Безпека операційних систем і комп'ютерних мереж

Лекція 19

Firewalling - міжмережне екранування

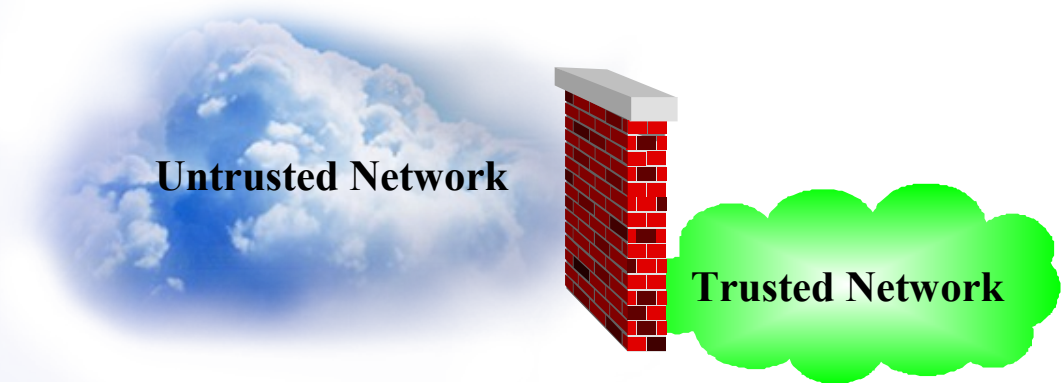
Брандмауер чи firewall? І як його краще називати?

- Стосовно засобів захисту комп'ютерних мереж крім поширеного терміну "брандмауер" і англомовного "firewall" рекомендується використовувати термін "мережний екран", або "міжмережний екран" (МЕ)
- *Міжмережні екрани*, або *брандмауери* призначені для захисту внутрішніх ресурсів мереж шляхом обмеження можливостей обміну між ними
  - Комп'ютер, на якому виконується ПЗ міжмережного екрану, або спеціалізований програмно-апаратний пристрій, що реалізує функції МЕ, є шлюзом між двома мережами, найчастіше – між Інтернет і корпоративною мережею
- Брандмауер (*brandmauer*) – німецький еквівалент англійського терміну *firewall*, що означає протипожежну капітальну стіну
  - В жодному разі не "стіна вогню" чи "вогняна стіна", як дехто помилково вважає!
  - Саме німецький термін увійшов у російську і в українську мови
  - Дотепно, але самі німці щодо міжмережних екранів застосовують термін **firewall**

Брандмауер також відомий як Firewall

Міжмережний екран (МЕ):

- Є бар'єром, що керує потоками між мережами
  - Між довіреною та не довіреною мережами
  - Зазвичай застосовується між корпоративною (захищеною) мережею і Інтернетом (незахищеною мережею)
- "Передова лінія оборони від хакерів"
  - Змушує користувачів входити / виходити з мережі лише через добре керовану точку
  - Забезпечує упевненість, що трафік обміну є прийнятним (відповідає політиці безпеки)



Можливості МЕ

- В загальному випадку робота МЕ базується на динамічному виконанні двох груп функцій:
  - фільтрації інформаційних потоків, що проходять крізь нього
  - посередництва при реалізації міжмережної взаємодії (проксі-сервер)

Фільтрація трафіка

- Фільтрація трафіка здійснюється на основі набору правил, які попередньо завантажуються до ME
  - Правила є відображенням мережних аспектів політики безпеки
  - Оскільки результат обробки пакету в загальному випадку залежить від послідовності застосування правил, правила є упорядкованими.
- Механізм застосування правил можна уявити як послідовність фільтрів.
  - Кожний фільтр містить набір критеріїв, яким повинен задовольняти пакет
  - Якщо пакет відповідає критеріям цього фільтру, по відношенню до пакету застосовується визначена дія

