5

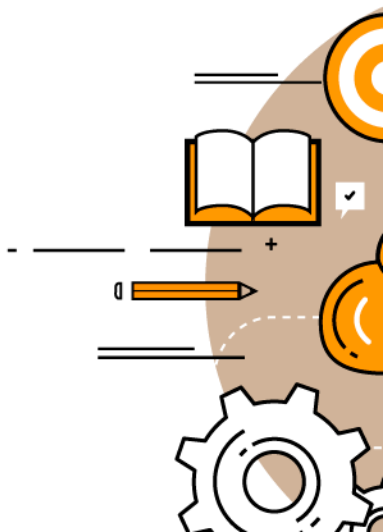
Основи інформаційної та кібербезпеки

Лекція 5.
Методи і технології захисту комп’ютерних мереж

1. Основні поняття та характеристики комп’ютерних мереж
2. Види мережевих атак
3. Методи протидії мережевим атакам
4. Захист інформації в мережах VPN

1 Основні поняття та характеристики комп’ютерних мереж

Комп’ютерна мережа — сукупність пристроїв, з’єднаних каналами передавання даних, для спільного користування апаратними, програмними та інформаційними ресурсами під керуванням спеціального програмного забезпечення.



1 Класифікація комп’ютерних мереж

1 Архітектура комп'ютерної мережі

Будь-яка комп’ютерна мережа характеризується своєю **архітектурою**, яка визначається її:

- **топологією**,
- **протоколами**,
- **інтерфейсами**,
- мережевими **технічними** і **програмними засобами**

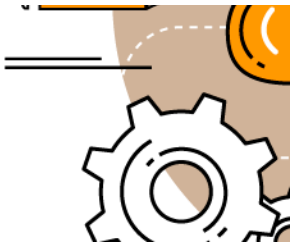
Топологія глобальних мереж характеризується достатньо складною, неоднорідною структурою.

топологія локальної мережі зазвичай має визначену структуру: лінійну, зіркову, кільцеву або деревоподібну.

1 Архітектура комп'ютерної мережі

Протоколами називають набір правил, що описують метод передачі інформації по мережі. Протоколи управляють форматом, часом передачі даних і виправленням помилок, що виникають при передачі.
Інтерфейси – це засоби сполучення функціональних елементів мережі.

В ролі функціональних елементів можуть виступати як окремі пристрої, так і програмні модулі. Відповідно до цього існують апаратні і програмні інтерфейси.



1 Архітектура комп'ютерної мережі

Під ***мережевими технічними засобами*** мають на увазі різноманітні пристрої, що забезпечують об’єднання комп’ютерів в єдину комп’ютерну мережу.

До цих пристроїв відносять мережеві контролери, вузли комутації тощо.

Мережеві програмні засоби керують роботою комп’ютерної мережі і забезпечують відповідний інтерфейс з користувачем.

До них належать мережеві операційні системи і допоміжні (сервісні) програми.

1 Модель OSI (Open Systems Interconnection)

Абстрактна **мережева модель** для комунікацій і розробки мережевих протоколів. Рівневий підхід до мережі.
Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.

Модель OSI

Дані	Рівень
Дані	**Прикладний** доступ до мережевих служб
Дані	**Представлення** представлення і кодування даних
Дані	**Сеансовий** керування сеансом зв'язку
Блоки	**Транспортний** безпечне та надійне з'єднання «точка - точка»
Пакети	**Мережевий** визначення маршруту та IP (логічна адресація)
Кадри	**Канальний** MAC та LLC (фізична адресація)
Біти	**Фізичний**

1 Модель OSI (Open Systems Interconnection)

Біти	**Фізичний**

Фізичний рівень – організовує передачу бітів по каналу передачі, визначає характеристики кабелів і роз'ємів, схеми кодування електричного або оптичного сигналу та ін. Функції фізичного рівня реалізує мережевий адаптер або послідовний порт.

Кадри	**Канальний** MAC та LLC (фізична адресація)

Канальний рівень – забезпечує надійну безпомилкову доставку даних у фізичній мережі.

На канальному рівні потік бітів між двома учасниками мережі поділяється на кадри (frame). Канальний рівень вирішує, хто може передавати дані в кожний момент часу, керує потоком даних (буферизацією) і контролює послідовність кадрів.

1 Модель OSI (Open Systems Interconnection)

Пакети	**Мережевий** визначення маршруту та IP (логічна адресація)

Мережевий рівень – забезпечує передачу даних між мережами. На цьому рівні знаходяться системи адресації учасників мереж і системи маршрутизації.

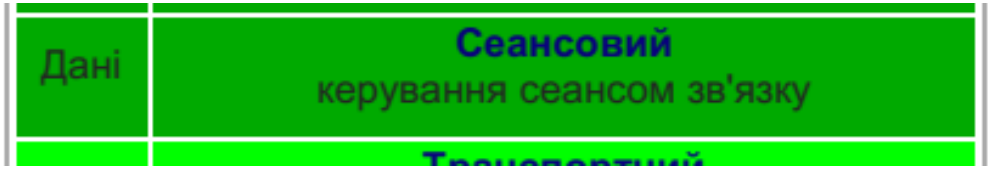
У **мережах з комутацією пакетів** мережевий рівень ділить потік даних на пакети, що незалежно маршрутизуються по мережі.

Приклади протоколів 3-го рівня: ARP (Address Resolution Protocol), IP (Internet Protocol), IPX (Internetwork Packet Exchange).

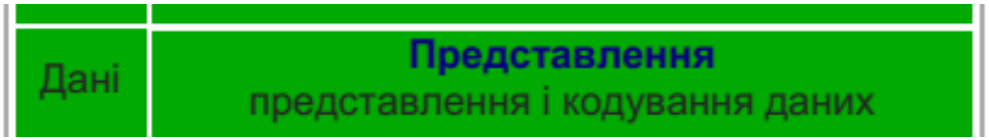
Блоки	**Транспортний** безпечне та надійне з'єднання «точка - точка»

Транспортний рівень – організовує інтерфейс системи, призначеної для користувача, з мережею передачі даних, відповідає за надійну передачу даних і розподіл обов'язків між учасниками мережі: SPX (Sequenced Packet Exchange), UDP (User Datagramm Protocol), TCP (Transmission Control Protocol)

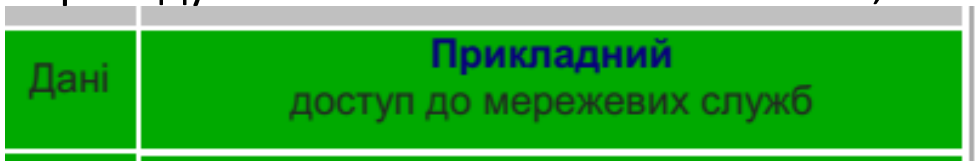
1 Модель OSI (Open Systems Interconnection)



Сеансовий рівень – призначений для організації діалогу між процесами. Основні функції рівня – обробка підключень (login) і відключень (logout), автентифікація, синхронізація. Приклад: NETBIOS (Network Basic Input/Output System), NETBEUI (Network Basic Extended User Interface).



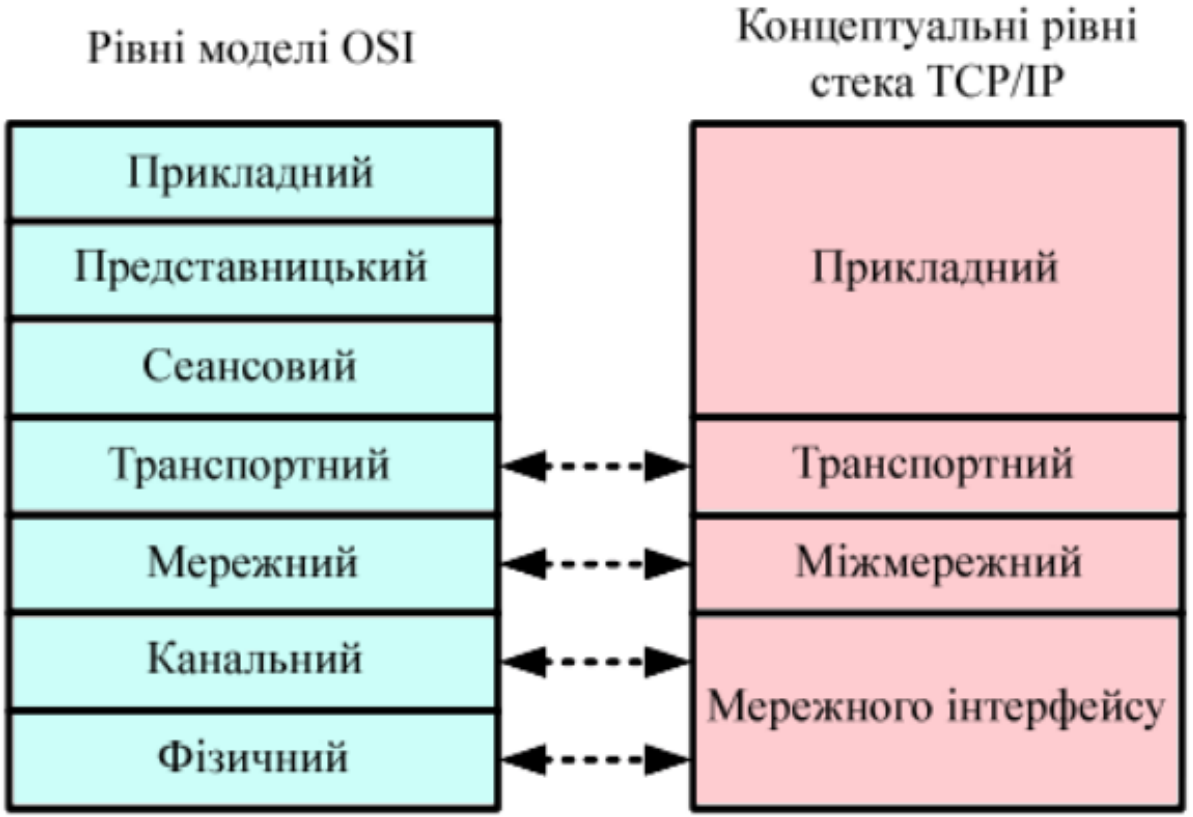
Презентаційний рівень – керує представленням інформації в мережі. Гарантує, що дані, якими обмінюються учасники, записані у форматі, який розуміють обидві сторони. Рівень має справу з наборами символів (character sets), форматами даних, кодуванням і упаковкою даних. Приклад: перекодування з KOI8-P в Windows 1251, SSL (Secure Socket Layer).



Прикладний рівень – інтерфейс між мережею і користувачем. Типові послуги, що надаються прикладним рівнем, – електронна пошта (X.400), передача файлів (FTP), веб-сервер (HTTP)

1 Модель TCP/IP

На даний час основним використовуваним стеком протоколів є **TCP/IP**, розробка якого не була пов'язана з моделлю OSI і до того ж була здійснена до її прийняття.



1 Прикладний рівень моделі TCP/IP

TCP (Transmission Control Protocol — протокол керування передаванням, відповідає за організацію сеансу зв'язку між двома комп'ютерами у мережі.

IP (Internet Protocol — міжмережний протокол) відповідає за маршрутизацію, тобто за те, щоб пакет було доставлено за певною адресою. За допомогою протоколу TCP ПК перевіряє, чи всі частини отримано. При отриманні всіх порцій TCP розміщує їх в потрібному порядку і збирає в одне ціле.

UDP (User Data Protocol), є ненадійним протоколом без встановлення з'єднання. Він також широко використовується в одноразових клієнт-серверних запитах і додатках, в яких оперативність важливіша за акуратність, наприклад, при передачі мови і відео.

