ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖ IIOT ІЗ ВИКОРИСТАННЯМ CISCO SECURE FIREWALL ISA3000»

Виконала: студентка 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»

(шифр і назва спеціальності)

Івахненко М.В.

(прізвище та ініціали)

Керівник Довженко Н.М.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтролер Чумак Н.С.

(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. У той час як світ рухається до четвертої промислової революції, Інтернет речей (IoT) розвивається експоненціально. Незважаючи на те, що більшість із цих пристроїв будуть споживчими, підприємства та промисловість уже вивчають можливості та можливості пристроїв Інтернету речей, щоб отримати конкурентну перевагу. Промисловий Інтернет речей (IIoT) — це назва пристроїв IoT, які використовуються для моніторингу та контролю промислових і пов'язаних процесів. До них належать транспорт, енергетика, охорона здоров'я, роздрібна торгівля, виробництво та операційна діяльність. Оскільки IIoT інтегрується в бізнес-процеси, він також зближується з хмарними обчисленнями, мобільними та іншими платформами. Це збільшує складність конструкції, а також підвищує ризик. Для організацій головною метою IoT є надання даних і бізнес-аналізу, щоб допомогти керівникам приймати обґрунтовані рішення за допомогою інформаційних панелей і візуалізації.

Інформаційна та кібербезпека часто нехтується або їх взагалі не існує, коли йдеться про IoT та IIoT. Нещодавно Європол зазначив, що зловмисники тепер покладаються на пристрої Інтернету речей для націлювання на критичну інфраструктуру за допомогою розподілених атак на відмову в обслуговуванні (DDoS). У всьому світі доступно багато IT-безпеки, стандартів управління та систем контролю від різних організацій. Що стосується стандартів IoT, то опубліковано багато стандартів, рамок і рекомендацій. Кожен постачальник IoT має власну інструкцію та хоче, щоб використовувався їхній стандарт. Наявність занадто великої кількості стандартів, рамок і елементів керування на вибір збільшує ймовірність вибору неправильного стандарту або його відсутності. Інша проблема полягає в тому, як далеко потрібно зайти, щоб захистити пристрій IoT або IIoT. Подано огляд відмінностей і подібностей між IoT та IIoT, а також пов'язаних із ними загроз, вразливостей, ризиків та інцидентів у транспортній інфраструктурі. Запропоновано методологію та рекомендації щодо забезпечення

стандартів, рамок і засобів контролю для управління та безпеки IoT та IIoT, специфічних для транспортної інфраструктури.

Об'єкт дослідження – промислові мережі IoT.

Предмет дослідження – технології та засоби забезпечення безпеки мереж IIoT.

Мета роботи – розробити рекомендації щодо забезпечення безпеки мереж IIoT із використанням технології Cisco Secure Firewall ISA3000.

Завдання:

- проаналізувати промислові мережі IoT,
- дослідити відмінності та подібності між IIoT та IoT
- дослідити проблематику промислових мереж IoT з наведенням методології аналізу безпеки STRIDE.
- роглянути рішення Cisco Secure Firewall ISA3000 для захисту промислових IIoT мереж від кіберзагроз,
- виконати огляд технології Cisco Secure Firewall ISA3000.
- продемонструвати налаштування технології брандмауера і основних компонентів та розробити рекомендації щодо забезпечення безпеки мереж.

Практичне значення одержаних результатів. Рекомендації щодо забезпечення безпеки мереж IIoT із використанням технології Cisco Secure Firewall ISA3000 можуть бути використані у сфері забезпечення інформаційної безпеки промислових мереж.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на конференції.

Всеукраїнська наукова-технічна конференція «Актуальні проблеми кібербезпеки», Навчально-науковий інститут захисту інформації, 27 жовтня 2022 р., 84-86 с.

1 АНАЛІЗ ПРОМИСЛОВИХ МЕРЕЖ ІОТ

1.1 Визначення поняття «мережі ІІоТ»

ІоТ — це поширення інтелектуальних пристроїв, таких як планшети, телефони, побутова техніка, телевізори та інші датчики тощо. Вигодою від використання інтелектуальних пристроїв удома буде зменшення рахунків за електроенергію та економія часу тощо. Управління використанням ресурсів на основі датчиків або планування та виконання важких службових завдань, таких як увімкнення посудомийної машини, пральної машини чи сушильної машини, коли споживання електроенергії найдешевше. Пристрої ІоТ зазвичай використовуються любителями або іншими споживачами, і навіть у промисловості. Однак ІІоТ розроблено для важких завдань, таких як виробництво, моніторинг тощо. Таким чином, ІІоТ використовує більш точні та довговічні (стійкі до тепла та холоду) пристрої, приводи, датчики тощо. І ІоТ, і ІІоТ мають однакові основні принципи, такі як дані управління, мережа, безпека, хмара тощо. Основні відмінності між ІоТ та ІІоТ полягають у масштабованості та об’ємі згенерованих даних, а також способах обробки даних. Оскільки пристрої ІІоТ генерують величезну кількість даних, ІІоТ потребує потокової передачі даних, великих даних, машинного навчання або штучного інтелекту. У домашній мережі втрата згенерованих даних була б тривіальною, але в ІІоТ це життєво важливо. Дані в ІІоТ мають бути більш точними, безперервними та чутливими. Наприклад, система моніторингу на атомній електростанції чи виробничому підприємстві має бути точною, безперервною та чутливою, щоб запобігти небезпечним подіям. Впроваджуючи ІІоТ на виробничих лініях або в інших промислових проектах, компанії прагнуть зменшити витрати на виробництво або технічне обслуговування, а також підвищити ефективність, стабільність, безпеку тощо.

7 принципів ІІоТ представлені таким чином [1]:

•Велика кількість аналогових даних: багато датчиків генерують аналогові дані, і ці дані потрібно відцифрувати для подальшої обробки, аналізу та зберігання.

•Постійне підключення: пристрої IIoT завжди підключені. Це має три ключові переваги:

1) Можливий моніторинг у реальному часі.

2) Постійний моніторинг може допомогти просувати оновлення програмного забезпечення, мікропрограм та виправлення.

3) Переваги підключених пристроїв мотивують окремих осіб та організації купувати продукти.

• Потокова передача даних у реальному часі: у галузі використовується багато механізмів безпеки, які постійно генерують дані. Розглядаючи атомну електростанцію, безпека є надзвичайно важливою з точки зору експлуатації. Моніторинг вимагає потокової передачі даних у реальному часі, оскільки можлива затримка даних може спричинити катастрофічні події. Отже, потокова передача даних у реальному часі та їх агрегація є дуже важливими.

• Аналіз даних: аналіз даних (спектр цінності) в IIoT шукає відповідь на таке запитання: «Що потрібно досягти?».

• Час до або глибина «розуміння»: це еквівалентно безпосередності знання порівняно з глибиною знання. Наприклад, під час моніторингу або аналізу даних атомної електростанції потрібна негайна увага, тоді як аналіз даних наукового експерименту (даних CERN або NASA) може зайняти роки, щоб виявити наукові проблеми.

• Видимість великих даних: коли дані зібрано та зберігаються в середовищі великих даних, згодом вони мають бути доступними, коли це буде потрібно для аналізу чи інших завдань.

• Граничні обчислення: обчислення та аналітика центру обробки даних буде зміщено на край (затримка, пропускна здатність, вартість, безпека, дублювання, надійність, корупція, відповідність і суверенітет даних).

Удосконалення технологій великих даних і потокової передачі даних дозволило організаціям ширше використовувати продукти штучного інтелекту

(ШІ) і машинного навчання (МН) в Industry 4.0. Програми штучного інтелекту та машинного навчання з'являються в сферах охорони здоров'я, освіти, оборони, безпеки, промисловості тощо. Багато технологічних гігантів вливають мільярди доларів у розробку продуктів штучного інтелекту, таких як автономні автомобілі (безпілотні автомобілі). Google, NVIDIA та інші розробляють алгоритми автономного керування на основі комп'ютерного зору разом із виявленням пішоходів, виявленням зіткнень тощо. Автомобільні компанії, такі як Ford, General Motors, Nissan, Tesla, Mercedes тощо, інвестували мільярди в дослідження та розробки. Сотні інших невеликих компаній створюють радари, камери, обчислювальні та комунікаційні системи, інші датчики тощо. Автономні автомобілі відповідають за генерацію величезної кількості даних за допомогою такого обладнання: радар, Сонар, GPS, Лідар і камери. Один передній радар (2800 МБіт/с) генерує приблизно 1,26 ТБ даних на годину. Двомегапіксельна камера (24 біти на піксель), що працює зі швидкістю 30 кадрів на секунду, генерує 1440 Мбіт даних на секунду (приблизно 1 ТБ даних на годину) [2].

У комп'ютерних науках такі дисципліни штучного інтелекту використовуються для різних цілей: обробка природної мови (NLP), багатоагентні системи (координація та співпраця – розподілене вирішення проблем, прийняття рішень і міркування, навчання, планування, моделювання), людські взаємодії (навчання, чат-боти, експертні системи), комп'ютерний зір, робототехніка, нейронаука та когнітивна наука (розуміння та моделювання мозку та нервової системи), підтримка прийняття рішень (теорія ігор, невизначеність, пояснюваність). Передбачається, що використання алгоритмів ШІ та МН сприятиме ефективності, зниженню витрат та ефективному управлінню промисловими мережами. Таким чином, такі алгоритми на основі ШІ також часто використовуються: евристика, логічне програмування, дедукція та доказ, міркування, планування, планування та пошук.

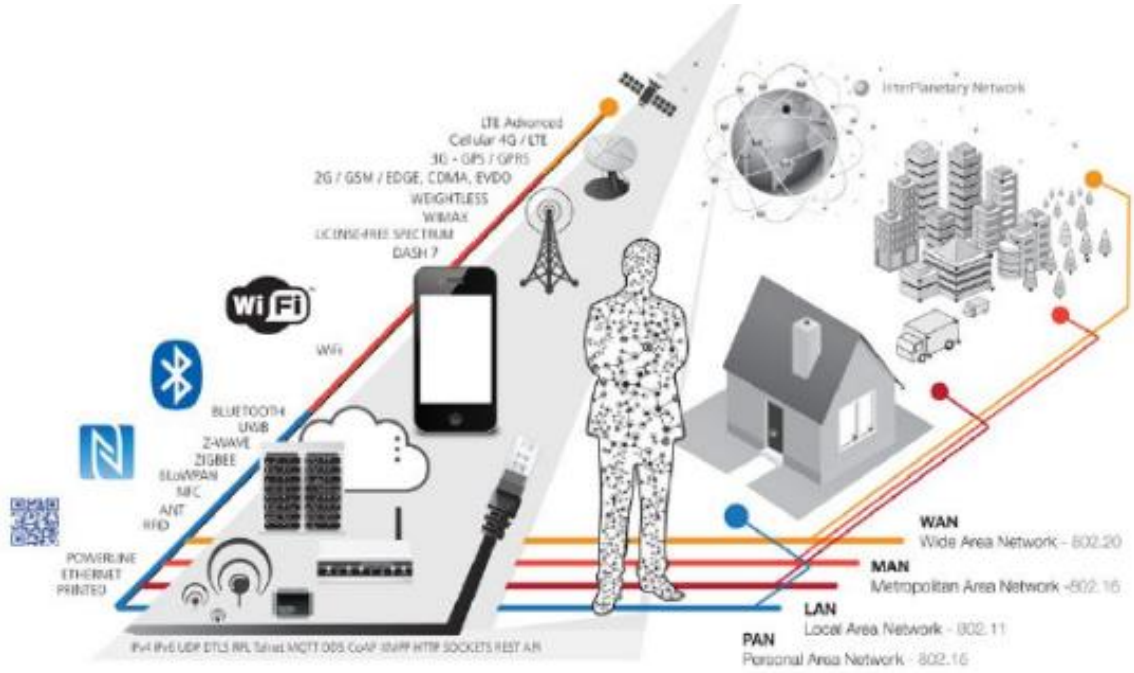

Рис.1.1. Діаграма підключення IoT

Технології дротового/бездротового зв’язку, які використовуються для мереж IIoT, показані на рис.1.1 і рис.1.2. Вони також узагальнені тут [1]:

•BLE: Bluetooth Low Energy (BLE) — це технологія бездротової мережі Personal Area Networking (PAN), яка широко використовується в інтелектуальних пристроях, таких як телефони, годинники, переносна електроніка тощо. Програми BLE можна знайти в індустрії розумного будинку, охорони здоров’я та спорту. Багато операційних систем мають вбудовану підтримку цієї технології, наприклад Android, BlackBerry, IOS, Linux, macOS, Windows тощо. BLE використовує радіочастоти 2,4 ГГц.

