

# ІНДИВІДУАЛЬНА БЕЗПЕЧНА ДОМАШНЯ МЕРЕЖА З TCR100

## КОРОТКИЙ ЗМІСТ

Кібератаки на мережі продовжують зростати з роками, саме тому розробники поспішають усунути будь-які вразливості, які можуть поставити під загрозу безпеку інформації. Це стосується не лише налаштувань IoT на рівні компанії, а й домашніх мереж. З плином часу ризиків для безпеки стає все більше. Розробляється нове шкідливе програмне забезпечення, а нові пристрої пропонують більше лазівок, якими можуть скористатися зловмисники. Навіть наші телефони не є безпечними, оскільки зловмисне програмне забезпечення для мобільних пристроїв стає одним із головних джерел витоку даних.

## ЧЕЛЕНДЖ

Захист домашньої мережі важливий для кожного, хто має доступ до Інтернету. Користувачі повинні переконатися, що їх мережа безпечна з боку Інтернету та будь-якого пристрою, який може спробувати отримати до неї локальний доступ. Власник мережі повинен контролювати будь-який вхідний і вихідний трафік.

Оскільки будь-який новий пристрій, який уже заражений, може поширювати зловмисне програмне забезпечення далі, користувачам потрібна можливість розділити та відокремити домашню мережу, щоб підвищити її безпеку. Ентузіасти, можливо, захочуть зробити ще один крок далі та встановити спеціальний дозвіл щодо того, хто може отримати доступ до кожного пристрою чи вмісту в цій мережі. Це змушує їх шукати апаратне забезпечення з такою функціональністю.

Крім того, ентузіасти, як правило, не терплять будь-яких простоїв своєї мережі. Незважаючи на наявність високошвидкісної дротової мережі, вони зазвичай вибирають використання з'єднання LTE як варіант відновлення після відмови. Зазвичай споживчі маршрутизатори не мають підключення LTE або мають низьку швидкість стільникового зв'язку.

## LA SOLUCIÓN

Більшість ентузіастів мають більше технічних знань, ніж звичайні користувачі, і їм подобається мати складніші налаштування вдома. Вони знають про можливі ризики, які можуть створити неавторизовані та ненадійні пристрої, які підключаються до мережі, і тому виконують різні заходи зміцнення мережі.

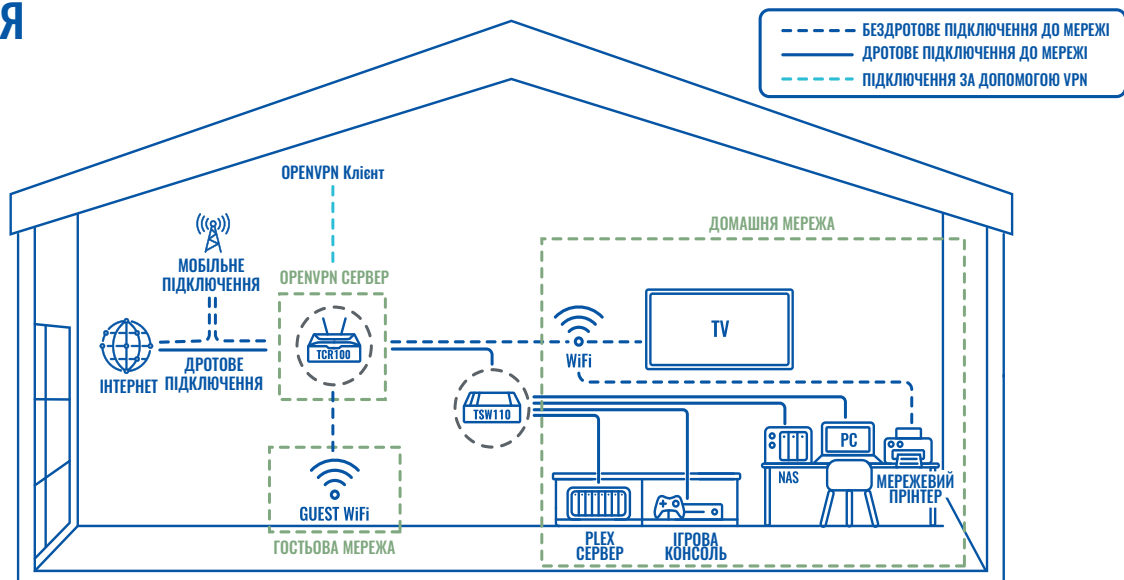
У цьому випадку ми пропонуємо наш останній продукт – стільниковий домашній маршрутизатор TCR100. Він дозволяє підключатися до Інтернету за допомогою дротового з'єднання та мобільної мережі WAN. Крім того, завдяки службі Dynamic DNS, що включає понад 70 шаблонів конфігурації провайдерів, користувачі можуть легко налаштувати власний домен і переконатися, що вони все ще можуть отримати доступ до своєї домашньої мережі після перемикавання або зміни динамічної IP-адреси.

Тут ми бачимо закриту гостьову мережу Wi-Fi, де підключені пристрої будуть ізольовані від домашньої мережі. Крім того, клієнти не будуть бачити один одного. Таке розділення гарантує, що ніхто ззовні не матиме доступу до апаратного забезпечення, і навіть якщо пристрій, заражений шкідливим ПЗ, він не зможе заразити інші пристрої в мережі.

Далі, у нас є сервер OpenVPN, який дозволяє підключатися до домашньої мережі віддалено. Метою тут є забезпечення безпеки домашньої мережі, оскільки перенаправлення портів створює вразливі місця в брандмауері. Однак, коли використовується OpenVPN, він запускає єдиний сервер, до якого користувачі можуть отримати доступ лише за допомогою належної конфігурації клієнта та сертифікатів доступу до нього з боку Інтернету. Таким чином, власник VPN може чітко контролювати доступ до мережі.

Нарешті, у нас є домашня мережа, куди за допомогою некерованого комутатора TSW110 ми підключили сервер PLEX, ігрову консоль, NAS (мережеве сховище) і ПК, використовуючи п'ять доступних портів LAN. Телевізор і мережевий принтер з'єднані бездротовим способом в одній мережі. Це налаштування дозволяє повністю контролювати, хто може отримати доступ до кожного пристрою, і встановлювати спеціальні дозволи, закриваючи небажані пристрої, які намагаються підключитися до мережі. Користувачі можуть навіть контролювати, який мережевий компонент може взаємодіяти з іншим, переконавшись, що один заражений пристрій не поширить шкідливе програмне забезпечення далі у мережу.

## ТОПОЛОГІЯ



## ПЕРЕВАГИ

- TCR100 підтримує кілька протоколів VPN, дозволяючи створювати безпечний тунель до домашньої мережі. За допомогою DDNS користувачі можуть встановлювати статичне доменне ім'я замість динамічної IP-адреси, яке може змінитися після відновлення після зміни IP-адреси.
- Брандмауер дозволяє створювати винятки щодо того, хто може отримати доступ до певних мереж, веб-сайтів і які порти можуть використовувати різні пристрої.
- Безпосередньо TCR100 підтримує багато різних протоколів VPN, дозволяючи користувачам вибирати, який з них вони хочуть використовувати.

## ЧОМУ САМЕ TELTONIKA NETWORKS?

Teltonika Networks має багаторічний досвід роботи з промисловими рішеннями IoT, де налаштування та безпека є ключовими елементами. Сьогодні ми використали те, що навчилися, щоб представити домашній маршрутизатор, який забезпечує безпеку та гнучкість, конкуруючи з промисловими продуктами. Ми прагнемо надавати всім нашим клієнтам тільки найкращий якісний продукт!

