

VPN ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ НА РІВНІ МЕРЕЖІ

У інтернеті досі мало матеріалу про таку стару і просту, але зручну, безпечну і особливо актуальну в зв'язку з розвитком Інтернету речей технологію, як мобільна VPN (віртуальна приватна мережа). У цій статті роздивимось, як і навіщо можна налаштувати доступ у приватну мережу будь-якого пристрою з сім-картою без необхідності налаштування на ньому спеціалізованого ПЗ.

VPN як технологія використовується для вирішення найрізноманітніших мережевих завдань, об'єднаних загальною ознакою - ізольованою передачею даних між двома пристроями крізь велику кількість проміжних вузлів. На базі цього вже будуються більш складні рішення і вирішуються ті самі різні завдання. У звичному всім випадку для побудови VPN використовується мережа оператора фіксованого зв'язку або безліч різних мережевих протоколів (GRE, IPSec, L2TP і інші) і програмні продукти, що працюють з ними (Cisco AnyConnect, OpenVPN, TOR), але їх використання на конкретному крайовому пристрої відразу ж висуває до нього ряд вимог, невиконання яких веде до певних обмежень.

Перше серйозне обмеження - пристрій повинен на апаратному та програмному рівнях вміти працювати хоча б з одним з цих протоколів. Найчастіше це визначається програмним забезпеченням, яке легко знайти для ноутбука або смартфона, але існують випадки, коли завдання стоїть перед дуже простим з апаратної точки зору пристроєм, або у його ПЗ є обмеження.

Інше важливе обмеження - необхідність налаштування. Воно працює як для «дурних» пристроїв з першого пункту, так і для класичних смартфонів і комп'ютерів, яким попереднє обмеження невідомо. І якщо з першими все відносно просто і впирається в кількість часу, витраченого на налаштування, то з другими є варіанти. Найчастіше організації використовують VPN з метою безпеки, щоб уберегти службовий термінал від виходу в публічну мережу без належного корпоративного захисту або від передачі службових даних по публічному каналі. Кінцеві ж користувачі можуть з якихось своїх причин відключити або забути включити VPN, в результаті чого багато систем безпеки компанії можуть опинитися «за бортом».

Обидва ці обмеження легко знімаються, якщо доступ до VPN забезпечується на мережевому рівні. У випадку з мобільним зв'язком це може

бути реалізовано за допомогою «мобільного VPN». Пристрій будь-якої складності здатний передавати дані, буде передавати їх в правильну мережу. Неважливо, які налаштування зроблені на пристрої, при правильно конфігурованій мережі він в будь-якому випадку буде передавати їх туди, куди потрібно, і нікуди більше.

Пристрій буде отримувати адресу з внутрішньої мережі, що налаштовується віддалено, і доступ до нього буде можливо отримати тільки зсередини цієї мережі (або фізично). Для певного класу пристроїв це дуже важливо.

Здавалося б, VPN - класична послуга всіх операторів зв'язку для B2B сегмента, і навіщо в такому разі загострювати на цьому увагу? Вся справа в тому, як влаштована мережа передачі даних для пристроїв, що підключаються через GPRS, HSPA, LTE або іншу технологію мобільного зв'язку. Тут немає звичних всім мережевим адміністраторам vlan, немає свічів, немає навіть маршрутизаторів в звичному їх значенні. Зате є мережа радіодоступу (RAN) і пакетне ядро (PS Core).

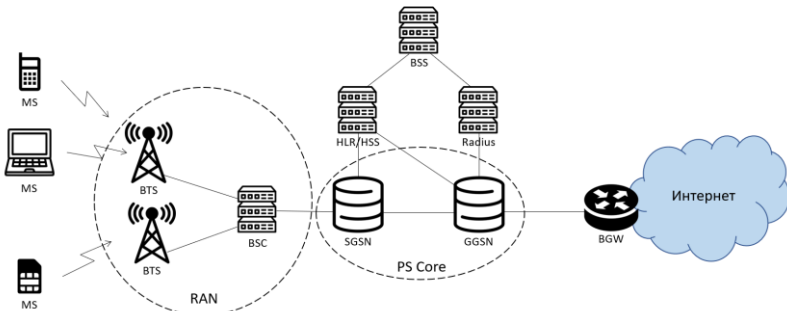


Рисунок 1 – Спрощена схема пакетної мережі оператора мобільного зв'язку.

У загальному випадку, кожен пристрій з сім-картою, зареєстрований в пакетній мережі (що пройшла процедуру GPRS attach або аналогічну), перед тим як почати передавати дані куди-небудь має ініціювати створення сесії передачі даних (PDP context) на маршрутизаторі ядра пакетної мережі, GGSN. Важливо: при ініціації сесії в запиті до GGSN в числі інших значаться параметри наступні параметри: APN, логін і пароль. APN (точка доступу) - дуже важлива сутність в логіці роботи GGSN: в залежності від того, з якою APN ініційована сесія, GGSN діє по-різному. В результаті успішної обробки запиту користувача GGSN повинен активувати у себе сесію передачі даних і повідомити пристрою її параметри, зокрема, видану пристрою IP адресу і адреси DNS. Тут є ряд важливих дуже важливих особливостей:

У запиті на ініціацію сесії пристрій ніколи не запитує, яку IP адресу він хотів б отримати;

Крім полів, що задаються в налаштуваннях пристрою «APN», «логін» і «пароль», в запиті до GGSN передається також номер телефону (MSISDN) абонента (тут і далі «абонент» - це кінцевий користувач, один пристрій з сім-картою, а «клієнт» - організація-замовник сервісу, до складу якої входять абоненти);

При активації сесії GGSN створює в своїй таблиці маршрутизації запис про нову IP адресу. Всі абоненти на GGSN позначаються записами в таблиці маршрутизації з префіксом / 32, тобто 1 абонент - 1 запис в таблиці. GGSN - це дуже продуктивний маршрутизатор;

Мережа оператора може на різних етапах (і на SGSN, і на GGSN) з різних причин змінювати поле APN в запиті на ініціацію сесії. Це дозволяє в деяких випадках зменшити, а в деяких взагалі виключити налаштування параметрів мережі на пристроях з сім-картою.