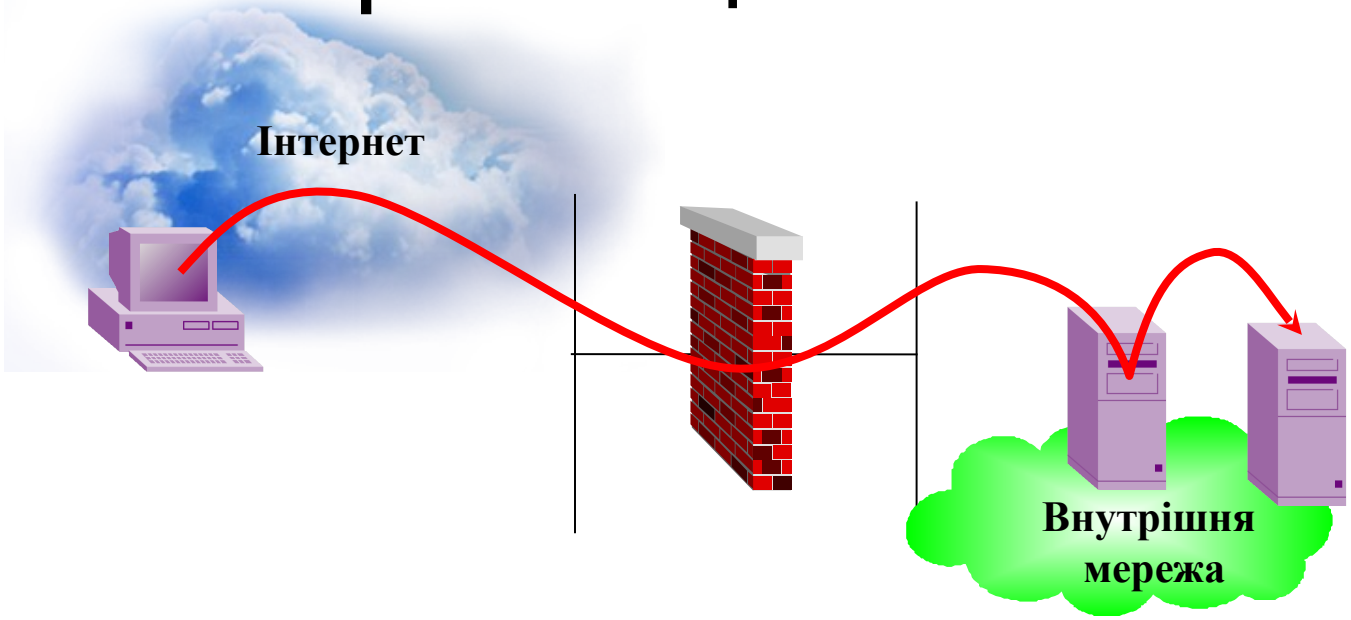
Можливі дії щодо пакету

- **Не пропустити пакет**, тобто вилучити його з інформаційного потоку і знищити (можлива реєстрація відповідної події, інформування відправника пакету про неможливість доставки, тощо);
- **Пропустити пакет**, тобто передати його на адресу призначення;
- **Обробити пакет** від імені одержувача і повернути результат відправнику;
- **Передати пакет визначеній програмі на обробку** (наприклад, шифрування-дешифрування, антивірусна перевірка, трансляція мережевих адрес тощо), після чого, як правило, пакет повертається для аналізу наступними фільтрами;
- **Передати пакет для аналізу наступним фільтром** або визначеним фільтром з послідовності (тобто, можливий пропуск певної кількості фільтрів).

Правило за умовчанням

- Набір правил повинен забезпечувати визначеність дій, що застосовуються до кожного пакета.
  - Тому повинно існувати “правило за умовчанням”, яке застосовується до будь-якого пакету, для якого не знайшлося відповідного йому фільтру
- Від того, яким є правило за умовчанням, залежить принцип політики безпеки, який реалізує МЕ. Фактично можливими є два правила за умовчанням – пропустити або не пропустити пакет
  - Відфільтровувати всі потенційно небезпечні пакети, а решту пропускати за умовчанням
    - Забезпечує доступність ресурсів мережі
    - Не гарантує достатнього рівня захисту
      - пропущеним буде будь-який пакет з непередбаченими параметрами
    - Цей підхід вважається хибним.
  - Відкинути всі пакети, що не відповідають явно заданим фільтрам
    - Дозволяє реалізувати принцип мінімуму повноважень: “заборонено все, що не дозволено явно”
    - Такий підхід можна легко зіпсувати занадто ліберальними правилами, що пропускають пакети
    - За відсутності “ліберальних” правил потрібен окремий явний дозвілу для кожного сервісу, який повинен бути доступним у мережі

