УДК 004.052.52

А. О. Азарова
Р. О. Білий

АНАЛІЗ БАЗОВИХ КОНЦЕПЦІЙ РОЗПОДІЛЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Вінницький національних технічний університет

Анотація

У даному дослідженні розглянуто концепцію та технологію організації розподіленої корпоративної мережі. Вивчено технології об'єднання розподілених мереж VPN та IPsec. Проаналізовано забезпечення інформаційної безпеки в корпоративних мережах та методи її реалізації.

Ключові слова: розподілена мережа, корпорація, безпека

Abstract

This article considers the concept and technology of organization of a distributed corporate network. Technologies for combining distributed VPN and IPsec networks have been studied. The provision of information security in corporate networks and methods of its provision are analyzed.

Keywords: distributed network, corporation, security

Корпоративна мережа − це складна інфраструктура, призначена для передавання великого обсягу різноманітних інформаційних потоків (телефонія, обмін даними, доступ в Інтернет, відеоконференції і т. п.) у межах одного підприємства [1]. При цьому домінантною задачею, яку має бути розв'язано під час побудови корпоративної мережі, є оптимізація оброблення і розподілу інформаційних потоків. Сучасною нагальною задачею в галузі технології побудови мережі є об'єднання пакетного трафіку і мовної інформації в одному каналі зв'язку. Такий підхід дозволяє отримати конструктивні можливості для застосування телекомунікаційних та мережевих технологій, тобто відбувається конвергенція мереж. Ця тенденція виділяє вибір базових технологій побудови мережі, протоколів обміну і обладнання до категорії достатньо складних завдань.

Вибір концепції побудови конкретної корпоративної мережі визначається цілою низкою чинників: забезпечення необхідних інформаційних послуг, обсяги трафіку передавання інформації, існуюча інфраструктура і т.п. Разом із тим, існують і загальні вимоги до корпоративних мереж, зокрема, вони мають будуватися засобами перевірених технологій, що уможливлюють як надійність, масштабованість, гнучкість та мультисервісність.

Мережа сучасних суб'єктів господарювання має підтримувати низку додатків і керованих сервісів, що є найбільш необхідними для ведення бізнесу, зокрема, таких, як можливість високошвидкісного доступу до мережі Інтернет, створення віртуальних приватних мереж, передавання голосу поверх ip, проведення відеоконференцій, захист інформації та зберігання даних [2].

У територіально розподіленого підприємства для об'єднання відокремлених підрозділів в єдину корпоративну мережу можуть бути задіяні виділені канали зв'язку або загальнодоступні мережі передавання даних. Якщо для передавання даних, голосового трафіку і відео використовуються виділені канали, інформація, що передається ними, захищена від зовнішніх впливів, але таке рішення, по-перше, є доволі витратним, а, по-друге, не кожне підприємство має технічну можливість отримати в своє розпорядження виділений канал.

У таких організаціях для створення єдиної корпоративної мережі часто використовуються з'єднання VPN через Інтернет по IPSec, іноді − засобами операторської мережі MPLS. Подібна мережева інфраструктура захищається за допомогою авторизації і управління доступом, тунелювання між майданчиками і шифрування.

Технологія віртуальних приватних мереж дозволяє отримати значні переваги за відносно невисокої вартості. Подібно до виділеного каналу, вона дозволяє створити захищене з'єднання між віддаленими майданчиками або локальними мережами. Під час організації VPN корпоративна мережа логічно відділена від публічних мереж, тобто трафік захищений від несанкціонованого доступу. Таким чином компанія отримує повний контроль над її функціонуванням. У середині такої мережі можна передавати різні види трафіку з поділом за класами обслуговування. Засобами VPN

об'єднують розподілені офіси в загальну мережу, створивши єдиний адресний простір локальної мережі та єдину нумерацію в системі корпоративної телефонії, тобто формують загальний інформаційний простір, доступний з будь-якої точки корпоративної мережі.

IPSec VPN − досить простий і поширений спосіб створення захищеної мережевої інфраструктури територіально розподілених компаній. Між пристроями створюються віртуальні тунелі, і весь трафік шифрується на обладнанні замовника. Таким чином забезпечується незалежність від оператора зв'язку. Хоча рішення і є менш вартісним, порівняно з орендою каналів, недоліком є потреба додаткового обладнання (або ПЗ), не завжди можна гарантувати якість сервісу.