•WiFi: Wireless Fidelity (WiFi) — це технологія бездротової мережі на основі IEEE 802.11, яка широко використовується на комп’ютерах, планшетах, інтелектуальних пристроях і транспортних засобах, таких як автомобілі, автобуси, дрони тощо.

•IPv4/IPv6: Інтернет-протоколи версій 4/6 (IPv4/IPv6) можна розглядати як магістраль Інтернету та інших мереж на основі комутації пакетів. Це одна з найбільш широко використовуваних технологій у реальному житті.

•NFC: зв’язок малого радіусу дії (NFC) – це комунікаційна технологія, за допомогою якої пристрої можуть підключатися приблизно на відстані 4 см. Пристрої NFC зазвичай використовуються в електронних платежах, ключ-картках, електронних квитках тощо. Багато смартфонів підтримують цю технологію, як-от Android, Blackberry, IOS тощо.

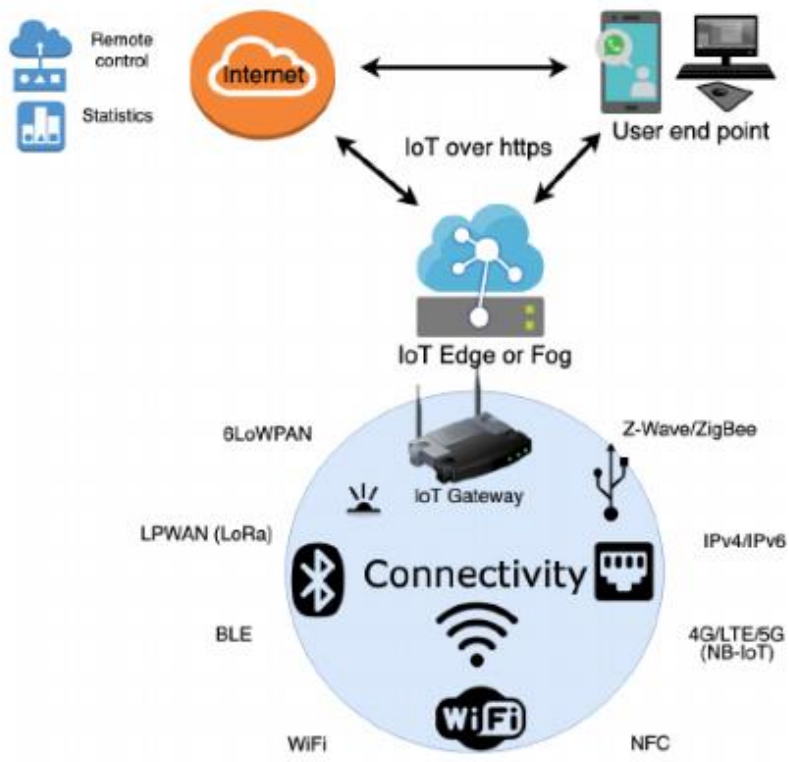

Рис.1.2. Проілюстровано підмножину комунікаційних технологій і протоколів IoT та IIoT

•Z-Wave/ZigBee: Z-Wave — це бездротовий протокол із низьким споживанням енергії. Zigbee також є малопотужним (з низьким енергоспоживанням) протоколом бездротового зв’язку на основі стандарту IEEE 802.15.4 для створення PAN. Z-Wave/ZigBee зазвичай використовуються в домашній автоматизації, медицині та промисловості.

•4G/LTE/5G: 4G (четверте покоління), LTE (довгострокова еволюція) і 5G (п’яте покоління) є домінуючими технологіями широкосмугових стільникових мереж у сучасних мобільних телекомунікаціях.

•NB-IoT: нещодавно мобільні оператори швидко розгорнули NB-IoT (вузькосмуговий Інтернет речей) із поширенням IoT. NB-IoT — це стандарт LPWAN, який зосереджений на недорогому, енергоефективному та внутрішньому покритті.

За словами одного з провідних представників сектору промислових інвестиційних компаній, IIoT стане одним із основних стовпів Industry 4.0 і буде описано так [3]: «IIoT — це мережа фізичних об'єктів, системних платформ і додатків, які містять вбудовану технологію для спілкування. і обмінюватися інтелектуальними даними один з одним, зовнішнім середовищем і людьми». Дотримуючись цього визначення та технологічних тенденцій, економічні прогнози роблять такий висновок: «Інтернет речей має здатність значно підвищити продуктивність і конкурентоспроможність індустріальних економік, але погані умови підтримки — особливо відсутність цифрової грамотності — стримають багато країн». Буде багато сфер застосування для IIoT, починаючи від розумних міст до точного землеробства, розумного трафіку до розумних мереж (майбутнє електричних мереж), і незабаром, як показано на рис.1.3.

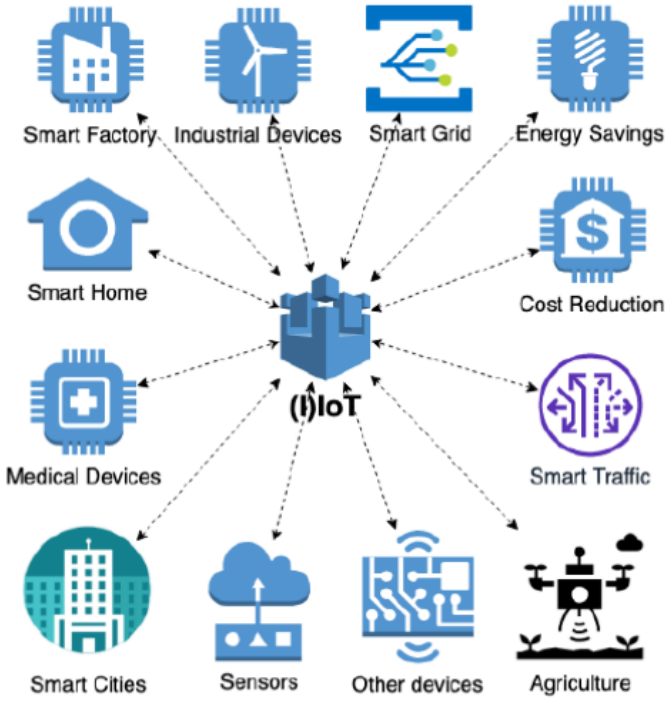

Рис.1.3. Проілюстровано підмножину варіантів використання IoT та IIoT

Мережі IoT вразливі до різних типів атак і слабких місць. Через відсутність фізичної лінії захисту безпека таких мереж викликає велике занепокоєння наукової спільноти. Крім того, кібератаки на промислові середовища відбуваються все частіше, а їх результати досягають руйнівних масштабів, ефективне виявлення вторгнень є надзвичайно важливим для промислових мереж. Тому виникають дослідження щодо систем виявлення вторгнень (IDS) для промислових мереж.

Запобігання та раннє виявлення вторгнень є важливими, особливо для критично важливих промислових мереж, таких як інтелектуальні електромережі.

Наприклад, концепція потокового передавання даних, може справді збільшити час виявлення/відповіді в IDS промислових мереж. Таким чином, майбутні впровадження Інтернету речей можуть виграти від потокової передачі даних не тільки для зменшення розміру даних висхідного потоку, але й для підвищення безпеки мережі, особливо за рахунок збільшення загального часу відповіді IDS.

Зараз існують приклади застосувань у промислових мережах (таких як системи SmartGrid), де датчики можуть генерувати дані зі швидкістю ~3 ГБ (Гігабайт) на годину [4, 5]. Це значно перевищує очікування Ericsson і Bloomberg [6], які складали ~280 ПБ (Петабайт) даних, які генеруватимуться 680 мільйонами розумних датчиків на рік (що еквівалентно 1 байту інформації на датчик на рік). Сучасна клієнт/серверна архітектура традиційних мереж не здатна передавати, зберігати та обробляти такий великий обсяг даних. Таким чином, використовується вибіркова версія згенерованих даних. Другою перевагою потокової передачі даних буде використання невикористаної частини згаданих великих даних, від яких також отримають вигоду IDS.

Централізовані системні архітектури, які збирають усі дані в хмарі для обробки, не можуть масштабуватися як через пропускну здатність зв’язку, так і через проблеми масштабованості обробка накопичених даних; напр. зіставлення шаблонів потоків даних на льоту є процесом із меншою затримкою порівняно з пошуком шаблонів у інтерабайтах/петабайтах збережених даних. Через це в таких інфраструктурах фактично обробляються та використовуються лише невеликі

частки згенерованих даних. Завдяки таким міркуванням можна побачити, що окрім допомоги у вирішенні ситуацій із вузькими місцями, потокова обробка може дозволити використовувати більше даних для програм загалом, а отже, і для IDS.

1.2 Загальні протоколи та архітектура IIoT

Опитування безпеки IIoT показує, що кінцеві точки IIoT є основним джерелом уразливостей у системі. Визначення кінцевої точки IIoT залежить від архітектури системи. Термін кінцева точка може означати сам пристрій IoT або групу пристроїв, відповідальних за будь-яку конкретну операцію або виконання будь-якої ролі в системі. Це означає, що, говорячи про кінцеві точки IIoT, не обов'язково мається на увазі кількість пристроїв, зареєстрованих у системі. Кінцеві точки управляються через мережу та використовуються для обміну даними, збору даних або контролю. Більшість кінцевих точок (близько 72%) покладаються на використання Інтернет-протоколів. Другими за популярністю протоколами (близько 53%) є IP-протоколи, специфічні для домену, які замінюють немаршрутизовані протоколи «точка-точка» для систем керування.

Як обговорювалося вище, для організації зв'язку між кінцевими точками використовується кілька протоколів. У міру розвитку міжмашинного зв'язку було створено набір протоколів, таких як MQTT, COAP, XMPP, AMQP тощо. Найбільш часто використовуваними промисловими протоколами є Message Queuing Telemetry Transport (MQTT) і Constrained Application Protocol (COAP). Ці протоколи є найбільш часто використовуваними в промисловому середовищі, оскільки вони перевершують інші з точки зору розміру заголовка, енергоспоживання та втрати даних.

Нижче наведено промислові протоколи, які зазвичай використовуються на різних рівнях мережі [7]:

• Message Queuing Telemetry Transport (MQTT): цей протокол є протоколом обміну повідомленнями на основі механізму видавець/передплатник. Видавець керує списком тем/подій, і підписник може зареєструватися на ці теми, щоб

отримувати інформацію, коли з’являється подія. Цей протокол розроблено спеціально для пристроїв IoT з низькою обчислювальною потужністю. Безпека протоколу базується на TLS/SSL для забезпечення шифрування на транспортному рівні. На прикладному рівні він передає ідентифікатор клієнта та облікові дані, такі як ім’я користувача/пароль, які можна використовувати для автентифікації пристрою. Оскільки TLS/SSL не оптимізовано для використання на критично важливих для живлення пристроях, використання його із сертифікатами та керуванням сеансовими ключами для кількох пристроїв є важкою операцією для пристроїв із низькою пропускною здатністю. Тож це можна вважати недоліком цього протоколу, який можна покращити в майбутньому.

• Протокол обмеженого застосування (COAP): цей протокол є модифікацією HTTP, щоб зробити його більш придатним для зв’язку між пристроями IoT. Це оптимізований протокол REST для сенсорних додатків, який підтримує запит/відповідь і архітектуру ресурс/спостерігач. COAP — це протокол UDP. Безпека зазвичай досягається за допомогою безпеки транспортного рівня датаграм (DTLS) або IPSec. Datagram Transport Layer Security (DTLS) додає конфіденційність, цілісність і автентифікацію.

