Основні відомості про кібербезпеку

План лекції

- Терміни та визначення
- Елементи інформаційної безпеки
- Загрози інформаційної безпеки
- Типи атак
- Механізми захисту від атак

Терміни і визначення

Терміни і визначення

- Ідентифікація - процедура розпізнавання суб'єкта по його ідентифікатору
- Аутентифікація - процедура перевірки автентичності суб'єкта, що дозволяє переконатися в тому, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує
- Авторизація - процедура надання суб'єкту певних прав доступу до ресурсів системи

Терміни і визначення

- Загроза - це потенційно можлива подія, неважливо, навмисна чи ні, яка може небажано вплинути на систему, а також на інформацію, що зберігається в ній
- Вразливість - це деяка невдала характеристика системи, яка робить можливим виникнення загрози
- Атака - це дія, що виконується зловмисником, яка полягає в пошуку і використанні тієї або іншої вразливості для реалізація загрози
- Експлоїт - комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують вразливості і застосовуються для здійснення атак

Терміни і визначення

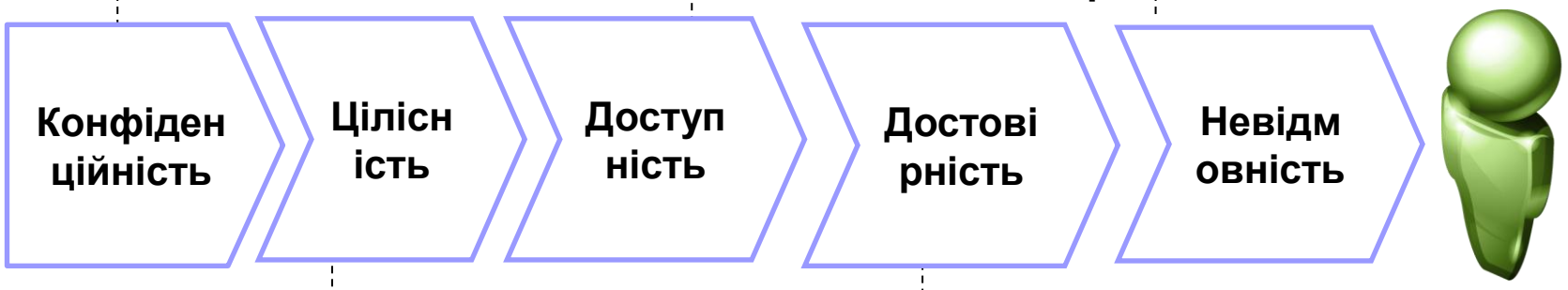
- Інформаційна безпека - стан захищеності інформації, при якому забезпечуються її конфіденційність, доступність і цілісність
- Невідмовність - здатність засвідчувати дію, що мала місце, або подію так, що вони не могли бути пізніше відкинуті
- Ризик - ймовірність використання вразливості системи для реалізації загрози
- Вразливість нульового дня (0 - day) - це раніше невідома вразливість, яка використовується зловмисниками для виконання атак

Елементи інформаційної безпеки

Гарантія того, що інформація доступна тільки для авторизованих користувачів

Гарантія того, що система, відповідальна за доставку, зберігання і обробку інформації доступна, у момент запиту авторизованим користувачем

