1. Безпека мережі

1.1 Загрози безпеці

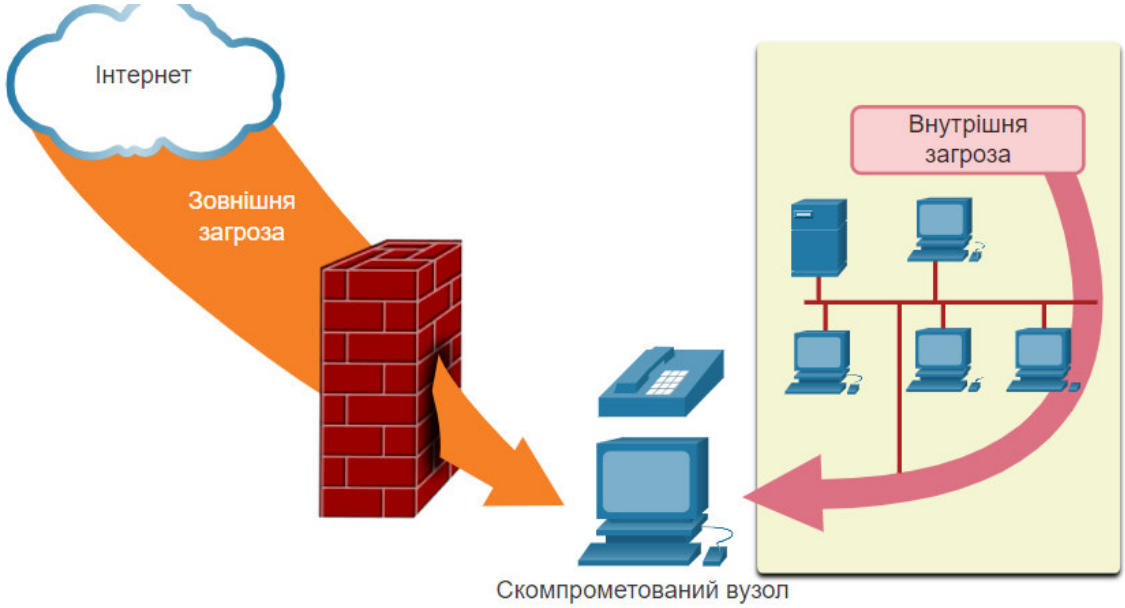
Без сумніву ви чули або читали новини про втручання до мережі компанії, і отримання зловмисниками доступу до особистої інформації тисяч клієнтів. З цієї причини безпека мережі завжди буде пріоритетним завданням для адміністраторів.

Мережна безпека є невід'ємною частиною комп'ютерних мереж, незалежно від того, чи це домашня мережа з єдиним каналом інтернет-зв'язку чи корпоративна мережа з тисячами користувачів. При забезпеченні мережного захисту потрібно брати до уваги середовище, а також інструменти та потреби мережі. Необхідно не лише захищати дані, але й зберегти якість обслуговування, на яку очікують користувачі мережі.

Безпека мережі передбачає використання протоколів, технологій, пристроїв, інструментів і методів, які захищають дані та пом'якшують наслідки загроз. Вектори загроз можуть бути зовнішніми або внутрішніми. Більшість зовнішніх загроз безпеці мережі сьогодні походять саме з інтернету.

Існує кілька поширених зовнішніх загроз для мереж:

- **Віруси, хробаки або троянські коні** - Шкідливе програмне забезпечення або код, запущений на пристрої користувача.
- **Шпигунська або рекламна програма** - Програми цього типу встановлюються на кінцевому пристрої і приховано збирають інформацію про користувача.
- **Атаки нульового дня** - Також відомі як атаки нульової години, виникають у перший день виявлення вразливості.
- **Напади зловмисника** - Зловмисник атакує пристій користувача або мережні ресурси.
- **Атаки з відмови в обслуговуванні** - Ці атаки сповільнюють роботу або зумовлюють відмову застосунків та процесів на мережному пристрої.
- **Перехоплення або крадіжка даних** - Ця атака захоплює приватну інформацію у мережі організації.
- **Крадіжка ідентичності** - Ця атака призначена для крадіжки облікових даних користувача з метою доступу до приватних даних.



