УДК 004.7

Охріменко Д. С., магістрант
Науковий керівник: Єфіменко А. А., канд. техн. наук, доцент, зав. кафедри КІ та КБ,
Вакалюк Т. А. д-р пед. наук, професор, професор кафедри ІПЗ
Державний університет «Житомирська політехніка»

ПРОТОКОЛ ТУНЕЛЮВАННЯ МЕРЕЖЕВИХ ПАКЕТІВ GRE

GRE (genericrouting encapsulation – загальна інкапсуляція маршрутів) – розроблений Cisco протокол тунелювання мережевих пакетів. Основне призначення – інкапсуляція пакетів мережевого рівня моделі OSI в IP-пакети. Номер протоколу в IP - 47. Протокол не підтримує ніяких режимів аутентифікації або шифрування, його завдання – доставка пакетів.

Отже, тунель GRE використовується, коли пакети повинні бути відправлені з однієї мережі в іншу через Інтернет або незахищену мережу. У GRE віртуальний тунель створюється між двома кінцевими точками (маршрутизаторами Cisco), а пакети відправляються через тунель GRE. Протокол GRE вимагає білих IP-адрес для обох сторін тунелю і є протоколом без збереження стану, тобто ніяк не контролює доступність протилежного вузла, хоча більшість сучасних реалізацій містять додаткові механізми, що дозволяють визначити стан каналу [1].

Важливо відзначити, що пакети, що проходять всередині тунелю GRE, не зашифровано, оскільки GRE не шифрується тунель, а інкапсулює його з заголовком GRE. Отже, GRE є протоколом інкапсуляції і не виконує шифрування.

Створення тунелю GRE точка-точка без будь-якого шифрування надзвичайно ризиковано, оскільки конфіденційні дані можуть бути легко вилучені з тунелю і переглянуті іншими. Якщо потрібен захист даних, IPSec повинен бути налаштований для забезпечення конфіденційності даних – тоді GRE-тунель перетворюється в безпечний VPN-тунель GRE. Тунель GRE використовує інтерфейс «тунель» – логічний інтерфейс, налаштований на маршрутизаторі з IP-адресою, де пакети інкапсулюються і декапсулюються при вході або виході з тунелю GRE[2].

Таким чином, використовуючи GRE + IPsec, можна домогтися збалансованого по співвідношенню складність налаштувань/безпека рішення без шкоди для конфіденційності особистих переданих даних. IPsec не може інкапсулювати multicast трафік, broadcast трафік або не-IP-пакети, а GRE не може автентифікувати та шифрувати пакети.

За допомогою технології GRE через IPsec багатоадресні (multicast) та широкомовні (broadcast) пакети можуть бути інкапсульовані за допомогою GRE, а потім зашифровані за допомогою IPsec. У той же час інтерфейс, що підтримує GRE, збирає статистику про обсяг зашифрованого та розшифрованого трафіку. Коли шлюзи взаємопов'язані в режимі GRE через IPsec, шлюзи інкапсулюють пакети за допомогою GRE, а потім IPsec [4].

Потік даних, захищений IPsec, йде від початкової точки GRE до кінцевої точки GRE. У заголовку IP, доданому GRE під час інкапсуляції, адреса джерела – це адреса джерела тунелю GRE, а адреса призначення – адреса призначення тунелю GRE.

Хоча багато хто може подумати, що тунель GRE IPSec між двома маршрутизаторами схожий на VPN-з'єднання IPSec між сайтами, це не так. Основна відмінність полягає в тому, що тунелі GRE дозволяють multicast пакетам проходити через тунель, тоді як IPSec VPN не підтримує multicast пакети [3].

Перелік використаних джерел

1. Generic Routing Encapsulation, створення GRE тунелів [Електронний ресурс]. URL: https://vds-admin.ru/networks/gre-generic-routing-encapsulation-sozdanie-tunnelei.
2. Налаштування GRE тунелю на обладнанні Cisco [Електронний ресурс]. URL: https://wiki.merionet.ru/seti/22/nastroyka-gre-tunnelya-na-cisco/
3. Налаштування тунелів GRE та IPIP в Debian та Ubuntu [Електронний ресурс]. URL: https://interface31.ru/tech_it/2021/09/nastroyka-tunneley-gre-i-ipip-v-debian-i-ubuntu.html.
4. Налаштування тунелю GRE у мережі VPN [Електронний ресурс]. URL: https://blog.sedicomm.com/2019/11/01/nastrojka-tunnelya-gre-v-seti-vpn/.