УДК 004.7

І.І. Пархоменко, кандидат технічних наук, доцент, О.О. Квачук
(Національний авіаційний університет, Україна)

ПЕРЕВАГИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ VPN В КОРПОРАТИВНИХ МЕРЕЖАХ

Ефективне застосування інформаційних технологій у поєднанні з технологіями в області інформаційної безпеки є найважливішим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств і організацій. Технологія віртуальних приватних мереж VPN дозволяє вирішувати ці завдання, забезпечуючи зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу, «прокладеного» у загальнодоступній мережі Інтернет.

Вступ. Ефективне застосування інформаційних технологій у поєднанні з технологіями в області інформаційної безпеки є найважливішим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств і організацій. Технологія віртуальних приватних мереж VPN дозволяє вирішувати ці завдання, забезпечуючи зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу (тунелю), «прокладеного» у загальнодоступній мережі Інтернет.

VPN - це об'єднання локальних мереж або окремих машин, підключених до мережі загального користування, в єдину віртуальну (накладену) мережу, що забезпечує секретність і цілісність інформації, яка передається по ній.

Суть даної технології полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується шифрований канал, що забезпечує високий рівень захисту переданої з цього каналу інформації за рахунок застосування спеціальних алгоритмів шифрування.

Використання технології VPN необхідно там, де потрібен захист корпоративної мережі від дії вірусів, зловмисників, некомпетентних користувачів, а також від інших загроз, які є результатом помилок в конфігурації або адміністрування мережі.

Постановка задачі. У міру розвитку компанії у керівництва обов'язково виникають питання: створення максимально гнучкої та ефективної системи управління підприємством, офісними майданчиками, створення єдиної системи документообігу, оперативного збору інформації та звітів зі складів і виробничих майданчиків, централізація інформаційно-фінансових потоків і т.д. Правильне вирішення цих питань дозволяє успішно керувати компанією в цілому, робить її гнучкою і динамічно розвивається. Світовий досвід великих компаній і корпорацій говорить про те, що таким рішенням є створення корпоративної мережі передачі даних. Сучасні IT-технології дозволяють створювати корпоративні мережі на основі високо надійних і захищених мереж передачі даних. Для найефективнішого впровадження такого рішення необхідно, щоби користувачі могли звертатися до корпоративної мережі, не встановлюючи комутоване з'єднання, що дозволяє скоротити чисельність модемів або взагалі відмовитися від них. Бажано обійтися і без виділених ліній, що з'єднують віддалені офіси. Все це має за мету підвищити продуктивність праці, так як співробітники можуть користуватися найшвидшими лініями зв'язку, які є в їх розпорядженні, замість того щоб витрачати час на встановлення комутованого з'єднання через банк модемів.

Метою матеріалу є розгляд, визначення і обґрунтування переваг впровадження і використання технологій VPN в корпоративних мережах.

Можна виділити три фундаментальні властивості, що перетворюють накладену корпоративну мережу, побудовану на базі мережі загального користування, у віртуальну приватну мережу: шифрування; аутентифікація; контроль доступу.

Тільки реалізація всіх цих трьох властивостей дозволяє захистити власні машини, сервери підприємства і дані, передані по фізично незахищених каналах зв'язку, від зовнішніх небажаних вторгнень, витоку інформації і несанкціонованих дій.

На рис. 1 наведена схема корпоративної мережі, захищеної з використанням VPN-технологій.

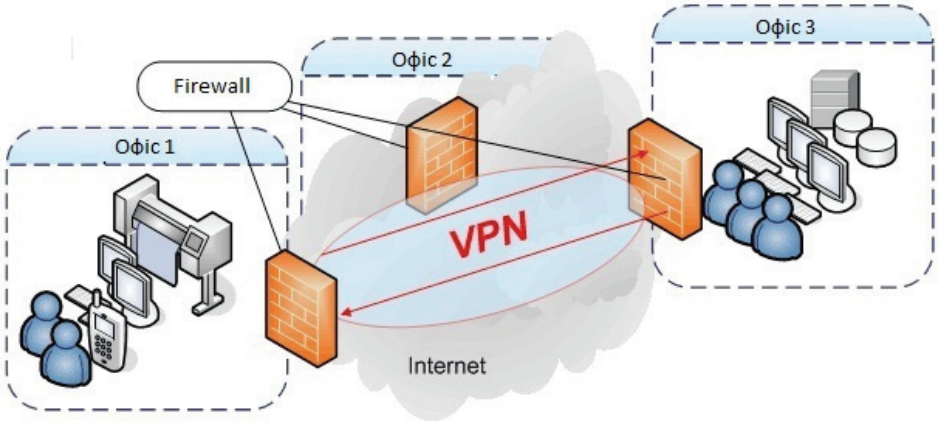

Рис.1 Корпоративна мережа, захищена з використанням VPN-технологій.

Переваги VPN-технологій

Програми віртуальних приватних мереж забезпечують шифровану передачу даних. Як правило, вони здатні безпечно виконувати різні функції віддаленого комп'ютера, не тільки передавати веб-трафік. Так що їх використання є одним з найбільш безпечних способів. Після налаштування програмного забезпечення, використовувати його дуже просто.