Архітектура ICS складається з 2 рівнів: фізичного рівня та кібер-рівня. Фізичний рівень включає всі датчики та апаратні компоненти, які утворюють мережу. Кібер-рівень складається в основному з систем SCADA. Системи диспетчерського контролю та збору даних (SCADA) — це набір протоколів, платформ і технологій, які використовуються для керування промисловими системами керування (ICS). Захист систем SCADA базується на фізичній ізоляції. Завдяки цій концепції системами цього типу керували ізольовано та з використанням нестандартних протоколів. В даний час системи SCADA почали підключатися до корпоративних мереж і, відповідно, використовувати стандартні протоколи для зв’язку, що викликало різні проблеми безпеки для середовища [8].

Архітектура системи SCADA складається з трьох основних компонентів:

• Мережа керування;

• Інфраструктура зв'язку;

• Мережа процесу.

Мережа керування може складатися із сітки ПЛК (програмний логічний контролер), RTU (віддалений термінал) та бездротових мереж датчиків і виконавчих механізмів (WSAN). RTU відповідають за підключення до фізичних систем і збір даних. ПЛК отримують дані від фізичного рівня та надсилають команди керування приводам. Крім того, ПЛК виконують команди, які вони отримують, і надсилають дані, отримані з фізичного рівня, на сервери SCADA. WSAN прийшли на зміну старому підходу збору даних мережею бездротових вбудованих датчиків. Це вимагає розробки інтерфейсу між фізичним рівнем і його цифровою частиною [8].

Кожен компонент систем SCADA має власні проблеми безпеки та специфічні вразливості [9].

Комунікаційна інфраструктура. Компоненти, що відповідають за зв'язок між іншими службами, є прямою мішенню для атак. Найбільш поширені атаки спрямовані на відмову в обслуговуванні (DOS). Цю проблему можна вирішити за допомогою безпечних мережевих протоколів, які охоплюють аспекти автентифікації, конфіденційності та цілісності. Але в промисловій автоматизації важко знайти протоколи, які реалізують ці специфікації. Зазвичай основним пріоритетом у цій галузі є задоволення вимог реального часу.

Використання захищених протоколів і проміжних попередніх перевірок призводить до проблем з продуктивністю та затримок зв’язку в критичних за часом інфраструктурах, але наявні вразливості змушують знайти баланс між затримкою та безпекою. Компоненти зв’язку також взаємодіють із зовнішніми мережами, тому важливо захистити не лише передані дані, але й доступ до функцій зв’язку.

Точки *мережевого з’єднання*, такі як точки бездротового доступу, сховища, корпоративні сервери, також є точками вторгнення, і їх потрібно контролювати системами виявлення вторгнень (IDS). Для обміну інформацією у зовнішніх і внутрішніх мережах IDS розгортають додаткові маршрутизатори та брандмауери, які здатні перевіряти ідентифікаційні дані та аналізувати трафік. Подібні рішення використовуються для захисту шлюзів.

Сервер додатків може виконувати три основні функції: приймати запит, обробляти його та повертати відповідь. Атаки в основному намагатимуться скористатися принаймні одним із цих процесів. Ризик можна мінімізувати за допомогою контролю доступу на основі ролей. Крім того, перевірка вхідних даних і політики кодування можуть бути факторами зниження ризику. Перевірка валідації включатиме перевірку формату повідомлення та параметрів, таких як перевірка схеми XML (розширювана мова розмітки) або JSON (JavaScript Object Notation), перевірка шкідливих символів для запобігання атакам ін'єкції та перевірка несподіваного порядку повідомлень.

DOS-атаки націлені на навантаження на сервер, який не зможе обробити більше трафіку, ніж його доступна пропускна здатність. У системах SCADA задача виявлення аномалій у поведінці вузла легша, ніж в інших випадках, оскільки вузли зазвичай є відомими компонентами системи з передбачуваними моделями поведінки.

Сервер бази даних — це місце, де зберігаються всі дані, і в основному це основне джерело для моніторингу процесів. Атака на цьому рівні може завдати шкоди системі в цілому. Сервер бази даних повинен мати реалізовані заходи безпеки, що забезпечують цілісність і конфіденційність збереженої інформації. Мірою конфіденційності може бути шифрування даних, тоді як цілісність може бути гарантована використанням надлишкових джерел інформації.

Людино-машинний інтерфейс (HMI) зазвичай є процесом управління з високим пріоритетом у системі SCADA, що означає, що команди, надіслані з HMI, виконуватимуться іншими компонентами майже наосліп. Для захисту HMI потрібно буде захистити кожен привод через його програмне забезпечення. Причиною вразливості можуть бути програмні драйвери, які є механізмами інтеграції. Вони забезпечують зв'язок між такими процесами, як файли, сигнали, сокети, повідомлення тощо. Крім того, HMI працює на машині, яка керується операційною системою (ОС). Уразливості ОС також є додатковою загрозою для загальної безпеки компонентів. Перебуваючи в позиції проміжного програмного забезпечення для запущених процесів, ОС здатна встановлювати політики

контролю доступу та блокувати несанкціоновані системні виклики даними процесами.

Програмний логічний контролер складається з наступних частин: ОС, сходова логіка (програма), система виконання, яка взаємодіє з схемою, передаючи їй вхідні дані та реєструючи вихідні дані, зв’язок по шині та служби керування, які зазвичай забезпечують віддалені служби керування, керовані HMI.

У випадку ПЛК файлова система є однією з потенційних загроз. Компоненти ПЛК постійно читають файли конфігурації та реєструють деяку інформацію у файлах журналу. Отримавши доступ до тих файлів, які використовуються системою виконання, зловмисник зможе отримати перевагу над усією системою.

Зв'язок потребує особливого захисту, оскільки він зазвичай використовується для підключення до віддаленого терміналу (RTU) або інших серверів. Також один важливий компонент, який потребує уваги, — це проміжне програмне забезпечення або драйвер у комунікаційних інфраструктурах. Поширеною проблемою є те, що деякі ПЛК працюють на монолітній ОС, яка не має вбудованих списків доступу користувачів. Одним із заходів безпеки є впровадження цієї функції для операційної системи.

Віддалений термінальний пристрій (RTU) також відомий як електронний інтелектуальний пристрій (EID). Вони служать датчиками та приводами, але їх також можна використовувати як вузли прийняття рішень. RTU можуть бути включені в підмережу підрозділів співпраці. Атаки, що компрометують RTU, можуть погіршити продуктивність системи в цілому, виконуючи атаки DOS на базові служби. Найновіші RTU, що володіють більшою обчислювальною потужністю, можуть мати кілька заходів безпеки на основі індивідуальної або розподіленої ієрархії.

1.3 Відмінності та подібності між IIoT та IoT

Відмінності між пристроями IIoT та IoT полягають не лише у формулюванні чи застосуванні, ступені чи семантиці. Якщо пристрій Fitbit виходить з ладу, це

може бути незручно. Однак, якщо гальмівна система поїзда виходить з ладу, це буде питанням життя і смерті [10].

За словами Боуна [11], незрозуміло, де схожість і відмінності між IIoT та IoT. Далі він пояснює, що IoT — це революція, а IIoT — це еволюція. Функції, які є новими для споживача та ринку, такі як віддалений доступ, хмара та машинно-машинний зв'язок, є революцією для IoT, але для IIoT вони існували деякий час і скоріше еволюціонували з цього [11]. IoT призначений для споживачів, тоді як IIoT призначений для промислового використання інженерами.

Карл Хеннінг спочатку вважав, що IIoT не є ідентичним IoT [12], показано на рис.1.4, але пізніше встановив, що IIoT є підмножиною IoT.

Рис.1.4. Початковий вигляд Карла Хеннінга [12]

Bowne [18] перелічує наступні характеристики IoT та IIoT у табл. 1.1.

Таблиця 1.1.

Порівняльний аналіз IoT і IIoT

IoT	IIoT
Революція	Еволюція
Речі	Дані
Спеціальне підключення	Структурована зв'язність
Важливо – але не критично	Вирішальна місія, аналітика, безпека, цілісність даних, час відповіді
Обслуговується користувачами	Обслуговується користувач + OEM + постачальник
Нові пристрої і стандарти	Існуючі пристрої і стандарти
Запатентовані рішення	Визначені стандарти

IIoT розвинувся з промислових систем. Промислові системи підпадають під інші назви, а саме: диспетчерське управління та збір даних (SCADA) і промислові системи управління (ICS). ICS і SCADA — це системи, які використовуються в експлуатації та промисловості для контролю та автоматизації керування. SCADA є підмножиною ICS і в основному є операційними системами, географічно розподіленими на великій території, такими як системи з використанням конвеєрних стрічок. Критична національна інфраструктура використовує системи ICS або SCADA [13]. Критична інфраструктура, якою керують ці системи, включає електромережі та виробництво електроенергії, а також трубопроводи.

У міру того, як компаніям було потрібно більше розуміння своїх операцій, системи ICS або SCADA поступово почали впроваджувати традиційні IT-протоколи та підключатися до корпоративних мереж, де раніше вони були автономними за допомогою спеціалізованих протоколів зв'язку [13]. Саме тут народився IIoT, оскільки це еволюція традиційних систем ICS або SCADA. Дані, отримані з промислових процесів, дали цінну інформацію таким чином, який ніколи не був можливим. IIoT — це чудовий спосіб для компаній контролювати всі свої операційні чи промислові сфери, включаючи аналіз ефективності або ключові показники ефективності (KPI) і прогнозне обслуговування. За словами Мандітерези [14], IIoT — це технологія, яка будується на основі систем ICS або SCADA. Він згадує чотири ключові відмінності, а саме масштабованість, аналітику даних, стандартизацію та взаємодію. Henning [15] згадує, що IIoT є частиною як IoT, так і Industrie 4.0, як показано на рис.1.5.

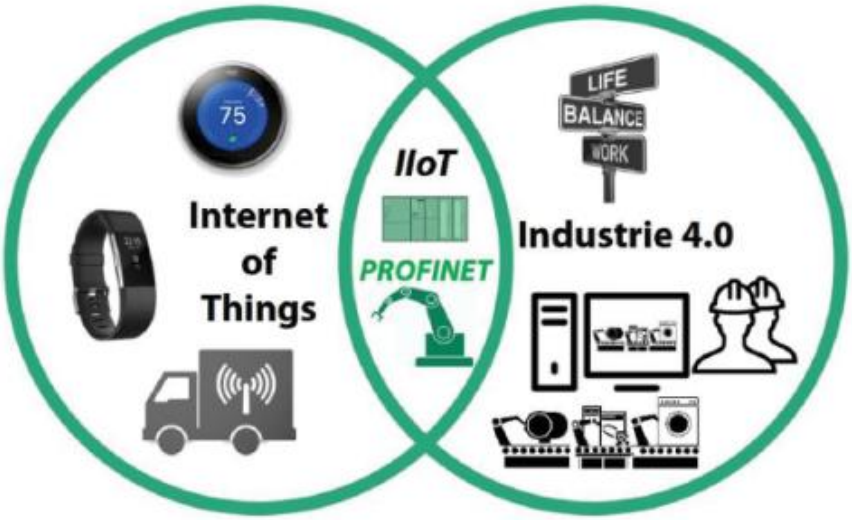

Рис.1.5. IoT проти IIoT проти Industrie 4.0

Якщо IIoT — це технологія, яка базується на системах ICS або SCADA, також беручи до уваги, що IIoT є частиною IoT і Industrie 4.0, можна згрупувати ICS або SCADA і Industrie 4.0 як операційну технологію та зробити висновок, що IIoT — це те, де IoT і Industrie 4.0 операційної технології перетинаються, як показано на рис.1.6.