Однаково важливо зважати на внутрішні загрози. Було проведено багато досліджень, які показали, що найпоширеніші втрати даних трапляються саме через внутрішніх користувачів мережі. Сюди можна віднести втрату або викрадення пристроїв, випадкові зловживання з боку працівників, а в бізнес-середовищі - навіть зловмисні наміри деяких працівників. Із розвитком стратегій BYOD, корпоративні дані стають дедалі вразливішими. Тому, як показано на рисунку. розробляючи політику безпеки, важливо вирішувати як зовнішні, так і внутрішні загрози безпеці.

1.2 Безпекові рішення

Не існує єдиного рішення, яке б захистило від різного роду наявних загроз. З цієї причини безпека повинна запроваджуватися на декількох рівнях, із використанням більш ніж одного рішення. Якщо один захисний компонент не зможе виявити загрозу та убезпечити мережу, іншим це може вдатися.

Зазвичай для захисту домашньої мережі достатньо базових рішень. Як правило, користувач запроваджує захист на кінцевих пристроях, а також у точці під'єднання до Інтернету, і навіть може покладатися на договірні послуги від Інтернет-провайдера.

Для домашньої або невеликої офісної мережі визначено такі основні компоненти безпеки:

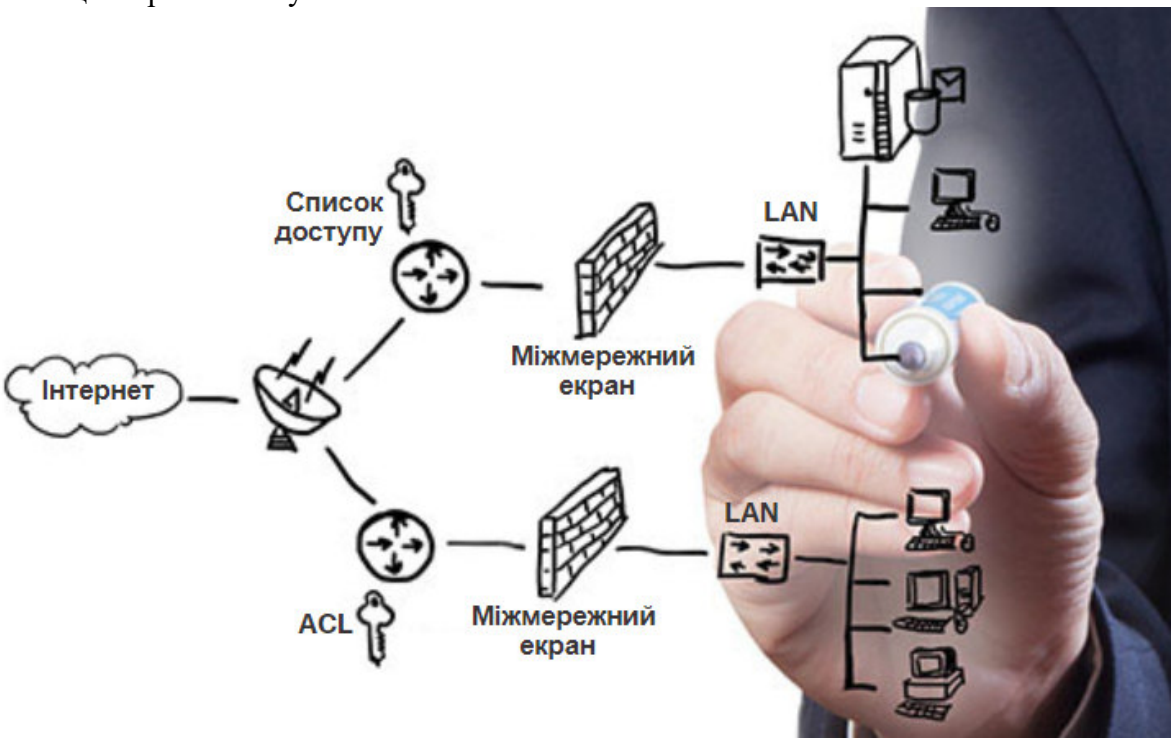
- **Антивірус і антишпигун** - Ці програми допомагають захистити кінцеві пристрої від ураження шкідливим програмним забезпеченням.
- **Фільтрування за допомогою міжмережного екрану** -Міжмережний екран (брандмауер, firewall) блокує несанкціоновані звернення, які надходять до мережі або ініціюються з неї. Може включати в себе систему брандмауера на основі вузла, яка запобігає неавторизованому доступу до кінцевого пристрою, або забезпечення базової фільтрації на домашньому маршрутизаторі, для попередження підозрілих звернень до мережі із зовнішнього світу.

