

*Колесник О. С., магістрант, гр. КБм-21-1,
Науковий керівник: Єфіменко А. А., канд. техн. наук,
доцент, зав. кафедри КІ та КБ,
Вакалюк Т.А., д-р пед. наук, професор, професор кафедри ІІЗ
Державний університет «Житомирська політехніка»*

ПРОЕКТ ПІДСИСТЕМИ ЗАХИЩЕНОГО БАГАТОТОЧКОВОГО ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ПРОВАЙДЕРА ІНТЕРНЕТ

На сьогоднішній день при створенні мережі малої чи великої компанії виникає важливе питання, від якого надалі залежить працездатність самої ж компанії: забезпечення високої доступності до інструментів праці, зокрема до мережі Інтернет. Існує чимало рішень для даного завдання. Кожне з них має різну вартість і свої складності реалізації. Проаналізуємо вибір рішення щодо побудови мережі (вибір маршрутизатора та міжмережевого екрану) у залежності від поставленого завдання. Розглянемо типові варіанти резервного підключення для будь-яких невеликих мереж офісного простору.

Першим є побудова високодоступної мережі передачі даних з використанням резервного обладнання, що знаходиться в режимі Standby (стабільний режим). Для реалізації даного рішення буде достатньо мати канали зв'язку у двох різних провайдерів. Це дозволить забезпечити резервування Інтернет-каналу в разі виходу з ладу каналного устаткування, або в разі виникнення проблем з передачею даних у основного провайдера. Як міжмережевий екран в даному варіанті можна використовувати багатофункціональні пристрої захисту від компанії Cisco - Cisco ASA [1].

У розпорядженні компанії в даному питанні виступають міжмережевий екран Cisco ASA та маршрутизатор Cisco. На перший погляд вони мають майже однакове застосування. На обох можливе налаштування маршрутизації та можливе налаштування захисту. Але, все ж таки, для більш коректної відповіді доведеться розглянути це питання й порівняти їх з урахуванням переваг та недоліків, виходячи з поставленої задачі.

Не секрет, що Cisco ASA, він же міжмережевий екран, у першу чергу являє собою захисний пристрій. Cisco ASA може маршрутизувати трафік і, що важливо, міжмережевий екран також підтримує протоколи динамічної та статичної маршрутизації. Якщо говорити про маршрутизатор, то не буде таємницею, що він також може маршрутизувати трафік та має більше доступних налаштувань [2].

Складність прийняття рішення полягає в тому, що часто функціонал не просто схожий, а походить один від одного. Тому відразу прийняти рішення є складно, що краще та надійніше буде служити на периметрі офісного простору. Для прикладу, розширені можливості функції SSL VPN постійно були перевагою ASA. Але не довелося довго чекати, щоб маршрутизатор встиг отримати багато функцій SSL VPN.

SSL VPN використовує протокол Secure Sockets Layer - або протокол безпеки транспортного рівня – в веб-браузерах, щоб надати користувачам можливість безпечного віддаленого доступу VPN. Наскрізь-не шифрування (end-to-end encryption) використовується для захисту всіх передач даних між підключеним до Інтернету пристроєм і сервером [3].

Список використаних джерел

1. Построение и резервирование центров обработки данных для малых и средних предприятий [Електронний ресурс] – Режим доступу до ресурсу: <http://gcs.kz/solution/27/>.
2. Межсетевые экраны Cisco ASA vs маршрутизаторы Cisco ISR [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco-parts.ru/articles/mezhsetevye-ekrany-asa-vs-marshrutizatory-isr/>.
3. What is SSL VPN and why you should use one? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.purevpn.com/blog/ssl-vpn/>.