Лекція 26. Віртуальна приватна мережа

VPN (Virtual Private Network — віртуальна приватна мережа) — загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

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).

Структура VPN

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 (загальнодоступної) 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.

Класифікація

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

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.

Рівні реалізації

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.

VPN-міст

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.

При використанні такого підходу ми все ще маємо можливість фільтрувати трафік на підставі способу підключення (наприклад, використовувати для локальної мережі та для віддалених користувачів різні фільтри), але виключається необхідність налаштування маршрутизації, а віддалені машини включаються прямо в локальну мережу, бачать ресурси, навіть здатні використовувати широкосмугові посилки взагалі без додаткового налаштування. Через такий VPN у них відображаються всі комп'ютери локальної мережі Windows, всі доступні XDMCP-сервери при XDMCP broadcast.

Реалізація

Існують реалізації віртуальних приватних мереж під TCP/IP, IPX і AppleTalk. На сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP/IP, і абсолютна більшість VPN рішень підтримує саме його. Адресація в ньому найчастіше вибирається згідно зі стандартом RFC 5735, з діапазону Приватних мереж TCP/IP

Протоколи VPN

- IPSec (англ. IP security) — часто використовується поверх IPv4.
- PPTP (англ. Point-to-point tunneling protocol) — розроблявся спільними зусиллями декількох компаній, включаючи Microsoft.
- PPPoE або PPP (англ. Point-to-Point Protocol over Ethernet)
- L2TP (англ. Layer 2 Tunnelling Protocol) — використовується в продуктах компаній Microsoft і Cisco.
- L2TPv3 (англ. Layer 2 Tunnelling Protocol version 3).
- OpenVPN SSL VPN з відкритим вихідним кодом, підтримує режими PPP, bridge, point-to-point, multi-client server