УДК 004.7
Г. Баран
(Тернопільський національний технічний університет імені Івана Пулюя)

ЛОГІЧНА ІЗОЛЯЦІЯ ТРАФІКУ У VPN

Трафік користувача ізолюється засобами транспортної мережі. Раніше в операторів проводового зв'язку користувалися популярністю технології виділення логічних L2-каналів "точка-точка" Frame Relay і ATM, але поступово вони були замінені протоколом MPLS (Multiprotocol Label Switching). Доступні й інші варіанти логічної ізоляції – для бездротових мереж поверх GPRS/UMTS, приміром, можливе виділення віртуальної приватної мережі з окремим ідентифікатором APN, для метромереж на базі технології Ethernet здійснюється тунелювання на другому рівні (QinQ).

MPLS ґрунтується на комутації міток. При одержанні пакета від користувальницького пристрою (Customer Equipment, CE) вхідним граничним маршрутизатором оператора (Provider Edge, PE) до нього додається одна або кілька міток. Вибір маршруту пакета до вихідного PE-маршрутизатора на транзитних вузлах мережі оператора зв'язку (P-маршрутизаторах) здійснюється не шляхом розбору IP-адреси, а за допомогою аналізу зовнішньої мітки. У випадку MPLS VPN вхідним PE-маршрутизатором до пакету додається ще й внутрішня VPN-мітка, що унікально визначає номер клієнтської VPN.

При коректному настроюванні PE-маршрутизаторів можна практично повністю виключити загрози, пов'язані із проникненням пакетів між VPN або DoS-атаками. Таким чином, можна без побоювань передавати інтернет-трафік і конфіденційну інформацію в різні частки підмереж.

Хоча технологія MPLS захищає користувачів приватних мереж один від одного, вона не має сил убезпечити користувацький трафік від цілеспрямованого перехоплення. Якщо зловмисник має адміністративні права або фізичний доступ до мережі передачі даних, він у стані "віддзеркалити" і записати будь-який трафік, що передається у відкритому виді. Зрозуміло, оператор зв'язку може організаційно-технічними засобами зменшити ймовірність нелегітимного прослуховування, але повністю виключити перехоплення йому не вдасться. Тому при передачі чутливої інформації бажано сполучати логічну ізоляцію із шифруванням між користувацькими пристроями. Традиційно для цього завдання застосовується IPSec поверх MPLS VPN. Але IPSec-тунелі "точка-точка" зводять нанівець переваги MPLS, такі як підтримка багатоадресних розсилань і можливість створення повнозв’язних часток мереж рівнів L2 або L3. Тому разом з MPLS слід переважно використовувати технологію шифрованого транспорту GET VPN, що задіює IPSec, але без необхідності організації тунелів.