Вибір на користь даної технології для забезпечення безпеки мережних рішень обумовлений наступними її перевагами: простота використання; використання механізмів сповіщень і авторегістрації; відсутність будь-яких обмежень на кількість одночасних з'єднань по VPN; мобільність; простота підключення партнерів або клієнтів до своїх ресурсів; безперебійність роботи мережі VPN при наявності в мережах NAT-пристроїв; забезпечення проходження між собою прямого трафіку при будь-яких конфігураціях; менша вартість; підвищена надійність і безпека функціонування інформаційних систем; можливість підтримки інфраструктури електронного цифрового підпису.

Розглянемо їх особливості докладніше.

1. *Простота використання*. Це програмне, легко встановлюване (не вимагаюче практично ніяких настройок для клієнтського місця), інтегроване з мережним екраном рішення, що забезпечує безпеку як окремого комп'ютера в локальній мережі (або її фрагментів), так і локальної мережі в цілому.

2. *Використання механізмів сповіщень і авторегістрації***.** При включенні в мережу VPN чергового мережного ресурсу механізми сповіщень і авторегістрації забезпечують моментальну настройку всіх учасників VPN, пов'язаних з новим ресурсом, на роботу з ним.

3. *Відсутність будь-яких обмежень на кількість одночасних з'єднань по VPN***.** Рішення ідеально працює одночасно і в локальній мережі, і при взаємодії із зовнішніми ресурсами. Відсутні будь-які обмеження на кількість одночасних з'єднань по VPN. Забезпечується підтримка стандартних служб імен (DNS, WINS).

4. *Мобільність***.** Мобільний користувач може працювати при будь-яких переміщеннях, навіть якщо у нього на комп'ютері розміщені серверні служби (за рахунок підтримки технології динамічного DNS).

5. *Простота підключення партнерів або клієнтів до своїх ресурсів***.** При підключенні партнерів або клієнтів до своїх ресурсів:

a. організується точкове їх підключення до строго заданого ресурсу по заданих протоколах з криптографічною аутентифікацією трафіку, не залежною від IP-адреси джерела;

b. за рахунок формування кожним модулем VPN унікальних віртуальних адрес не потрібне узгодження адрес взаємодіючих мереж; система дозволяє об'єднувати в VPN-вузли з однаковими IP-адресами.

6. *Безперебійність роботи мережі VPN при наявності в мережах NAT-пристроїв***.** Присутні в мережях NAT-пристрої не порушують безперебійність роботи мережі VPN. Доступ до вузлів, що знаходяться за NAT-пристроями, можливий як шляхом настройки правил пропуску UDP-пакетів по заданому порту, так і за рахунок спеціальних механізмів підтримки автоматично створюваних на NAT-пристрої динамічних правил.

7. *Забезпечення проходження між собою прямого трафіку при будь-яких конфігураціях.* Модулі VPN забезпечують проходження між собою прямого трафіку при будь-яких конфігураціях, без перешифрування на проміжних вузлах.

8. *Менша вартість.* За наявності каскадів подвійне шифрування трафіку і, відповідно, його подвійна інкапсуляція не проводяться, що виключає витрати, пов'язані з цим.

9. *Підвищена надійність і безпека функціонування інформаційних систем.* Використовування симетричної ключової структури і наявність системи автоматичного розподілу ключів значно підвищують надійність і безпеку функціонування інформаційних систем в порівнянні з будь-якими іншими рішеннями VPN, що базуються на PKI-технологіях.

10. *Можливість підтримки інфраструктури електронного цифрового підпису.* В системі присутні всі необхідні рішення для підтримки інфраструктури електронного цифрового підпису, інтегровані з різними додатками.

Також маємо:

• можливість захисту всієї корпоративної мережі - від великих локальних мереж офісів до окремих робочих місць. Захист може бути поширена на всі ланки мережі - від сегментів локальних мереж до комунікаційних каналів глобальних мереж, у тому числі виділених і комутованих ліній;

• масштабованість системи захисту, тобто для захисту об'єктів різної складності і продуктивності можна використовувати адекватні за рівнем складності, продуктивності і вартості програмні або програмно-апаратні засоби захисту;

• використання ресурсів відкритих мереж як окремих комунікаційних ланок корпоративної мережі; всі загрози, що виникають при використанні мереж загального користування, будуть компенсуватися засобами захисту інформації;

• забезпечення підконтрольності роботи мережі і достовірна ідентифікація всіх джерел інформації. При необхідності може бути забезпечена аутентифікація трафіку на рівні окремих користувачів;

• сегментація ІС та організація безпечної експлуатації системи, що обробляє інформацію різних рівнів конфіденційності, програмними та програмно-апаратними засобами захисту інформації.

Висновки. В роботі розглянуто та визначено переваги технологій VPN. Обґрунтовано основні переваги впровадження і використання технологій VPN в корпоративних мережах.

Список літератури

1. Браун С. Виртуальные частные сети — №3(18), 2003, 503 с.
2. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей — №10, 2003, 248 с.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети – 2006, 958 с.
4. Таненбаум Э. Компьютерные сети. – 2003, 992 с.