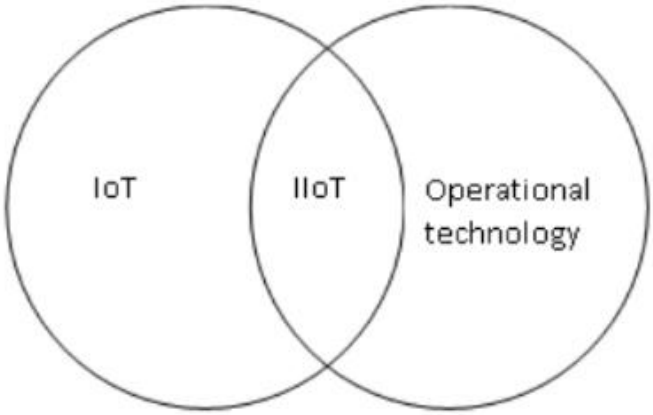

Рис.1.6. IoT проти IIoT проти операційної технології

Чан описав десять відмінностей між IoT та IIoT, серед яких [16]:

•Безпека – Інтернет речей вимагає більш надійних заходів безпеки, ніж Інтернет речей. Порушення процесу транспортування великого обсягу призведе до втрати доходу в мільйони разів на день. DDoS системи управління трафіком впливає на логістичну діяльність мільйонів людей і ставить під загрозу національну

безпеку. Інтернет речей потребує розширених заходів безпеки порівняно зі звичайним Інтернетом речей. До них належать безпечні та стійкі системні архітектури, автентифікація та шифрування, спеціалізовані набори мікросхем, виявлення загроз та процеси керування.

•Інтероперабельність – рішення IIoT повинні співіснувати із застарілими технологіями операцій (OT), які включають ICS/SCADA. Пристрої IIoT повинні без проблем інтегруватися в ICS/SCADA та інші OT. IIoT також має інтегруватися в корпоративні мережі для аналізу даних, візуалізації та інтерфейсу до традиційних систем планування ресурсів підприємства (ERP).

•Масштабованість. Промислові мережі — це спеціалізовані великомасштабні мережі, що підтримують десятки тисяч (або більше) контролерів, роботів, машин та інших спеціально створених програм. Рішення IIoT, розгорнуті в промислових мережах з десятками тисяч кінцевих точок (датчиків, контролерів, роботів тощо), повинні легко масштабуватися, щоб підтримувати існуючі пристрої, не пов’язані з IoT, а також тисячі нових датчиків, пристроїв і контролерів. Ця підтримка повинна включати збір і аналіз даних, інтеграцію робочого процесу, взаємодію, планування, прийняття рішень та інтеграцію з виробничими системами.

•Точність. Розгортання IIoT має підтримувати промислові операції, де висока точність є нормою. На відміну від середовищ Інтернету речей, де достатньо «досить близько», промислові середовища вимагають точності в реальному часі, де великі обсяги та високошвидкісні виробничі процеси синхронізовані з точністю до мілісекунд, що може призвести до втрати виробництва, простою та прибутку.

•Програмованість – пристрої IIoT мають бути гнучкими та допускати часте перепрограмування та реконфігурацію, подібно до систем OT, таких як системи ICS/SCADA, для підтримки операцій.

•Низька затримка. Пристрої IIoT повинні підтримувати вимоги промислових додатків до низької затримки для обробки аномалій майже в режимі реального часу. Це надзвичайно важливо, оскільки датчики постійно контролюють кожен аспект операції, де кожна секунда має значення. Затримки в прийнятті рішень,

реакції, виявленні, оцінці або виконанні будуть дорогими. Це призводить до втрати прибутку та потенційної втрати життя.

- Надійність – пристрій IIoT у промисловому середовищі піддається тим самим умовам, що й OT. ICS/SCADA та інші OT були розроблені таким чином, щоб служити від 20 до 30 років, оскільки вони працюють у суворих умовах. До них відносяться пил, тепло, холод, тиск, сильна вібрація та інші небезпечні умови. Пристрої IIoT мають бути захищені, щоб підтримувати ці суворі умови та забезпечувати високу доступність.

- Стійкість – промислові системи та OT розроблені з урахуванням стійкості, оскільки недоступність не є варіантом. Збій в одній частині системи не повинен зупиняти роботу. Пристрої IIoT у критичних робочих середовищах повинні підтримувати стійкість і відмовостійкість у своїй архітектурі та дизайні. Це повинно задовольнити втрату з'єднання або втрату датчиків для належного завершення процесів і операцій.

- Автоматизація. Оскільки промислові процеси високоавтоматизовані, пристрої IoT, що працюють у промислових середовищах, повинні підтримувати вимоги до автономності.

- Зручність обслуговування. Пристрої IIoT, що працюють у промислових умовах, мають передбачати технічне обслуговування для підтримки необхідного рівня продуктивності. Технічне обслуговування включає оновлення прошивки або патчів, конфігурації, заміну датчиків або з'єднань. Потрібне регулярне технічне обслуговування, щоб забезпечити надійну роботу пристроїв IIoT у важких умовах протягом багатьох років.

Нагарадж [10] перераховує три неправильні уявлення, коли йдеться про IIoT. *Помилка 1*: IIoT – це те саме, що споживчий IoT, але зустрічається в промисловості. IoT має набагато суворіші вимоги, ніж споживчий IoT. Подібно до того, що вказав Чан [16], ці пристрої повинні працювати в суворих умовах, бути надійними та вимагати невеликого втручання людини. *Помилкове уявлення 2*: IIoT — це здебільшого пристрої, які «витягують і витягують інформацію про статус і команди з мережевого світу». Там, де IoT споживача забезпечує комфорт, безпеку та

ефективність завдяки втручанню людини, IoT, навпаки, не сприяє втручанню людини, але має бути в змозі допомогти в автономному спілкуванні між різними пристроями. *Помилка 3*: власники пристроїв IIoT чинять опір або не зацікавлені в з'єднанні розумних пристроїв. Окремі пристрої IIoT можуть генерувати невеликі обсяги даних, але в поєднанні вони стають «великими даними», які можна використовувати для аналітики, моніторингу та інтелектуального керування.

Висновки до першого розділу

Визначено поняття «промислових мереж» та приведено принципи IIoT і технології дротового/бездротового зв'язку, які використовуються для даних мереж.

Досліджено архітектуру IIoT та промислові протоколи, які зазвичай використовуються на різних рівнях мережі.

Обґрунтовано компоненти системи SCADA і продемонстровано відмінності та подібності між IIoT і IoT згідно з представленнями науковців.

Представлено підмножину варіантів використання IoT та IIoT. Проведено порівняльний аналіз IIoT і IoT та продемонстровано у вигляді таблиці. Наведено десять відмінностей та перераховано три помилкові уявлення щодо промислових мереж.

2 ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ В ПРОМИСЛОВИХ МЕРЕЖАХ ІОТ

2.1 Проблеми в промислових мережах

Промислові мережі стикаються з багатьма технічними проблемами, які необхідно враховувати до, під час або після будь-якого впровадження. Ці проблеми полягають у наведеному нижче, але не обмежуються ними:

Бездротове співіснування означає безпечну роботу пристроїв, які використовують бездротову технологію для зв'язку. Зокрема, «перешкоди сигналу» є головною проблемою проти співіснування різних стандартів бездротового зв'язку, що може спричинити завмирання сигналів, якщо вони працюють в однакових діапазонах частот. Це доповнює існуючі проблеми бездротового зв'язку, такі як відбивання, заломлення, дифракція, розсіювання та втрати на шляху вільного простору сигналів у повітрі. Згодом перешкоди бездротового сигналу можуть спричинити скидання пакетів, втрату даних, тремтіння та затримку передачі, а також асинхронізацію між двома сторонами, що спілкуються. Таким чином, під час проектування IIoT слід підтримувати бездротове співіснування пристроїв, наприклад, забезпечуючи достатню фізичну відстань між пристроями та/або шляхом ефективного розподілу та спільного використання частотного спектру, який використовується.

Затримка, яку іноді називають затримкою, (для промислових мереж) – це час, що минув між часом випуску певної команди та часом початку виконання цієї конкретної команди. У деяких конкретних випадках його також можна назвати часом, що минув між збором даних і результатом реакції. Наприклад, навіть за наявності хмарної реалізації Ferrari et al. показали, що за допомогою недорогих пристроїв промислового класу IIoT затримка додатків IIoT може становити менше 300 мс для міжконтинентального зв'язку та менше 50 мс для внутрішньоконтинентального зв'язку. Незважаючи на те, що будь-яка цифра нижче 300 мс вважається достатньою для телефонного зв'язку, щоб уникнути небажаної

«розмови» під час розмов, кожна мс має значення, якщо розглядати промислові мережі. Особливо реагування в режимі реального часу може знадобитися для установок, які включають високошвидкісне обладнання з вимогами безпеки. Зокрема, представлені бездротові технології наступного покоління, такі як 5G і наднадійний зв'язок із малою затримкою (URLCC), включаючи теоретичні обмеження та затримку. Ретельно обговорюються компроміси зв'язку з низькою затримкою для приймачів з обмеженнями обчислювальної складності. Відповідно, наголошується, що для критично важливих розгортань IIoT, таких як заводські впровадження, які потребують відповіді в режимі реального часу, затримка є надзвичайно важливою. З дуже жорсткими вимогами до затримки та IIo-приймачами з низьким рівнем складності час, необхідний для декодування пакету (не має складати операцію, що вимагає обчислень), також слід враховувати під час аналізу загальної затримки.

Сумісність. Інтероперабельність означає важливу здатність різних комп'ютеризованих торговельних систем або систем оперативно з'єднуватися та обмінюватися даними одна з одною без будь-яких обмежень. Існує два типи проблем сумісності, визначених для IIoT [17]:

1. Міжрівнева сумісність (також відома як неоднорідність), яка визначається як оркестровка рівнів взаємозв'язку відкритої системи (OSI) безшовним і легким способом. Нещодавно цю проблему вирішено за допомогою двох нових технологій віртуалізації, а саме програмно-визначене радіо (SDR) і програмно-визначена мережа (SDN). З одного боку, SDN — це мережева архітектура, заснована на розділенні площини керування та площини даних, що дає змогу отримати безпосередньо програмовану мережу. Це поділ уніфікує рівень керування всіма типами мережевих пристроїв, роблячи мережу конфігурованою та оптимізованою на основі стану мережі. З іншого боку, забезпечуючи вищий ступінь гнучкості в розробці бездротових інтерфейсів, достатньо компетентних для підтримки багатьох комунікаційних технологій, SDR може бути рішенням для вирішення проблем сумісності. Akyildiz та ін. [18] зазначив, що величезна кількість пристроїв в IoT є фундаментальною проблемою для повсюдної передачі інформації через

магістральні мережі. Гетерогенність пристроїв Інтернету речей і апаратних, негнучких стільникових архітектур створюють ще більші проблеми для забезпечення ефективного зв'язку. Таким чином, вони запропонували архітектуру бездротового SDN і запропонували програмно визначені шлюзи, які спільно оптимізують міжрівневі комунікаційні функції між різнорідними пристроями IoT і стільниковими системами.

2. Міжсистемна сумісність, яка визначається як підтримка безперервної роботи мереж і систем в рамках існування різних системних архітектур. Наприклад, частина IIoT може складатися з кінцевих пристроїв на основі LoRa, а в іншій частині можуть домінувати кінцеві пристрої Nb-IoT. Цю проблему можна вирішити за допомогою моделей семантичної системи, які забезпечують глибше розуміння необроблених даних датчиків, дозволяючи машинам на основі ШІ приймати рішення на основі простих правил. Розробка шлюзів для сумісності також може бути досягнута шляхом визначення комплексних централізованих метаданих і визначення абстрактних моделей з них, які можуть бути автоматично згенеровані для багатьох мов програмування.

Потокова передача даних датчика — це новий і потужний інструмент для промислових мереж, який розширить можливості груп аналізу даних (особливо в галузі кібербезпеки). Однак є кілька проблем, які необхідно враховувати [19]:

- План масштабованості: Шукає відповідь на питання, наскільки деталізація та обробка потрібна для даних, щоб мережа розумно масштабувалася та могла бути під контролем.
- План довговічності даних: шукає шляхи довгострокового захисту даних під час зберігання даних, щоб вони не страждали від бітових помилок, деградації чи інших пошкоджень. Замість того, щоб зосереджуватися на резервуванні апаратного забезпечення, довговічність більше стурбована надмірністю даних, щоб дані ніколи не були втрачені або скомпрометовані.
- План відмовостійкості: також важливо включити відмовостійкість як на рівні зберігання, так і на рівні обробки.