1 Прикладний рівень моделі TCP/IP

Він містить всі **протоколи високого рівня**:

HTTP (Hyper Text Transfer Protocol) — протокол передачі гіпертексту. Використовують при пересиланні Web-сторінок з одного комп'ютера на інший.

FTP (File Transfer Protocol) — протокол передачі файлів зі спеціального файлового сервера на комп'ютер користувача.

POP (Post Office Protocol) — стандартний протокол поштового з'єднання. Сервери POP опрацьовують вхідну пошту, а протокол POP призначено для опрацювання запитів на отримання пошти від клієнтських поштових програм.

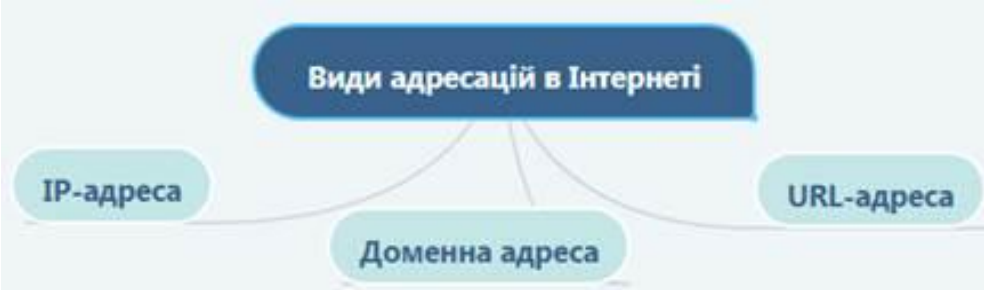
SMTP (Simple Mail Transfer Protocol) — протокол, який задає набір правил для передавання пошти.

Telnet — протокол віддаленого доступу, що дає можливість працювати на будь-який ЕОМ мережі Інтернет, як на своїй власній, тобто запускати програми, змінювати режим роботи тощо.

DNS (Domain Name Service – служба імен доменів), яка дозволяє перетворювати імена хостів в мережеві адреси

……

1 IP- адресація



IP-адреса — це ідентифікаційний номер комп’ютера в мережі. Як і в локальній мережі, IP-адреса комп’ютера в Інтернеті створюється за протоколом **IPv4** та складається з чотирьох десяткових чисел від 0 до 255, розділених крапками, наприклад 78.111.176.233.

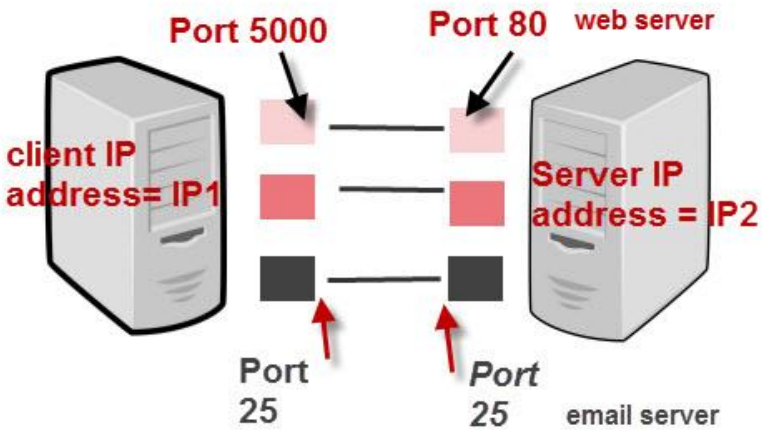
IPv6. За ним IP-адреса записується вісьмома шістнадцятковими числами, розділеними двокрапками, наприклад 011:0db2:11d3:087f:07a0:345e:8a2e:32c2.

1 Порти

Відправником і одержувачем даних, які передаються через мережу, з погляду транспортного рівня, є застосування (процес). Як будь-яка програма, процеси створюються і знищуються, на кожному вузлі може виконуватися декілька процесів, а кожен процес може мати декілька пунктів підключення до мережі.

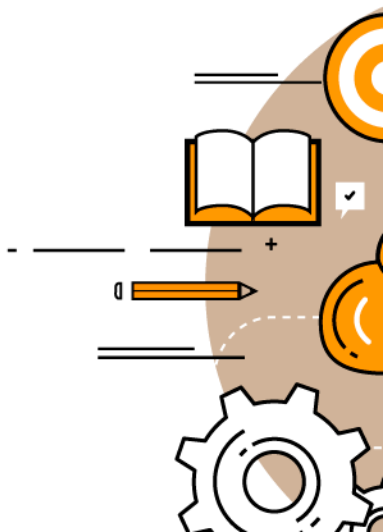
Такі логічні пункти (програмно організовані, як правило, у вигляді черг повідомлень) називаються **портами** (**port**). Номер порту однозначно ідентифікує процес.

Всі порти розділені на три діапазони - загальновідомі (або системні, 0-1023), зареєстровані (або призначені для користувача, 1024-49151) і динамічні (або приватні, 49152-65535).



IP Address + Port number = Socket

TCP/IP Ports And Sockets



2 Види мережевих атак

Найбільша кількість атак найчастіше реалізується на п’яти рівнях (**фізичний, канальний, мережний, транспортний, прикладний**).

Загрози на сеансовому та представницькому рівнях пов’язані, в першу чергу, з процедурами ідентифікації, автентифікації та шифрування, алгоритми і протоколи яких реалізовані в операційних системах і вплив на роботу яких з боку адміністраторів мереж мінімальний.

2 Атаки фізичного рівня

Атаками фізичного рівня на такі об’єкти, як канали передачі даних, є

- фізичне пошкодження;
- несанкціоновані зміни у функціональному середовищі;
- вимкнення фізичних каналів передачі даних;
- постановка шумів по всій полосі пропускання каналу

Найбільш захищеним рішенням є використання **оптичного кабелю**

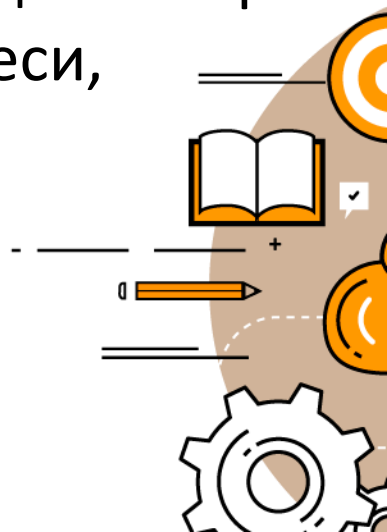
Єдиною можливістю захисту від несанкціонованого доступу до інформації при використанні інших ліній зв’язку є шифрування даних

2 Мережеві атаки

Активні атаки включають у себе явний вплив на систему, який змінює її стан.

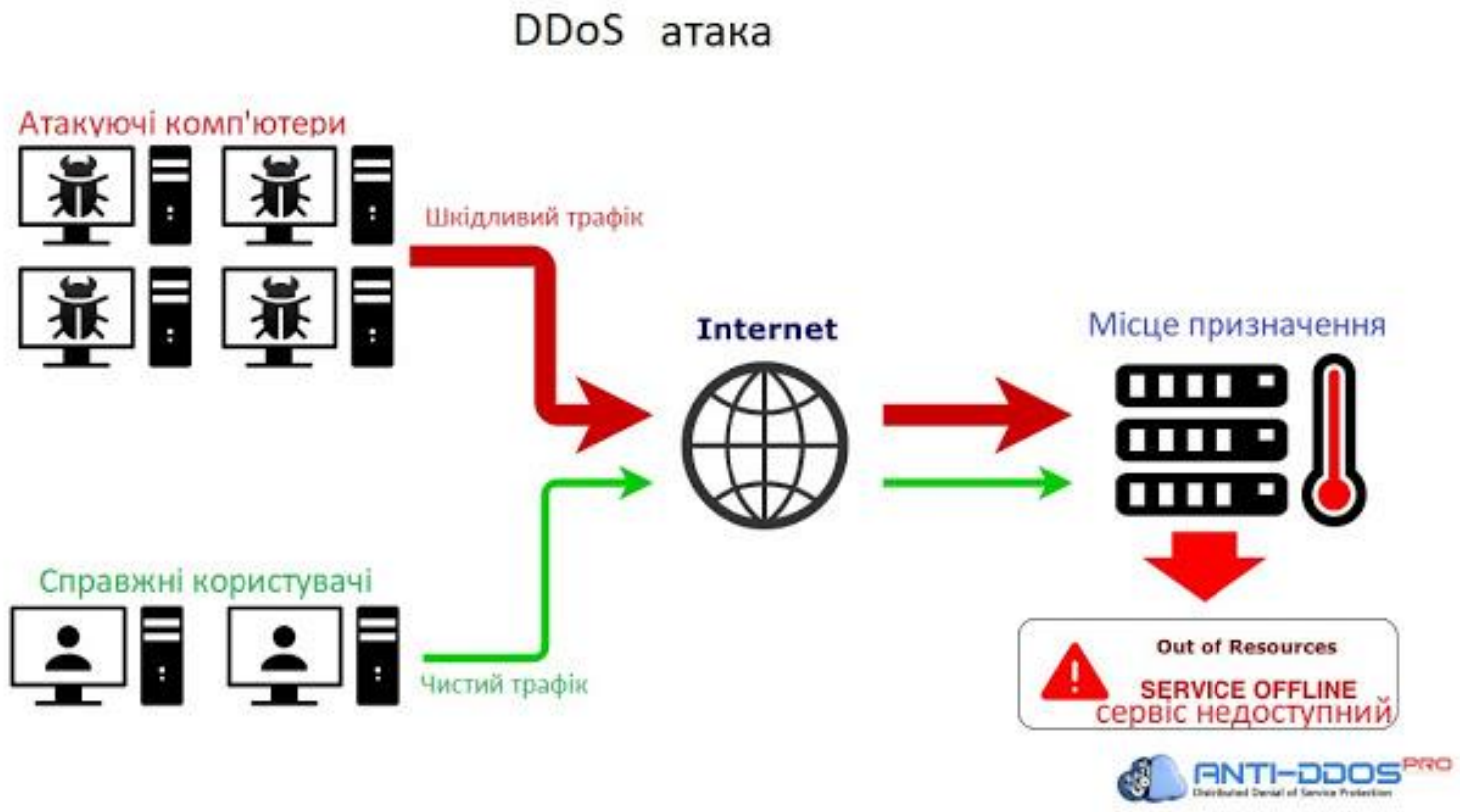
Пасивні атаки не порушують нормальну роботу системи: вони пов'язані зі збором інформації про систему.

Гібридні - етап збору інформації про цільову систему, а потім активне втручання в її роботу. До корисної для хакера інформації відносяться типи ОС і додатків, IP-адреси, номера портів, імена і паролі користувачів.



