Захист з’єднань. IPsec, фаєрволи, віртуальні приватні мережі.

Захист з’єднань.

Безпека з'єднань полягає у тому, як таємно і без ризику підміни даних передавати біти від пункту відправлення до пункту призначення, а також, як не пускати на лінію зв’язку сторонні біти. Це ні в якому разі не повний список проблем мережевої безпеки, однак перераховані питання є одними з найбільш важливих.

Довгий час між фахівцями з питань безпеки велась дискусія про те, на якому рівні стеку протоколів TCP/IP треба впроваджувати захист у мережі Інтернет. Більшість експертів вважають, що найнадійніша система та, яка виконує наскрізне шифрування і перевірку цілісності даних, тобто розміщуватись на прикладному рівні. Але такий підхід має недолік - для забезпечення безпеки треба вносити зміни у всі прикладні програми Інтернету. Тому було вирішено розробити стандарт безпеки, який розміщується на мережному рівні.

Так виник стандарт IPsec (IP secutity – IP-безпека) в 1998 році. Він досить складний, тому описується у декількох документах: RFC 2401, 2402, 2406 та інших. Протокол IPsec - традиційний метод віртуальних приватних мереж VPN (див. нижче).

IPsec

Psec служить основою для декількох послуг, алгоритмів і модулів. Причиною наявності декількох послуг є те, що далеко не всі хочуть постійно платити за всі можливі послуги, тому необхідні послуги надаються порційно. Завдяки набору алгоритмів забезпечується незалежність Psec від якогось одного алгоритму у випадку його зламу. І завдяки різним модулям можна захищати як одне TCP-з’єднання так і увесь трафік між парою хостів і т. д.

«З'єднання» в контексті IPsec називається захищеним з’єднанням (Security Aconnection - SA). Захищене з’єднання - це симплексне з'єднання між двома кінцевими точками, з яким пов'язаний спеціальний ідентифікатор захисту. Якщо потрібна передача захищених даних в обох напрямках, знадобляться два захищених з'єднання.

Технічно IPsec складається з двох основних частин. Перша описує два нових заголовка Authentication Header (AH) і Encapsulating Security Payload (ESP), які можна додавати до пакету для передачі ідентифікатора захисту,

даних контролю цілісності та іншої інформації. Друга частина, ISAKMP (Internet Security and Key Management Protocol- інтернет-безпека і протокол управління ключами), призначена для створення ключів.

IPsec може працювати в двох режимах. У транспортному режимі заголовок IPsec вставляється відразу за заголовком IP. Транспортний режим реалізується при SA між двома IP-вузлами.

У режимі тунелювання весь IP-пакет разом з заголовком вставляється всередину нового IP-пакета з абсолютно новим заголовком – створюється так званий VPN-туннель.

Цей режим хороший тоді, коли тунель закінчується десь поза кінцевого пункту. У деяких випадках кінцем тунелю є шлюз, що забезпечує безпеку, наприклад, корпоративний фаєрвол (міжмережевий екран). Він зазвичай використовується для VPN (Virtual Private Network - віртуальна приватна мережа). В цьому режимі фаєрвол вставляє і витягує пакети, що проходять через нього в різні боки. При такій організації машини ЛВС компанії гарантовано будуть обслужені за стандартом IPsec. (див. рис).