Безпека. Датчики та пристрої IIoT відіграють вирішальну роль у промисловій безпеці (виробництво, транспортування тощо). IIoT використовує недорогі та малопотужні пристрої для впровадження енергоефективних протоколів безпеки та підвищення продуктивності. Основна увага безпеки зосереджена на внутрішніх проблемах, заснованих на ризиках, у виробничому трубопроводі, щоб запобігти проблемам широкого спектру, як-от повсякденна робота, пов'язана з невеликими аваріями, а також великі катастрофи, такі як ядерні аварії та інциденти. Багато промислових об'єктів використовують багаторівневі протоколи безпеки, такі як моніторинг керування процесами та сигналізація, системи приладів безпеки (SIS), системи фізичного захисту, системи реагування на надзвичайні ситуації (локальні/зовнішні). Сигналізація є механізмом для інформування про перевищення певного порогу для контрольованої події. Моніторинг: Моніторинг є одним із найважливіших компонентів протоколів безпеки. Більшість виробничих трубопроводів вимагають постійного моніторингу в режимі реального часу. Датчики генерують аналогові/цифрові дані в реальному часі та передають їх на блок керування для аналізу та виконання дій на основі значення моніторингу. Затримка є важливою проблемою в системах моніторингу. Крім того, фізичний моніторинг також важливий, як і моніторинг корозії/ерозії, щоб визначити шкідливі наслідки. Система фізичного захисту включає наступне обладнання: клапани скидання тиску, розривні мембрани, потокові пастки, електричні розподільні пристрої, станції для промивання очей, захисні душі тощо. Останні тенденції у системах безпеки IIoT є такі [19]:

• Комп'ютерне бачення (CV): технологія CV використовується для виявлення аномалій (під час виявлення фізичних структурних чи машинних проблем) разом з іншими IIoTsensors.

• Електроніка, що носиться: передбачає моніторинг життєво важливих вимірювань життєвих сигналів, виявлення падінь, ураження електричним струмом тощо.

Безпека Інтернету речей для забезпечення безпеки: кібербезпека також є основною проблемою для систем безпеки. Усі пристрої IIoT повинні бути

надійними для кібербезпеки на етапі експлуатації. Зовнішня сторона, як-от конкуренти чи хакери, не повинна зупиняти чи спричиняти фізичне знищення виробничого об’єкта чи трубопроводу. Наприклад, у червні 2010 року Іран зазнав кібератаки на ядерний об’єкт, розташований у Натанзі, через кібер-хробака Stuxnet. Ще один серйозний інцидент стався 31 березня 2015 року, коли іранські хакери зламали енергомережу Туреччини, що спричинило масштабне відключення електроенергії на 12 годин у 44 містах із 81. Приблизно 40 мільйонів людей постраждали під час цього збою.

• Робототехніка: програмні технології, керовані штучним інтелектом, вбудовані для створення автономних механізмів прийняття рішень, які називаються роботами. Ці пристрої можуть працювати там, де не може людина. Наприклад, на атомній електростанції чи під водою тощо.

Безпека та конфіденційність. Інтерфейс інтелектуальних фабрик із кіберфізичними системами (CPS) і IIoTim покращує інтелектуальну інфраструктуру, але створює вразливості кібербезпеки, які можуть призвести до критичних проблем, таких як системні збої, порушення конфіденційності та/або порушення цілісності даних. Оскільки конфіденційність громадян стає все більш важливою, особливо в ЄС з актом GDPR, конфіденційну інформацію користувачів Інтернету речей, таку як персональна ідентифікаційна інформація (PII), потрібно добре обробляти, щоб вона залишалася конфіденційною. Багато мереж IoT не мають навіть базових елементів безпеки. У середньому це аналіз кібербезпеки сучасних COTS (комерційних готових) продуктів IoT: на кожному пристрої виявлено 25 уразливостей, 60% мають вразливі мікропрограми та інтерфейси користувача, 70% взагалі не шифрують жодних комунікацій, і 80% не запитують пароль для автентифікації, який має безпечну довжину. Відтепер існують два основні методи боротьби з вторгненнями та кібератаками на IIoT. Один із них полягає в тому, щоб дозволити вторгненню статися, а потім виявити його за допомогою систем виявлення вторгнень (IDS). Інший – запобігання атакам за допомогою аутентифікації, авторизації та контролю доступу.

Виявлення вторгнень. На практиці IDS встановлюються за запитом з усіх аспектів технологічного життя, від корпоративних до університетів, де існують IT-відділи. Особливо цікавлять наступні теми:

- Безпека промислових мереж і Інтернет речей.
- Безпека розумної мережі.
- Безпека критичної інфраструктури.
- Розумна безпека міста/фабрики/будинку.

Основна відмінність між IDS на основі аномалій і IDS на основі неправильного використання/специфікації полягає в тому, що системи на основі виявлення аномалій можуть виявляти будь-яку погану поведінку (теоретично) на льоту, але системи на основі виявлення неправильного використання/специфікації можуть розпізнавати лише раніше відомі погані поведінки (підписи). Це пояснюється наступним чином: системи, засновані на виявленні неправильного використання/специфікації, розроблені таким чином, щоб відповідати раніше змодельованим векторам і правилам атак. Якщо випадок можна віднести до цих категорій, то він називається нападом. В іншому випадку він називається нормальною поведінкою. Ці системи дуже добре працюють із визначеними та класифікованими атаками до моменту впровадження.

Однак вони абсолютно марні у випадку нових векторів атаки, які не можна вказати зі старими. Для таких ситуацій пропонується IDS на основі виявлення аномалій. Отже, легше змоделювати нормальний стан, ніж ненормальний, він моделюється, щоб визначити хорошу (або нормальну) фазу поведінки системи. Тому це логічно протилежно системам, заснованим на виявленні неправильного використання/специфікації, в яких сигнатури та вектори атаки визначаються безпосередньо. Отже, IDS на основі виявлення аномалій використовує своєрідний алгоритм міркування в реальному часі, тобто рішення щодо майбутнього інциденту може відрізнятися від минулого, навіть якщо це однакові події. Крім того, як уже згадувалося в обговореннях вище, їх легше налаштувати, оскільки моделювати нормальні умови роботи (фазу) мережі легше, ніж конкретно ідентифікувати кожен вектор атаки. Кожен із цих підходів потім класифікується на різні методи.

Запобігання вторгненням. Це називається виконанням усіх необхідних дій, необхідних для запобігання вторгненням. Це може бути аналогічно системам захисту від крадіжки в реальних додатках безпеки, таких як встановлення розширених дверних замків, інфрачервоних детекторів тощо. Деякі з методів, які слід згадати, це наступним чином, але не обмежуючись [1]: автентифікація, авторизація, контроль доступу, шифрування (шифрування/дешифрування), хешування тощо.

Монітор безпеки під час виконання працює на основі стану промислової системи та спостерігає за аномальною поведінкою, яка виникає через збої та операційні помилки або загрози безпеці з боку зловмисників. Щоб гарантувати успішну роботу, монітор безпеки під час виконання потребує знань про систему, а також про довірені стани, умови роботи, а також про вихідну інформацію системи, тобто про те, що виробляє система. Метою монітора безпеки під час виконання є виявлення підозрілих і аномальних індикаторів, коли, наприклад, система припиняє виробляти те, що заплановано. Вони зображуються як збої або загрози безпеці (рис.2.1). Потім він діє проактивно, замінюючи систему на так звану «реверсійну» систему, яка виконує мінімальну функціональність промислової системи, визначену вимогами. Реверсійна система забезпечує резервування та надійність.

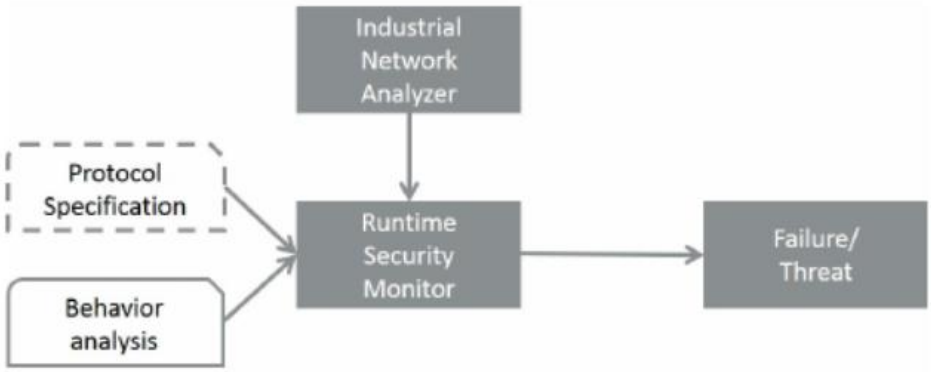

Рис.2.1. Концепція моніторингу безпеки під час виконання

Наявність монітора безпеки під час виконання завжди має поєднуватися з аналізатором промислової мережі (рис.2.1), оскільки події та дані, якими

обмінюються в промисловій мережі, кодуються у власних протоколах і форматах повідомлень. Прикладом аналізатора мережі є Wireshark 11, який підтримує деякі промислові протоколи, такі як Modbus і DNP3, а також бібліотеки та розширення для інших власних протоколів.

2.2 Методології аналізу безпеки

Протягом багатьох років безпека не розглядалася як важливий аспект архітектури програмного забезпечення. Довгі роки досліджень показали, що аналіз безпеки повинен бути частиною життєвого циклу розробки програмного забезпечення (SDLC). З цієї причини аналіз безпеки архітектури відіграє важливу роль для усунення загроз безпеці, які містяться в архітектурі. Метою аналізу загроз є виявлення, визначення пріоритетів і пом’якшення потенційних загроз безпеці. Аналіз загроз системи особливо важливий, оскільки доведено, що причиною багатьох вразливостей є потоки архітектурного проектування. Виправлення цих вразливостей на ранніх етапах зменшить витрати в процесі та зменшить вектор атаки.

Найбільш часто використовуваними методологіями є випадки неправильного використання, дерева атак, проблемні рамки та кілька підходів, орієнтованих на програмне забезпечення. Загалом можна згрупувати всі методи, орієнтовані на ризик, атаки та програмне забезпечення:

1. Випадки неправильного використання (MUC): Ця методологія є розгалуженням розробки на основі варіантів використання та вимог. Випадки зловживання використовуються для захоплення потоків загроз, альтернативних потоків, сценаріїв пом’якшення, тригерів, профілів зловмисників тощо. Компоненти, які використовуються в методології, поділяються на 3 типи: випадки зловживань, карти MUC і сценарії MUC. Різниця між зловживанням і зловживанням полягає в тому, що зловживання — це сценарій зловживання з додатковим зловмисним наміром.

• Дерева атак: у цьому підході кореневий вузол розгалужується на можливі вектори атак. Таким чином, єдиний шлях атаки почнеться з гілки та закінчиться в кореневому вузлі. Цей підхід зазвичай використовується в поєднанні з іншими. Перша частина аналізу полягає в картографуванні атак за допомогою дерев атак, а в другій частині комбінований підхід дозволяє визначити сценарії зловживання.

• Фрейми проблем: цей підхід використовується для опису проблем у програмному забезпеченні. Зазвичай це виконується на рівні абстракції класів і звертається до інтерфейсів і вимог.

• Цільово-орієнтоване розроблення вимог (GORE): це цільовий підхід, і він знаходиться на рівні абстракції систем, які спілкуються одна з одною для досягнення цілей.

2. Аналіз загроз, орієнтований на ризик: ця методологія зосереджена на активах і цінності для компанії. Основною метою цієї методології є пошук відповідного пом’якшення, щоб мінімізувати ризик. Основна увага приділяється оцінці фінансових втрат у разі можливої атаки. У результаті для цієї методології будуть визначені вимоги безпеки, а активи з найвищими активами матимуть найвищий пріоритет.

Однією з найбільш часто використовуваних методологій є STRIDE. Його можна визначити на різних рівнях абстракції. З цієї причини вона вважається однією з найбільш гнучких моделей для моделювання загроз. STRIDE — це модель аналізу загроз, може забезпечити повне покриття для аналізу загроз. Моделювання загроз може бути реалізовано на рівні компонентів або на рівні функціональності системи. Ця методологія забезпечує чітке розуміння вразливостей системи та можливого впливу вразливості кожного компонента на всю систему. STRIDE означає аналіз загроз безпеці в 6 категоріях: спуфінг, фальсифікація, відмова, розкриття інформації, відмова в обслуговуванні (DOS), підвищення привілеїв.