Схема розміщення МЕ

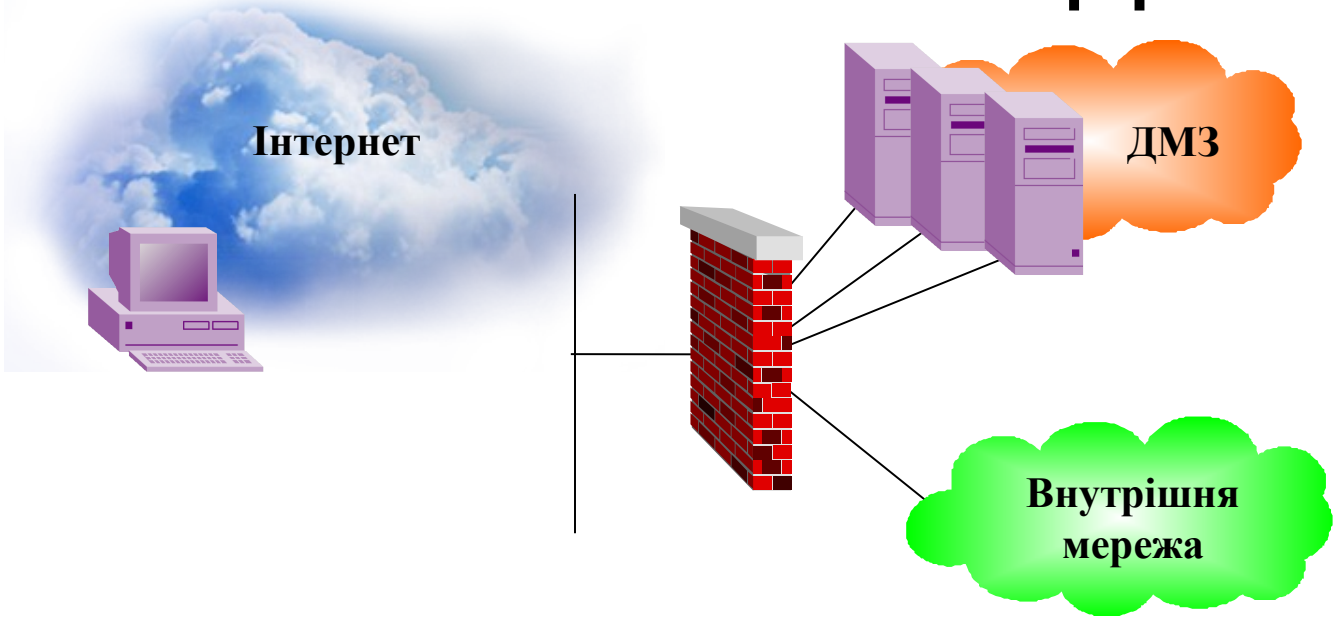


- 2 зони безпеки – довірена і не довірена мережі, що розділені МЕ
- Якщо відкритий для доступу сервер має вразливості системи безпеки, порушник може отримати доступ до сервера і використати цей доступ для доступу до інших систем у захищеній мережі

Демілітаризована зона

- Типовим є виділення так званої *демілітаризованої зони* (*ДМЗ*), правила обміну з якою відмінні від правил обміну з внутрішньою (захищеною) мережею
  - В ДМЗ переважно розміщують сервери, до яких необхідно відкрити доступ із зовнішньої мережі (наприклад, корпоративний Web-сайт)
  - Це дозволяє встановити більш жорсткі обмеження на взаємодію із внутрішньою мережею
    - Наприклад, винесення в ДМЗ FTP, HTTP і поштового серверів дозволяє повністю заборонити доступ до внутрішньої мережі за номерами портів 21, 25 і 80
    - При цьому на внутрішніх серверах та робочих станціях можуть функціонувати сервери, доступ до яких буде можливим лише зсередини захищеної мережі.