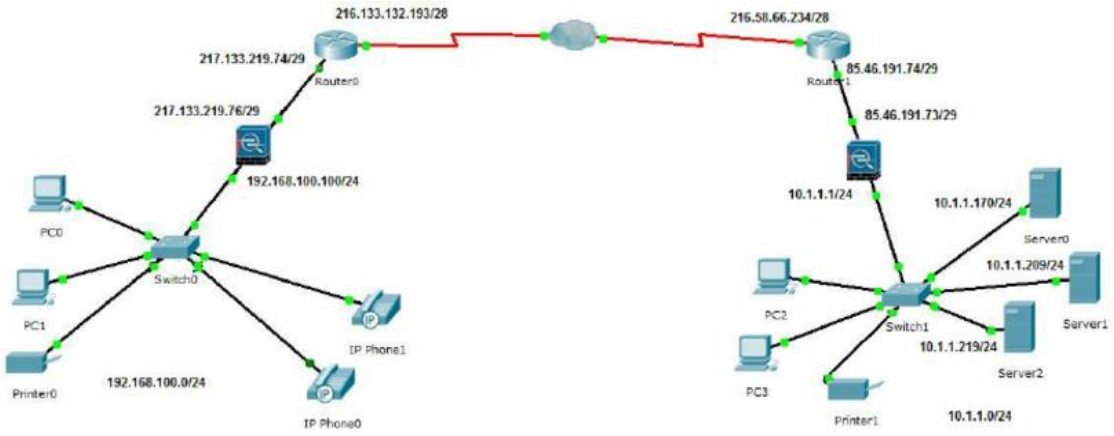


Рис. Використання фаєрволів для організації VPN між локальними мережами

Віртуальні приватні мережі

Віртуальна приватна мережа (VPN) розширює приватну мережу через загальнодоступну мережу і дає можливість користувачам надсилати та отримувати дані через спільні або загальнодоступні мережі так, ніби їхні обчислювальні пристрої були безпосередньо підключені до приватної мережі. Тому програми, що працюють в кінцевій системі (ПК, смартфон тощо) через VPN, можуть скористатися функціональністю, безпекою та управлінням приватної мережі.

Для створення VPN крім IPsec використовують також такі протоколи: OpenVPN, IKEv2, PPTP, Wireguard, L2TP, SSTP, L2TP/IPSec, SSL/TLS та інші.

Крім використання технології VPN для організації зв'язку між локальними мережами організації він також використовується як VPN-сервіс. VPN-сервіси дозволяють захистити інтернет-трафік і приховати особисті дані користувачів при роботі в Інтернеті.

При підключенні до безпечного VPN-сервера інтернет-трафік користувача перенаправляється через зашифрований VPN-тунель (див. рис).

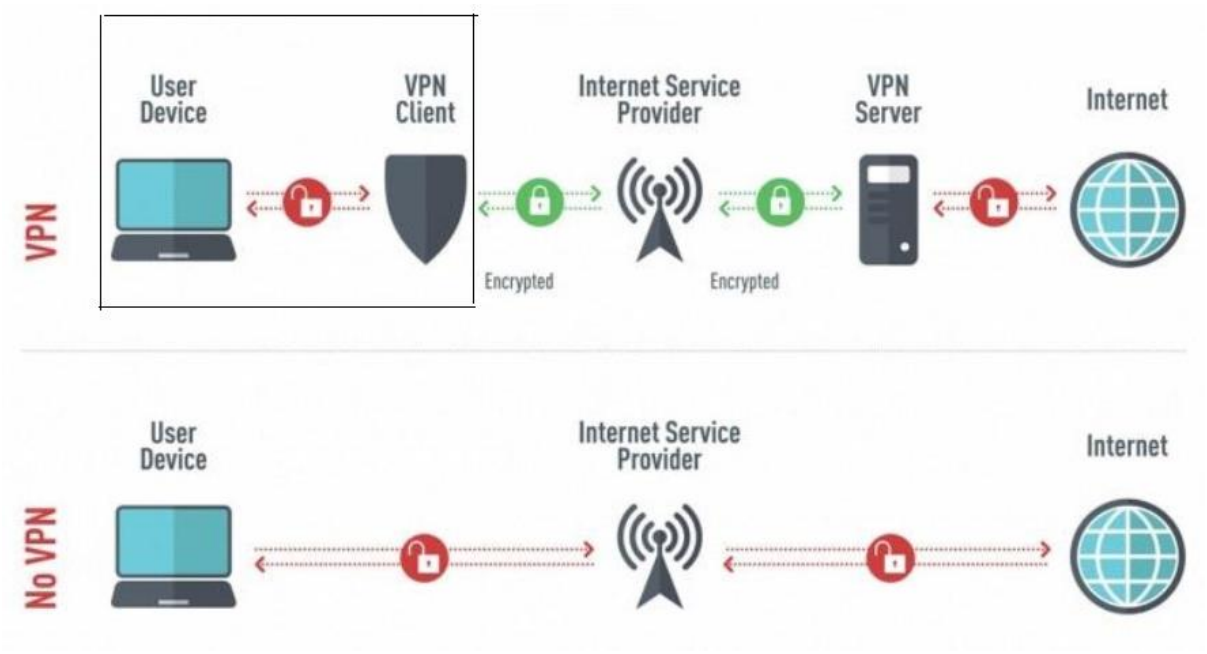


Рис. Схема роботи VPN-сервісу

Використання VPN-сервісу дає користувачу такі переваги:

- Приховування розташування. Використання VPN змінює IP-адресу користувача, за якою можна легко ідентифікувати особу та місцеперебування. За допомогою нової IP-адреси можна користуватися Інтернетом, нібито користувач перебуває у Великобританії, Німеччині, Канаді, Японії або будь-який іншій країні, в якій у VPN-сервісу є сервери.
- Захист конфіденційності завдяки як зміні IP-адреси, так і шифруванню даних, що передаються мережею

- Підвищення безпеки. Використання VPN захищає від багатьох форм злому, включаючи сніффінг пакетів, підроблені мережі Wi-Fi і атаки через посередника. Наприклад, мандрівники, віддалені співробітники і всі, хто часто перебуває поза домом, можуть використовувати VPN щоразу, коли підключаються до ненадійної мережі, наприклад, до безкоштовної публічної мережі Wi-Fi.
- Доступ до веб-сайтів. Якщо користувач перебуває в країнах, де обмежується доступ до Google, Вікіпедії, YouTube або інших сайтів і сервісів, підключення до VPN дозволить вільно використовувати Інтернет. Це стосується також обходу блокування фаєрволів в шкільних або офісних мережах.

Фаєрволи (брандмауери, міжмережеві екрани)

Брандмауер - це поєднання програмних і апаратних засобів, які ізолюють внутрішню мережу організації від великого Інтернету, пропускаючи одні пакети і блокуючи інші.

Брандмауер вирішує три практичні завдання:

• Через брандмауер проходить весь трафік, що надходить в корпоративну мережу ззовні, а також йде в зворотному напрямку.

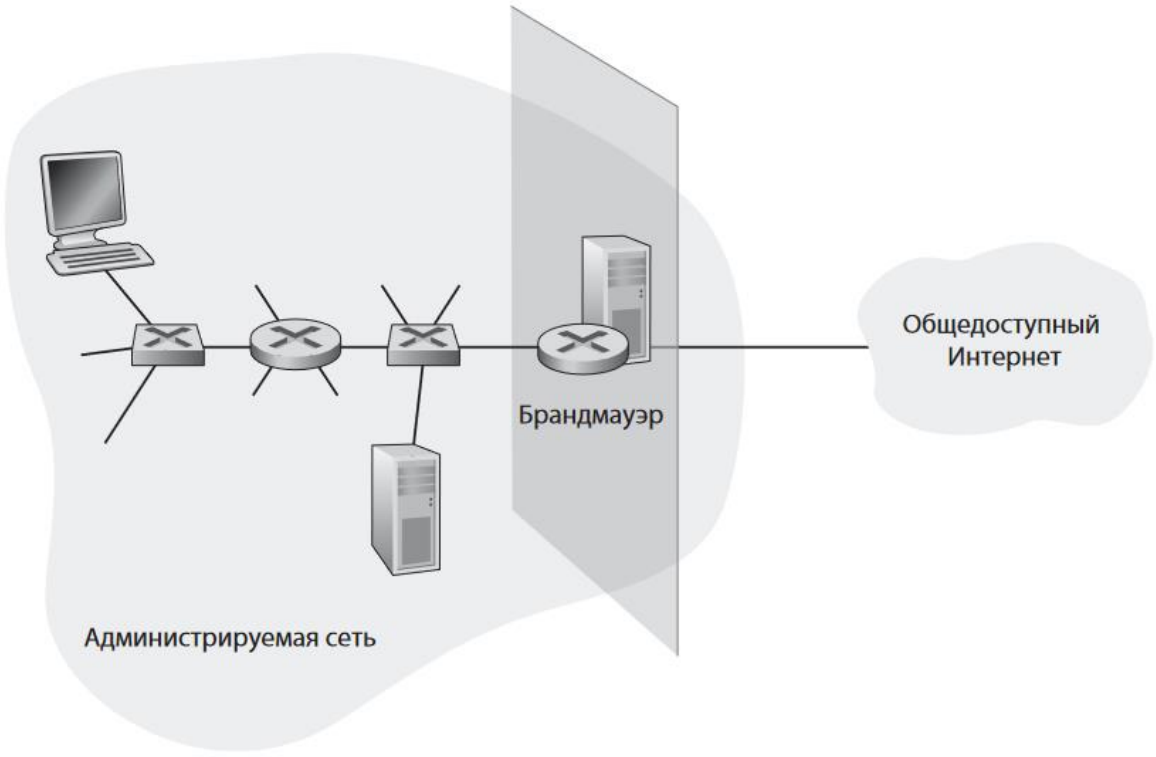


Рис. Розміщення брандмауера між локальною мережею і Інтернетом

• У систему потрапляє тільки той трафік, який задовольняє політиці безпеки, визначеної в локальній мережі.

