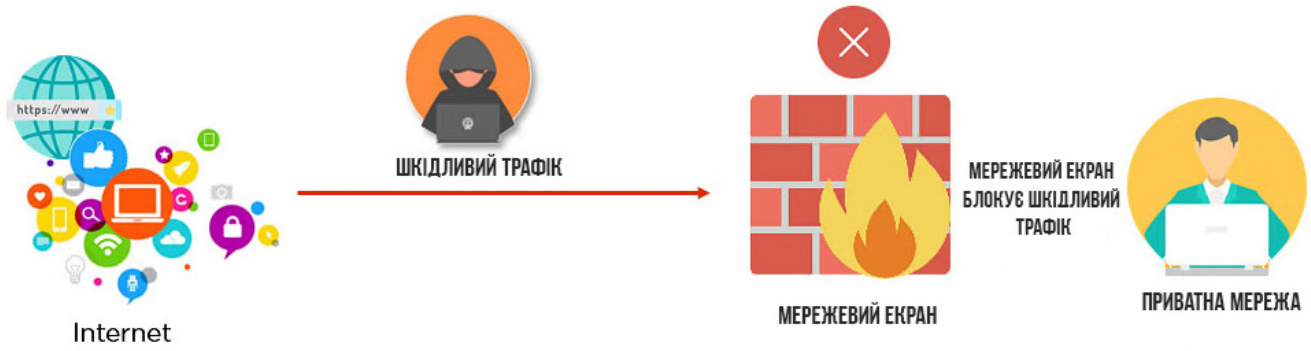
Мережевий екран

Міжмережевий екран, мережевий екран, брандмауер, фаєрво́л, файрво́л (англ. Firewall, вогняна стіна) — узагальнювальна назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки.

Це засіб безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік, дотримуючись політик безпеки, визначених організацією. По суті, він діє як захисна стіна між приватною внутрішньою мережею та публічним Інтернетом.



Огорожа вашої власності захищає ваш будинок і утримує порушників на відстані; так само брандмауери використовуються для захисту комп’ютерної мережі. Брандмауери — це системи безпеки мережі, які запобігають несанкціонованому доступу до мережі. Це може бути апаратне або програмне забезпечення, яке фільтрує вхідний і вихідний трафік у приватній мережі відповідно до набору правил для виявлення та запобігання кібератакам.

Мережевий трафік

Мережевий трафік або **трафік даних** — це кількість даних, що переміщуються по мережі в певний момент часу. Дані в комп'ютерних мережах здебільшого інкапсульовані в мережеві пакети, які власне і забезпечують навантаження в мережі. Мережа може мати безліч варіантів передачі пакетованого трафіку, але, щоб програми могли розуміти одна одну, трафік створюється відповідно до попередньо домовлених правил, такі правила називаються протоколами мережі, отже, пакетований трафік, який передається відповідно до списку протоколів.

Пакети даних, наприклад, так саме як у випадку з автомобілями на дорозі, можуть мати різний пріоритет, підлягають комутації, маршрутизації, інколи шифруванню, фільтрації вузлами мережі, а по прибуттю, в залежності від правил і протоколів, можуть потребувати перевірки контролю цілісності і джерела надходження. Може виявитись, що передача має втрату пакетів, що вказує на порушення функціонування мережі. Якісні та кількісні характеристики мережевого трафіку є однією із основних характеристик мережі в цілому. Контроль, аналіз, моделювання та управління є запорукою правильного функціонування складних мереж.

- **Аналіз мережевого трафіку** — моніторинг трафіку, його зміни, тенденцій, виявлення атипової поведінки
- **Контроль мережевого трафіку** — управління, встановлення пріоритетів, контроль або зменшення мережевого трафіку
- **Вимірювання мережевого трафіку** — вимірювання кількості та виду трафіку в мережі
- **Моделювання мережевого трафіку** — для вимірювання ефективності комунікаційної мережі
- **Модель генерації трафіку** — це стохастична модель потоків трафіку або джерел даних у комунікаційній комп'ютерній мережі .

Вчасний аналіз та моніторинг мережевого трафіку забезпечує в організації належну безпеку мережі, допомагає вчасно попередити вторгнення у мережу, виявляє потенційні до вразливості вузли мережі.

Як працюють різні типи брандмауерів?