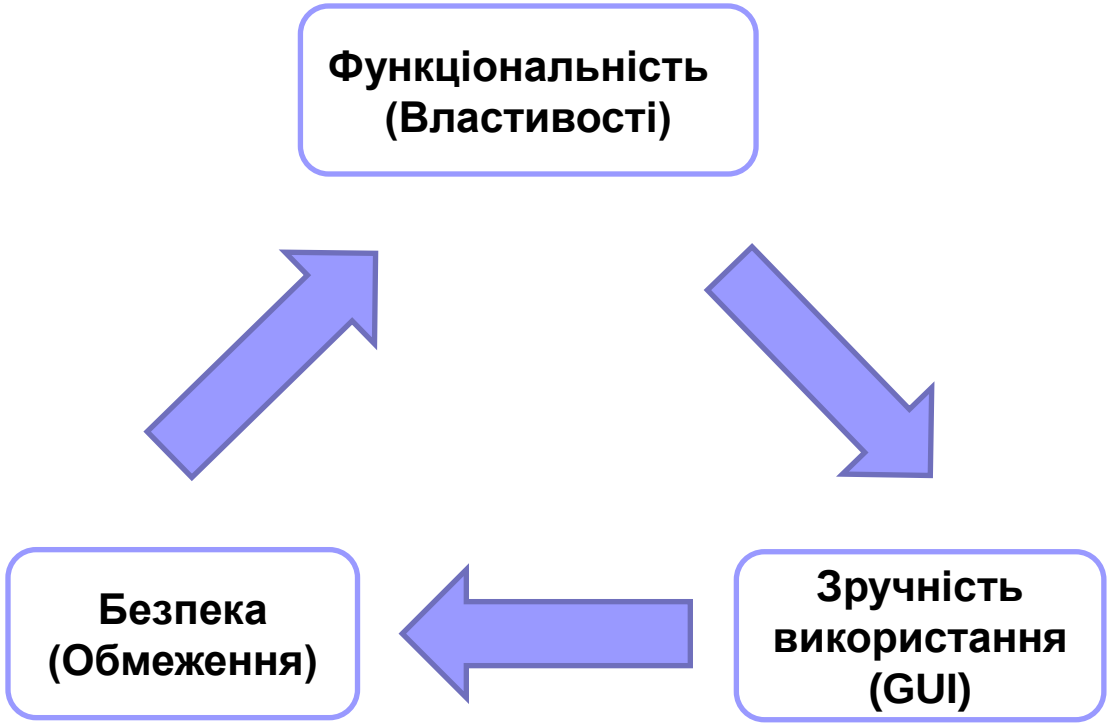
Гарантує, що відправник повідомлення не може пізніше заперечувати факт відправки повідомлення і що одержувач не може заперечувати факт його отримання



Запобігання зміни інформації неавторизованими користувачами

Характеризує ступінь автентичності інформації (відсутність відмінностей від оригіналу)

Трикутник інформаційної безпеки



Трикутник інформаційної безпеки

Загрози інформаційної безпеки

Загрози мережі

- Збір інформації
- Сніффінг і підслуховування
- Підміна параметрів
- Перехоплення сеансу і атака «Людина посередині»
- SQL-ін'єкції
- Отруєння ARP
- Атаки перебором паролів
- Атака «Відмова в обслуговуванні»

Загрози вузла

- Шкідливе ПЗ
- Збір інформації про вузол
- Атаки, засновані на паролі
- Довільне виконання коду
- Несанкціонований доступ
- Підвищення привілеїв
- Бекдор атаки
- Загрози фізичної безпеки

Загрози програм

- Проблеми контролю введення даних
- Атаки аутентифікації та авторизації
- Управління конфігурацією
- Розкриття інформації
- Проблеми управління сеансами
- Проблеми переповнення буфера
- Криптографічні атаки
- Зміна параметрів застосувань
- Неправильна обробка помилок
- Проблеми аудиту та журналювання дій

Типи атак

- Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі:
  - порушення конфіденційності переданої інформації;
  - порушення цілісності та достовірності інформації, що передається;
  - порушення працездатності системи в цілому або окремих її частин.

Типи атак

- Атаки доступу
- Атаки модифікації
- Атаки «відмова в обслуговуванні»
- Комбіновані атаки