Встановлення МЕ з ДМЗ



- Доступні ззовні сервери підключені до ДМЗ
  - Захист від зовнішньої мережі
  - Ізоляція від внутрішньої мережі
- ДМЗ не є частиною внутрішньої мережі і не є частиною Інтернету

Рівні реалізації

- *Пакетні фільтри*, які також називають *екрануючими (фільтруючими) маршрутизаторами* (Packet Filters)
  - Працюють головним чином на 3-му (мережному) рівні моделі взаємодії відкритих систем (OSI)
  - Як правило, аналізують також інформацію із заголовків протоколів 4-го (транспортного) рівня
- *Шлюзи сеансового рівня*, які також називають *екрануючим транспортом* (Stateful Packet Filters)
  - Працюють головним чином на 5-му (сеансовому) рівні моделі OSI
- *Прикладні,* або *екрануючі шлюзи* (Application Gateway)
  - Працюють на прикладному рівні моделі OSI

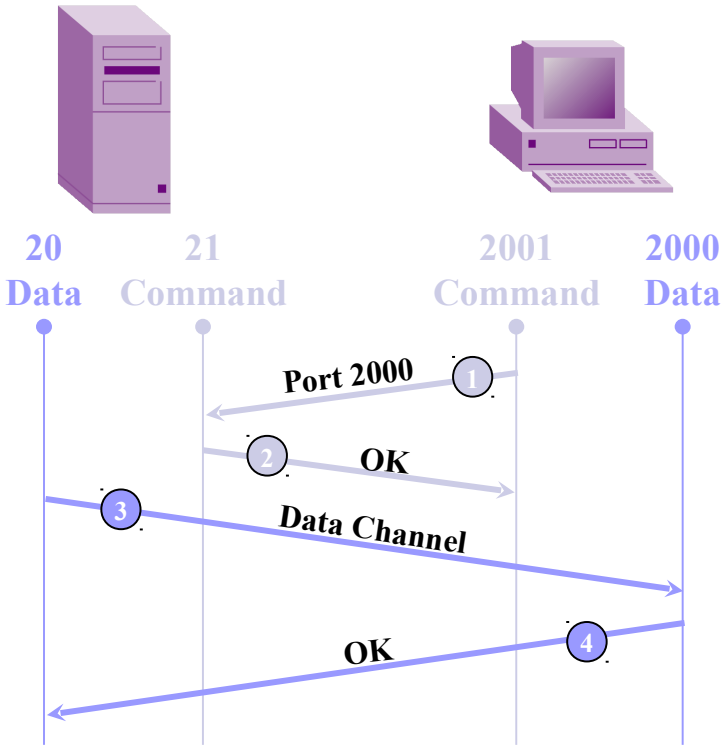
Пакетні фільтри

- *Пакетні фільтри* здійснюють розбір заголовків пакетів для протоколів TCP, UDP, IP і, в залежності від заданого адміністратором безпеки набору правил, приймають рішення про дії з пакетом під час їх маршрутизації
- Кожний пакет аналізується окремо, без зв'язку з іншими
- Забезпечується фільтрація пакетів за такими параметрами:
  - IP-адреси відправника й одержувача;
  - тип пакету (протокол);
  - ознака фрагментації пакету;
  - номери портів TCP (UDP) відправника й одержувача;
  - прапорець SYN (ознака першого пакету при встановленні з'єднання);
  - інші прапорці;
  - типи повідомлень ICMP;
  - напрям передачі пакета (вхідний / вихідний).

Переваги і недоліки

- Переваги пакетних фільтрів
  - простота самого МЕ
  - простота процедур інсталяції та конфігурування
  - прозорість для прикладних програм
  - мінімальний вплив на продуктивність мережі
  - фактично, інтегровані з кожним маршрутизатором
  - низька вартість
- Суттєві недоліки пакетних фільтрів
  - перевірка лише заголовків пакетів, і через це вразливість до підробки заголовків – адрес відправника та інших параметрів
  - неможливість реалізації складних політик
  - неможливість роботи з певними протоколами (FTP)
  - відсутність перевірки цілісності й справжності пакетів
  - відсутність автентифікації кінцевих вузлів
  - недостатні можливості реєстрації подій
  - погана масштабованість

