ОПТИМІЗАЦІЯ ПРОЦЕСА СТВОРЕННЯ VPN З'ЄДНАННЯ

студ. К.К. Чередниченко Національний технічний університет "Харківський політехнічний інститут", м. Харків.

У загальному випадку VPN (Virtual Private Network – "віртуальна приватна мережа") – це об'єднання локальних мереж або окремих машин, підключених до мережі загального користування, у єдину віртуальну мережу. При цьому у встановленому з'єднанні організується зашифрований канал, що забезпечує захист інформації за рахунок застосування спеціальних алгоритмів шифрування. Використання VPN дозволяє створювати, групувати і перегруповувати сегменти мережі без зміни фізичної інфраструктури і від'єднання користувачів і серверів, що зменшує витрати на закупівлю, монтаж і конфігурування серверів віддаленого доступу, мережне обладнання, контроль трафіку віддаленого доступу. Таким чином, задача оптимізації створення VPN з'єднання є актуальною.

Проведено аналіз програмних рішень організації VPN за допомогою наступних протоколів: SSH та PPP, SSL/TLS та PPP, IPSec, FreeS/WAN, PPTP, VTun, cIPe, tinc. В результаті аналізу були виявлені переваги та недоліки цих протоколів. Виявлено, що найбільш оптимальним є використання нестандартного протоколу VTun.

VTun (Virtual Tunnel, віртуальний тунель) використовує тунельний інтерфейс, в якому дані шифруються по мірі входу в тунель і дешифруються на виході з нього. Обидві сторони тунелю мають про протилежну сторону інформацію про мережну адресу й те, які мережі лежать між ними. Коли на сервер приходить пакет, призначений для мережі, що перебуває на іншому кінці тунелю, він направляється на локальний тунельний інтерфейс. Потім ядро проводить інкапсуляцію даного пакета в IP-пакети й передає пакет, на відому адресу на іншому кінці тунелю. При досяганні віддаленого кінця тунелю пакет перевіряється, деінкапсулюється й передається на кінцеву адресу.

Таким чином, проведено аналіз програмних рішень організації VPN. Запропоновано рекомендації по оптимізації створення VPN з'єднання за допомогою протоколу VTun.