УДК 004.49

Брайко В.В.
Центральноукраїнський національний технічний університет

Дослідження принципів роботи технологій VPN

VPN (Віртуальна приватна мережа, англ. Virtual Private Network) — це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Прикладом створення віртуальної мережі використовується інкапсуляція протоколу PPP в будь-який інший протокол — IP (ця реалізація називається також PPTP — Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Деякі інші протоколи так само надають можливість формування захищених каналів (SSH).

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або при установці з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

Перш ніж приступити до налаштування VPN, необхідно познайомиться із загальноприйнятою термінологією і з деякими проблемами налаштування. Розпочнемо з термінології. VPN з'єднання завжди складається з каналу типу точка-точка, також відомого під назвою тунель. Тунель створюється в незахищеній мережі, якою найчастіше виступає Інтернет. З'єднання точка-точка має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються вузлами або peers.

Кожен peer відповідає за шифрування даних до того, як вони потраплять в тунель і розшифровку цих даних після того, як вони покинуть тунель.

Хоча VPN-тунель завжди встановлюється між двома точками, кожен peer може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьом віддаленим станціям необхідно зв'язатися з одним і тим же офісом, буде створено три окремих VPN-тунелю до цього офісу. Для усіх тунелів peer на стороні офісу може бути одним і тим же. Це можливо завдяки тому, що вузол може шифрувати і розшифровувати дані від імені усієї мережі.

У цьому разі VPN-вузол називається VPN-шлюзом, а мережа за ним — доменом шифрування(encryption domain). Використання шлюзів зручне з кількох причин. По-перше, усі користувачі повинні пройти через один пристрій, який полегшує завдання управління політикою безпеки і контролю вхідного та вихідного трафіку мережі. По-друге, персональні тунелі до кожної робочої станції, до якої користувачеві потрібно отримати

доступ, дуже швидко стануть некерованими (оскільки тунель — це канал типу точка-точка).

За наявності шлюзу, користувач встановлює з'єднання з ним, після чого користувачеві відкривається доступ до мережі(домену шифрування).

Цікаво відмітити, що усередині домену шифрування самого шифрування не відбувається. Причина в тому, що ця частина мережі вважається безпечною і такою, що знаходиться під безпосереднім контролем в протилежність Інтернет. Це справедливо і при з'єднанні офісів за допомогою VPN-шлюзів. Таким чином гарантується шифрування тільки тієї інформації, яка передається по небезпечному каналу між офісами.

Мережа А вважається доменом шифрування VPN-шлюзу А, а мережа В — доменом шифрування VPN-шлюзу В, відповідно. Коли користувач мережі А виявляє бажання відправити дані до мережі В, VPN шлюз А зашифрує їх і відішле через VPN-тунель. VPN шлюз В розшифрує інформацію і передасть одержувачеві в мережі В.

Кожного разу, коли з'єднання мереж обслуговують два VPN-шлюзи, вони використовують режим тунелю. Це означає, що шифрується увесь пакет IP, після чого до нього додається новий IP- заголовок. Новий заголовок містить IP- адреси двох VPN-шлюзів, які і побачить пакетний сниффер при перехопленні. Неможливо визначити комп'ютер-джерело в першому домені шифрування і комп'ютер-одержувач в другому домені.

Існує багато варіантів VPN-шлюзів і VPN-клієнтів. Це може бути апаратний пристрій або програмне забезпечення, яке встановлюється на маршрутизаторах або на ПК. Скажімо, ОС FreeBSD поставляється разом з ПЗ для створення VPN-шлюзу і для налаштування VPN-клієнта. Свої VPN-рішення існують і для ПО компанії Microsoft.

На щастя, в Інтернет є багато джерел інформації про VPN, технічні статті, FAQ і варіанти налаштувань. Я можу порекомендувати Tina Bird's VPN Information, VPN Labs, і Virtual Private Network Consortium (VPNC).