Вибір технології і варіанти підключення залежать від виду трафіку інформації, що передається, структури організації та її бізнес-процесів, вимог до інформаційної безпеки, тарифів оператора, послугами якого компанія збирається скористатися, та ін. Потрібно оцінити необхідну пропускну здатність і обсяг трафіку, вимоги до параметрів каналу зв'язку (включаючи надійність і ступінь захисту) для трафіків різного типу. Аналіз бізнес-процесів допомагає виявити, наскільки критичні для діяльності підприємства використовуються сервіси.

У теперішній час виникає нагальна потреба безпечного користування хмарними сервісами, що забезпечується компетенцію провайдера. Однак передбачені технології захисту не вирішують проблем, пов'язаних зі своєчасним припиненням або правильним розподілом прав доступу до ресурсів. ІТ-адміністратор повинен вибудувати процес управління доступом (Identity Management), який дозволить своєчасно блокувати звернення співробітника до зовнішніх сервісів під час зміни його статусу (перехід в інший відділ, майбутнє звільнення). Крім цього, такі процеси повинні враховувати і зміну ІТ-адміністратора.

Отже, для організації безпечної роботи в корпоративній мережі потрібен комплексний підхід. Різні технічні рішення − міжмережеві екрани, антивірусні і антиспам-системи, VPN та ін. − необхідно доповнювати організаційними заходами. Це особливо актуально, коли підприємство має територіально віддалені філії або потрібно створити умови для безпечної роботи мобільних співробітників, які перебувають у відрядженні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корячко В. П., Перепелкин Д. О. Корпоративные сети: технологии, протоколы, алгоритмы: Москва : Радио И Связь, 2011. 216 с.
2. Золотов С. Ю. Проектирование информационных систем : навч. посіб. Томск : Эль Учебное пособие Контент, 2013. 86 с.
3. Azarova A., Azarova L., Rosol N., Bystritskiy O. Models and methods of electronic digital signature. Theoretical and scientific fo undations of engineering: collective monograph / International Science Group. Boston : Primedia eLaunch, 2020. 180 p. P. 24 – 33.
4. Азарова А. О., Хісматулліна В. Ф. Електронні засоби політики інформаційної безпеки на державних підприємствах. Тези XLVIII науково-технічної конференції ВНТУ. 2019.
5. Азарова А. О., Азарова Л.Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.
6. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Процедура реєстрації у захищеному месенджері для організації комунікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97857. Дата реєстрації 05.06.2020 р. Заявка №99245 від 02.06.2020 р.
7. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Отримання та надсилання повідомлень користувачами у створеному месенджері для реалізації комунікаційного процесу на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97858. Дата реєстрації 05.06.2020 р. Заявка № 99246 від 02.06.2020 р.
8. Азарова А. О., Погребняк О. В., Азарова Л. Є., Міронова Ю. В., Ляхович Л. М. Комп'ютерна програма «Автентифікація користувача на основі клавіатурного почерку в режимі реального часу». Свідоцтво про реєстрацію авторського права на твір № 98144. Дата реєстрації 16.06.2020 р. Заявка № 99489 від 15.06.2020 р.
9. Азарова А. О., Азарова Л. Є., Міронова Ю. В., Бойчук Ю. В., Пазюк О. С. Комп'ютерна програма «Захист потокового відео засобів масової інформації з використанням підпису векторів руху». Свідоцтво про реєстрацію авторського права на твір № 98401. Дата реєстрації 06.07.2020 р. Заявка №99598 від 18.06.2020 р.

Азарова Анжеліка Олексіївна − к.т.н., професор каф. МБІС, заст. декана ФМІБ з наукової роботи та міжнародного співробітництва.

Білий Роман Олександрович – ст. гр. УБ-16б, Факультет менеджменту на інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: wintervinnitsa@gmail.com.

Azarova Anzhelika A. – PhD in technique, professor, deputy Dean of the Faculty of management and information security by scientific work and international cooperation.

Bilyi Roman O. – student of group UB-16b, Faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail: wintervinnitsa@gmail.com.