Багатошаровий захист

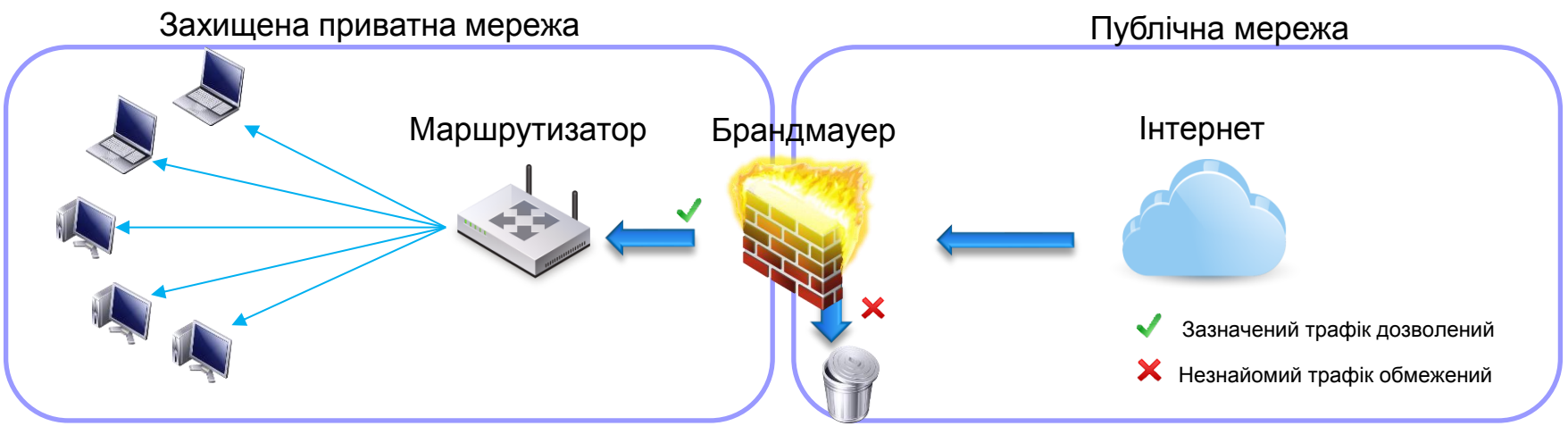
- **Багатошаровий захист** – це стратегія безпеки, в якій кілька захисних шарів розміщені через всю інформаційну систему.
- Допомагає уникнути прямих атак проти інформаційної системи і даних, оскільки злом одного шару призводить зловмисника тільки до наступного рівня.

Механізми захисту від атак

- Мережні фільтри (брандмауери) та системи виявлення вторгнень
- Захищені мережні криптопротоколи

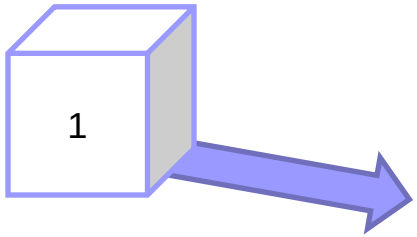
Брандмауер

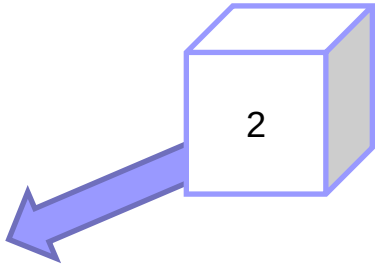
- Брандмауер - це програма та / або апаратне забезпечення, розроблене для запобігання несанкціонованого доступу в / з приватної мережі
- Вони розташовуються на прикордонному маршрутизаторі або шлюзі між двома мережами, якими зазвичай є приватна і публічна мережі
- Брандмауер досліджує всі повідомлення, що входять або виходять з Інтранет і блокує ті, які не відповідають деяким критеріям безпеки
- Брандмауери можуть бути пов'язані з типами трафіку або ж з адресами або портами джерела і призначення