Як зазначено в табл. 2.1, категорії STRIDE можна описати наступним чином:

Таблиця 2.1

Категорії аналізу загроз STRIDE

Загроза	Категорія безпеки
Спуфінг	Автентифікація
Фальсифікація	Цілісність
Відмова	Нерепутабельність
Розкриття інформації	Конфіденційність
Відмова в обслуговуванні (DOS)	Доступність
Підвищення привілеїв	Авторизація

Спуфінг: спуфінг — це тип атаки, коли зловмисник заволодіває компонентом/користувачем і виконує дії від їх імені, фальсифікуючи власну особу. Прикладом такого типу атак може бути незаконне отримання доступу до аутентифікаційної інформації користувача та її використання для виконання різноманітних дій у системі.

Іншим прикладом, більш пов’язаним із промисловим середовищем, є зловмисник, який витягує криптографічний ключ із пристрою, використовуючи вразливості апаратного чи програмного забезпечення пристрою та періодично звертаючись до системи та виконуючи дії під ідентичністю оригінального власника ключа.

Фальсифікація: може являти собою будь-яку форму саботажу, але в основному це означає навмисну модифікацію компонента/мережі, щоб зробити його шкідливим для системи. Втручання включає неавторизовані зміни в даних, якими обмінюються компоненти або зберігаються в одному з них. Втручання на рівні пристрою може здійснюватися шляхом повної або часткової заміни програмного забезпечення пристрою. Ця дія потенційно відкриває компонент для описаної вище атаки спуфінгу.

Відмова: відмова — це термін у сфері безпеки, що описує нездатність компонента, який виконує дію, змінити право власності на дію. Хорошим прикладом цього є підписані транзакції в системі, що підтверджують автентичність

власника транзакції. Загроза відмови — це здатність одного з компонентів виконувати незаконну операцію в системі, яка не має можливості відстежувати заборонені операції.

Розкриття інформації: розкриття інформації — це термін, що описує сценарій, коли компонент може надати інформацію неавторизованим третім особам. Наприклад, якщо компонент працює з інфікованим програмним забезпеченням, зловмисник може потрапити в компонент і отримати витік інформації або проникнути в канал зв'язку між компонентами.

Відмова в обслуговуванні (DOS): атаки типу «відмова в обслуговуванні» в основному мають на меті зробити службу/компонент тимчасово недоступними або відмовити в обслуговуванні дійсним користувачам системи. DOS-атаки можуть завдати серйозної шкоди загальній системі, якщо компоненти взаємозалежні. Відмова в обслуговуванні, як правило, досягається шляхом затоплення, що означає надсилання ненормальної кількості запитів до цільової служби за короткий проміжок часу. У індустріальному світі ця атака також може бути виконана на фізичному рівні.

Підвищення привілеїв: у цій атаці непривілейований компонент/користувач отримує привілейований доступ і може виконувати неавторизовані дії в системі. Цю атаку можна здійснити, використовуючи слабкі місця потоку проектування або конфігурації системи. Більш складний сценарій для здійснення атаки полягає в проникненні в усі системи захисту та перетворенні в довірену частину системи. Це може спричинити ризик невизначеної атаки.

Аналіз безпеки

Було вирішено використовувати методологію аналізу на основі STRIDE. Результати підсумовуються в наведених нижче таблицях, у яких розглядаються атаки, ризики та пом'якшення за типом компонента запропонованої архітектури.

Щоб зрозуміти, як можна захистити пристрої IIoT, слід розібратись в тому, які інциденти сталися, пов'язані з ними ризики, уразливості та загрози. Найбільша на сьогоднішній день кібератака, яка вивела з ладу половину американського Інтернету, сталася в жовтні 2016 року, і її спричинили пристрої IoT, заражені

шкідливим програмним забезпеченням. Ці пристрої IoT були заражені зловмисним програмним забезпеченням, відомим як ботнет Mirai, і спільно використовували DDoS-атаку на сервери доменних імен (DNS), контрольовані компанією під назвою Dyn, щоб перевести більшість веб-сайтів в автономний режим. Іншим інцидентом стала компанія St. Jude Medical's Cardiac Devices. У січні 2017 року Управління з контролю за продуктами й ліками США (FDA) оголосило, що медичні пристрої, зокрема кардіостимулятори, є вразливими. Хакери можуть перехоплювати бездротові радіочастотні сигнали певних передавачів і надсилати команди, які можуть вбивати пацієнтів. У 2015 році два хакери Чарлі Міллер і Кріс Валасек продемонстрували, як працює віртуальний викрадення автомобіля з Jeep Cherokee, успішно взявши його під контроль. 28 грудня 2018 року стрибок напруги в аеропорту Ла-Гуардія, який тривав 45 хвилин, міг бути потенційно спричинений IoT-атаками з бот-мережі IoT зламаних пристроїв, що призвело до припинення рейсів.

Кілька інших інцидентів безпеки було зареєстровано в транспортному секторі (трубопроводи, залізниця, морський транспорт, повітря, автотранспорт тощо). Хоча не всі компрометують IIoT/IoT, вони вплинули на системи, ключові до роботи критичної транспортної інфраструктури та пов'язаних організацій. Найпомітніші з них:

- «Нафтогаз» – у 1999 році хакери за допомогою незадоволеного інсайдера використали троян для доступу до елементів керування трубопроводами [13].
- CSX Corporation – у 2003 році вірус Sobig вимкнув декілька систем, що спричинило затримки поїздів [13].
- Польська трамвайна система – у 2003 році в Лодзі, Польща, 14-річний підліток, очевидно, перетворив трамвайну систему на власний персональний потяг за допомогою модифікованого пульта від телевізора. Підліток спровокував хаос, коли він зійшов з рейок чотири трамваї поранили 12 людей, коли він змінив точки колії як частину жарту.

- Система екстреного сповіщення Chevron – у 1992 році колишній співробітник, якого звільнили, зламав і вимкнув мережу екстреного сповіщення. Його не було виявлено, доки не виникла реальна надзвичайна ситуація і система не вийшла з ладу [13].
- Платна дорога Carmel Tunnels – 8 вересня 2013 року троянська програма заразила ізраїльську платну ділянку, націлившись на систему відеоспостереження, заважаючи основним операціям протягом двох днів і завдавши фінансової шкоди.
- Conficker – у 2009 році хробак Conficker вразив французький військовий аеродром, не даючи злетіти літакам і британським військовим кораблям.
- Порт Антверпена – у 2013 році хакери використовували пристрої віддаленого доступу для сприяння контрабандним операціям у порту; цілком можливо, що хакери могли контролювати логістичну систему.
- WannaCry – у 2017 році приблизно 450 комп'ютерів німецької залізниці (DB) були заражені програмою-вимагачем WannaCry, залишивши повідомлення про викуп із вимогою оплатити 300 доларів США в біткойнах. Це вивело з ладу системи інформації про пасажирів, квиткові автомати та мережі відеоспостереження.
- A.P. Møller-Maersk – у червні 2017 року небезпечна програма-вимагач під назвою NotPetya, модифікована версія Petya, заразила підприємства по всій Європі. Постраждала транспортно-логістична корпорація Maersk group. Атака була настільки масовою, що компанія Maersk зазнала збитків у розмірі понад 300 мільйонів доларів і була змушена перевстановити понад 4000 серверів, 45 000 ПК і 2500 програм.

Ці інциденти вказують на те, що загрози для транспорту та критично важливих систем є реальними та є просто ажіотажем, який створює непотрібну паніку. Далі описано вразливості та методи атак, які загрози використовують для їх націлювання.

Загрози, уразливості та методи атаки проти IIoT та IoT. Щоб повністю зрозуміти вразливості, необхідно провести детальну оцінку всіх елементів системи (наприклад, датчиків, шлюзових пристроїв, мережевої інфраструктури), щоб визначити наявність уразливостей.

Відповідно до останнього «Звіту про загрози безпеці в Інтернеті» [20], кількість атак на IoT зросла на 600% з 6 тисяч у 2016 році до 50 тисяч у 2017 році. Це збільшення могло відбутися через кількість розгортань IoT та IIoT. Аналізуючи дані [20], основні загрози, виявлені IoT honeypot у 2017 році, відображені в табл. 2.2 і на рис.2.2, де показано понад 60% загроз, пов'язаних із DDoS і зловмисним програмним забезпеченням із 26%.

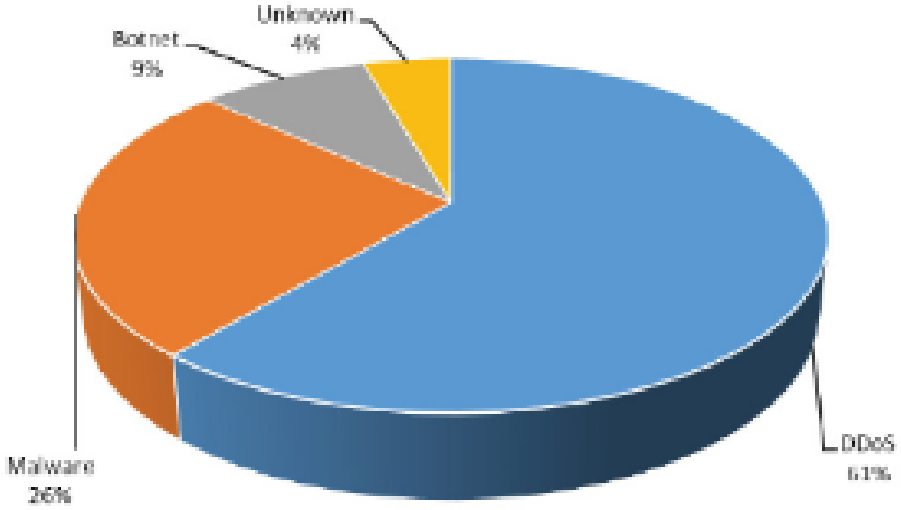

Рис.2.2. Загрози/атаки IoT [20]

Дайджест звіту про витоки даних [21] 35% порушень або інцидентів у секторі транспортування та складання були спричинені атаками на веб-додатки, 26% – DoS-атаками, 16% – кібершпигунством і 10% – злочинним програмним забезпеченням, як показано на рис.2.3.

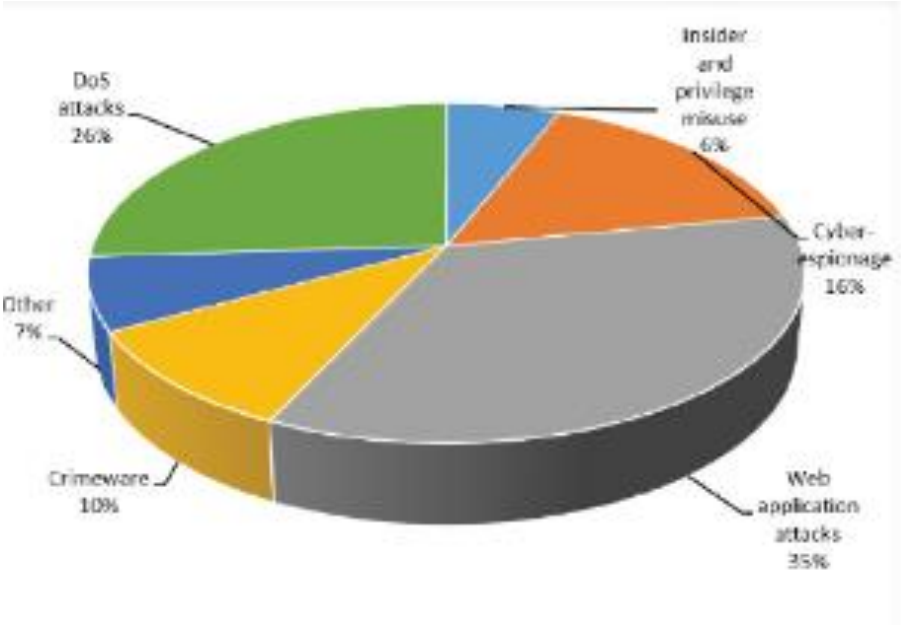

Рис.2.3. Загрози в транспортному секторі

Таблиця 2.2.