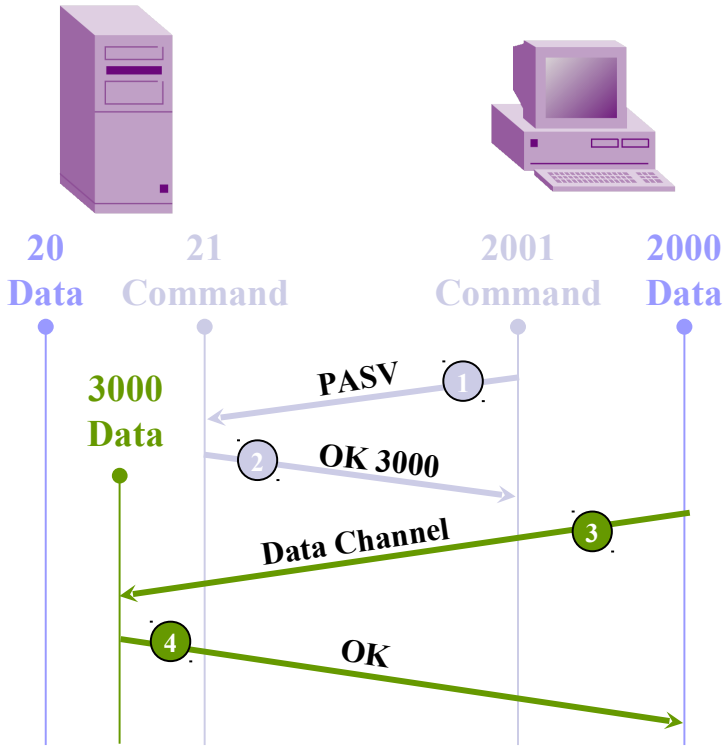
FTP і статичні фільтри



- Звичайний режим FTP з'єднання
- Сервер прослуховує порт 21
- Клієнт обирає 2 непривілейованих TCP порта
  - один використовує для встановлення каналу керування
  - і повідомляє серверу другий
- Сервер відкриває клієнту з'єднання для передачі даних на вказаний порт
- Проблема відкриття з'єднання зі статичними фільтрами:
  - З'єднання дозволяються із зовнішньої мережі з порту 20 на будь-який невідомий порт >1023

FTP і статичні фільтри

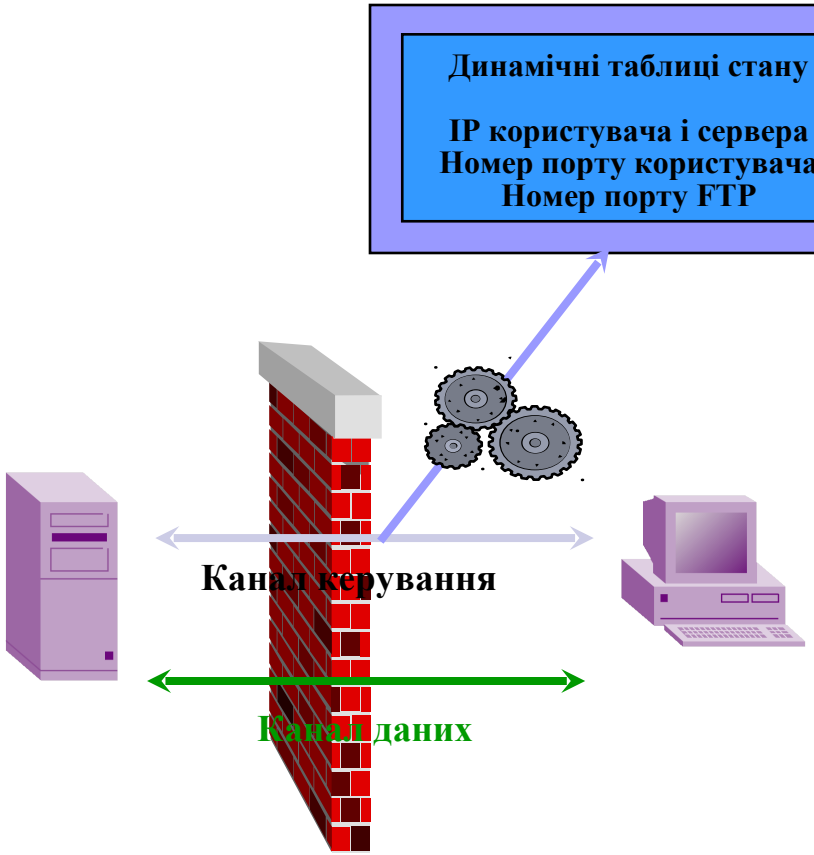
- FTP з'єднання у пасивному режимі
- З'єднання завжди ініціюють зсередини
- Підтримується не всіма клієнтами і серверами
- Який режим застосовувати – обирає клієнт
  - За умовчанням – активний режим