Типи брандмауерів

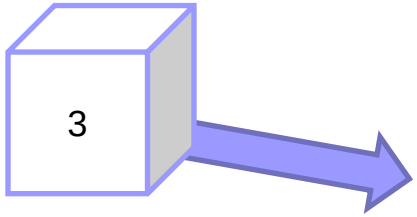
1. Фільтр пакетів

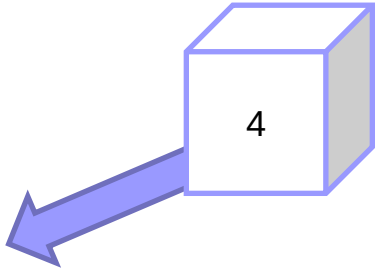




2. Шлюзи сеансового рівня

3. Шлюзи програмного рівня

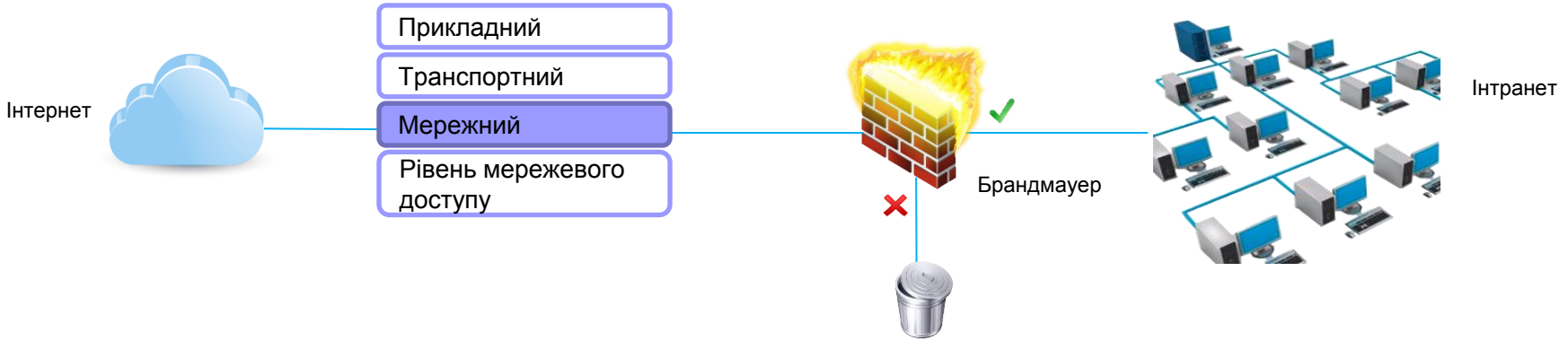




4. Мультирівневий брандмауер з урахуванням стану

Фільтр пакетів

- Фільтр пакетів працює на мережному рівні моделі OSI (або на IP рівні TCP / IP), як правило, є частиною маршрутизатора.
- У даному брандмауері кожен пакет порівнюється з набором критеріїв перед тим як він буде пропущений
- Залежно від пакета чи критеріїв брандмауер може відкинути пакет, пропустити його або відправити повідомлення до ініціатора.
- Правила можуть включати в себе IP адресу, порти джерела та одержувача, а також протокол, що використовується.

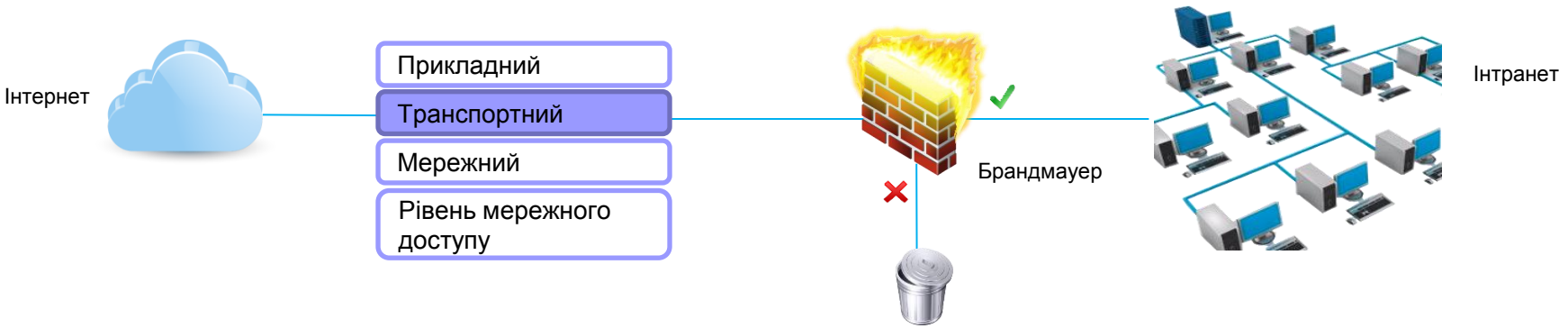


Дозволений трафік, заснований на IP адресі, типі пакету і номері порту джерела і одержувача

Заборонений трафік

Шлюзи сеансового рівня

- Шлюзи сеансового рівня працюють на сеансовому рівні моделі OSI або на TCP рівні стека TCP / IP.
- Вони стежать за запитами по створенню сесій і визначають чи дозволені ці сесії.
- Шлюзи сеансового рівня пропускають або забороняють потоки даних, вони не фільтрують окремі пакети.

