УДК: 004.7: 004.72 DOI: https://doi.org/10.30837/IYF.PCEIP.2024.061

СЦЕНАРІЙ ПОБУДОВИ ЗАХИЩЕНОГО СЕГМЕНТУ МЕРЕЖІ МІЖ ВІРТУАЛЬНИМИ ОФІСАМИ

Свергун В.А.
Науковий керівник – ас. Чепурна І.С.
Харківський національний університет радіоелектроніки, каф. ЕОМ
м. Харків, Україна
e-mail: vladyslav.sverhun@nure.ua

The article discusses scenarios for building corporate computer networks that take into account the requirements of secure remote access and fault tolerance by creating reliable virtual communication channels. Provision of secure access to nodes of corporate networks is implemented on the basis of hardware and software tools. The article considers the scenario of building a protected network segment between virtual offices according to the site-to-site scheme, where the Mikrotik CHR software is used as the end nodes.

Сучасні технології дистанційної роботи у бізнесі та державному секторі призвели до збільшення попиту на програмні рішення з організації дистанційних робочих місць. Наприклад, в Україні – це стало особливо актуально під час пандемії коронавірусної хвороби COVID-19 та повномасштабної збройної агресії рф [1]. У задачах організації відділених робочих місць виникає й інша задача, пов’язана із забезпеченням належного рівня мережної безпеки та створенню надійних віртуальних каналів зв’язку. Саме тому, у сучасних сценаріях побудови корпоративних комп’ютерних мереж вирішується комплексна задача системного та, власне, мережного рівня з урахуванням вимог захищеного віддаленого доступу, відмовостійкості віддалених віртуальних машин, конфіденційності та цілісності даних.

Мета даної роботи полягає у створенні сценаріїв функціонування корпоративних комп’ютерних мереж, які складаються щонайменше із декількох сегментів, поєднаних між собою за допомогою технології віртуальних тунелів. Цю мету можна досягти використовуючи стандартні підходи, на кшталт, традиційного VPN-тунелювання, а також можна застосувати нестандартні рішення, які включають в себе різні технології, як-от, багатошарове шифрування, агрегацію віртуальних каналів, асинхронні шляхи передачі даних тощо.

Серед інших рішень, які у сукупності можуть забезпечити наведені вище вимоги, для забезпечення захищеного доступу до вузлів корпоративних комп’ютерних мереж можуть бути використані рішення на основі програмно-апаратних засобів. Наприклад, це можуть бути міжмережні екрани та проксі-сервери.

З огляду на організацію сегментації корпоративних комп’ютерних мереж рівня віртуальних офісів можуть використовуватися мікросервіси хмарних

вендорів або класичні рішення VLAN, які підтримуються віртуалізованими рішеннями щодо комутації та маршрутизації трафіку, наприклад Open vSwitch [2].

Інші комплексні рішення можуть включати використання міжмережних екранів, каскадування proxy-серверів та ланцюгів VPN для досягнення зазначених вище вимог, однак це також може призводити до падіння швидкості передачі даних за рахунок багаторазового перепакування пакетів даних, їх шифрування та дешифрування зі сторони користувача [3].

В роботі досліджено сценарій побудови захищеного сегменту мережі між віртуальними офісами за схемою site-to-site, де у якості кінцевих вузлів використано програмне забезпечення Mikrotik CHR. Встановлено, що таке рішення надає такі переваги:

- можливість використання різних VPN-протоколів, за допомогою яких шифруються дані. Наприклад, протокол WireGuard надає можливість використовувати сценарій site-to-site в різних типах мережних топологій із забезпеченням максимальної стійкості віртуальних тунелів [4];
- часові затримки при передачі еластичного трафіку становлять на 15% вище, ніж у традиційних мережах, а нееластичного – до 5%.

Таким чином, розглянутий сценарій, за результатами проведених досліджень, показав, що для побудови захищених сегментів корпоративних мереж наразі є задовільним рішенням використання схеми site-to-site. У якості подальших досліджень планується вивчення питань тунелювання в віртуальних середовищах провідних вендорах.

Список використаних джерел

1. Hvozdetska K. P. Organization of teleworking via VPN technology / K. P. Hvozdetska, V. M. Tkachov // Збірник тез доповідей одинадцятої міжнародної науково-технічної конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління", 8-9 квітня 2021 року. - Том 2: секція 4. - Баку-Харків-Київ-Жиліна. - 2021. - С. 79.

2. Afanasieva A. DEVELOPMENT OF PRINCIPLES OF VPN-TUNNELING [Електронний ресурс] / A.M. Afanasieva // Information society: technological, economic and technical aspects of formation (issue 67) – 2022. – Режим доступу до ресурсу: http://www.konferenciaonline.org.ua/ru/article/id-520/.

3. Tkachov, V Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V.Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – 2020. – С. 82.

4. Верховський, І. Методи побудови віртуальних тунелів EXTRANET-систем / І. Верховський, В. Ткачов // Scientific review, –(2023). – 4(89), с. 22-40.