2 Мережеві атаки (активні)

Відмова в обслуговуванні і розподілена атака відмови в обслуговуванні (*DoS attack, DDoS attack*)

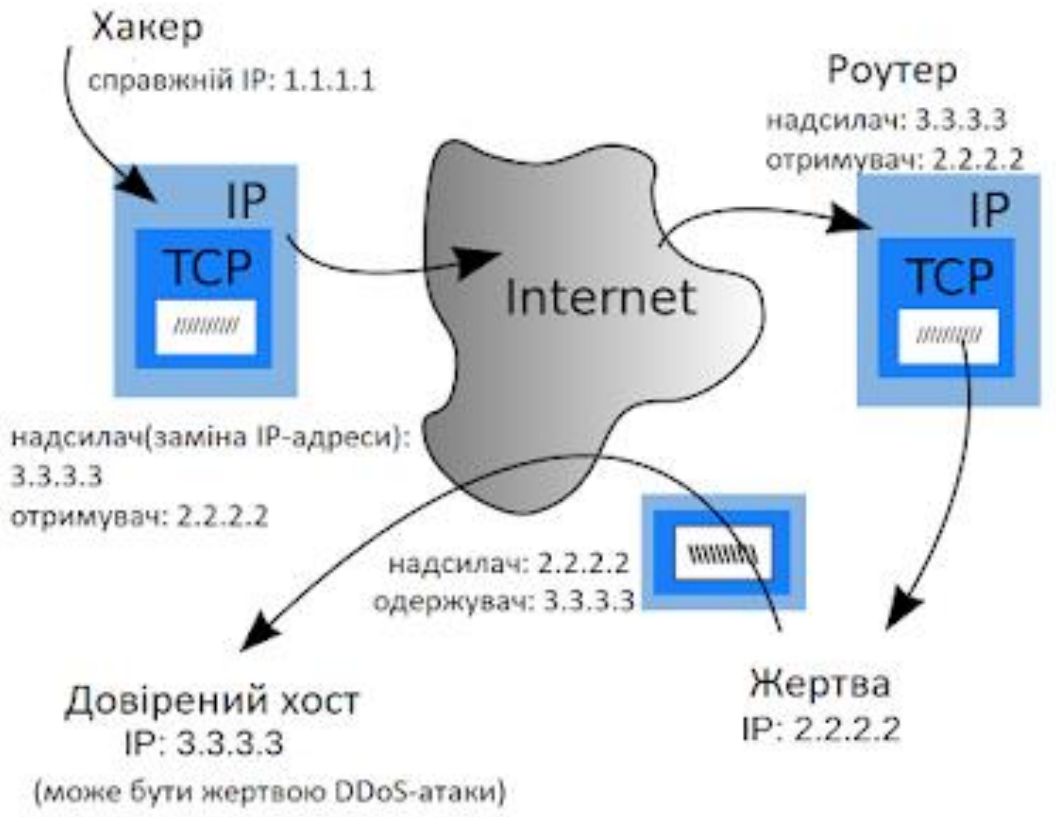


2 Мережеві атаки (активні)

Спуфінг (*підміна вмісту пакетів, spoofing*)

Коли хакер прагне приховати реальне місце розташування в Інтернеті того місця, звідки запитуються або куди відправляються дані користувача / жертви, то зазвичай використовується спуфінг з підміною IP-адреси.

Мета IP-спуфінгу полягає в тому, щоб змусити комп'ютер жертви думати, що інформація, що відправляється шахраєм користувачеві, виходить з надійного джерела, що дозволяє шкідливому контенту доходити до користувача.



2 Мережеві атаки (активні)

Впровадження шкідливих програм

(*malware - malicious software*)

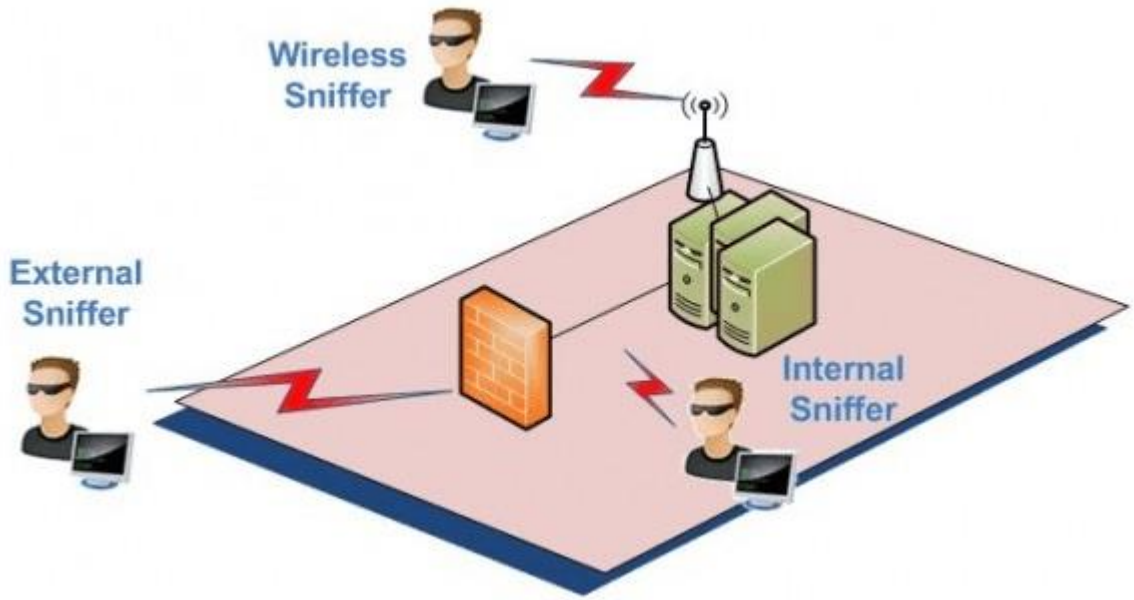
2 Мережеві атаки (активні)

Фішинг (*спроба оманливим шляхом отримати від вас особисту інформацію в Інтернеті*)

2 Мережеві атаки (пасивні)

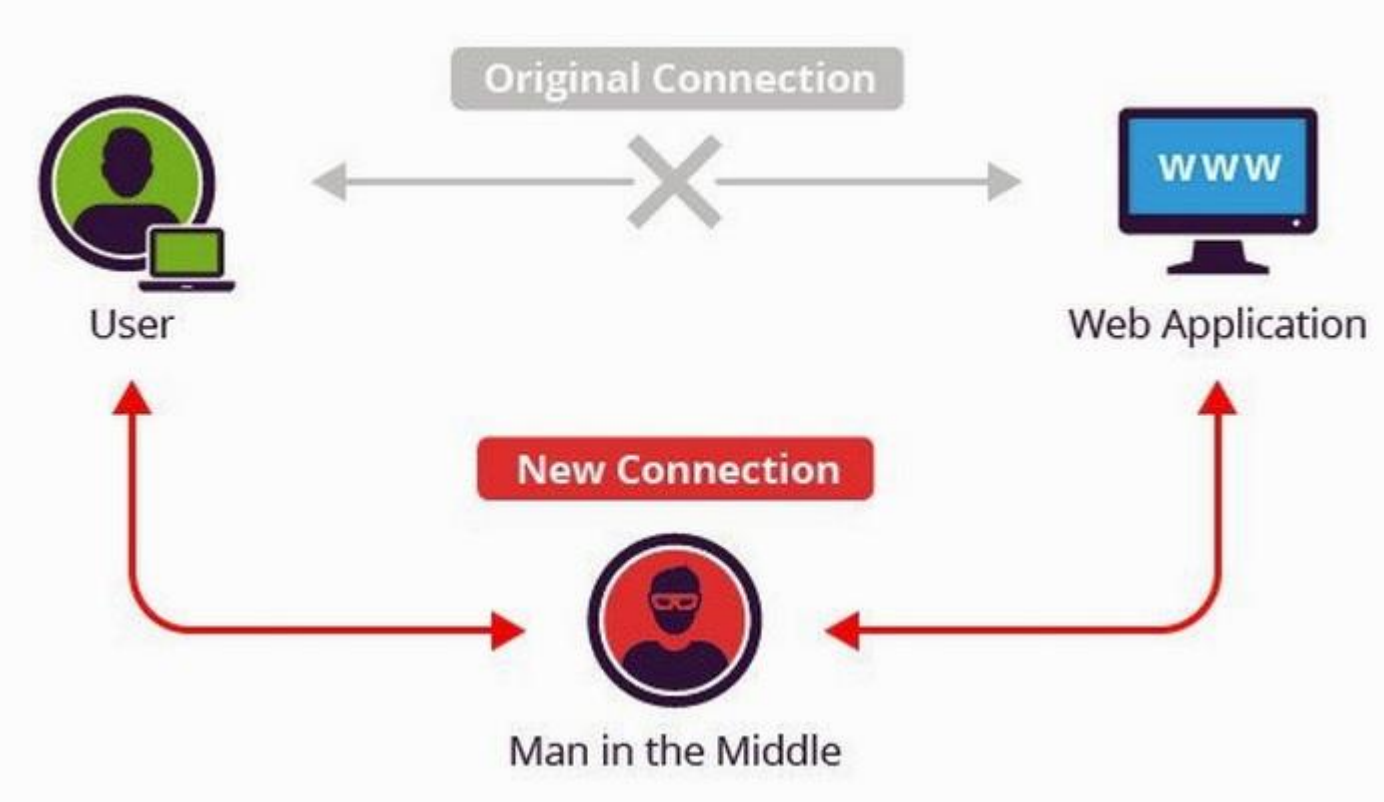
Сніфери пакетів (*програми, які перехоплюють весь мережевий трафік*)

Telnet
Rlogin
HTTP
SMTP
NNTP
POP
FTP
IMAP



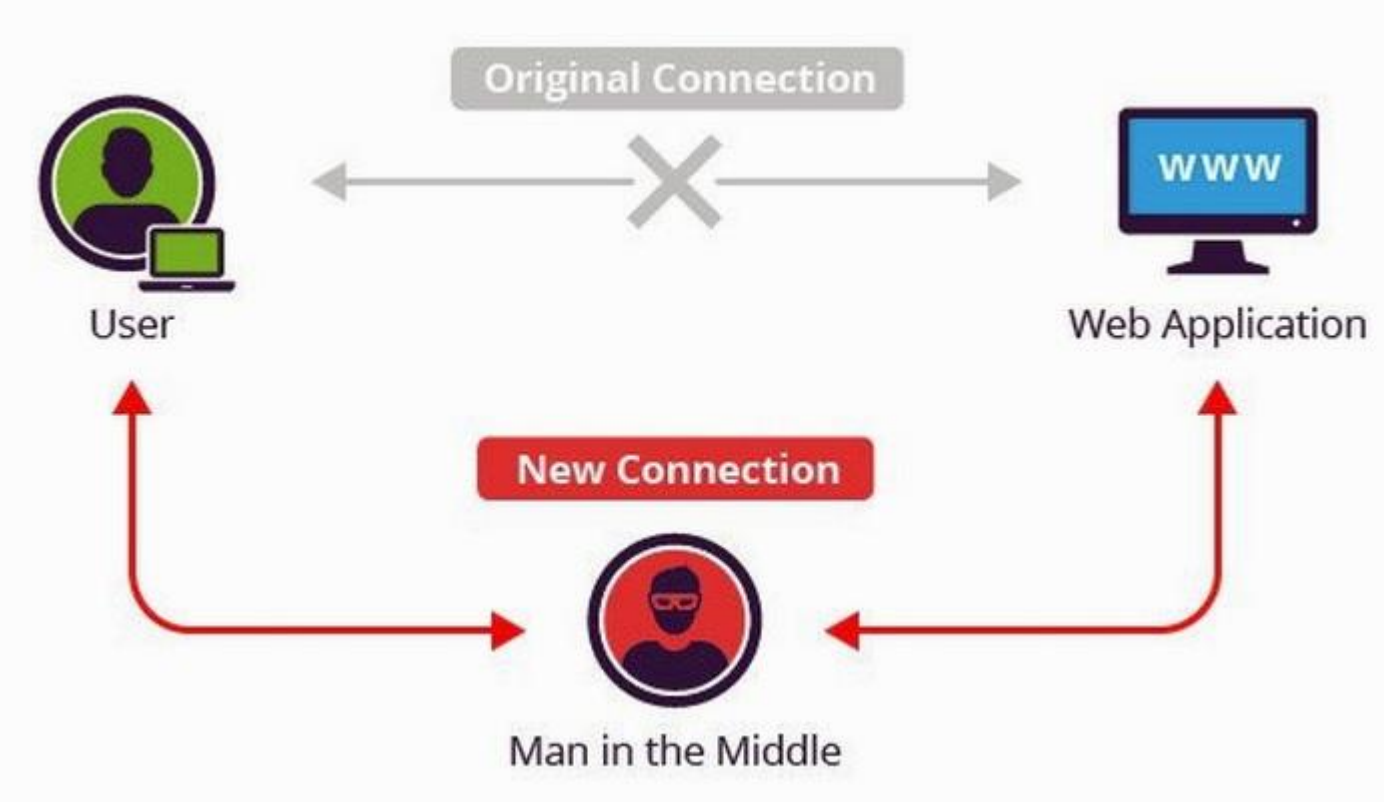
2 Мережеві атаки (пасивні)