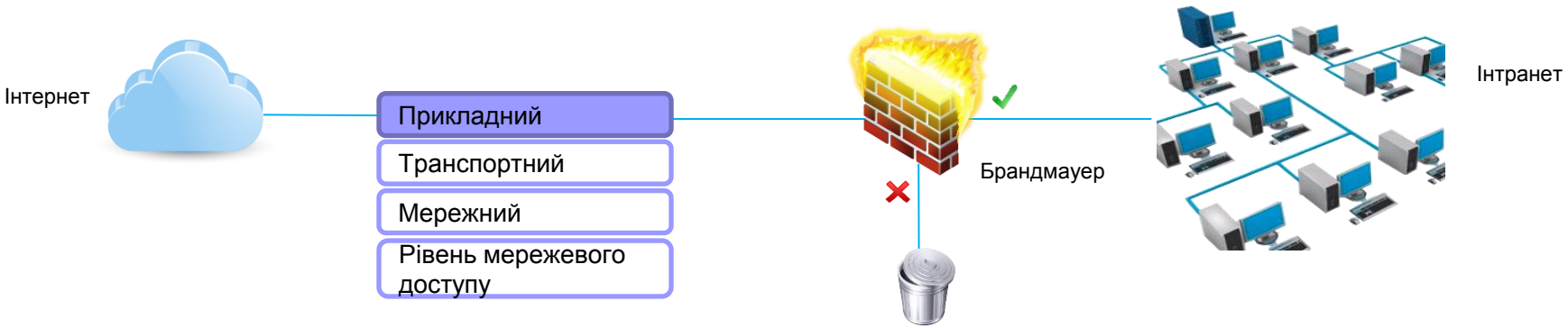


✓ Дозволений трафік, заснований на правилах сесій, наприклад, коли сеанс ініціюється з довіреної комп'ютера

✗ Заборонений трафік

Шлюзи програмного рівня

- Шлюзи програмного рівня (проксі) можуть фільтрувати потоки на прикладному рівні моделі OSI
- Вхідний і вихідний трафік обмежений сервісами, які підтримують проксі; запити до інших сервісів відхиляються
- Шлюзи програмного рівня налаштовуються як веб-проксі, що забороняють FTP, gopher, telnet або інший трафік.
- Шлюзи програмного рівня досліджують трафік і фільтрують команди конкретних застосувань, таких як HTTP: POST і GET

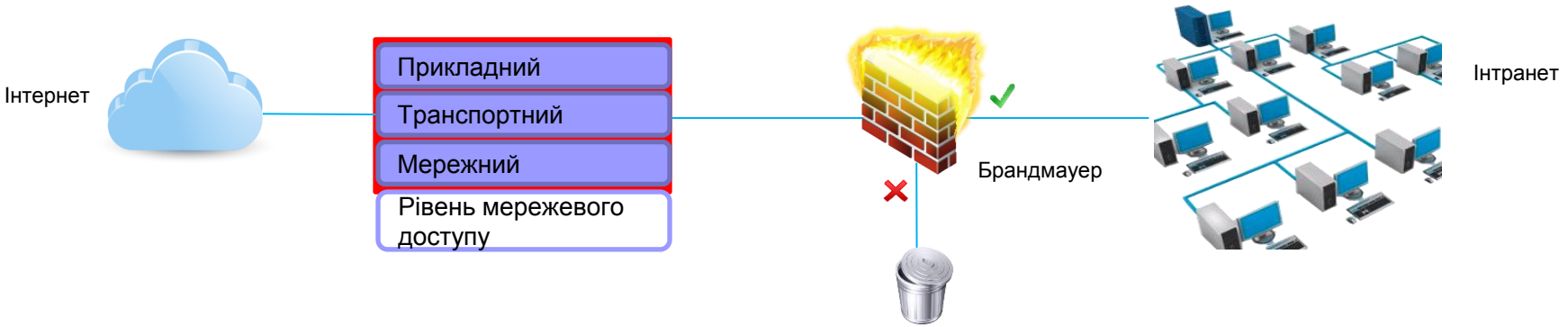


✓ Дозволений трафік, заснований на певних програмах (таких як браузер) або протоколах (як FTP) або їх комбінаціях

