РОЗПОДІЛЕНА МЕРЕЖА ДЛЯ СЕНСОРІВ

Заболотний Д.О.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: danylo.zabolotnyi@nure.ua

Abstract

There are many different reasons to have up-to-date information from many different points and different measurements across large area. It can be required by both civilian (weather stations, seismic sensors, road traffic sensors and controls, security cameras etc.) and military (acoustic, visual and radio drone detectors, video surveillance systems, radio-electronic intelligence systems, radio-electronic warfare systems etc.) purposes. This work is dedicated to development principles and practical approaches in implementing fast, reliable, secure, cost-efficient and scalable network for such installations.

Поточні проблеми

На поточний момент розповсюджена практика використання різного роду наборів сенсорів являє собою окремі осередки пристроїв, що побудовані та обслуговуються за залишковим принципом — тобто рішення по способу отримання даних, їх передачі, захисту і керуванням приймаються різними особами на свій погляд. Такий підхід призводить до того, що дані передаються з затримкою (в тому числі і через людський фактор), у різних форматах і представленнях, мережі для них будуються не на оптимальному обладнанні, а також вимагають додаткових часовитрат на обслуговування кожного кластеру. Наслідки такого підходу цілком очевидні — це додаткові витрати часу, фінансових і людських ресурсів, а також може призвести до неотримання критичної інформації. Також під час війни в Україні особливо гострою стала проблема електропостачання, тому відсутність загального підходу до енергоефективності обладнання також відіграє роль в надійності функціонування існуючих рішень.

Шляхи розв'язання

Як варіант рішення вищенаведених проблем пропонується розробка принципів побудови захищеної мережі, що дозволить кінцевим отримувачам (замовнику) інформації мати прямий доступ в режимі реального часу до відповідних систем і джерел. Це дозволить своєчасно виявляти зміни в навколишньому середовищі, дорожній обстановці в містах і поза ними, безпекових ризиках, та найважливіше — своєчасно виявляти та відслідковувати військові загрози.

Таблиця 1. Вимоги до мережі та засоби їх забезпечення

Пропускна здатність мережі має бути достатня для своєчасного отримання інформації без втрат	Для підключення джерел інформації (сенсорів) пропонується використовувати наступні канали доступу: • Послуги наземних операторів зв'язку • Послуги мобільних операторів зв'язку • Послуги супутникового зв'язку • Побудова окремих ділянок мережі При виборі каналів зв'язку в кожній окремій точці присутності мережі слід враховувати такі фактори як: • Наявність покриття • Надійність оператора (з залученням SLA) • Можливість побудови провайдеронезалежної ділянки (радіо- або кабельний канал до існуючого вузла)
Мережа має бути стійкою до втрати зв'язку в окремо взятому каналі передачі даних	Для збереження працездатності слід мати як мінімум 2 незалежні канали зв'язку в кожній окремій точці, наприклад пари наземний оператор + супутниковий оператор або власний канал зв'язку + мобільний оператор. Для автоматичного переключення між активними каналами слід використовувати обладнання, яке підтримує роботу з як мінімум 2 зовнішніми каналами зв'язку
Мережа має бути захищеною від стороннього втручання	Засоби протидії стороннього втручання: • Вузли зв'язку слід встановлювати в антивандальних ящиках, в закритих приміщеннях або на охороняємій території. • Доступ до обладнання має надаватися виключно після авторизації • Передача даних між вузлами має шифруватись
Має бути врахована можливість масштабування мережі	Мережа матиме масштабованість у випадку коли: • За потреби наявне обладнання може бути оновлене або замінене на аналогічне з вищими показниками (пропускна здатність, кількість та тип інтерфейсів і т.д.) • Канали зв'язку мають запас пропускної здатності або можливість розширення її (інший тариф у оператора або заміна типу інтерфейсу у власній мережі) • Можливість використовувати кінцевий вузол зв'язку в якості проміжного
Має бути енергоефективною	Поточна ситуація в Україні довела необхідність критично підходити до енергоефективності. В такому випадку пропонується при виборі обладнання надавати пріорітет такому, що потребує найменшу кількість енергії при співрозмірній продуктивності. Також варто враховувати можливість заживлення обладнання від джерел пос-