Брандмауер може бути програмним або апаратним. **Програмні брандмауери** – це програми, встановлені на кожному комп’ютері, і вони регулюють мережевий трафік за допомогою програм і номерів портів. Тим часом **апаратні брандмауери** – це обладнання, встановлене між шлюзом і вашою мережею.

Брандмауери традиційно вставляються в мережеве з’єднання та переглядають увесь трафік, що проходить через цю точку. Коли вони це роблять, їм доручається визначити, який трафік мережевого протоколу є безпечним, а який - частиною атаки.

Усі брандмауери застосовують правила, які визначають критерії, згідно з якими певний пакет або набір пакетів у транзакції може бути безпечно направлений до призначеного одержувача.

> Сучасні брандмауери часто мають вбудовані додаткові системи безпеки, наприклад віртуальні приватні мережі (VPN), системи запобігання та виявлення вторгнень (IPS/IDS), управління ідентифікацією, управління додатками та веб-фільтрація.

Ось п’ять типів захисту мережі, які сьогодні продовжують відігравати важливу роль у корпоративному середовищі.

Брандмауер фільтрації пакетів

Брандмауери з фільтрацією пакетів контролюють та фільтрують мережевий трафік на основі набору правил. Ці правила визначають, які пакети дозволено, а які ні.

Брандмауери фільтрації пакетів працюють, аналізуючи заголовки пакетів даних. Заголовок пакета містить інформацію про джерело та призначення пакета, а також тип протоколу, який використовується. Брандмауер порівнює цю інформацію з набором правил і дозволяє або блокує пакет відповідно.

Однак ці брандмауери не маршрутизують пакети, скоріше вони порівнюють кожен отриманий пакет із набором встановлених критеріїв, таких як дозволені IP-адреси, тип пакета, номер порту та інші аспекти заголовків протоколу пакетів.

Шлюз ланцюгового рівня

Інший відносно швидкий спосіб виявлення зловмисного вмісту, шлюзи на рівні каналів відстежують зв’язки TCP та інші повідомлення про ініціацію сеансу мережевого протоколу в мережі, коли вони встановлюються між локальним і віддаленим хостами, щоб визначити, чи ініційований сеанс є законним – чи віддалена система вважається надійною. Однак самі пакети вони не перевіряють.

Приклади шлюзів ланцюгового рівня:
Міст (Bridge): використовується для об'єднання двох сегментів Ethernet.
Маршрутизатор (Router): застосовується для з'єднання сегментів Ethernet, Token Ring або FDDI.
Комутатор (Switch): служить для об'єднання декількох сегментів Ethernet.

Функції шлюзу ланцюгового рівня:

- Маршрутизація трафіку: шлюз використовує таблицю маршрутизації, щоб визначити найкращий шлях для пересилання даних між різними сегментами мережі.
- Перетворення протоколів: пристрій може конвертувати протоколи ланцюгового рівня, дозволяючи сегментам з різними протоколами спілкуватися один з одним.
- Фільтрація трафіку: шлюз здатний фільтрувати трафік, запобігаючи несанкціонованому доступу до мережі.
- Забезпечення безпеки: пристрій може використовуватися для захисту мережі, наприклад, за допомогою брандмауера.

Шлюз прикладного рівня (Application-level gateway, ALG)

Шлюз прикладного рівня – це компонент безпеки комп'ютерної мережі, який доповнює звичайний брандмауер або NAT-маршрутизатор.

Він працює аналізуючи не лише заголовки пакетів, а й вміст самих даних. Це дозволяє забезпечити додаткові можливості безпеки та управління трафіком.

Функції шлюзу прикладного рівня:

- Безпека: Шлюз може контролювати та фільтрувати трафік на основі правил, що враховують специфіку додатків. Наприклад, він може блокувати небажані команди в протоколах обміну повідомленнями або запобігати передачі конфіденційних даних.
- Управління трафіком: Шлюз може пріоритезувати певні типи трафіку, наприклад, відеоконференції, або обмежувати швидкість передачі даних для деяких додатків. Це допомагає оптимізувати використання мережевих ресурсів.
- Перетворення протоколів: Шлюз може перетворювати дані між різними форматами, що дозволяє додаткам, які зазвичай не сумісні один з одним, працювати разом.
- Розширення функцій брандмауера: Шлюз може доповнювати стандартні функції брандмауера, забезпечуючи захист від конкретних загроз, пов'язаних із певними

додатками.