Атаки Man-in-the-Middle (*доступ до пакетів, що передаються по мережі)*



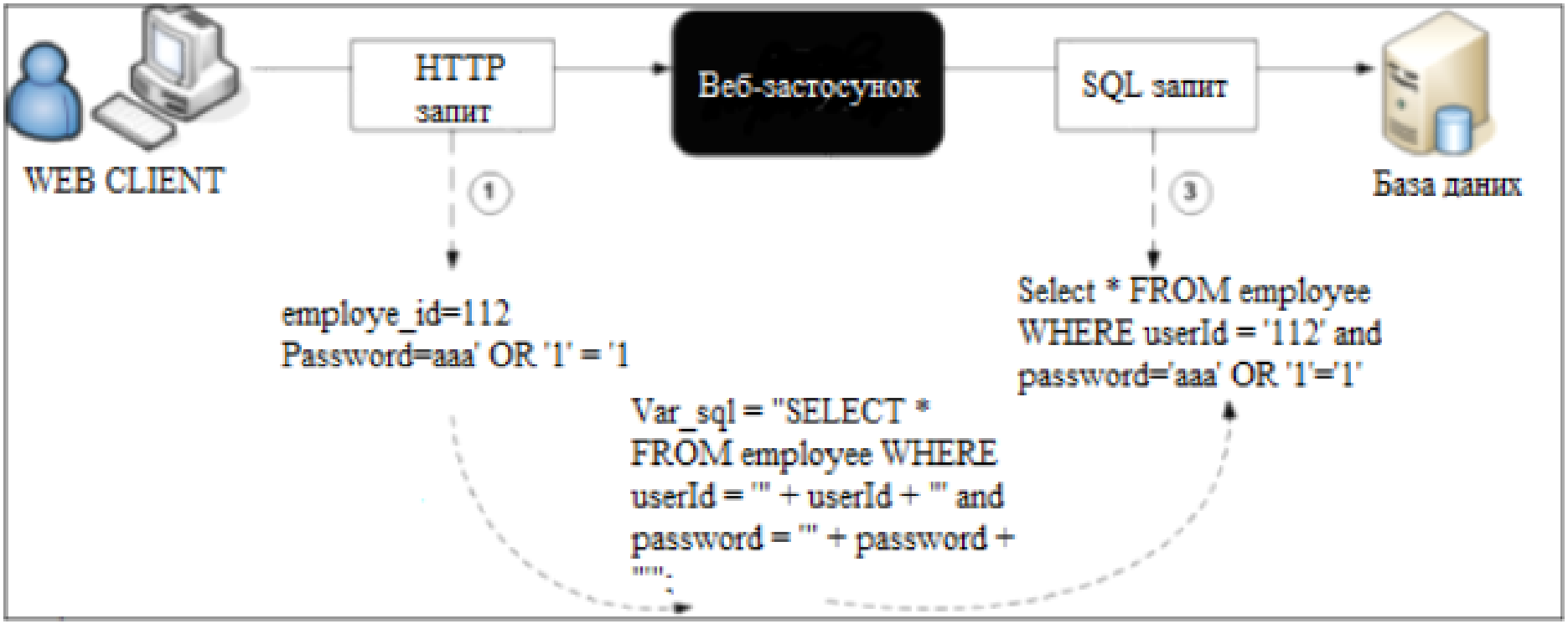
2 Мережеві атаки (пасивні)

Атаки Man-in-the-Middle (*доступ до пакетів, що передаються по мережі)*



2 Мережеві атаки (пасивні)

SQL-ін’єкція (*злом сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.)*



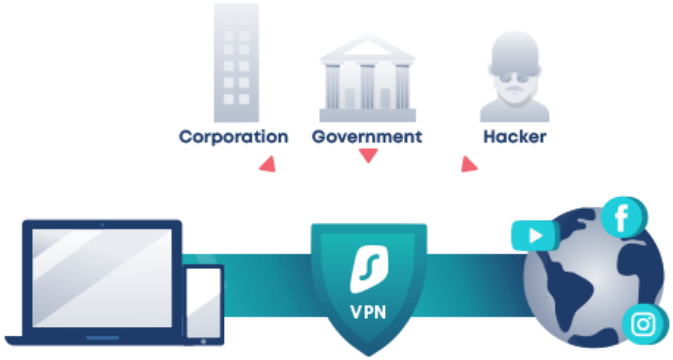
3 Методи протидії мережевим атакам

Антивірусна програма (антивірус)

Міжмережевий екран (брандмауер, файрвол англ. Firewall)

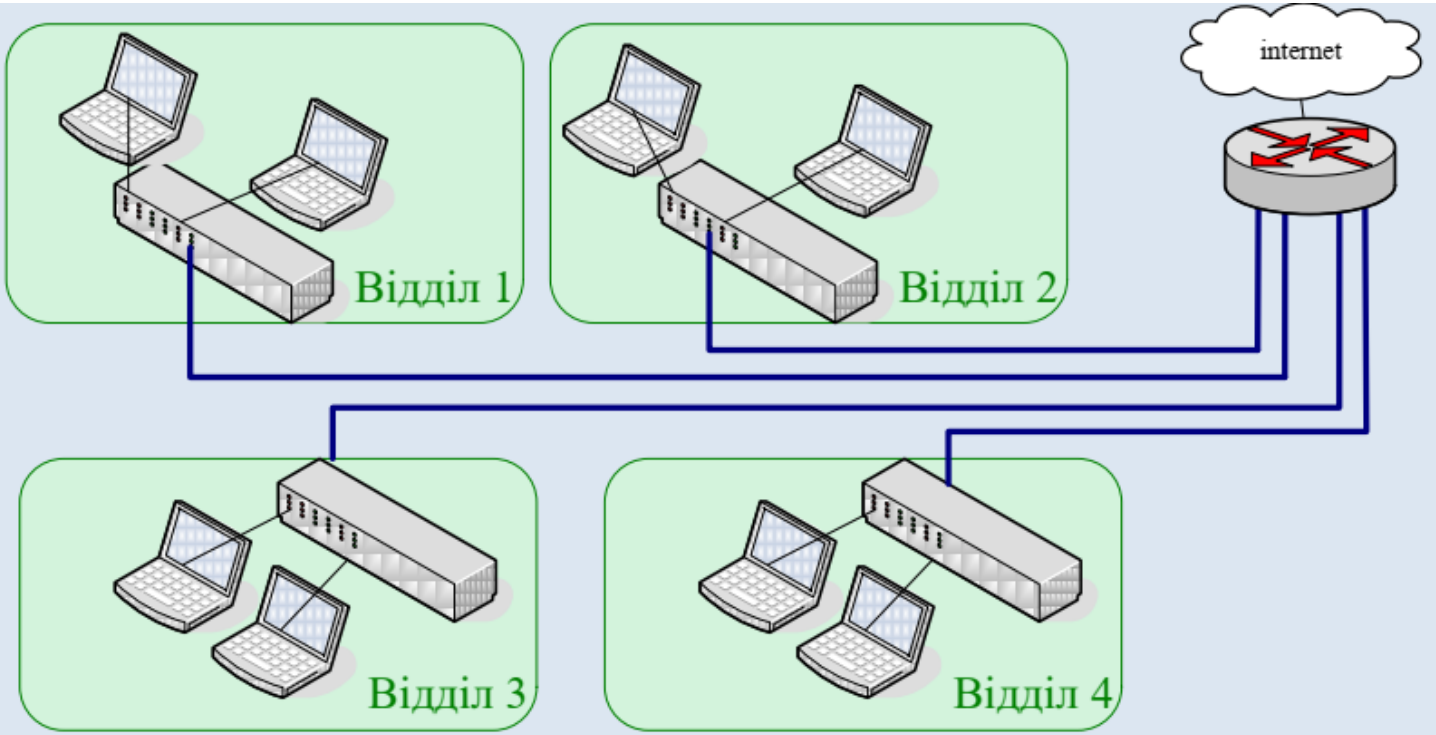
VPN (Virtual Private Network — віртуальна приватна мережа)

Secure Shell, SSH («безпечна оболонка»)



3 VLAN – віртуальні локальні мережі

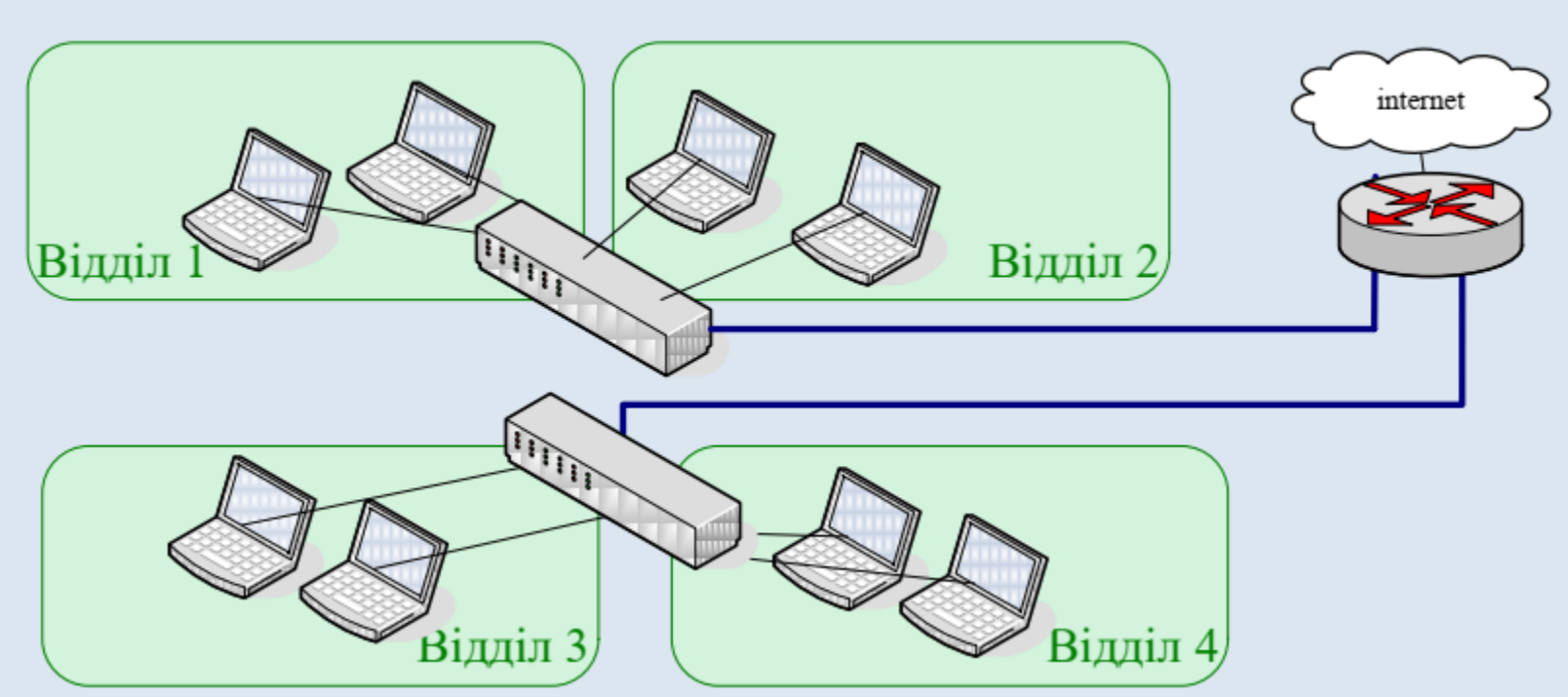
Фізична сегментація мережі



Кожний відділ (робоча група) має свій комутатор, який підключено до маршрутизатора.
Таке рішення підходить для невеликих компаній з незмінною структурою.
Не дозволяє легко змінювати склад робочих груп, та переналаштовувати доступ