Stateful Firewall

- Обробляє пакети як частини потоку інформації
  - Не перевіряє вміст кожного пакета (на відміну від прикладного шлюзу)
- Прозорий для користувачів
- Контролює стан з’єднань
  - Контроль з’єднань полягає у контролі за встановленням TCP з’єднання і відстеженні послідовності пакетів і квитанцій-підтверджень у встановлених з’єднаннях
  - Для цього шлюз сеансового рівня повинен зберігати інформацію про встановлені з’єднання у спеціальних таблицях

Stateful Firewall – з’єднання FTP



- Відстежує сеанс FTP
- Визначає FTP порт
- Поміщає у таблицю станів:
  - IP адреси
  - Динамічні номери портів
- Пропускає пакети з відповідними номерами портів
  - Після завершення сеансу FTP одразу блокує номери портів, які використовувались у ньому

Stateful Firewall – переваги

- Хороший компроміс між безпекою і продуктивністю
- Здатність контролювати віртуальні з'єднання і здійснювати трансляцію внутрішніх IP адрес
- Масштабованість
- Прозорість для користувачів
- Із самого початку розроблявся як ME (на відміну від маршрутизаторів)
  - Широкі можливості реєстрації події і реагування на них

Stateful Firewall + NAT = шлюз сеансового рівня

- Якщо не здійснювати трансляцію адрес, внутрішні пакети ідуть в Інтернет, демонструючи в Інтернеті внутрішні IP адреси
- Шлюзи сеансового рівня дозволяють здійснювати трансляцію IP адрес (Network Address Translation, NAT) під час взаємодії із зовнішньою мережею
  - Головною перевагою таких МЕ є можливість приховати внутрішню структуру захищеної мережі
  - МЕ сеансового рівня може поєднувати дві мережі з різними адресними просторами

Де такі МЕ знайти?

- Переважна більшість шлюзів сеансового рівня постачаються разом із шлюзами прикладного рівня
- Але функції шлюзів сеансового рівня можуть мати і програмні засоби, які переважно розглядаються як пакетні фільтри
  - Приклад: **ipfw**, що входить до складу ОС FreeBSD
    - Він містить функції, які реалізують *statefull firewall*
    - За можливостями, це саме шлюз сеансового рівня

Прикладні шлюзи

- Прикладні шлюзи, або МЕ прикладного рівня, працюють як проксі-сервери протоколів прикладного рівня (HTTP, FTP, Telnet тощо)
- Їхні функції – посередницькі
- Такий МЕ містить в собі сервери прикладних протоколів
- Крім можливості приховування внутрішньої структури захищеної мережі, такі МЕ дозволяють використовувати для розмежування доступу достатньо широкий спектр засобів автентифікації прикладного рівня, обмежуючи доступ на основі комбінації адрес, номерів портів, повноважень окремих користувачів, реального часу
- Здійснення фільтрації на прикладному рівні означає, що МЕ переглядає всю інформацію всередині пакетів
  - Це надає можливості відфільтровувати окремі види команд або окремі типи інформації в прикладних протоколах
  - Наприклад, прикладний шлюз може забороняти використання команди PUT клієнтам FTP, або не пропускати вкладення заданих типів файлів в листах електронної пошти

Додаткові функції захисту прикладних шлюзів

- Ідентифікація й автентифікація користувачів при спробі встановити з'єднання через МЕ
- Перевірка справжності інформації, яку передають через МЕ
- Розмежування доступу до ресурсів мереж
- Фільтрація й перетворення потоку повідомлень
  - антивірусні й антиспамові перевірки
  - шифрування й дешифрування
- Аудит
  - Реєстрація подій
  - Реагування на події
  - Аналіз зареєстрованої інформації
  - Генерація звітів
- Кешування даних, що надходять із зовнішньої мережі