Основні виявлені загрози

Назва загрози за рангом	Тип загрози	Відсоток
Linux.Lightaidra	DDoS	57.5
Trojan.Gen.NPE	Шкідливе програмне забезпечення	10.2
Linux.Mirai	Ботнет	8.7
Trojan.Gen.NPE.2	Шкідливе програмне забезпечення	4
Linux.Kaiten	DDoS	3.6
Downloader.Trojan	Шкідливе програмне забезпечення	3
Linux.Gafgyt	Шкідливе програмне забезпечення	2.7
Trojan.Gen.8!cloud	Шкідливе програмне забезпечення	2.2
SecurityRisk.gen1	Шкідливе програмне забезпечення	1.9
Trojan.Gen.6	Шкідливе програмне забезпечення	1.7
Невідомий	Невідомий	4.5

Це показує, що DDoS або DoS є поширеними як загрози Інтернету речей, а також загрози в транспортній галузі. У табл. 2.3 наведено короткий перелік

поширених уразливостей, семи серйозних уразливостей Інтернету речей, і десяти найкращих уразливостей Інтернету речей.

Таблиця 2.3.

Поширені вразливості IoT

Категорія	Вразливість
Доступ	Перерахування імен користувачів шляхом взаємодії з механізмом автентифікації
	Неможливо змінити паролі за умовчанням
	Немає можливості блокування облікового запису. Може дозволити спроби автентифікації після кількості невдалих спроб входу.
	Неналежні методи автентифікації або їх відсутність. Відсутність механізмів двофакторної автентифікації (наприклад, маркер безпеки)
	Немає засобів керування паролями (довжина пароля, складність, термін дії паролів тощо)
	Можливість отримати доступ до консолі шляхом підключення до послідовного інтерфейсу (наприклад, USB, порт Ethernet, послідовний порт).
Виправлення / оновлення прошивки	Немає можливості вручну примусово перевірити оновлення для пристрою
	Немає можливості оновити пристрій
	Надмірні права доступу дозволяють змінювати файли оновлення та розповсюджувати їх серед усіх користувачів
	Поточна версія мікропрограми не відображається та/або дата останнього оновлення не відображається
	Мікропрограма містить конфіденційну інформацію, як-от вихідний код, паролі за замовчуванням, ключі ssh і двійкові файли запущених служб.
	Мікропрограма містить конфіденційну інформацію, як-от вихідний код, паролі за замовчуванням, ключі ssh і двійкові файли запущених служб.
Конфігурація	Управління потоком виконання коду пристрою. Можливість змінювати виконання вбудованого програмного забезпечення в пристрої та обходити майже всі програмні засоби контролю безпеки.

Продовження таблиці 2.3.

Категорія	Вразливість
	Атаки по бічному каналу також можуть змінити потік виконання або можуть бути використані для витоку цікавої інформації з пристрою.
Шифрування	Незашифровані мережеві служби дозволяють зловмисникам прослуховувати або втручатися.
	Погано реалізоване шифрування. Він неправильно налаштований або не оновлюється належним чином, напр. за допомогою SSL v2.
	Оновлення передаються через мережу без використання TLS або шифрування самого файлу оновлення.
Змінний носій	Видалення носія даних Можливість фізично видалити носій даних із пристрою.
DDoS	IIoT можна атакувати таким чином, щоб відмовити в обслуговуванні цієї служби або всього пристрою за допомогою розподіленої атаки на відмову в обслуговуванні (DoS).
Протоколи	Деякі протоколи, такі як MQTT, небезпечні. Деякі уразливості не криються в самих протоколах конфігурації та способах їх реалізації.
Ненадійні інтерфейси	Недоліки у вихідному коді веб-інтерфейсу роблять інтерфейс уразливим до кібератак. наприклад включав впровадження SQL, міжсайтовий сценарій і підробку міжсайтового запиту.
	Хмарний інтерфейс представляє ще одну потенційну вразливість безпеки.
	Ненадійний мобільний інтерфейс.
Конфіденційність	Стерти особисті або корпоративні дані не так просто.
	Дані на пристрої IoT не зашифровані, що робить дані вразливими для прихованого викрадення та крадіжки.

На додаток до вищезазначених уразливостей, вразливість в інтерфейсі або зв’язку між транспортними інженерними системами та системами розваг для пасажирів. Це може надати хакерам доступ до критично важливих систем, і їх слід ізолювати.

Згідно з попередніми дослідженнями, які були зосереджені на ICS/SCADA, основними загрозами були зловмисне програмне забезпечення, ненавмисні

неавторизовані дії персоналу та незадоволений персонал, які вплинули на ICS/SCADA у Південній Африці. Якщо IIoT — це технологія, яка базується на системах ICS/SCADA [14], ці загрози та ризики можуть бути успадковані пристроями IIoT/IoT.

Загрози та ризики показують важливість, яку відіграє характеристика доступності інформації в ОТ або промисловому середовищі. Щоб забезпечити доступність пристроїв IIoT та IoT, необхідно припинити атаки на відмову в обслуговуванні. У табл. 2.4 представлені розглянуті атаки спуфінгу.

Таблиця 2.4.

Загроза спуфінгу

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Імітація світлих вузлів	Створюючи підроблений вузол, подібний до оригінального, зловмисник може впроваджувати підроблену інформацію в систему, надсилати команди на різні пристрої та виконувати будь-які дії в межах функціональності оригінального вузла.
Світловий вузол (датчик/привід)	Кража цифрової ідентичності	Атаки можуть здійснюватися за допомогою вразливостей в апаратному чи програмному забезпеченні легких вузлів і можуть призвести до виконання зловмисником будь-яких дій від імені вузла. Ця спуфінгова атака може стати відправною точкою для атак інших категорій, таких як підробка та розкриття інформації
Диспетчер групи пристроїв	Кража цифрової ідентичності	Основним ризиком цієї атаки є публікація зловмисником підробленого списку пристроїв у клубку, підписавши його закритим ключем початкового менеджера. Підробивши особу менеджера, будь-який пристрій можна ввести в систему та отримати доступ для виконання різних дій.

Продовження таблиці 2.4.

Компонент	Атака	Ризик
Шлюз пристрою	Підробка ідентифікатора шлюзу	Маскуючись як шлюз пристрою, зловмисник може виконувати різні дії в системі, наприклад перехоплювати функції генерації ключів і публікувати транзакції в мережі з неавтентифікованих вузлів.
Панель адміністратора	Отримання контролю над адмінпанеллю від її імені	Отримавши контроль над панеллю адміністратора, зловмисник може реєструвати, анулювати або вимикати пристрої з системи. Ці дії можуть спричинити частковий або повний збій системи, оскільки ці дії служать вхідними даними для створення списку пристроїв і процесів автентифікації.
Координатор мережі Tangle	Вкрасти насіння.	Оскільки роль координатора в клубковій мережі полягає в тому, щоб фіксувати стан системи шляхом створення знімка, який використовуватиме вузли клубка для процесу створення консенсусу, шляхом викрадення вихідного коду зловмисник зможе надіслати підроблені етапи та порушити процеси в мережі клубка

У табл. 2.5 показано атаки втручання, які беруться до уваги.

Таблиця 2.5.

Загрози втручання

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Модифікація зібраних/проаналізованих даних, що зберігаються на вузлі	Ця атака відноситься до атак фізичного рівня і може бути виконана шляхом зміни середовища, з якого датчик збирає дані, або модифікації компонентів датчика, відповідальних за аналіз середовища та збір даних.

Продовження таблиці 2.5.

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Людина в середині атаки	Зловмисник може модифікувати пакети, надіслані від світлового вузла до шлюзу, або пакети, що йдуть у протилежному потоці - від шлюзу до світлового вузла. Пакунки можна модифікувати різними способами, наприклад модифікувати тіло пакета або його джерело та призначення. У результаті пакети можуть бути доставлені на вузли, які не повинні мати доступу до інформації, або вузли отримають пакет із підробленими даними та джерелом.
Світловий вузол (датчик/привід)	Модифікація конфігурацій на датчиках	Змінюючи конфігурації легких вузлів, зловмисник може змусити вузли створювати підроблені дані, надсилати або виконувати команди та може спричинити неочікувану поведінку вузла у фізичному світі.
Диспетчер групи пристроїв	Модифікація закритого ключа	Змінюючи закритий ключ менеджера, зловмисник може спричинити відмову в обслуговуванні для пристроїв, зареєстрованих після цієї модифікації, оскільки щойно опублікований список пристроїв буде підписаний ключем, який не розпізнається системою.
Диспетчер групи пристроїв	Зміна списку збережених пристроїв	Змінюючи збережений список пристроїв, зловмисник може додавати або видаляти вузли з існуючої системи, що створює ризик ін’єкцій для розкриття інформації та атак на відмову в обслуговуванні.

Продовження таблиці 2.5.

Компонент	Атака	Ризик
Шлюз пристрою	Модифікація збережених ключів пристрою	Змінюючи збережені ключі пристрою, зловмисник може викликати конфлікт у процесі автентифікації
Шлюз пристрою	Зміна пакетів	Зловмисник може змінювати пакети, надіслані від шлюзу до клубка, або пакети, що йдуть у протилежному потоці - від клубка до шлюзу. Пакунки можна модифікувати різними способами, наприклад модифікувати тіло пакета або його джерело та призначення. У результаті пакети можуть бути доставлені на вузли, які не повинні мати доступу до інформації, або вузли отримають пакет із підробленими даними та джерелом.
Панель адміністратора	Зміна запитів на реєстрацію/відкликання пристроїв	За допомогою цієї атаки можна спричинити відмову в обслуговуванні для анульованих вузлів або ввести в систему ненадійні пристрої

У табл. 2.6 наведено враховані атаки відмови.

Таблиця 2.6.

Загрози відмови

Компонент	Атака	Ризик
Диспетчер групи пристроїв	Публікація списку пристроїв у клубку.	Зловмисник може опублікувати список пристроїв без підпису або з підробленим підписом і спробувати вплинути на механізм аутентифікації системи.

Продовження таблиці 2.6.

Компонент	Атака	Ризик
Шлюз пристрою	Публікація пакетів з підробленим підписом у клубок	Для цієї атаки може бути 2 можливі вектори ризику. 1 – одержувач може не ідентифікувати відправника, якщо підпис не розпізнається системою. 2. Одержувач може прийняти пакет, оскільки він має підроблений підпис довіреного вузла в системі, який не є початковим відправником.
Шлюз пристрою	Відправка пакетів з підробленим підписом на світлові вузли	Ця атака може спричинити неправильну роботу світлового вузла. Система моніторингу не зможе відстежити джерело пакета, який спричинив неправильну роботу вузла призначення.
Панель адміністратора	Створення та використання підробленого облікового запису адміністратора	Зловмисник може отримати ті самі привілеї в системі, що й початкові користувачі-адміністратори

Табл. 2.7 демонструє перевірені атаки на розкриття інформації.

Таблиця 2.7.

Загрози розголошення інформації

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Злом пристрою шляхом використання вразливостей програмного/апаратного забезпечення	Зловмисник може спробувати передати інформацію, що зберігається на пристрої, ненадійним стороннім особам. Це може призвести до втрати конфіденційної інформації про стан системи або функціональність вузла, яка може бути використана для майбутніх атак

Продовження таблиці 2.7.

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Сніфінг комунікацій	Виконуючи атаку людини посередині на комунікаційну мережу між легким вузлом і шлюзом, зловмисник матиме доступ до всіх даних, якими обмінюється цей вузол.
Диспетчер групи пристроїв	Сніфінг комунікацій	Шляхом нюхання каналу зв'язку зловмисник може викрасти інформацію про пристрої та їхні UUID, зареєстровані в системі, а з іншого боку, він може нюхати зв'язок між диспетчером пристроїв і шлюзом і збирати відкриті ключі, згенеровані для зареєстрованих пристроїв. Здійснюючи цю атаку, можна збирати конфіденційну інформацію про пристрої та використовувати її для майбутніх атак
Диспетчер групи пристроїв	Розкриття збережених даних через уразливості програмного/апаратного забезпечення	Отримавши доступ до збережених даних, таких як останній список пристроїв, зловмисник може збирати інформацію про існуюче середовище та всі його компоненти та використовувати її для розробки майбутніх планів атак
Шлюз пристрою	Несанкціонований доступ до обмінюваних пакетів даних	Виконуючи цю атаку, зловмисник може збирати інформацію про згенеровані відкриті ключі для щойно зареєстрованих пристроїв або пакети даних, якими обмінюються світлові вузли

Продовження таблиці 2.7.

