УДК 004.932

ЗАХИЩЕНИЙ ДОСТУП НА ОСНОВІ DMVPN В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

к.т.н., с.н.с. Волошко С.В., Сергєєв В.В.

Полтавський національний технічний університет імені Юрія Кондратюка
Email: sergijvolosko@gmail.com

У останнє десятиліття у зв'язку з бурхливим розвитком мережі Інтернет і мереж загального доступу у світі стався якісний стрибок в поширенні і доступності інформації. Користувачі отримали дешеві і доступні канали зв'язку. Прагнучи до економії коштів, організації використовують такі канали для передачі критичної та управлінської інформації.

На сьогоднішній час існують різноманітні послуги, методи та протоколи передачі інформації в мережі Інтернет, такі як послуги мережі Інтернет: електронна пошта, доступ до файлів віддалених комп'ютерів, пошук інформації в базах даних, спілкування з іншими користувачами мережі Інтернет, доступ до інформаційної системи WWW, які використовують різного роду протоколи: TCP/IP, FTP, NNTP, HTTP, UDP, SMTP, POP, IMAP, TELNET.

Різке зростання масштабів і складності інформаційно-телекомунікаційних мереж (ІТМ) та збільшення кількості інформації, що в них циркулює, призводить до збільшення загроз інформації (як випадкових, так і умисних), збитків (фінансових та інших) від реалізації цих загроз. Це призводить до впровадження нових технологій для захищеної передачі даних в мережах Інтернет та Інтранет.

Virtual Private Network (VPN) – це об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку даних, що циркулюють по ній.

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеки двох основних типів:

− несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі, отримуваний зловмисником в результаті несанкціонованого входу в мережу;

− несанкціонований доступ до корпоративних даних в процесі їх передачі по відкритій мережі.

Забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті мережі, зокрема через мережу Інтернет, можливо шляхом ефективного рішення наступних завдань:

− захисту підключених до відкритих каналів зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища;

− захисту інформації в процесі це передачі по відкритих каналах зв'язку.

Завдання захисту інформації в процесі її передачі по відкритих каналах зв'язку переходить на перший план, побудова захищених мереж базується на впровадженні технології VPN [1].

VPN мережі стали вирішенням цієї проблеми, тому вивчення, використання та побудова для захищеної передачі даних в мережі Інтернет та Інтранет вважаю актуальною темою сьогодення.

Метою даної роботи є аналіз застосування віртуальних приватних мереж в ІТМ спеціального призначення.

В роботі запропоновано технологію DMVPN для застосування у складі комплексних апаратних зв'язку та елементів стаціонарних вузлів зв'язку з метою захисту інформації.

DMVPN – динамічна багатоточкова віртуальна приватна мережа – рішення на основі Cisco IOS Software для створення масштабованих віртуальних приватних мереж, захищених на рівні IP-протоколу.

DMVPN використовує централізовану архітектуру для полегшення впровадження і управління розгортанням, які потрібні для розмежування контролю доступу різних груп користувачів і співробітників, у тому числі мобільних, комутованих і користувачів зовнішніх мереж.

DMVPN дозволяє філіальним структурам підтримувати зв'язок один з одним безпосередньо, використовуючи Інтернет. При цьому між сайтами не вимагається підтримувати постійне підключення до VPN. Це дозволяє звести до мінімуму розгортання захищених каналів VPN і покращує продуктивність мережі за рахунок скорочення часу затримки і коливань під час оптимізації використання смуги пропускання.

Одна з головних переваг DMVPN – можливість побудови відмовостійких віртуальних мереж на базі класичного підходу за допомогою використанням протоколів динамічної маршрутизації. Шифрована mGRE хмара фактично є легко масштабованим L3 транспортом, прозорим для протоколів маршрутизації, – в цьому основна перевага перед класичним IPsec.

Література

1. Суленбергер Майк. Динамические многоточечные виртуальные частные сети IPSec (с применением протокола GRE/NHRP для масштабирования сети VPN IPSec) / Майк Суленбергер. – [Електронний ресурс] – Режим доступу до ресурсу: http://www.cisco.com/cisco/web/support/RU/9/92/92098_dmvpn.html

2. Лукацький А. Невідома VPN / А. Лукацький. – М.: Комп'ютер Пресс. – №10, 2001; http://abn.ru/inf/comdivss/network4.shtml

3. Норманн Р. Вибираємо протокол VPN / Р. Норманн. – М.: Windows IT Pro. – №7, 2000.

4. Петренко С. Захищена віртуальна приватна мережа: сучасний погляд на захист конфіденційних даних / С. Петренко – М.: Світ Internet. – №2, 2001.

5. Салліван К. Прогрес технології VPN. PCWEEK / Р. Салліван – М.: RE. – № 2, 1999.

6. Файльнер М. Віртуальні приватні мережі нового покоління LAN / М. Файльнер – М.: Журнал мережевих рішень. – №11, 2005.