	тійного току для уникнення додаткових втрат на інвертування при роботі від батарей.
Стікість до зовнішніх нетехнічних факторів.	Основний фактор , який слід врахувати — використання прицнипу AnyVendor. У випадку неможливості замінити обладнання такою ж моделлю (застарівання, вихід з ринку країни, припинення виробництва, санкції, тощо) має бути можливість заміни або масштабування елементів мережі з обладнанням іншого виробника. З цією метою пропонується використання стандартизованих, не закритих інтерфейсів та протоколів (наприклад, слід утриматись від використання пропрієтарного протоколу EIGRP на користь відкритого OSPF).
Фінансово-матеріальна складова має бути найбільш оптимальною	При виборі обладнання слід враховувати баланс між його можливостями та наявним бюджетом.

Запропоноване рішення

Виходячи з вищенаведеного пропонуться створення в якості основного підходу масштабуємої захищеної віртуальної приватної IP-мережі (VPN) з шифруванням даних in-transit (IPSec).

З точки зору кінцевого мережного обладнання пропонується розглянути доступні варіанти маршрутизаторів, що мають функціонал VPN-клієнтів з використанням шифрування, мають налаштування безпеки (firewall або ACL), мають підтримку динамічної маршрутизації, а також можливість автоматичного використання резервування каналів. Що стосується вузлового обладнання (VPN-серверів) то пропонується розглянути програмні або аппаратні рішення в кількості 2 та більше одиниць і розміщенням в залежності від вимог користувача та законодавства.

Кінцеве обладнання

- Mikrotik HeX Refresh https://mikrotik.com/product/hex_2024
- Mikrotik HeX S https://mikrotik.com/product/hex_s
- Mikrotik hAP AC3 LTE6 Kit https://mikrotik.com/product/hap_ac3_lte6_kit
- Mikrotik SXT LTE6 Kit https://mikrotik.com/product/sxt_lte6_2023
- Cisco ISR 11xx series https://www.cisco.com/c/en/us/support/routers/1110-integrated-services-router/model.html
- Cisco IR series https://www.cisco.com/c/en/us/support/routers/1101-industrial-integrated-services-router/model.html

Вузлове обладнання

- Mikrotik CCR2004-16S-2S+ https://mikrotik.com/product/ccr2004_16g_2splus
- Mikrotik CHR https://mikrotik.com/

- Cisco Cloud Services Router 1000v https://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v/model.html

- Cisco ISR 11xx series https://www.cisco.com/c/en/us/support/routers/1110-integrated-services-router/model.html

Висновки

Використання надійної та захищеної мережі сенсорів є важливим аспектом для підтримки безпеки, ефективності і надійності сучасних систем збору даних, особливо в умовах, де від точності та стабільності залежить не лише зручність, але й життя та здоров'я людей, безпека інфраструктури та суспільства в цілому

Література

1. RFC 4301: *Security Architecture for the Internet Protocol*. IETF, 2005. https://tools.ietf.org/html/rfc4301.
2. Cisco Systems, *Cisco's IPsec VPN Configuration Guide*. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/v1-0/b-bgp-xr/b-bgp-xr-book/b-bgp-xr-bgp/8-3-0-2015.
3. RFC 5206: *Fault Tolerant Networking: From Concepts to Implementation*. IETF, 2008. https://www.ietf.org/rfc/rfc5206.txt.
4. Cisco Systems, *High Availability Network Design*. Cisco Whitepaper. https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5500/v1-0/b-bgp-xr/b-bgp-xr-book/b-bgp-xr-bgp/8-3-0-2015.
5. Szalay, D., & Gubacsi, L. *MikroTik RouterOS: The Cookbook - Configuring Routing and VPN Services*. Packt Publishing, 2015.
6. MikroTik Academy. *MikroTik RouterOS and MikroTik RouterBOARD – Complete Configuration Guide*. MikroTik, 2020.