Незалежно від використовуваного ПО, усі VPN працюють по наступних принципах: кожен з вузлів ідентифікує один одного перед створенням тунелю, щоб упевнитися, що шифровані дані будуть відправлені на потрібний вузол; обидва вузли вимагають заздалегідь налаштованої політики, що вказує, які протоколи можуть використовуватися для шифрування і забезпечення цілісності даних; вузли звіряють політики, щоб домовитися про використовувані алгоритми; якщо це не виходить, то тунель не встановлюється. Як тільки досягнута угода по алгоритмах, створюється ключ, який буде використаний в симетричному алгоритмі для шифрування/розшифровки даних.

Є декілька стандартів, що регламентують вищеописану взаємодію. Ви, мабуть, чули про деяких з них: L2TP, PPTP, і IPSec. Оскільки IPSec — найширше підтримуваний стандарт, частину статті, що залишилася, варто присвятити саме йому.

VPN класифікують за типом використовуваного середовища таким чином:

- захищені (найпоширеніший варіант віртуальних приватних мереж. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, зазвичай, Інтернету. Прикладом захищених протоколів VPN є: IPSec, SSL та PPTP. Прикладом використання протоколу SSL є програмне забезпечення OpenVPN);

- довірчі (використовують у випадках, коли середовище, яким передають дані, можна вважати надійним і необхідно вирішити лише завдання створення віртуальної

підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol). (Коректніше сказати, що ці протоколи перекладають завдання забезпечення безпеки на інших, наприклад L2TP, як правило, використовують разом з Ipsec).

Захист інформації в розумінні VPN включає в себе шифрування (encryption), підтвердження справжності (authentication) та контроль доступу (access control). Кодування увазі шифрування переданої через VPN інформації. Читати всі отримані дані може лише володар ключа до шифру. Найбільш часто використовуваними в VPN-рішеннях алгоритмами кодування в наш час є DES, Triple DES і різні реалізації AES. Ступінь захищеності алгоритмів, підходи до вибору найбільш оптимального з них - це теж окрема тема, яку ми не в змозі обговорити.Підтвердження справжності включає в себе перевірку цілісності даних та ідентифікацію осіб та об'єктів, задіяних у VPN. Перша гарантує, що дані дійшли до адресата саме в тому вигляді, в якому були послані. Найпопулярніші алгоритми перевірки цілісності даних на сьогодні - MD5 і SHA1. Контроль трафіку увазі визначення і керування пріоритетами використання пропускної смуги VPN. З його допомогою ми можемо встановити різні пропускні смуги для мережевих додатків і сервісів в залежності від ступеня їхньої важливості.

Зазвичай VPN утворюють на рівнях не вище мережевого, так як застосування криптографії на цих рівнях дозволяє використовувати в незмінному вигляді транспортні протоколи (такі як TCP, UDP).

Користувачі Microsoft Windows позначають терміном VPN одну з реалізацій віртуальної мережі — PPTP, причому вона частіше використовується не для створення приватних мереж.

Найчастіше для створення віртуальної мережі використовується інкапсуляція протоколу PPP в який-небудь інший протокол — IP (такий спосіб використовує реалізація PPTP — англ. Point-to-Point Tunneling Protocol) або Ethernet (PPPoE) (хоча і вони мають відмінності). Технологія VPN останнім часом використовується не тільки для створення приватних мереж, але і деякими провайдерами на пострадянському просторі для надання виходу в Інтернет.

При належному рівні реалізації та використанні спеціального програмного забезпечення мережа VPN може забезпечити високий рівень шифрування переданої інформації. При правильному підборі всіх компонентів технологія VPN забезпечує анонімність в Мережі.

Зазвичай, при створенні VPN, використовують підключення типу точка-точка до певного сервера, або установку ethernet-тунелю з певним сервером, при якій тунелю призначають певну підмережу. Сервер VPN при цьому виконує функції маршрутизації та фільтрування трафіку для доступу до локальної мережі через VPN.

Список використаних джерел

1. *Аудит інформаційної безпеки інформаційних систем та інформаційно-телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov.ua/audit-of-information-security*
2. *iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс]. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.*
3. *Open Source Security Testing Methodology Manual (OSSTMM) [Електронний ресурс]. – Режим доступу: http://www.isecom.org/research/osstmm.html.*