмауера: брандмауер у провайдера нічого не коштує, і його можна видалити.

Третій стосується контейнерів. Docker вписує власні записи в пакетний фільтр ядра, і порт, який він публікує для контейнера, перевіряється раніше за все, що поставила на хості роль посилення захисту. Отже, контейнер може стати досяжним ззовні, хоч би що наказали брандмауеру. Контейнери цієї платформи працюють під systemd через Podman і Quadlet у мережі хоста й не публікують портів, тож контейнерного порту, яким щось могло б обійти правила, просто немає.

Де виникають проблеми

Правило є у виводі статусу, але ніколи не спрацьовує. Правила перевіряються по черзі, і виграє перше, що збіглося, тож широкий дозвіл над вужчим обмеженням чи забороною повністю його затіняє. Список і далі показує обидва. Читайте правила так, як їх читає ядро, — з номерами й по порядку, ставте конкретні правила над загальними і перевіряйте з машини ззовні:

```
ufw status numbered
nft list ruleset
```

Контейнер відповідає на порту, який брандмауер забороняє. Docker публікує порти, перенаправляючи трафік у таблиці NAT ядра ще до ланцюжків, які фільтрує ufw, і власна документація Docker визнає, що так конфігурацію брандмауера фактично ігнорують. Публікуйте лише на адресу loopback, поставте перед сервером брандмауер провайдера або запускайте контейнери без опублікованих портів, як описано вище.

IPv4 закрито, а IPv6 відчинено навстіж. Дві родини адрес мають в iptables окремі набори правил, а ufw пише правила для IPv6 лише тоді, коли IPv6 увімкнено в його налаштуваннях за замовчуванням. Сервер із публічною адресою IPv6 і правилами лише для IPv4 відкритий на кожному порту, який слухає. Використовуйте таблицю nftables родини `inet`, що бачить обидві, або перевіряйте обидва списки, і скануйте IPv6-адресу сервера ззовні.

Сесія SSH завмирає тієї ж миті, коли вмикається брандмауер. Заборона за замовчуванням почала діяти раніше за правило для SSH, або демон SSH перенесли на інший порт, а правило досі згадує 22. Додавайте правило для SSH першим, тримайте консоль провайдера відкритою в іншому вікні й плануйте автоматичний відкат за кілька хвилин, який скасовують, щойно нова сесія увійшла.

Правило відкриває більше, ніж задумав автор. В ufw правило, що називає порт без протоколу, відкриває його і для TCP, і для UDP. Указуйте протокол у кожному правилі й декларуйте очікувану поверхню цілком, щоб усе зайве валило перевірку, а не чекало наступного аудиту.

Що почитати далі

- Firewall — визначення, якими користуються публікації NIST, кожне з посиланням на своє джерело.
- SP 800-41 Rev. 1: Guidelines on Firewalls and Firewall Policy — типи брандмауерів, заборона за замовчуванням і ведення правил, від NIST.
- ufw(8) — оболонка брандмауера в Ubuntu, зокрема порядок правил і правило `limit`.
- nftables wiki — документація проєкту netfilter для підсистеми, що замінює iptables.
- Packet filtering and firewalls — власний опис Docker того, як опубліковані порти обходять правила хоста.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке брандмауер?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/firewall/