адаптивності, веб-додаток має можливість бути вбудованим у різні платформи 3D-індустрії, маючи перевагу над пропрієтарними, водночас менш специфічними та гнучкими системами. Таким чином, процес перегляду та інтеракції з майже будь-якою 3D-моделлю стає простішим та доступнішим.

Література:

1. The Most Common 3D File Formats [Електронний ресурс] // Dibya Chakravorty – Серпень, 2019. – https://all3dp.com/3d-file-format-3d-files-3d-printer-3d-cad-vrml-stl-obj (дата звернення: 21.03.2021).
2. Khronos Group glTF Briefing [Електронний ресурс] // Khronos Group – Вересень, 2016. – https://www.khronos.org/assets/uploads/developers/library/overview/gltf-overview.pdf (дата звернення: 05.04.2021).

Яковенко К.О., студент
Харківський національний університет радіоелектроніки, м. Харків
Кафедра Електронних обчислювальних машин

БАГАТОШАРОВА ВІРТУАЛЬНА МЕРЕЖА

У наші дні до Інтернету підключено більше людей, ніж будь-коли раніше. Але з ростом цієї глобальної мережі зростає і постійно розвивається загроза кібербезпеки, яка турбує багатьох користувачів Інтернету.

Метою доповіді є огляд технології багатошарової (подвійної) мережі.

Для боротьби з постійно зростаючими загрозами конфіденційності та заради безпеки в Інтернеті розроблено багато програмного забезпечення, включаючи VPN та багатошарові VPN. [1]

Багатошаровий VPN - це декілька віртуальних мереж, з’єднаних між собою. За допомогою VPN між користувацьким комп’ютером та сервером VPN створюється зашифрований тунель. Весь відправлений користувачем трафік спочатку зашифровується VPN, а потім направляється через цей тунель на сервер. Подвійний VPN додає до цього рівняння ще один захищений тунель та сервер.

Якщо користувацький VPN зазвичай пропонує 256-бітове шифрування AES, використання подвійного VPN не означає, що у вас тепер є 512-бітове шифрування. Використання подвійного VPN просто означає, що трафік перенаправляється та зашифровується двічі.

Хоча існують різні типи багатошарових VPN, основна ідея полягає у використанні двох (або більше) безпечних тунелів разом. Спочатку між користувацьким комп’ютером та VPN створюється зв’язок. Потім між першим і другим сервером встановлюється другий зашифрований тунель.

Один з типів налаштування багатошарового VPN - це «вкладений ланцюжок», у якому використовуються дві або більше різних служб VPN з різним розташуванням. "Вкладений ланцюжок" пропонує посилений захист даних, які можуть бути скомпрометовані.

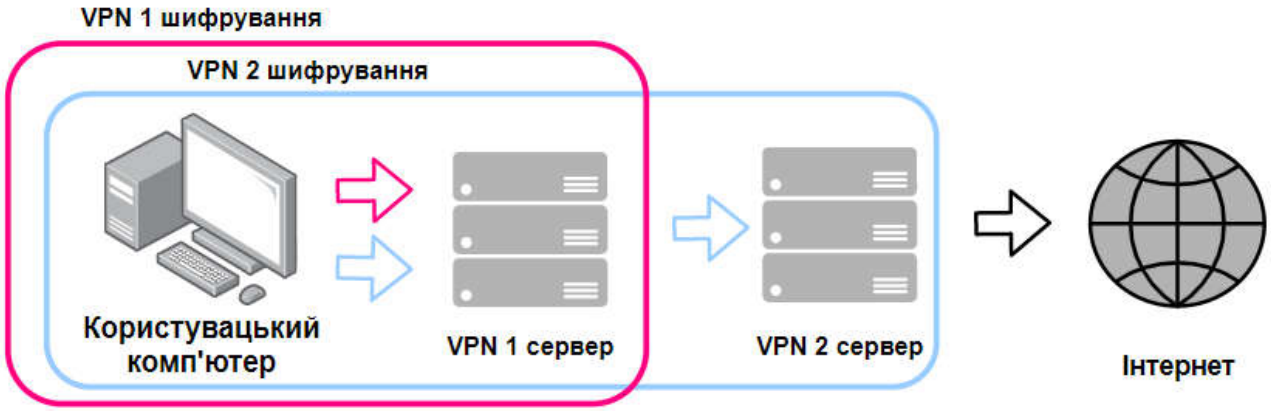

Рисунок 1 – принцип роботи «вкладеного ланцюжка»

В ідеальному виді весь трафік шифрується та перенаправляється послідовно через декілька захищених тунелів. Це те, що відоме як каскадування серверів VPN - основна ідея подвійних VPN. За допомогою подвійного VPN реальна IP-адреса користувача маскується двічі, а не лише один раз. [2]

Таким чином, забезпечення безпечної передачі даних через мережу Інтернет це досить важлива задача. Слід зазначити, що хоча подвійний VPN пропонує додатковий захист для тих, хто цього потребує, один VPN-сервер від преміум-провайдера задовільнить буденні потреби більшості користувачів через те, що багатошарова мережа VPN уповільнює швидкість передачі даних, а один сервер швидко справляється із поставленою задачею.

Література:

1. Коваленко А.А. Метод забезпечення живучості комп’ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв’язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.
2. Tkachov, V., Bondarenko, M., Ulyanov, O., & Reznichenko, O. (2019, December). Overlay Network Infrastructure for Remote Control of Radio Astronomy Observatory. In 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT) (pp. 161-165).

Ящук Ю.Р.
Державний університет телекомунікацій, місто Київ
Кафедра системного аналізу, студент

ОПТИМІЗАЦІЯ РОЗРАХУНКІВ ДЛЯ МАГІСТРАЛЬНОЇ ЛІНІЇ ЗА ДОПОМОГОЮ ІНФОРМАЦІЙНОЇ СТОРІНКИ

Інформаційні системи сьогодні досить часто використовуються для автоматизації будь-яких процесів для полегшення виконання завдань.

Аналізуючи результати стрімкого розвитку, можна зі впевненістю сказати, що технології магістральних мереж зв`язку невпинно вдосконалюються і не втрачають своєї актуальності.