УДК 004.056:65.012.8(045)

ЗАХИСТ ЦИФРОВИХ КАНАЛІВ ЗВ'ЯЗКУ ЗА ДОПОМОГОЮ СИСТЕМ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Василина А.В., Яловий М.М.
Львівський державний університет безпеки життєдіяльності
НК – Цибуляк Б.З., канд. фіз.-мат. наук
Львівський державний університет безпеки життєдіяльності

Забезпечення безпечної передачі даних через мережу Інтернет зараз становить одну з найважливіших проблем. Кількість мережевих атак постійно зростає, вони якісно змінюються, тому пошук надійної системи захисту інформації завжди актуальний, особливо у віртуальних приватних мережах (VPN), які стають все більш популярними та поширеними [1].

Згідно стандартного визначення, запропонованого Internet Engineering Task Force (IETF), VPN – це емуляція WAN (Wide Area Network – глобальної обчислювальної мережі), тобто територіально розподіленої інтрамережі чи мережі передачі даних, яка покриває значний географічний простір (регіон, країну, низку країн) і забезпечує передачу інформації з використанням комутованих та виокремлених ліній або спеціальних каналів зв'язку, IP-обладнання спільного чи загального доступу, такого як Інтернет чи приватні IP-магістралі.

Відповідно, сучасні VPN поділяють на три категорії:

1) VPN з віддаленим доступом;

2) внутрішні мережі на основі VPN;

3) зовнішні мережі на основі VPN.

Впровадження VPN значно полегшує виконання задачі встановлення зовнішньої мережі, а також здешевлює цей процес.

Суть віртуальної приватної мережі полягає в наступному:

- на всі комп'ютери, які мають вихід в Інтернет, встановлюється засіб, що реалізує VPN (VPN-агент);
- VPN-агенти автоматично шифрують всю вихідну інформацію (і, відповідно, розшифровують вхідну). Вони також слідкують за її цілісністю з допомогою електронного цифрового підпису (ЕЦП) чи криптографічної контрольної суми, розрахованої з використанням ключа шифрування. Мережа VPN формується на основі каналів зв'язку відкритої мережі.

Відкрите зовнішнє середовище передачі інформації можна розділити на середовище швидкісної передачі даних, для якого використовується мережа Інтернет, і повільніші загальнодоступні канали зв'язку, для яких звичайно застосовуються канали телефонної мережі. Ефективність VPN визначається ступенем захищеності інформації, що циркулює відкритими каналами зв'язку. Захист інформації в процесі її передачі по відкритих каналах базується на побудові захищених віртуальних каналів зв'язку, які ще називають тунелями VPN.

Захищена VPN повинна включати засоби запобігання НСД до внутрішніх ресурсів корпоративної локальної мережі і до корпоративних даних, що передаються по відкритій мережі. Звідси випливає, що до засобів VPN може бути віднесене вельми широке коло пристроїв захисту: маршрутизатор з вбудованими можливостями фільтрації пакетів, proxy-сервер, багатофункціональний міжмережевий екран, апаратний і програмний шифратори трафіку, що передається.

VPN-пристрої можуть виконувати у віртуальних приватних мережах роль

шлюзу безпеки або клієнта. Шлюз безпеки VPN (security gateway) – це мережевий пристрій, що підключається до двох мереж, і виконує функції шифрування і автентифікації для численних хостів позаду нього. Розміщення шлюзу безпеки VPN виконується так, щоб через нього проходив весь трафік, призначений для внутрішньої корпоративної мережі. Мережеве з'єднання шлюзу VPN прозоре для користувачів позаду шлюзу; воно представляється виділеною лінією, хоча насправді прокладається через відкриту мережу з комутацією пакетів. Адреса шлюзу безпеки VPN вказується як зовнішня адреса вхідного тунельованого пакету, а внутрішня адреса пакету є адресою конкретного хоста позаду шлюзу [3].

Основні переваги VPN з віддаленим доступом перед традиційним вирішенням проблеми віддаленого доступу:

- відпадає повністю необхідність в серверах та пов'язаних з ним модемних пулах;
- також не має потреби в обслуговуючому персоналі, оскільки віддалений зв'язок забезпечується Інтернет-провайдером;
- можна обійтись без високовартісного комутованого з'єднання з дуже віддаленими користувачами, оскільки такі з'єднання у VPN замінюються на локальні комутовані з'єднання;
- обслуговування таких з'єднань є відносно недорогим для віддалених користувачів;
- через використання локального комутованого з'єднання модеми працюють з меншими перевантаженнями ніж при традиційному способі віддаленого доступу;
- VPN забезпечують кращу доступність до корпоративного сайту, тому що підтримують мінімальний рівень послуг доступу, не зважаючи на зростання числа одночасних користувачів мережі. Навіть якщо при великій кількості користувачів рівень надання послуг і знизиться, доступність до мережі не переривається повністю.

Водночас, у VPN даного типу спостерігаються і ряд недоліків:

- на жаль, VPN з віддаленим доступом наразі не гарантують належної якості;
- можливість втрати даних доволі висока; крім того, пакети можуть доставлятися пошкодженими;
- внаслідок ускладнених алгоритмів шифрування вартість протоколів значно зростає; це призводить до затримки процесу автентифікації, до того ж, компресія даних на базі IP та PPP виявляється надзвичайно повільною і не зовсім вдалою;
- внаслідок накладання ресурсів Інтернет-мережі, при передачі надважливих чи секретних мультимедійних даних по тунелях VPN віддаленого доступу затримка передачі може виявитися дуже значною, а пропускна здатність – надто низькою.

Отже, застосування програмно-реалізованих технологій VPN дозволяє ефективно забезпечити швидку та безпечну передачу конфіденційної інформації через мережу Інтернет. Перевагою технології VPN в даному застосуванні є те, що організація віддаленого доступу робиться не через виділені канали зв'язку, а через Інтернет, що набагато дешевше й легше. Недолік технології VPN в тому, що засоби побудови VPN не є повноцінними засобами виявлення та блокування атак.

ЛІТЕРАТУРА

1. Фратто М. Секреты виртуальных частных сетей // Сети и системы связи. – 1998. - N 3. - С. 138-148.
2. . BollapragadaV., Mohamed Kh., Wainner S. IPSec VPN Design. – Cisco Press, 2005. – 384 p.
3. Gupta M. Building a Virtual Private Network. – Premier Press, 2003. – 448 p.