3 VLAN – віртуальні локальні мережі

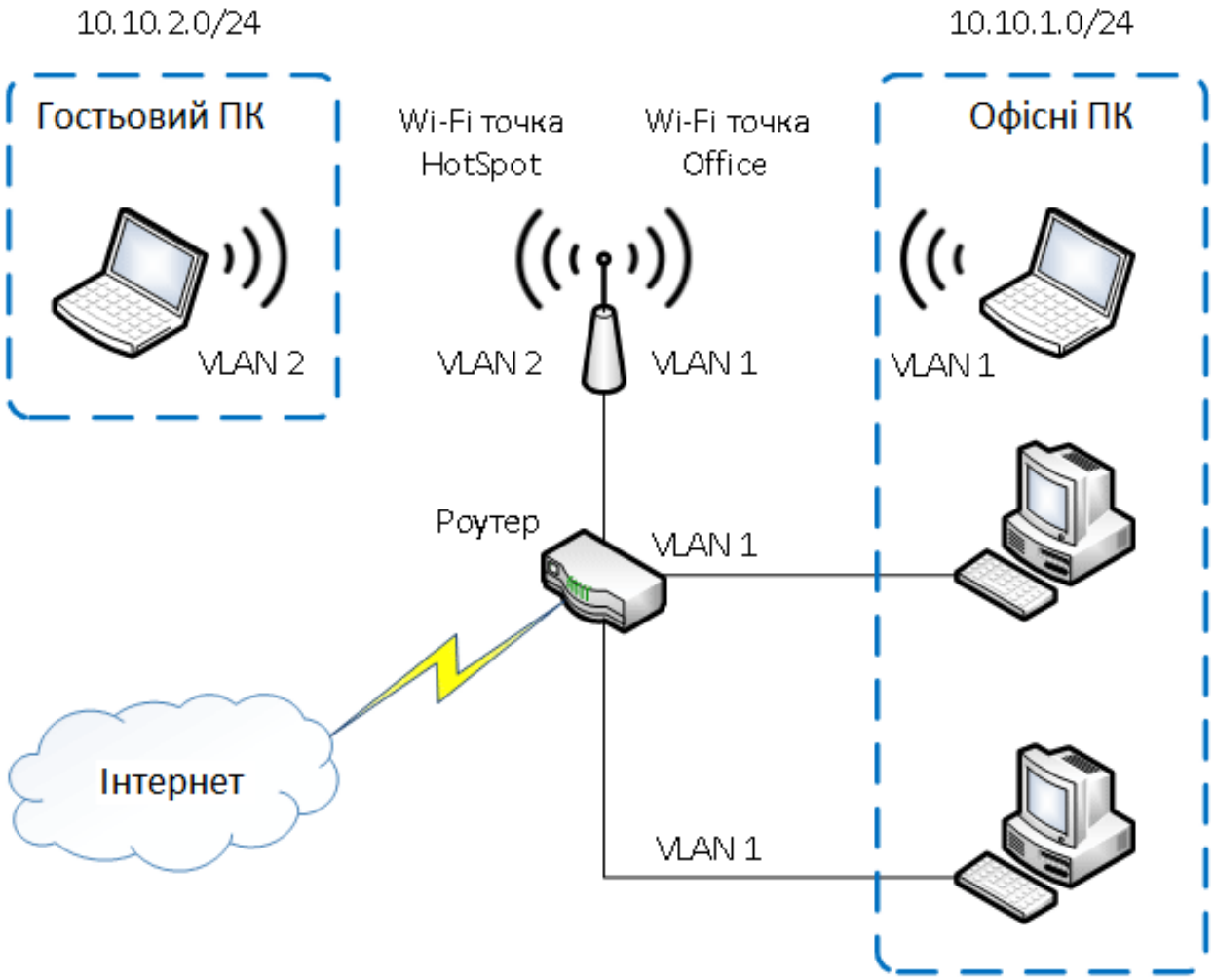
Логічне групування VLAN



- Декілька відділів можуть бути підключені до одного комутатора
- Сегментація логічна, задається програмно, отже легко переналаштовується
- Зменшується кількість портів маршрутизатора

3 VLAN – віртуальні локальні мережі

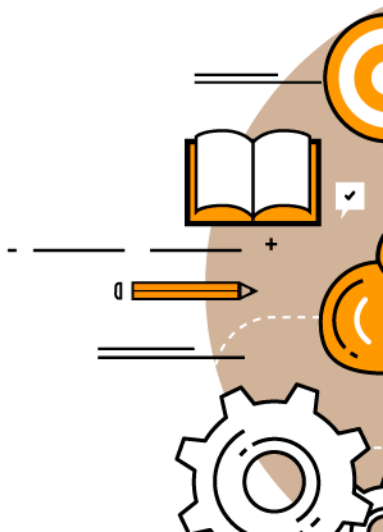
Розділення мереж



3 VLAN – віртуальні локальні мережі

Типи VLAN

- на основі портів;
- на основі стандарту IEEE 802.1Q;
- на основі стандарту IEEE 802.1ad (Q-in-Q VLAN);
- на основі портів та протоколів IEEE 802.1v;
- на основі MAC-адрес:
  - Функція асиметричні VLAN.
  - Функція Traffic Segmentation.



3 Технологія міжмережевих екранів

Міжмережевий екран (firewall, брендмауер) – це локальний (однокомпонентний або функціонально розподілений) програмний та/або апаратний засіб (комплекс), який реалізує контроль за інформацією, яка потрапляє до ІКС та/або виходить з ІКС.

МЕ - один з найбільш ефективних засобів захисту мережі від НСД, вірусних і DOS (або DDoS) атак.

МЕ часто визначають як набір засобів, що існують для заборони небажаного доступу в локальну мережу або просочування інформації з мережі.
Зазвичай екран не є симетричним. Для нього визначені поняття вхідна і вихідна інформація.

3 Технологія міжмережевих екранів

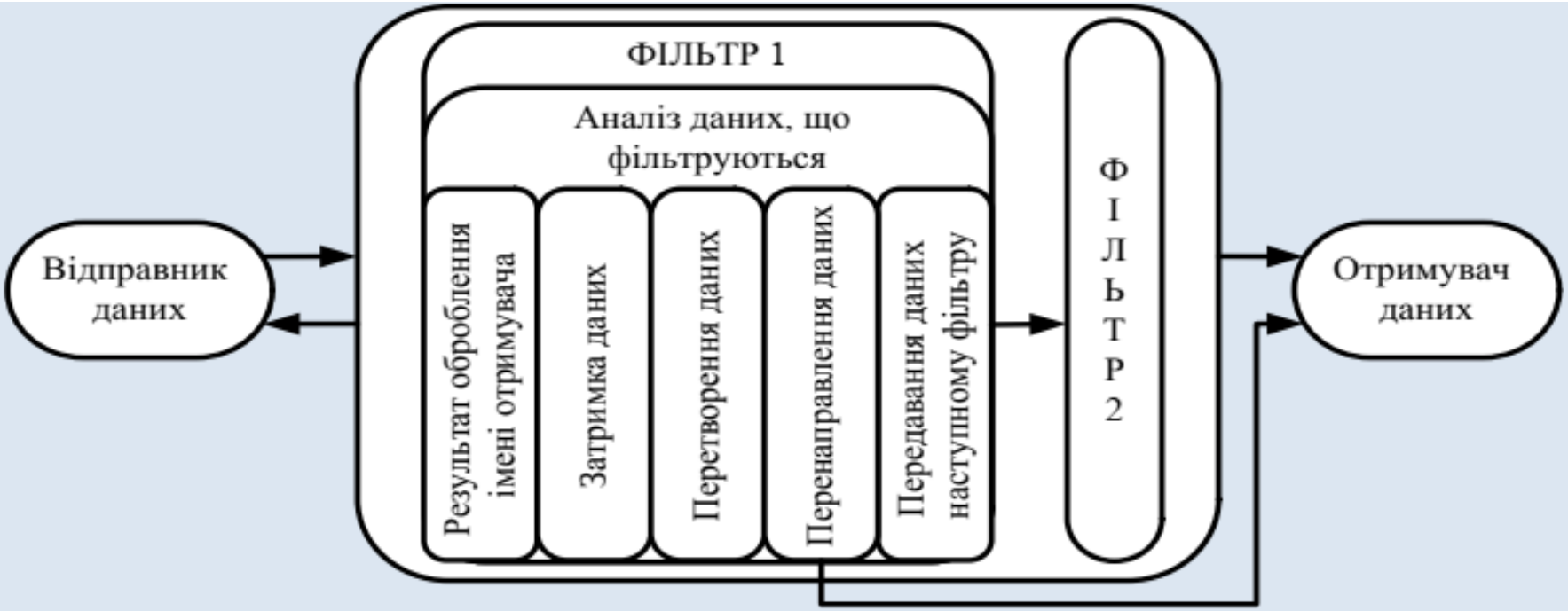
Завдання **екранування** - захист внутрішньої області від неконтрольованої і потенційно небезпечної зовнішньої.

МЕ забезпечує захист ІКС шляхом **фільтрації** інформації – тобто її аналізу за сукупністю критеріїв та прийняття рішення про її розповсюдження в/з ІКС на основі заданих правил, проводячи таким чином розподіл доступу суб'єктів з однієї ІКС до об'єктів іншої.