✗ Заборонений трафік

Мультирівневий брандмауер з урахуванням стану

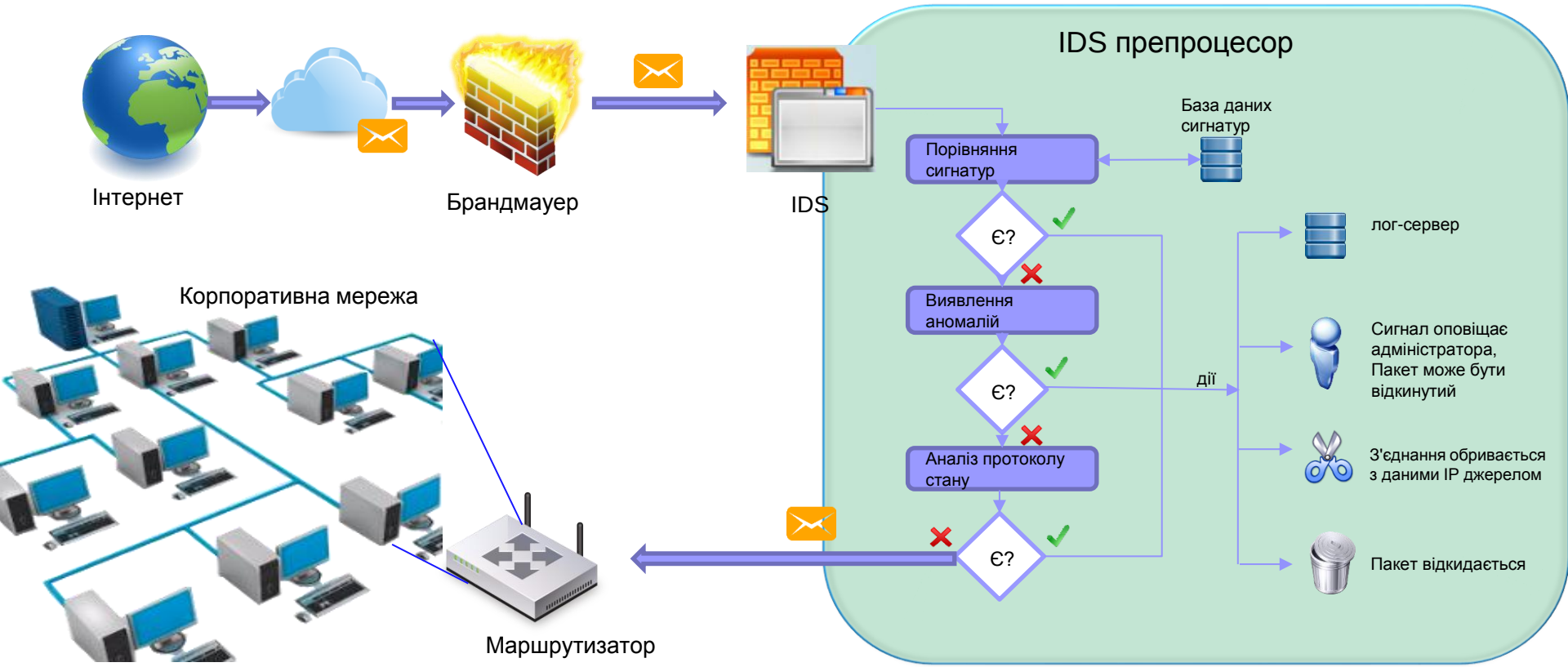
- Мультирівневий брандмауер з урахуванням стану об'єднує всі три типи брандмауерів
- Він фільтрує пакети на мережному рівні, визначає, чи є законною сесія, а також оцінює вміст запитів прикладного рівня



✓ Трафік фільтрується на трьох рівнях, базуючись на певному застосуванні, сесії і правилах фільтрації пакетів

✗ Заборонений трафік

Як працює система виявлення вторгнень (IDS)



Протоколи, що формують захищений канал на різних рівнях

Прикладний	HTTP/S, S/MIME	Непрозорі для застосувань, що не залежать від транспортної інфраструктури
Представлення	SSL/TLS	
Сеансовий		
Транспортний		
Мережний	IPSec	Прозорі для застосувань, залежать від транспортної інфраструктури
Канальний	PPTP	
Фізичний		