Переваги і недоліки

- Переваги шлюзів прикладного рівня
  - Забезпечує найвищий рівень захисту локальної мережі завдяки реалізації функцій посередництва
  - Захист на прикладному рівні дозволяє здійснювати перевірки, специфічні для окремих прикладних програм, що надає можливість нейтралізувати притаманні їм вразливості
  - В разі відмови прикладного шлюзу, трафік через нього буде повністю блоковано, і таким чином безпека локальної мережі порушена не буде
    - але, звичайно, буде порушена доступність
- Недоліки шлюзів прикладного рівня
  - Значна складність самого МЕ, а також процедур його встановлення й конфігурування
  - Значні вимоги до продуктивності та наявних ресурсів комп'ютерної платформи, на якій реалізовано МЕ
  - Висока вартість
  - Відсутність прозорості для користувачів
  - Зниження перепускної здатності мережі при передачі трафіку через МЕ

Особливості персональних брандмауерів

- Серед програмних МЕ виділяють окремий клас так званих *персональних брандмауерів*
  - Такі програми встановлюються на кінцевих вузлах мережі (найчастіше – на робочих станціях користувачів) і контролюють лише той трафік, який адресований конкретно цьому комп'ютеру
  - У загальному випадку, персональні брандмауери контролюють як вхідний, так і вихідний трафік
  - Оскільки такий брандмауер вбудовується у ланцюг драйверів, що працюють з мережним адаптером, він здатний перехоплювати весь трафік, що обробляється стандартним стеком протоколів у системі, і може здійснювати контроль на усіх рівнях взаємодії.

Переваги персонального брандмауера

- Перевагою персонального брандмауера є його інтеграція з ОС комп'ютера, що дозволяє визначати
  - від яких прикладних програм надходять запити на встановлення з'єднань з віддаленими вузлами
  - яким прикладним програмам адресовані пакети, що надходять з мережі
- Легко реалізується контроль не лише на рівні мережних і транспортних протоколів (IP-адреси, номери портів), і не лише на рівні прикладних протоколів (наприклад, FTP, HTTP), а й на рівні прикладних програм
  - Наприклад, можна визначити, чи запит на встановлення з'єднання за протоколом HTTP надходить від Web-браузера, якому така діяльність дозволена, чи від іншої програми (на кшталт медіа-плеєра), де рішення про дозвіл слід приймати окремо

Типові можливості персонального брандмауера (1)

- Встановлення правил фільтрації пакетів за мережними адресами, протоколами і номерами портів
- Встановлення правил для прикладних програм, які можуть повністю дозволяти або забороняти взаємодію конкретної програми з мережею, а можуть вводити конкретні обмеження (або конкретні дозволи) на окремі мережні адреси, протоколи, номери портів тощо
- Виявлення типових атак за параметрами отриманих пакетів або характеристиками трафіка
  - наприклад, пакети із спеціальними комбінаціями прапорців і параметрів заголовків, або сканування портів
- Реєстрація подій, що пов’язані з мережною взаємодією, як стосовно вхідних пакетів, так і стосовно вихідних
  - наприклад, спроба атаки, або встановлення з’єднання за ініціативою певної програми

Типові можливості персонального брандмауера (2)

- Реакція на виявлені атаки, яка може бути
  - пасивною (реєстрація події, сигнал тривоги)
  - активною (блокування вузла, з якого розпочата атака)
- Інтелектуальний дружній до користувача режим встановлення правил
  - Спочатку за умовчанням все заборонено
  - При появі будь-якої активності, здійснюється інформування користувача про подію і пропонується
    - її однократно дозволити чи заборонити
    - перманентно дозволити чи заборонити
    - відредагувати правило щодо такої події
  - В подальшому така процедура виконується лише для тих події, для яких ще не створені відповідні правила.