Правила фільтрації – це перелік умов, за якими з використанням заданих критеріїв фільтрації здійснюється дозвіл або заборона подальшої передачі пакетів (даних) і перелік дій, що проводяться МЕ для реєстрації і/або здійснення додаткових захисних функцій

3 Технологія міжмережевих екранів

Багатоетапна ідентифікація запитів, що надходять в мережу



3 Класифікація міжмережевих екранів

3 Класифікація міжмережевих екранів

Пасивні

Виконують фільтрацію пакетів, виконуючи над ними такі операції

- Allow - пропустити пакет далі
- Deny Drop - відкинути пакет (повторне надсилання)
- Reject - пакет відкидається, але - відправникові повідомляється по протоколу ICMP про недоступність сервісу на комп'ютері-одержувачі

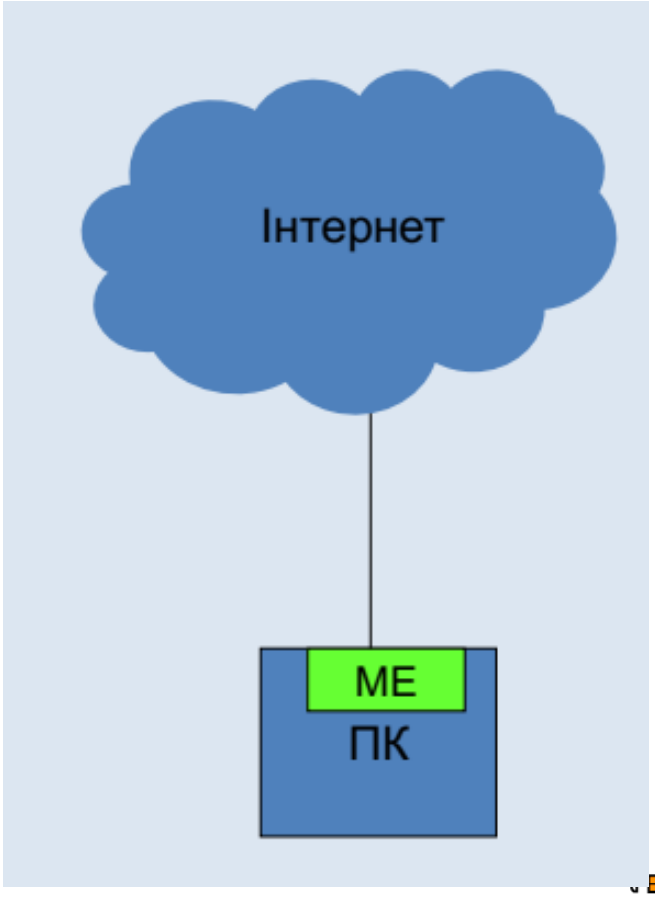
Активні

виконують **фільтрацію пакетів**, а також залежно від встановлених правил видають повідомлення для інших систем, в результаті чого можуть навіть переписуватись правила міжмережевого екрану

3 Класифікація міжмережевих екранів

Програмні

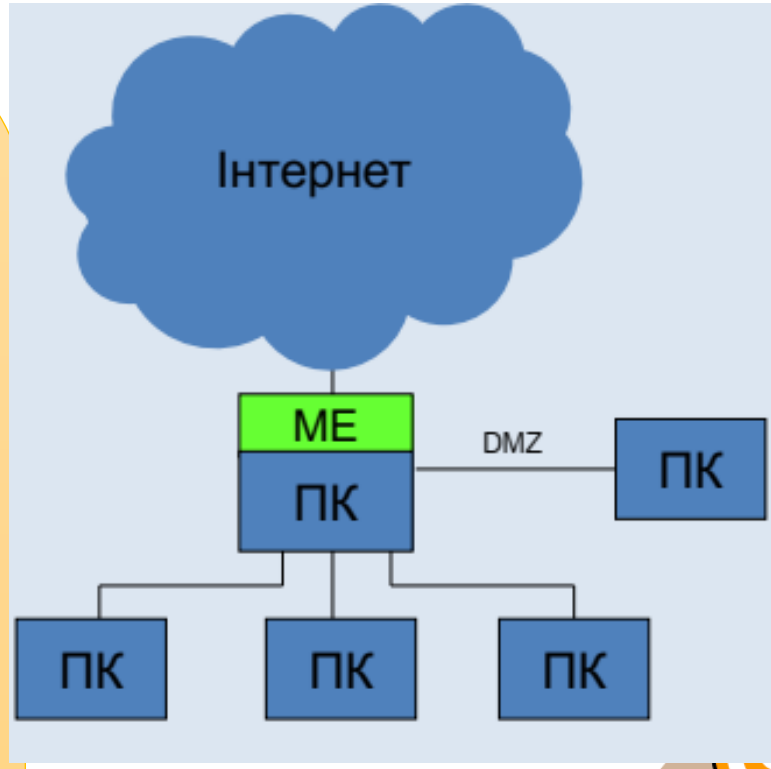
- Програмне забезпечення, яке захищає ЛИШЕ цей комп'ютер (персональні МЕ).
- Багато ОС мають вбудовані програмні МЕ.
- Є комерційні версії, проте є багато безкоштовних чи умовно-безкоштовних продуктів
- Мають гірші показники швидкодії



3 Класифікація міжмережевих екранів

Програмно-апаратні

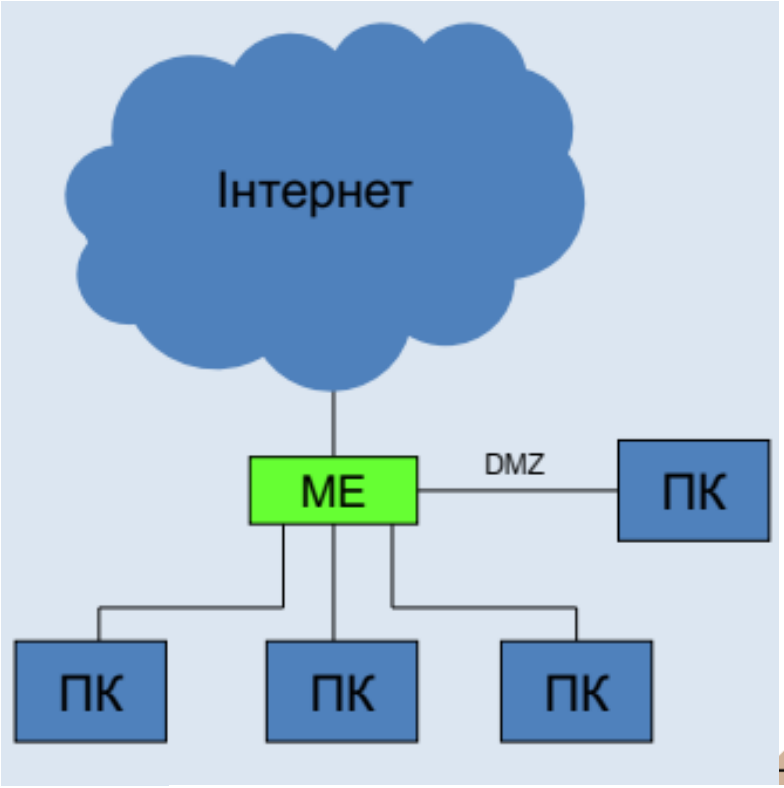
- Програмно-апаратні МЕ розташовуються між Інтернетом та ПК
- Зазвичай це спеціалізовані ОС, які реалізують функції МЕ, та додаткові захисні функції, що доцільно розміщувати на межі з Інтернет (IDS).
- Захищає всі комп'ютери, що знаходяться за ним.
- Багато з них дозволяють формувати DMZ
- Можуть виконувати трансляцію адрес (NAT).
- Потребують висококваліфікованого адміністратора.
- Реалізуються на базі серверних ПК.
- Мають достатньо високу продуктивність



3 Класифікація міжмережевих екранів

Апаратні

- Апаратні МЕ розташовуються між Інтернетом та ПК.
- Захищає всі комп'ютери, що знаходяться за ним.
- Багато з них дозволяють формувати DMZ
- Можуть виконувати трансляцію адрес (NAT).
- Вартість достатньо висока
- Мають високу продуктивність



3 Класифікація міжмережевих екранів

Три **рівні функціональності** МЕ:

1. **Пакетні фільтри**, або екрануючі маршрутизатори, — функціонують переважно на третьому (мережному) рівні моделі взаємодії відкритих систем (OSI); як правило, аналізують також інформацію із заголовків протоколів четвертого (транспортного) рівня.
2. **Шлюзи сеансового рівня**, які ще називають екрануючим транспортом, — функціонують здебільшого на п'ятому (сеансовому) рівні моделі OSI.
3. **Прикладні, або екранні шлюзи** — функціонують на прикладному рівні моделі OSI.

Мережні екрани, що реалізують функціональність якогось із рівнів, зазвичай реалізуютьфункціональність нижчих рівнів.

3 Класифікація міжмережевих екранів

Пакетні фільтри

Апаратним мережевим фільтром є маршрутизатор, який оброблює пакети на підставі інформації, що міститься в заголовках пакетів (Списки ACL).

Маршрутизатори Cisco, Nortel тощо мають функції мережевої фільтрації.

Програмні мережеві фільтри – це, в більшості, безкоштовні або умовнобезкоштовні утиліти, що реалізовані для ряду мережевих платформ.

При обробці пакетів враховується такі дані:

– IP-адреса відправника;

– IP-адреса одержувача;

– протокол (TCP, UDP, ICMP);

– номер програмного порту відправника;

– номер програмного порту одержувача.

Адміністратор задає правила.

3 Класифікація міжмережевих екранів

Шлюзи сеансового рівня

Шлюзи сеансового рівня призначені для здійснення контролю за віртуальними з'єднаннями і трансляції IP-адрес (Network Address Translation, **NAT**) під час взаємодії із зовнішньою мережею.

Захисні функції шлюзів сеансового рівня є посередницькими. Наприклад, такий шлюз може удавати, що з'єднання встановлюється з одним із його власних TCP-портів, тоді як насправді він згідно із своїми настроюваннями ініціює з'єднання з портом іншого комп'ютера (як правило, всередині захищеної мережі), після чого передає дані в обох напрямках.

Для комп'ютера-ініціатора з'єднання виглядатиме так, ніби він працює з сервісом на самому МЕ.

Головна перевага таких МЕ полягає в наявності можливості приховати внутрішню структуру захищеної мережі.

3 Класифікація міжмережевих екранів

Прикладний шлюз

Прикладні шлюзи, або МЕ прикладного рівня, працюють як проксі-сервери протоколів прикладного рівня (HTTP, FTP, Telnet тощо). Їхні функції, як і функції шлюзів сеансового рівня, — посередницькі. Але, на відміну від шлюзу сеансового рівня, такий МЕ містить у собі не лише транслятор з'єднань, а й сервери прикладних протоколів. Забезпечує такі додаткові функції захисту:

♦ ідентифікація й автентифікація користувачів за спроби встановити з'єднання через МЕ;

♦ перевірка достовірності інформації, яку передають через МЕ; розмежування доступу до ресурсів мереж;

♦ фільтрація й перетворення потоку повідомлень (наприклад, антивірусні й антиспамові перевірки, шифрування й дешифрування);

♦ реєстрація подій, реагування на події, аналіз зареєстрованої інформації, генерування звітів;

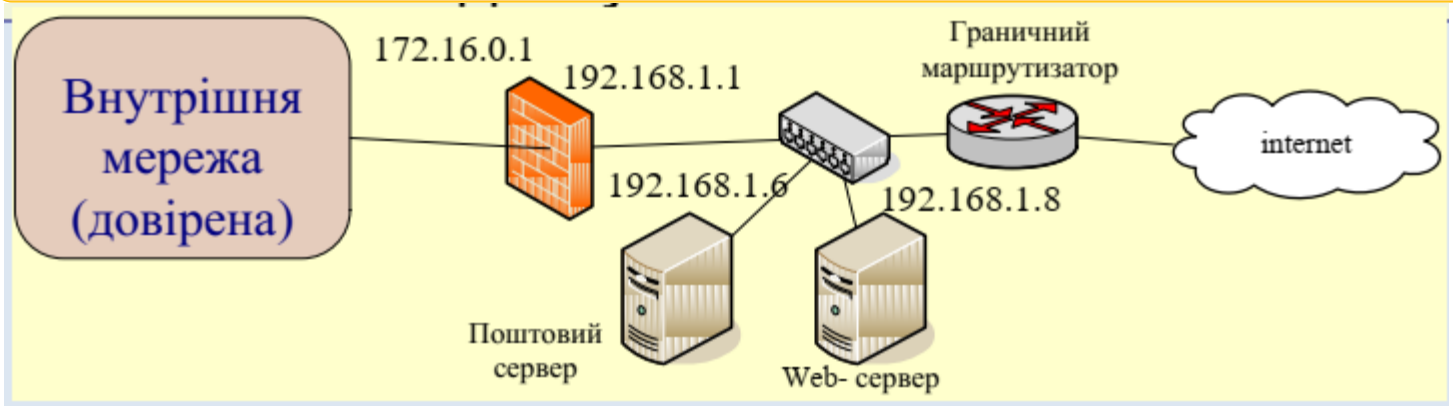
♦ кешування даних, що надходять із зовнішньої мережі.

