УДК 004.415
Костик С.– ст. гр. РІ-51
Тернопільський державний технічний університет імені Івана Пулюя

ОГЛЯД ТЕХНОЛОГІЙ VPN

Науковий керівник: к.т.н. асистент Луцків А.М.

Так історично склалося, що під одним терміном VPN розуміються дві різні по своїх цілях, завданнях і використовуваних алгоритмах інформаційні технології:

- технології забезпечення гарантованої якості обслуговування для корпоративного трафіку, що транспортується через глобальні мережі.
- технології забезпечення інформаційної безпеки корпоративного трафіку передаваного через глобальні мережі (наприклад, інтернет).

До першої групи VPN-технологій відносяться різні спеціалізовані технології управління QOS (RSVP, DiffServ, MPLS), а також деякі базові мережеві технології з вже вбудованими елементами QOS (ATM, Frame relay).

Друга група VPN-технологій виконує функції авторизації абонентів корпоративних мереж і функції криптографічного захисту передаваних даних. Як правило, технології цієї групи є різними реалізаціями механізму інкапсуляції стандартних мережевих пакетів канального (технології PPTP, L2F, L2TP), мережевого (технології SKIP, IPSec/IKE) і вище розміщених рівнів моделі OSI/ISO (технології SOCKS, SSL/TLS). Ці технології нестримно розвиваються і вже сьогодні використовуються для створення розподілених захищених мереж.

Слід зазначити, що існують різні види реалізації VPN - тунелювання: VPN на базі маршрутизаторів; VPN на базі мережевих операційних систем; VPN на базі міжмережевих екранів; VPN на базі спеціалізованого програмного забезпечення.

В кожного з вище перелічених рішень є свої достоїнства і недоліки.

До недавнього часу для створення VPN найширше застосовувався протокол канального рівня L2TP. Він забезпечує інкапсулювання протоколів мережевого рівня (NETBIOS, IPX, IP і ін.) в пакети канального рівня (PPP). Цей протокол володіє рядом переваг: незалежність від транспортного рівня, що дозволяє використовувати його в гетерогенних мережах; підтримка в ОС Windows 2000, що дозволяє будувати комбіновані VPN.

Проте L2TP має дуже серйозний недолік, обумовлений його "канальною природою": для гарантованої передачі захищеного пакету через складені мережі всі проміжні маршрутизатори повинні підтримувати цей протокол, що є практично нездійсненною умовою, що обмежує його вживання.

На сьогоднішній день одним із самих реалізованих і досконалих інтернет-протоколів, для побудови VPN є протокол IPSec (IP Security). Він забезпечує аутентифікацію, перевірку цілісності і шифрування повідомлень на рівні кожного пакету. Для управління криптографічними ключами IPSec використовує протокол IKE(Internet Key Exchange - протокол обміну Інтернет-ключами). Головною перевагою IPSec є те, що це протокол мережевого рівня. VPN, побудовані на його базі, працюють абсолютно прозоро для всіх додатків, мережевих сервісів. IPSec дозволяє маршрутизувати зашифровані пакети мережам без додаткового налаштування проміжних маршрутизаторів, оскільки він зберігає, прийнятий в IPv4, стандартний IP-заголовок.

Виходячи з вище сказаного, при організації VPN, можна запропонувати використання технології на основі IPSec, що дасть усі вагомі переваги.