• Сам брандмауер повинен бути невразливий для вторгнення.

В даний час основними виробниками брандмауерів є компанії Cisco і Check Point. Можна створити брандмауер (фільтр пакетів) на основі Linux, скориставшись інструментом iptables (це загальнодоступна програма, яка зазвичай надається в дистрибутивах Linux).

Рис. Брандмауер Cisco ASA5510-SEC-BUN-K9

Всі брандмауери можна поділити на три категорії: традиційні фільтри пакетів, фільтри, що враховують стан з’єднання і шлюзи додатків.

Брандмауер, який є фільтром пакетів окремо перевіряє кожну дейтаграму, визначаючи, як вчинити з нею відповідно до правил, встановлених адміністратором обчислювальної мережі: пропустити в мережу або відкинути. Рішення, пов'язані з фільтрацією, зазвичай ґрунтуються на наступних факторах:

• Вихідна або кінцева IP-адреса

• Тип протоколу у відповідному полі IP-дейтаграми: TCP, UDP, ICMP, OSPF і т. д.

• Порти і відправника і одержувача TCP- або UDP-з'єднання

• Біти прапорів TCP: SYN, ACK і т. д.

• Тип повідомлення ICMP

• Різні правила, що характеризують вхідні та вихідні дейтаграми даної мережі

• Різні правила, що стосуються інтерфейсів маршрутизатора

Брандмауери, які є фільтрами, що враховують стан з'єднання, відстежують TCP-з'єднання і виконують фільтрацію на основі цієї інформації. Тобто, брандмауер буде пропускати тільки ті пакети, які відносяться до поточних з’єднань.

Брандмауер, який є шлюзом додатків це сервер, що працює саме на прикладному рівні, і через такий шлюз повинні протікати всі дані додатків (як вхідні, так і вихідні).

Персональний брандмауер

Персональний брандмауер є додаток (застосування) який контролює мережевий трафік до і з комп'ютера, дозволяючи або забороняючи зв'язок на основі політики безпеки комп’ютера.

Персональний брандмауер відрізняється від звичайного брандмауер з точки зору масштабу. Персональний брандмауер зазвичай захищає лише комп'ютер, на якому він встановлений, порівняно зі звичайним брандмауером, який зазвичай встановлюється між двома або більше мережами.

На відміну від мережевих брандмауерів, багато персональних брандмауери здатні контролювати дозволений мережевий трафік програм на захищеному комп'ютері. Коли програма намагається здійснити вихідне з’єднання, брандмауер може заблокувати його, або запитати у користувача, чи дозволити цій програмі з’єднання. Це захищає від шкідливих програм, реалізованих як виконувана програма.

Загальні функції персонального брандмауера:

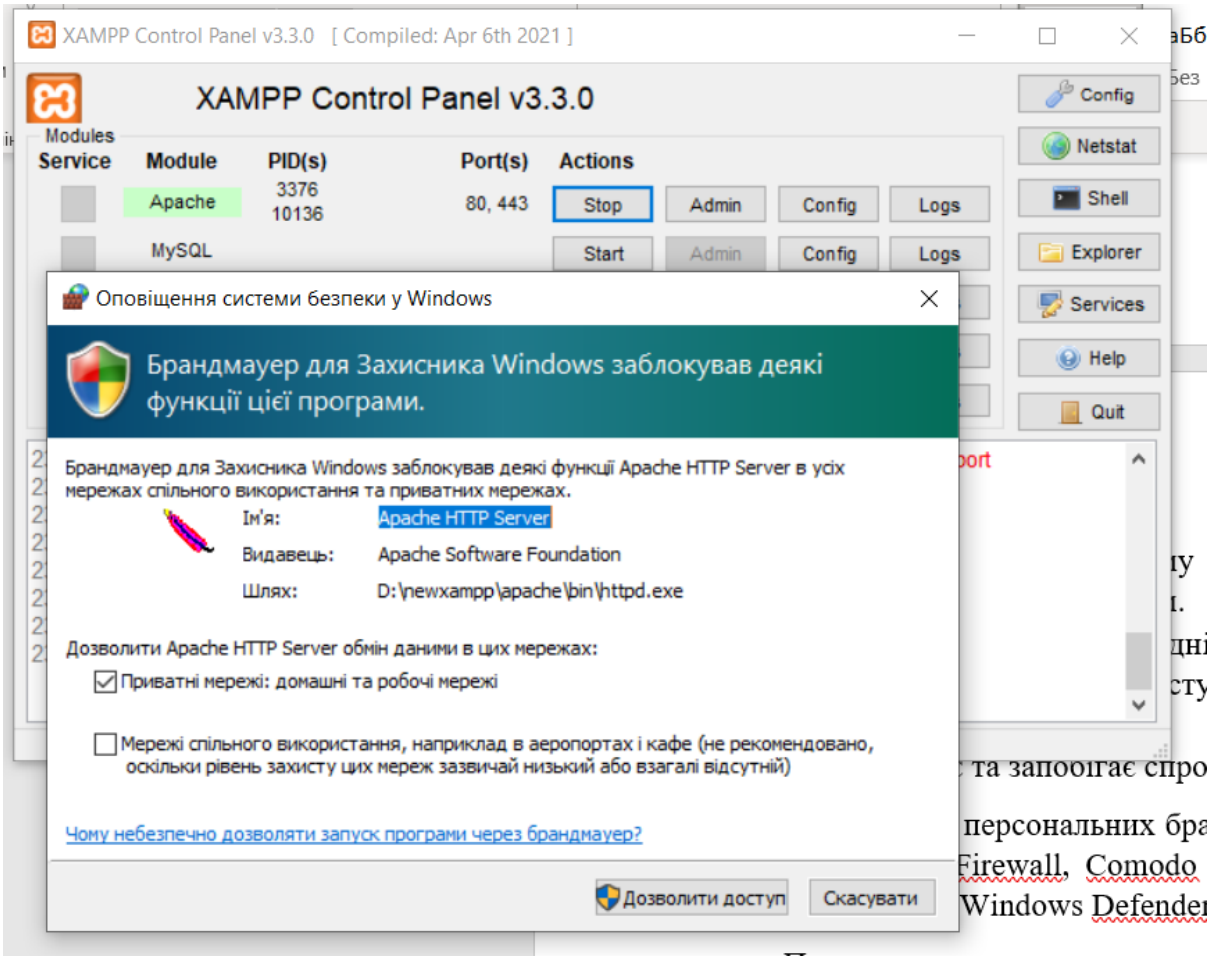
- Блокує або попереджає користувача про всі несанкціоновані спроби вхідного або вихідного з'єднання.
- Дозволяє користувачеві контролювати, які програми можуть і не можуть отримати доступ до локальної мережі та / або Інтернету і надати користувачеві інформацію про програму, яка робить спробу підключення.
- Сховати комп’ютер від сканування портів, не реагуючи на небажаний мережевий трафік.
- Відстежує програми, які прослуховують вхідні з'єднання.

- Запобігає небажаному мережевому трафіку від локально встановлених програм.
- Відстежує останні вхідні, вихідні з’єднання та вторгнення, щоб дізнатись, хто мав доступ до системи або намагався отримати доступ.
- Блокує та запобігає спробі злому або атаки з боку хакерів.

Існує багато персональних брандмауерів, наприклад, Norton Personal Firewall, McAfee Firewall, Comodo Firewall, брандмауер Avast Antivirus, Windows Firewall (Windows Defender Firewall) та ін.

Продемонструємо як створити правило у Брандмауері Windows щоб дозволити отримувати вхідні підключення для Web-сервера (наприклад, Apache, який входить у склад пакету XAMPP).

Найпростіший спосіб, просто при старті Apache у вікні «Оповіщення системи безпеки у Windows» вибрати «Дозволити доступ».



Якщо з якихось причин це вікно не з’являється, можна створити правило для програми Web-сервера.

Для цього треба відкрити брандмауер: Настройки – Мережа й Інтернет – Брандмауер Windows. Далі зайти у “Додаткові настройки” – Inbound Rules (Вхідні підключення) – New Rule – Program – за допомогою кнопки Browse знайти програму (наприклад, D:\newxampp\apache\bin\httpd.exe) – Allow all connections – обрати профіль мережі (Domain, Private, Public) – ввести ім’я правила.

Інший варіант – відкрити порт протоколу TCP і UDP , на якому працює Web-сервер (які?).