На противагу цьому, реалізація захисту корпоративної мережі зазвичай передбачає використання багатьох компонентів, вбудованих у мережу для контролю та фільтрації трафіку. В ідеалі всі компоненти працюють разом, що мінімізує обслуговування та покращує безпеку. Великі корпоративні мережі використовують антивіруси, антишпигунські програми та фільтрування за допомогою міжмережних екранів, проте вони також вимагають інших засобів безпеки:

- **Спеціалізовані системи міжмережних екранів** - Забезпечують розширені можливості брандмауера, які здатні ретельніше фільтрувати велику кількість трафіку.
- **Списки контролю доступу (Access Control Lists, ACL)** - Додатково перевіряють звернення і потоки трафіку на основі IP-адрес і цільових застосунків.
- **Системи запобігання вторгненням (Intrusion Prevention Systems, IPS)** - Ідентифікують загрози, що швидко поширюються, такі як атаки нульового дня або нульові години.
- **Віртуальні приватні мережі (Virtual Private Networks, VPN)** - Забезпечують захищений віддалений доступ до ресурсів організації.

Вимоги щодо безпеки мережі повинні враховувати середовище, а також різні програми та обчислювальні потреби. Як для домашніх так і корпоративних мереж потрібно мати можливість захистити дані, зберігаючи якість обслуговування, на яку очікують користувачі мережі. Крім того, впроваджені заходи безпеки повинні адаптуватися до щораз більших та мінливих мережних тенденцій.

Вивчення загроз мережній безпеці та методів пом'якшення наслідків починається з чіткого розуміння основної інфраструктури комутації та маршрутизації, яка використовується для організації мережних служб.



1.3 *Питання для самоперевірки - Мережна безпека*

1. Яка атака призводить до сповільнення роботи або відмови обладнання та програм?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

2. Яке рішення створює безпечне з'єднання для віддалених працівників?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

3. Який засіб запобігає несанкціонованому доступу до вашої мережі?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

4. Який з варіантів описує мережну атаку, яка виникає у перший день виявлення уразливості?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

5. Який варіант описує шкідливий код, що запускається на пристроях користувача?

- ◯ Міжмережний екран
- ◯ Вірус, хробак або троянський кінь
- ◯ Нульовий день або нульова година
- ◯ Віртуальна приватна мережа (VPN)
- ◯ Відмова в обслуговуванні (DoS)

4. Який з варіантів описує мережну атаку, яка виникає у перший день виявлення уразливості?

Правильно!

- ○ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ◉ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)

5. Який варіант описує шкідливий код, що запускається на пристроях користувача?

Правильно!

- ○ Міжмережний екран
- ◉ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)

1. Яка атака призводить до сповільнення роботи або відмови обладнання та програм?

Правильно!

- ○ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ◉ Відмова в обслуговуванні (DoS)

2. Яке рішення створює безпечне з'єднання для віддалених працівників?

Правильно!

- ○ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ◉ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)

3. Який засіб запобігає несанкціонованому доступу до вашої мережі?

Правильно!

- ◉ Міжмережний екран
- ○ Вірус, хробак або троянський кінь
- ○ Нульовий день або нульова година
- ○ Віртуальна приватна мережа (VPN)
- ○ Відмова в обслуговуванні (DoS)