3 Класифікація міжмережевих екранів

Прикладний шлюз

3 Сегментація мережі на базі МЕ

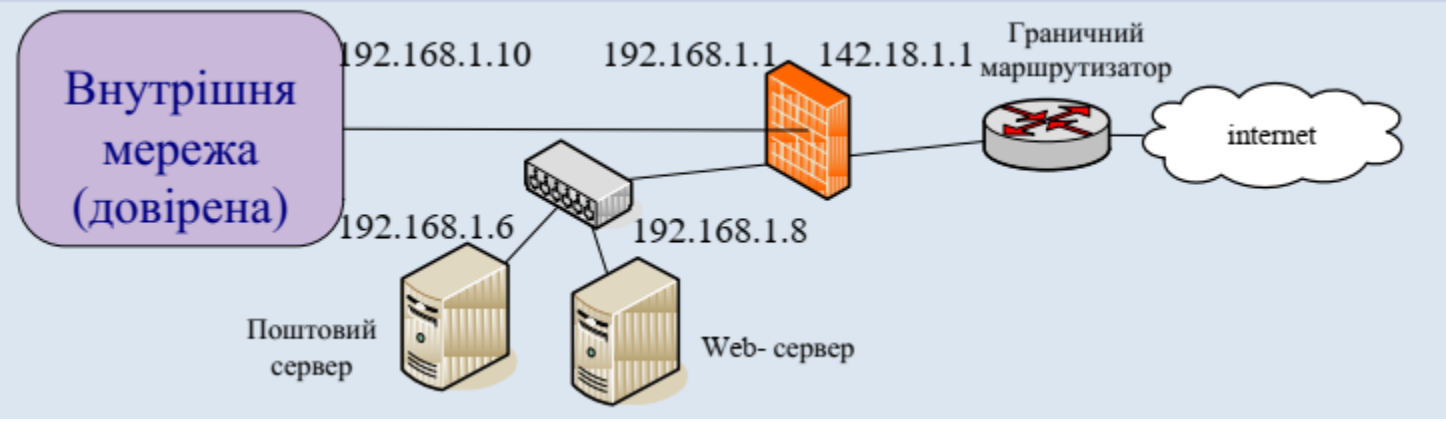
Системи за межами міжмережевих екранів доступні з Інтернету



Номер	IP-адреса відправника	IP-адреса одержувача	Служба	Дія
1	Внутрішній поштовий сервер 172.16.0.6	Поштовий сервер 192.168.1.6	SMTP	Accept
2	ПК з внутрішньої мережі 172.16.0.10	Веб-сервер 192.168.1.8	HTTP, HTTPS, FTP, telnet, SSH	Accept
3	Внутрішній DNS	Any	DNS	Accept
4	Any	Any	Any	Deny

3 Сегментація мережі на базі МЕ

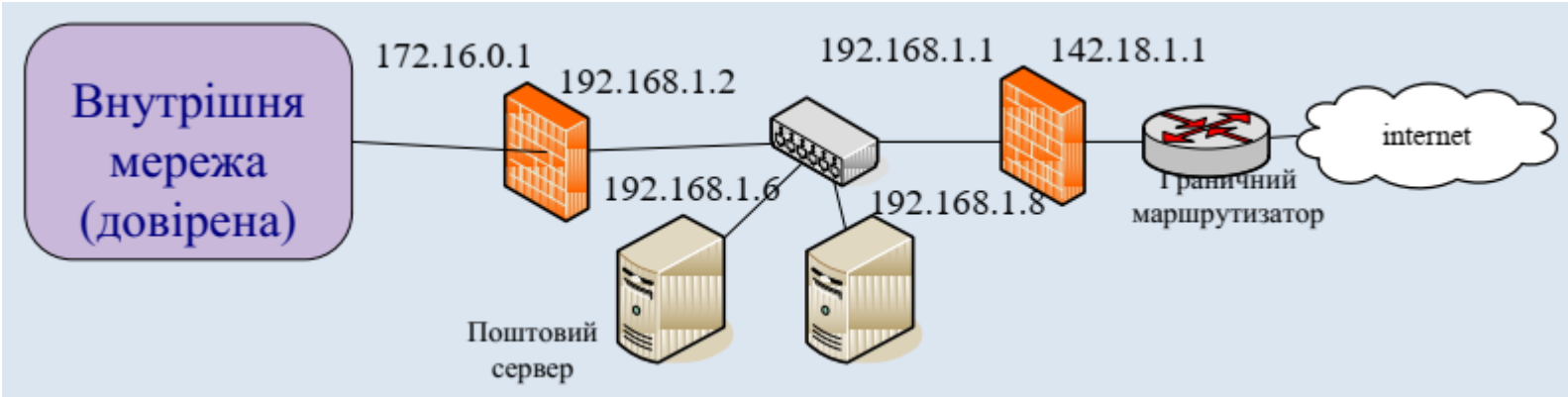
Один міжмережевий екран



Номер	IP-адреса відправника	IP-адреса одержувача	Служба	Дія
1	Any	Поштовий сервер	SMTP	Accept
2	Any	Веб-сервер	HTTP, HTTPS, FTP, telnet, SSH	Accept
3	Поштовий сервер	Any	SMTP	Accept
4	ПК з внутрішньої мережі	Any	HTTP, HTTPS, FTP, telnet, SSH	Accept
5	Внутрішній DNS	Any	DNS	Accept
6	Any	Any	Any	Deny

3 Сегментація мережі на базі МЕ

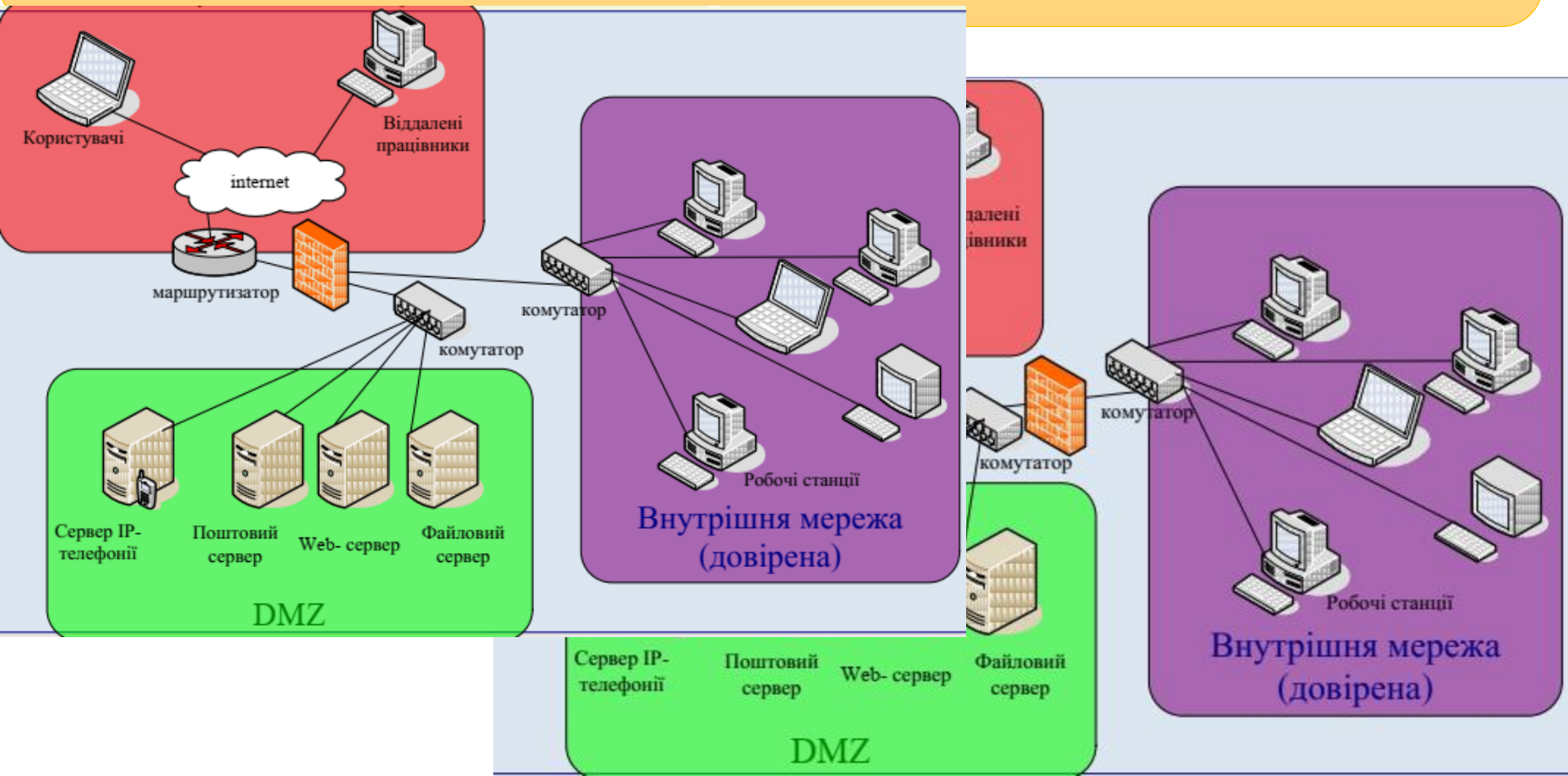
Два міжмережевих екрани



Номер	IP-адреса відправника	IP-адреса одержувача	Служба	Дія
1	Внутрішній поштовий сервер	Поштовий сервер	SMTP	Accept
2	ПК з внутрішньої мережі	Any	HTTP, HTTPS, FTP, telnet, SSH	Accept
3	Внутрішній DNS	Any	DNS	Accept
4	Any	Any	Any	Deny

3 DMZ (Демілітарізована зона)

Фізична або логічна підмережа, яка містить та використовує сервіси, що доступні іншим не довіреним мережам (зазвичай Інтернет).



4 Захист інформації в мережах VPN

VPN представляє собою об'єднання окремих машин або локальних мереж у віртуальну мережу, яка забезпечує цілісність та безпеку переданих даних. Вона має властивості виділеної приватної мережі й дозволяє передавати дані між двома комп'ютерами через проміжну мережу, наприклад Internet

Побудова VPN припускає створення захищених від стороннього доступу тунелів між декількома локальними мережами або користувачами.