IPSec

- Сукупність механізмів IPsec забезпечує основу для захисту мережевого трафіку на IP-рівні, безпеки IP-пакетів, захищеної взаємодії мобільних систем з корпоративною мережею, реалізації віртуальних приватних мереж (Virtual Private Networks - VPN) і т.п. Ядро IPsec складають три протоколи: протокол автентифікуючого заголовка (Authentication Header, AH), протокол Інкапсуляції захисту вмісту (Encapsulating Security Payload, ESP) і протокол обміну ключами в мережі Інтернет (Internet Key Exchange, IKE). Функції з підтримки захищеного каналу передачі даних по мережах IP-розподіляються між цими протоколами наступним чином :
  - Протокол AH забезпечує цілісність IP-пакетів, аутентифікацію джерела даних, а також захист від відтворення раніше переданих IP-пакетів
  - Протокол ESP підтримує конфіденційність, аутентифікацію і цілісність IP-пакетів, а також частковий захист від аналізу трафіку
  - Протокол IKE дозволяє взаємодіючим сторонам автоматично генерувати і безпечно розподіляти симетричні секретні ключі

Контекст безпеки в IPSec

- Контексти безпеки (Security Associations) утворюють основу криптографічних сервісів безпеки на базі протоколів IPsec. Для захисту двостороннього зв'язку між вузлами мережі необхідні два контексти безпеки: один - для вхідних потоків, інший - для вихідних. Контексти безпеки містять інформацію про IP-адреси, типи захисного протоколу (AH або ESP), криптографічні алгоритми, ключі для аутентифікації і шифрування і періоді їх дії.
- **Контекст безпеки унікально ідентифікується трьома елементами**
  - Індексом параметрів безпеки (Security Parameters Index - SPI)
  - Цільовою IP-адресою
  - Ідентифікатором захисного протоколу

Протоколи SSL і TLS

- Протокол безпеки транспортного рівня (Transport Layer Protocol - TLS) забезпечує захист комунікацій між додатками, розробленими в архітектурі клієнт-сервер, в основному між веб-клієнтом і веб-сервером. Специфікація TLS базується на популярному протоколі Secure Socket Layer (SSL), розробленому корпорацією Netscape. Ці протоколи створювалися для забезпечення аутентифікації, цілісності та конфіденційності даних, якими обмінюються взаємодіють один з одним додатки. Обидва протоколи мають дворівневу організацію: протокол встановлення з'єднання (Handshake Protocol) і протокол передачі записів (Record Protocol).
- **Протокол встановлення з'єднання** дозволяє серверу та клієнту виконати взаємну аутентифікацію, узгодити застосовуваний алгоритм шифрування і криптографічні параметри перед тим, як протокол прикладного рівня почне передачу даних.
- **Протокол передачі записів** забезпечує захист протоколів більш високого рівня, включаючи протокол встановлення з'єднання. Протокол передачі записів залежить від надійності транспортного протоколу, такого як TCP.

Протоколи SSL і TLS

- Протоколи SSL і TLS незалежні від протоколів прикладного рівня, тому будь-який протокол прикладного рівня може прозоро оперувати поверх SSL і TLS. Протоколи SSL і TLS забезпечують три сервісу безпеки
  - Аутентифікацію (підтвердження ідентичності з'єднання: протокол встановлення з'єднання використовує сертифікати та верифікацію цифрових підписів для підтвердження ідентифікаційних ознак і повноважень віддаленої програми)
  - Цілісність (захист даних протоколу від несанкціонованої модифікації: протокол передачі записів використовує значення біта контролю цілісності для підтвердження того, що передані дані не змінювалися)
  - Конфіденційність (забезпечення секретності з'єднання: після узгодження симетричного ключа шифрування на основі протоколу встановлення з'єднання виконується шифрування даних, якими обмінюються сторони під час сеансу зв'язку)
- Протоколи SSL і TLS здатні підтримувати взаємну аутентифікацію сторін, але зазвичай на базі сертифіката виконується аутентифікація сервера клієнтом, а потім клієнт аутентифікується іншим способом, наприклад, вводячи за запитом сервера своє ім'я і пароль