Пекарєв М. Д., магістрант,
Державний університет «Житомирська політехніка»

ТЕХНОЛОГІЇ VPN В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Зв'язок та обмін інформацією в мережі стали необхідністю сучасного світу, але разом з цим з'явилися й загрози для конфіденційності та безпеки. Віртуальні приватні мережі (VPN) стали ключовим інструментом для забезпечення захисту даних під час передачі через публічні мережі, такі як Інтернет.

Site-to-site VPN використовуються для з'єднання декількох локальних мереж в одну велику мережу, щоб дозволити обмін даними та ресурсами між ними. Вона забезпечує захист всієї мережі, а не лише окремих пристроїв, і може економити кошти, оскільки не потрібно встановлювати окремі з'єднання з кожною локальною мережею. Проте, її налаштування може бути складним, вимагає високої пропускної здатності та спеціального обладнання та програмного забезпечення.

Site-to-point VPN використовується для з'єднання віддалених користувачів з локальною мережею. Вона дозволяє віддаленим користувачам зв'язуватися з локальною мережею з будь-якої точки світу, гарантує безпеку та приватність з'єднання, і легко налаштовується та використовується. Однак, пропускна здатність зв'язку може бути обмеженою, оскільки вся передача даних відбувається через одне з'єднання, і вона може бути дорожчою, коли потрібно підключити більше одного користувача.

Для найкращого вибору технології VPN потрібно врахувати такі параметри, як безпека, швидкість, надійність та сумісність з іншими системами. Для реалізації роботі було обрано GetVPN, оскільки він є надійним та стійким до атак, створює глобальну політику безпеки для всіх тунелів мережі та шифрує дані, що зменшує навантаження на мережевий протокол.

GetVPN, як одна з технологій VPN, забезпечує захищений тунель для передачі даних між вузлами. Його основна мета - забезпечити конфіденційність, цілісність та аутентичність даних у відкритих мережах. Система GetVPN оперує на рівні мережевого шару (Layer 3) і використовує технологію IPsec для шифрування даних та захисту їх від несанкціонованого доступу.

Основні переваги використання GetVPN полягають у його масштабованості та простоті управління. Він може легко інтегруватися з існуючими мережами та не потребує складних налаштувань на окремих пристроях. Крім того, GetVPN надає централізоване управління ключами, що спрощує процес управління безпекою.

Ця технологія також дозволяє ефективно використовувати широкосмугові канали і забезпечує високу швидкість передачі даних, що робить її привабливим рішенням для великих корпоративних мереж.

Важливим аспектом використання VPN є не лише захист від перехоплення даних ззовні, але й забезпечення конфіденційності у внутрішніх мережах. GetVPN вирішує цю проблему, застосовуючи механізм шифрування до внутрішніх трафіків, що уникне несанкціонованого доступу до внутрішніх мережевих ресурсів.

Інтеграція GetVPN з іншими інструментами кібербезпеки, такими як файрволи та системи моніторингу, дозволяє створити комплексний захист для мережі. Це дозволяє реагувати на загрози в реальному часі та вчасно уникати потенційних атак.

Незважаючи на всі переваги, впровадження технології VPN може вимагати уважного аналізу потреб мережі та правильного налаштування для досягнення максимальної ефективності. Проте в умовах постійного росту кіберзагроз, використання GetVPN залишається однією з найефективніших стратегій забезпечення конфіденційності та безпеки мережі.

Список використаних джерел

1. GetVPN // IPWITHEASE [Електронний ресурс] – Режим доступу до ресурсу: https://ipwithease.com/introduction-to-getvpn/
2. Чому користувачі використовують VPN [Електронний ресурс]. Режим доступу до ресурсу: http://businessua.com/telekom/83841chomu-bagato-koristuvachiv-internetu-vikoristovue-vpn-prichini.html
3. Що таке EDR та як він працює [Електронний ресурс]. Режим доступу до ресурсу: https://experience.dropbox.com/uk-ua/resources/what-is-vpn