За перших трьох пунктів відразу виникає питання: що за IP адреса видається абоненту? Це визначається налаштуваннями тієї APN, з якої прийшов запит на активацію сесії. Порядку 99% користувачів передачі даних в мобільних мережах використовують звичайний доступ в Інтернет. Це відомі всім точки доступу internet.mts.ua, internet.lifacell.ua і так далі. У випадку з доступом в Інтернет GGSN видає адреси за принципом класичного DHCP із прописаних в налаштуваннях сірих підмереж. При виході в публічну мережу вони закриваються класичним NAT'ом (а точніше тієї його версією, яка PAT).

Але GGSN здатний на більше. Для вибору IP адреси він може зробити AAA запит до сервера авторизацій (Radius, наприклад). Така логіка налаштовується для окремих APN в залежності від їх призначення. Найпростіший випадок - послуга з надання постійної публічної IP адреси. Такі адреси, як правило, закріплюються за абонентами у біллінзі (BSS) оператора, і в залежності від IT архітектури потрапляють в ту чи іншу базу даних, до якої і звертається із запитом GGSN. Завдяки тому, що йому відомий MSISDN (номер телефону) абонента, який і буде міститися в запиті, така БД буде досить простою і може містити лише зв'язку номера та адреси. Додатково, в разі, якщо клієнт планує використовувати одну сім-карту для підключення декількох пристроїв (якщо сім-карта знаходиться в WiFi-роутері віддаленого офісу, наприклад), ця таблиця може містити також так званий «framed route» - префікс мережі, що знаходиться « за »сім-картою, який буде анонсований всім пристроям в мережі по протоколам динамічної маршрутизації.

Крім видачі адрес потрібно ще доставити трафік абонентів до клієнтських мереж, кожного до своєї. Тут все працює вже куди більш традиційно. На GGSN трафік спеціалізованих під роботу з VPN APN

маршрутизується на окремий маршрутизатор мережі оператора (він може називатися по-різному, іноді - VPN роутер), який в свою чергу виконує функцію класичного PE в схемі L3VPN. Він додає необхідні мітки, заголовки і це все і відправляє весь цей потік трафіку через маршрутизатори транспортної мережі в попередньо налаштовані стики або тунелі до мережі клієнта.

З урахуванням всіх цих деталей, способів організації мобільного VPN може бути кілька, і вони будуть відрізнятися один від одного комбінацією таких особливостей:

IP адреси, як вже було описано, можуть видаватися динамічно (кожен раз різна адреса з заданою підмережі) і статично (кожен раз одна і та ж адреса у конкретного абонента), що визначається і / або налаштуваннями APN, і / або налаштуваннями Radius-сервера;

IP адреси можуть видаватися Radius-сервером під управлінням оператора або під керуванням клієнта;

Пристрої, підключені до мобільного VPN, можуть взаємодіяти або тільки один з одним, або мати доступ до звичайної L3VPN мережі клієнта через прямий стик (VPN порт) з оператором або через тунелювання поверх мережі Інтернет;

У деяких випадках використання логіна і пароля для успішної активації сесії може бути обов'язково, а іноді не потрібно навіть заповнювати поле «APN».

Таких комбінацій з різними типами тунелювання, балансування трафіку між каналами доступу до «основного» VPN клієнта і принципом видачі адрес налічується кілька десятків. Для більшості випадків загальна схема виглядає наступним чином.

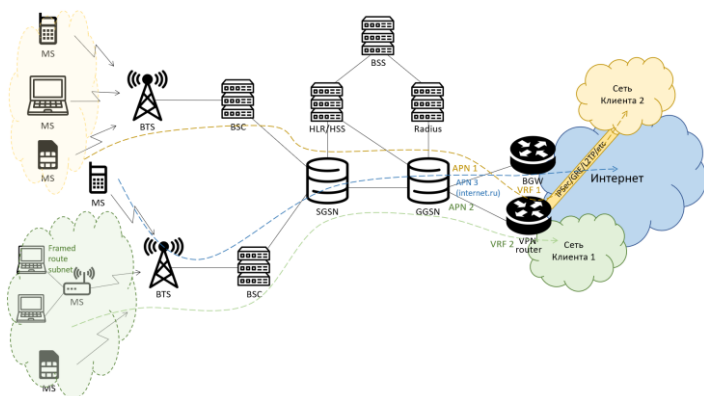


Рисунок 2 – Загальна схема організації мобільного VPN.

У підсумку після досить швидкого процесу реєстрації в мережі і отримання IP адреси пристрій отримує доступ в мережу клієнта, а мережа клієнта отримує доступ до пристрою. При цьому абонент знаходиться в ізоляції від усіх інших абонентів оператора, що не мають відношення до конкретного клієнта, йому не потрібно ніяких додаткових налаштувань, і весь трафік безальтернативно направляється в мережу клієнта, де обробляється вже відповідно до внутрішніх політик клієнта.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Брайан Клифтон. Google Analytics. Профессиональный анализ посещаемости веб-сайтов / Клифтон Брайан – М.: Вильямс, 2009. – 400 с.