Приклади використання шлюзу прикладного рівня:

- Захист веб-сервера від атак типу SQL-ін'єкція.
- Контроль доступу до файлів та принтерів у мережі.
- Обмеження використання P2P-мереж для завантаження файлів.
- Пріоритезація потокового відео та аудіо для покращення якості зв'язку.

Брандмауер з переглядом стану (Stateful inspection firewall)

Тип брандмауера, який забезпечує додатковий рівень безпеки порівняно з простими брандмауерами фільтрації пакетів. Він працює не лише аналізуючи заголовки пакетів даних, але й відстежуючи стан з'єднань між пристроями. На основі цієї інформації брандмауер може приймати більш обґрунтовані рішення щодо дозволу або блокування трафіку.

Основні принципи роботи брандмауера з переглядом стану:

- Відстеження стану з'єднань: Брандмауер зберігає інформацію про активні з'єднання, включаючи IP-адреси пристроїв, що беруть участь, порти, що використовуються, та напрямок передачі даних.
- Динамічні правила фільтрації: На відміну від статичних правил брандмауерів фільтрації пакетів, правила брандмауера з переглядом стану є динамічними та адаптуються до стану з'єднань. Наприклад, він може дозволити вхідний трафік, який є частиною встановленого з'єднання, але блокувати аналогічний трафік, якщо з'єднання не існує.
- Захист від різних типів атак: Брандмауер з переглядом стану може виявляти та блокувати різні типи атак, які використовують нетипові схеми встановлення з'єднань або передачі даних. Наприклад, він може блокувати сканування портів, атаки типу SYN-flood та інші.

Брандмауер наступного покоління (NGFW)

Брандмауер наступного покоління (Next-generation firewal, NGFW) - це передова система безпеки мережі, яка виходить за рамки традиційних функцій брандмауера, пропонуючи комплексний захист від різноманітних загроз. Він поєднує в собі традиційну фільтрацію пакетів з додатковими функціями безпеки, такими як:

- Захист від вторгнень (IPS): Виявляє та блокує відомі та невідомі атаки в режимі реального часу.
- Антивірусне програмне забезпечення: Сканує трафік на наявність шкідливого програмного забезпечення та блокує його виконання.
- Фільтрація веб-контенту: Блокує доступ до небажаних веб-сайтів та категорій контенту.
- Застосування контролю: Контролює використання додатків та запобігає несанкціонованому доступу до певних програм.
- VPN: Забезпечує безпечне з'єднання між віддаленими користувачами та мережею.
- Sandboxing: Ізолює підозрілі файли для безпечного аналізу перед дозволом доступу до мережі.

Апаратні брандмауери

Апаратний брандмауер - це пристрій, який діє як безпечний шлюз між пристроями всередині периметра мережі та тими, що знаходяться за її межами. Оскільки це автономні пристрої, апаратні брандмауери не споживають обчислювальну потужність або інші ресурси хост-пристроїв.

Також відомі як мережеві брандмауери, ці пристрої ідеально підходять для середніх та великих організацій, які бажають захистити багато пристроїв. Для налаштування та керування апаратними брандмауерами потрібні більші знання, ніж для їх аналогів на базі хоста.

Програмні брандмауери

Програмний брандмауер, або брандмауер хоста, працює на сервері або іншому пристрої. Програмне забезпечення брандмауера хоста потрібно встановлювати на кожному пристрої, що потребує захисту. Таким чином, програмні брандмауери споживають частину ресурсів процесора та оперативної пам'яті хост-пристрою.

Програмні брандмауери забезпечують окремим пристроям значний захист від вірусів та іншого шкідливого вмісту. Вони можуть розрізняти різні програми, які працюють на хості, фільтруючи вхідний та вихідний трафік. Це забезпечує детальний контроль, дозволяючи зв'язок з/до однієї програми, але забороняти його з/до іншої.

Хмарні / хостингові брандмауери

Хмарні/хостингові брандмауери, також відомі як Firewall as a Service (FWaaS), є типом брандмауера, який надається як послуга через Інтернет постачальником керованих послуг безпеки (MSSP). Вони відрізняються від традиційних апаратних або програмних брандмауерів тим, що вся інфраструктура та управління брандмауером знаходяться у хмарі, а не на локальних пристроях чи мережі організації.

Джерела

- Мережевий екран
- What Is Firewall: Types, How Does It Work, Advantages & Its Importance
- Мережевий трафік
- Брандмауер
- The 5 different types of firewalls explained