Додаткові функції персонального брандмауера

- До функцій персонального брандмауера іноді включають перевірку цілісності програм, що працюють з мережею
  - Наприклад, після встановлення нової версії браузера при першій спробі виходу в Інтернет персональний брандмауер заблокує роботу браузера в мережі до підтвердження користувачем, що останній знає про зміну програми і продовжує їй довіряти

Проблеми сумісності

- Для коректної роботи різних програм, що виконують однакові завдання, слід перевіряти їх на сумісність
- Як правило, на одному комп’ютері не можуть коректно працювати два різних персональних брандмауери
  - так само, як і два антивіруси
- Через дублювання окремих функцій, можуть виникати проблеми і при роботі персонального брандмауера з антивірусом чи системою виявлення атак

Обмеження МЕ (1/4)

- Проникнення в захищену мережу через канал, який не контролюється МЕ
  - У правильно спроектований ІКС таких каналів не має бути
  - У реальних системах вони часто існують
    - Поширеною ситуацією утворення такого неконтрольованого каналу є використання модемів
      - Адміністратори систем не завжди можуть точно сказати, скільки модемів встановлено і для чого вони використовуються
      - Користувачі, порушуючи політику безпеки, можуть встановлювати модеми для доступу до робочих каталогів з дому, або для несанкціонованого виходу в Інтернет
    - Особливо важко проконтролювати використання в якості модемів мобільних телефонів
  - Через такі канали в захищену мережу можуть потрапляти віруси та “троянські кони”
  - Якщо модем встановлений стаціонарно, цілком ймовірною є й безпосередня атака через нього

Обмеження МЕ (2/4)

- Атака зсередини захищеної мережі
  - Зловмисники можуть:
    - вербувати легальних користувачів
    - деяким чином вводити “своїх” людей у число користувачів
    - іноді спрацьовує обман довірливих користувачів, в тому числі провокування їх на дії, що, зрештою, приводять до порушення політики безпеки
      - Однією з можливостей є передача користувачам програм, які містять віруси або приховані функції (“троянських коней”).
  - В результаті атака або буде здійснюватись всередині мережі, і її трафік взагалі не буде проходити через МЕ, або ініціатором з’єднання з комп’ютером зловмисника буде виступати комп’ютер з захищеної мережі, внаслідок чого таке з’єднання не буде заборонено

Обмеження МЕ (3/4)

- Використання дозволених протоколів
  - Практично завжди МЕ дозволяє обмін за протоколами SMTP (електронна пошта) та дуже часто – HTTP (WWW)
    - Якщо МЕ є пакетним фільтром, він не буде контролювати вміст пакетів
  - Кваліфіковані зловмисники можуть здійснювати атаки, створюючи тунель в рамках дозволеного протоколу
    - Найпростіший приклад – проникнення в корпоративну мережу шкідливих програм у вигляді вкладень у повідомлення електронної пошти
    - Також прикладом може бути атака Loki, яка дозволяє тунелювати різні команди у запитах і відповідях ICMP Echo
- У багатьох випадках головним заходом захисту, що дозволяє доступ через МЕ лише авторизованим користувачам, є автентифікація
  - У такому разі жодний МЕ не зможе захистити від проникнення порушника у корпоративну мережу, якщо той підібрав або заволодів паролем авторизованого користувача

Обмеження МЕ (4/4)

- Часто МЕ поєднують з організацією віртуальних приватних (захищених) мереж (VPN)
  - Поєднання VPN з МЕ надає надійний захист мережі… лише доти, доки мережний обмін здійснюється виключно у VPN-з'єднаннях
    - Якщо у будь-якій точці одночасно з VPN є і незахищений вихід у зовнішню мережу, то у цій точці можлива компрометація системи
    - В подальшому зловмисники будуть здійснювати з цієї точки атаки на інші вузли системи
  - Цілком можливо, що контроль на МЕ буде послабленим, тому що трафік передається з довіреного вузла через VPN
    - У такому разі ефективність атаки буде ще вище.
- Міжмережні екрани часто самі є об'єктами атаки
  - Якщо атака на МЕ буде успішною, зловмисники можуть без перешкод реалізовувати свої плани щодо ресурсів захищеної мережі
  - У ПЗ МЕ, як і в інших програмах, періодично виявляють вразливості
    - Такі вразливості виявляли як у суто програмних МЕ (наприклад, **ipfw** і **ip6fw**), так і програмно-апаратних (наприклад, Cisco Secure Pix Firewall, WatchGuard Firebox тощо)

Чого не можуть МЕ

- Не можуть зупинити атаки зловмисних авторизованих користувачів (інсайдерів)
- Не можуть захистити від з’єднань, які через них не проходять
- Не можуть замінити навчання
- Не можуть замінити політики безпеки і дій із захисту
- Не можуть забезпечити 100% захисту проти всіх загроз