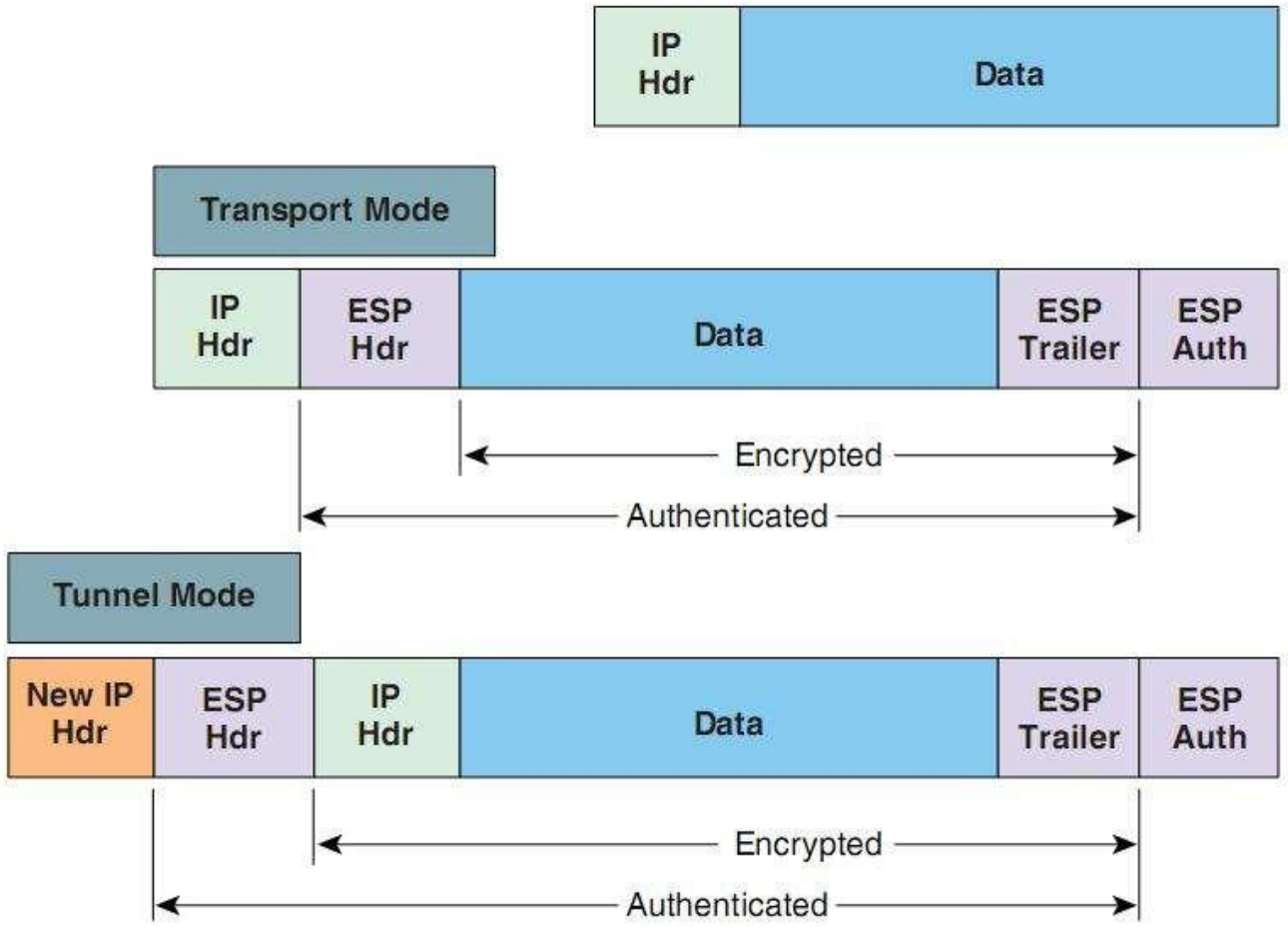
4 Захист інформації в мережах VPN

Ефективність віртуальної приватної мережі VPN визначається мірою захищеності інформації, циркулюючої по відкритих каналах зв'язку.
Для безпечної передачі даних через відкриті мережі широко використовують **інкапсуляцію** і **тунелювання**.
За допомогою методики тунелювання пакети даних передаються через загальнодоступну мережу, як по звичайному двоточковому з'єднанню. Між кожною парою «посилач — одержувач даних» встановлюється своєрідний тунель — логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

4 Захист інформації в мережах VPN

Щоб забезпечити конфіденційність передаваних даних, посилач шифрує початкові пакети, упаковує їх в зовнішній пакет з новим IP заголовком і відправляє по транзитній мережі.

Приклад пакету, підготовленого для тунелювання



4 Захист інформації в мережах VPN

Аутентифікація

Аутентифікація здійснюється або **відритим тестом** (clear text password), або за схемою запит / відгук (challenge / response).
При відкритій аутентифікації клієнт посилає серверу пароль, де він порівнюється з еталоном. На основі цього порівняння робиться висновок щодо дозволу або заборони доступу. Відкрита аутентифікація практично не зустрічається.

Схема запит / відгук набагато більш поширена. Клієнт посилає серверу запит (request) на аутентифікацію, на що сервер повертає випадковий відгук (challenge). Клієнт знімає зі свого пароля хеш , шифрує їм відгук і передає його серверу.
Те ж саме проробляє і сервер, порівнюючи отриманий результат з відповіддю клієнта:якщо зашифрований відгук збігається, аутентифікація вважається успішною.

4 Захист інформації в мережах VPN

Протоколи VPN

OpenVPN – це VPN-протокол з відкритим вихідним кодом. Він швидкий, безпечний і оптимально підходить для підключень на великій відстані.

IKEv2 – швидкий і безпечний VPN-протокол. Йому віддають перевагу у разі підключення на коротших відстанях.

PPTP і L2TP – це застарілі протоколи тунелювання. Вони не мають ні рівень безпеки, ні рівень надійності протоколів OpenVPN і IKEv2.

IPSec – це протокол безпеки, який забезпечує шифрування. Саме тому він використовується в поєднанні із застарілими протоколами тунелювання, як LT2P.

4 Захист інформації в мережах VPN

PPTP

PPTP - перший протокол, підтримуваний на платформі Windows. Протокол має слабке шифрування і може бути зламаний.
З плюсів варто відзначити відсутність необхідності встановлювати додаткове програмне забезпечення і швидкість роботи.
PPTP VPN вимагає мінімальних ресурсів і в порівнянні з OpenVPN майже не витрачає заряд при використанні на мобільних пристроях.

Чому цей протокол до сих пір використовується? Головна його проблема - слабкий захист передачі ключа, але це не означає, що будь-хто може зламати шифрування. PPTP має і свої плюси: простоту в налаштуванні і використанні, непоганий захист і зміну IP-адреси. PPTP, може, і не самий захищений протокол, але безперечно краще, ніж нічого.

4 Захист інформації в мережах VPN

L2TP/IPsec

- повільніше інших через подвійне інкапсулювання (створюється IPsec-тунель, а дані ходять через L2TP);
- використовує стандартні порти, і тому його легко може заблокувати інтернет-провайдер або системний адміністратор;
- операційні системи мають вбудовану підтримку цієї технології, немає необхідності ставити додаткове ПО;
- при його правильному налаштуванні немає інформації про можливості розшифрувати дані.

4 Захист інформації в мережах VPN

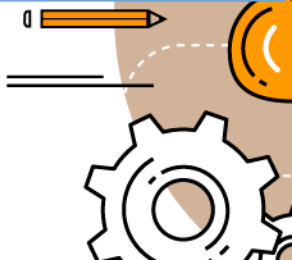
IPsec IKEv2

Що таке IKEv2 в цій зв'язці?

Це, якщо говорити дуже просто, авторизація через сертифікат, і вона, на жаль, не сумісний з усіма пристроями.

Що про нього треба знати:

- працює швидше, ніж L2TP / IPsec, можна порівняти з OpenVPN, повільніше PPTP;
- підтримується не всіма операційними системами (хоча сам IPsec підтримується всюди);
- при правильному налаштуванні його не можуть розшифрувати ні спецслужби, ні зловмисники (принаймні так вважається в середовищі IT-фахівців).



4 Захист інформації в мережах VPN

OpenVPN

OpenVPN - безкоштовне рішення з відкритим вихідним кодом, яке, за визнанням більшості фахівців, є найкращим на сьогоднішній день для створення приватної віртуальної мережі (VPN).

- не входить до складу стандартних дистрибутивів сучасних операційних систем, тому вимагає установки додаткового програмного забезпечення;
- при правильному налаштуванні його не зможуть розшифрувати ні спецслужби, ні зловмисники;
- при нестандартних налаштуваннях складно блокується.

OpenVPN вимагає установки додаткового програмного забезпечення, але це перевірений часом софт з відкритим вихідним кодом, установка і настройка якого не створить проблем. OpenVPN працює на всіх сучасних операційних системах: Windows, macOS, Linux, Android, iOS.

5 Як хакери зламують VPN?

При використанні публічних Wi-Fi **VPN є фундаментальним інструментом безпеки**. Якщо ви в публічних місцях підключаєтеся до Wi-Fi без VPN, боюся, цей курс нічим вам не зможе допомогти.

Сьогодні ми пограємо в хакера, який на замовлення зламав Wi-Fi роутер в квартирі жертви. Жертва використовує VPN. Тому, все, що ми можемо побачити, це зашифрований інтернет-трафік кудись в Нідерланди.

Так, ми можемо з'ясувати, які пристрої і коли підключаються до роутера, але замовник чекає доступу до акаунтів жертви на ряді цікавих йому сайтів. Ми вже підготували точні копії цих сайтів і чекаємо в гості жертву, але VPN не дає нам можливості перенаправити її туди.

Якщо б у нашої жертви була дружина, яка підключалася б до цього роутера без VPN, можна було б скомпрометувати її комп'ютер, а там вже включити прослушку квартири через мікрофон, перегляд периметра через камеру, в кінці кінців, спробувати через email від дружини або загальну флешку перебратися на робочий комп'ютер потрібної нам особи. Але наша жертва налаштувала безпеку і своїй дружині, по принаймні, всі пристрої підключаються до Wi-Fi тільки через VPN, навіть мобільні телефони.

5 Як хакери зламують VPN?

Отже, VPN - це непереборна перешкода, і за всяку ціну треба змусити позбутися його. Зате є доступ до Wi-Fi роутера.

І ось наша жертва приходить з роботи, включає ноутбук і виявляє, що інтернет не працює. Вона вмикає, вимикає інтернет, перезапускає додаток, операційну систему, і тільки потім розуміє, що причина в VPN. VPN зламався, і будьте впевнені, він не запрацює самостійно. Що трапилося? Його заблокували ми. Є маса шляхів заблокувати VPN, найпростіший з яких додати IP-адресу в чорний список або заблокувати порт.

Весь трафік в наших руках, але це ще не повна перемога. Залишається HTTPS - ще один рівень шифрування, не такий криптостійкий, як AES 256, який використовували в VPN, але все-таки ми не АНБ і HTTPS нам не по зубах.

Розшифровувати HTTPS ми не станемо, ми будемо проводити підміну DNS.Для більшості сайтів DNS-сервер зловмисника видаватиме коректну IP-адресу, крім деяких сайтів, для яких він завчасно пропише свій IP. Це, швидше за все, будуть сайти банків, платіжних систем, соціальних мереж і поштових сервісів. Зловмисник завчасно розмістить в мережі точні копії цих сайтів і відправить жертву на них.

5 Як хакери зламують VPN?

Жертва навряд чи помітить підміну, адже у неї в браузері буде вказано коректний домен, а сайт буде зовні не відрізнятись від оригіналу. Після того як користувач на підробленому сайті введе дані, наприклад логін і пароль, він буде автоматично перенаправлений на оригінальний сайт, а логін і пароль виявляться у зловмисника.

Користувач, безумовно, помітить, що після введених даних авторизації не відбулося або не відбулося оплати після введення коректних даних банківської карти, однак з другої спроби вже на оригінальному сайті у нього все вийде, і він заспокоїться.

Які висновки?
Якщо у вас раптом перестав працювати VPN, це може бути не випадково. Скористайтеся будь-яким іншим VPN, ні в якому разі не сидіть без шифрування.