Компонент	Атака	Ризик
Шлюз пристрою	Розкриття збережених даних через уразливості програмного/апаратного забезпечення	Якщо зловмисник отримає доступ до збережених даних шлюзу, він зможе витягти всі пари ключів, згенеровані на шлюзі для всіх пристроїв, що існують у середовищі. Ці ключі можна використовувати для наступних атак

Табл. 2.8 підсумовує оцінку атак на відмову в обслуговуванні

Таблиця 2.8.

Загрози відмови в обслуговуванні

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Фізична атака на вузол	Зловмисник може виконувати фізичні дії, наприклад перерізати дроти, вимикати живлення, створювати перешкоди на радіочастотах тощо. Це призведе до пошкодження пристрою або його з'єднання та призведе до тимчасових або постійних проблем із доступністю. Крім того, атаки флуду та використання вразливостей можуть зупинити нормальну роботу пристроїв.
Диспетчер групи пристроїв	Втрата списку пристроїв	Зловмисник може спробувати досягти відмови в обслуговуванні, видаливши список пристроїв із диспетчера груп пристроїв. Втрата списку пристроїв може спричинити відмову в обслуговуванні для всіх пристроїв, які намагаються зареєструватися в системі, або пристроїв, які запитується на відкликання/вимкнення. Крім того, атаки флуду та використання вразливостей можуть зупинити нормальну роботу пристроїв.

Продовження таблиці 2.8.

Компонент	Атака	Ризик
Диспетчер груп пристроїв, шлюз пристроїв	Затоплення	Зловмисник може організувати лавинну мережу, що призведе до відмови в обслуговуванні, оскільки сервіси не зможуть прийняти будь-які запити, або, використовуючи вразливості, можуть зупинити нормальну роботу пристроїв.
Диспетчер груп пристроїв, шлюз пристроїв	Фізична DoS атака	Фізичні атаки на повні вузли можуть завдати шкоди серверам, на яких розміщено ці компоненти
Панель адміністратора	Скасування наявних пристроїв, менеджерів та шлюзів	Ця атака безпосередньо впливає на механізм автентифікації, оскільки будь-який відкликаний компонент не пройде автентифікацію в системі. Зловмисник може викликати відмову в обслуговуванні для групи пристроїв, просто скасувавши груповий шлюз
Координатор мережі Tangle	Видалення насіння.	Якщо зловмисник спричинить втрату початкового числа координатора, він не зможе створити знімки для процесу прийняття рішень іншими вузлами, що призведе до відмови в обслуговуванні та простою загальної інфраструктури.

Табл. 2.9 показує розглянуті атаки на підвищення привілеїв.

Таблиця 2.9.

Загрози підвищення привілеїв

Компонент	Атака	Ризик
Світловий вузол (датчик/привід)	Отримання доступу до конфігурації пристрою	Отримавши доступ до процесу конфігурації пристрою, зловмисник може внести несанкціоновані зміни конфігурації. Це може призвести до неправильної роботи вузла або відкрити бекдор для майбутніх атак

Продовження таблиці 2.9.

Компонент	Атака	Ризик
Диспетчер групи пристроїв	Зловживання функціями компонента, використовуючи вразливості в базових операційних системах, службах і обладнанні	Націлюючись на бізнес-функції менеджера, зловмисник може виконувати внутрішні дії, які не були дозволені задумом. Одним із ризиків для менеджера може бути захоплення функції створення ключів. Шлюз пристрою буде виключено з процесу реєстрації та не отримуватиме сповіщення про нові зареєстровані пристрої в системі
Шлюз пристрою	Зловживати функціями компонента, використовуючи вразливості в підкреслених операційних системах, службах і апаратному забезпеченні.	Націлюючись на бізнес-функції шлюзу, зловмисник може виконувати несанкціоновані дії, такі як публікація списку пристроїв або видалення згенерованих ключів пристрою

Після застосування STRIDE представлені та обговорені основні ризики та пом’якшення, а також відкриті проблеми. Оскільки повні вузли клубкової мережі мають більше обов’язків у системі, вони мають найвищий ризик атак. Атакуючи повні вузли клубкової мережі, відкривається додатковий вектор ризику, який можна описати наступним чином:

• Повний вузол, що генерує підказки щодо транзакцій, які надають пріоритет транзакціям зловмисників над звичайним алгоритмом вибору підказок.

• Атаки подвійних витрат, які змушують координатора надсилати непослідовні віхи. Вузли виявляти невідповідність у етапах і зупиняти процеси прийняття рішень і підтвердження транзакцій.

• Повні вузли зупиняють процес розподілу транзакцій етапів, що спричинить заморожування процесів підтвердження транзакцій.

2.3 Firewall, як вирішальний компонент для захисту мережі в IIoT

З IIoT приходить більше пристроїв, більше даних і більше взаємозв'язків з IT та Інтернетом. Усі ці фактори роблять промислову кібербезпеку, яка вже є важливою, ще більшою. Взаємозв'язок між мережами та зовнішніми пристроями створює нові загрози з усіх боків і в багатьох формах. Не лише у вигляді більшої «поверхні загрози» для зовнішньої атаки, але й збільшення можливостей для збоїв пристроїв, помилок програмного забезпечення чи помилок користувача – усе це може значно та негативно вплинути на роботу системи.

Брандмауери необхідні для забезпечення безпеки мережі та підвищення надійності та відмовостійкості системи. Без них не обходиться жодна модель безпеки. Подібно до різноманітних пристроїв у мережі IIoT, брандмауери бувають різних форм не лише з точки зору апаратних функцій і галузевих схвалень, але й із різними можливостями фільтрації. Хоча брандмауер може здатися одним типом пристрою, насправді це різноманітна сукупність пристроїв, що залишає завдання визначити, який тип брандмауера найкраще підходить для кожної частини програми чи середовища.

Брандмауери захищають мережі та пристрої, такі як промислові ПК, системи керування та камери, від несанкціонованого доступу, запобігаючи мережевому трафіку до чи від цих систем. Вони є основним елементом сегментації мережі та відіграють вирішальну роль у будь-якій стратегії безпеки мережі, пов'язаній з IIoT.

Брандмауери мають кілька основних цілей, зокрема:

- Захист будь-яких з'єднань між корпоративними та промисловими мережами та запобігання зовнішнім загрозам.
- Створення бар'єрів у мережі, щоб запобігти поширенню внутрішніх проблем.

- Дозвол лише дозволеного зв’язку між пристроями для захисту від зловмисних атак і помилок пристрою чи оператора.

Для досягнення цих цілей брандмауери приймають різні форми, від простої фільтрації пакетів до підтримки спеціалізованих промислових протоколів. Для належного захисту мережі та продуктивності потрібно вибрати відповідний тип брандмауера для використання в кожній частині системи.

Розглядаючи варіанти безпеки брандмауера, слід пам’ятати про низку факторів. Відмінності фільтрації, проблеми мережевого середовища та способи керування брандмауерами в мережі повинні бути стандартними міркуваннями для кожного, хто шукає рішення брандмауера [22].

- Спеціально для обраної мережі: брандмауери, як і вибір конкретних пристроїв IIoT, повинні мати можливість виконувати дуже конкретні завдання, які підтримують власні потреби та програми. Слід обирати брандмауери, які відповідають унікальним моделям зв’язку та потребам пристроїв у мережі.
- Перевірка на багатьох рівнях: залежно від того, де він буде знаходитися у системі, знадобляться різні механізми фільтрації. Брандмауери, які використовуються поблизу машин як частина стратегії безпеки «зон і каналів», повинні розуміти промислові протоколи та виконувати глибоку перевірку пакетів. Навпаки, брандмауер, який використовується для захисту периметра між віддаленим сайтом та Інтернетом, потребуватиме здатності обробляти трафік Інтернет-протоколу (IP).
- Витримують стійке середовище: залежно від обраного мережевого середовища, брандмауери можуть піддаватися розширеному діапазону температур, значній вібрації та іншим факторам навколишнього середовища. Потрібно переконатися, що будь-який брандмауер, який буде обраний, витримує жорсткі умови та відповідає всім галузевим стандартам і дозволам. Вибір брандмауера без надійності, необхідної для поточної програми, дуже швидко зірватиме проект.
- Простота: без потужного інструменту керування для простої та масової конфігурації брандмауерів завдання можуть забирати багато часу та бути схильними до помилок. Команди повинні мати можливість ефективно керувати

пристроями та налаштовувати їх під час використання кількох брандмауерів. Важливо, щоб брандмауери могли централізовано контролюватись інструментами керування мережею, щоб забезпечити безперебійну роботу.

Брандмауери є лише одним із компонентів ефективної стратегії безпеки для компаній, які використовують переваги IIoT. Але не слід применшати їх використання – вони є наріжним каменем, який утримує цілісну модель безпеки. Тверде розуміння доступних типів брандмауерів і ролі кожного з них призводить до успішного захисту мережі від низки внутрішніх і зовнішніх загроз, які ховаються ззовні.

Впроваджуючи цілісну стратегію захисту, яка включає брандмауери, можна розробляти мережі, які ефективно пом’якшують загрози та захищають від помилок і вразливостей, створених дедалі більшою кількістю пристроїв і середовищ IIoT.

Пристрої IIoT створюють значні ризики для безпеки мережі організації. Брандмауери IIoT захищають ці пристрої від експлуатації та можуть бути реалізовані одним із двох способів:

- Мережні брандмауери IIoT: мережеві брандмауери IIoT розгортаються як частина мережевих шлюзів і дозволяють як макро-, так і мікросегментацію розгортання IIoT в організації. Брандмауери мережі IIoT можуть використовувати VPN для шифрування трафіку між шлюзом і віддаленими серверами, які обробляють дані, зібрані пристроями IIoT.
- Вбудовані брандмауери IIoT: вбудовані брандмауери IIoT вбудовані в операційну систему пристрою IIoT. Вони встановлюються виробником пристроїв IoT і можуть фільтрувати трафік до пристрою та потенційно діяти як кінцева точка VPN.

Важливість брандмауерів IIoT

Пристрої IIoT сумно відомі своєю низькою безпекою. Серед поширених ризиків безпеки IIoT [22]:

- Застарілі операційні системи: пристрої IIoT можуть працювати під керуванням застарілих версій операційної системи. Це робить їх уразливими для використання через публічно відомі вразливості.

- Відсутність вбудованої безпеки: більшість пристроїв IIoT не мають вбудованих брандмауерів і антивірусів, які є типовими для настільних систем. Це полегшує зловмисникам використання цих систем і зараження їх шкідливим програмним забезпеченням.
- Складне керування виправленнями: виправлення проблем із функціональністю та безпекою є життєво важливим для безпеки всього програмного забезпечення. Однак пристрої IIoT рідко оновлюються, що робить їх вразливими для атак.
- Слабкі паролі: пристрої IIoT зазвичай розгортаються без зміни пароля за замовчуванням і можуть мати жорстко закодовані паролі, які користувачі не можуть змінити. Коли ці паролі стають загальновідомими, зловмисники можуть просто увійти на вразливі пристрої.
- Погана фізична безпека: багато пристроїв IIoT, наприклад камери, підключені до Інтернету, призначені для розгортання в публічних і віддалених місцях. Маючи фізичний доступ до пристроїв, зловмисники можуть обійти та знищити захист пристрою.
- Використання незахищеного протоколу: хоча більшість інтернет-трафіку уникає використання незахищених протоколів, таких як Telnet, це не стосується пристроїв Інтернету речей. Використання цих протоколів полегшує зловмисникам крадіжку облікових даних для входу та використання вразливих протоколів.

Ці проблеми з безпекою роблять пристрої IIoT значним ризиком для їхніх власників і мереж, де вони розгорнуті. Брандмауери IoT допомагають керувати цим ризиком, ускладнюючи атаку на пристрої та обмежуючи вплив скомпрометованого пристрою.

Пристрої IIoT розгортаються в різних галузях промисловості, але ці пристрої та архітектури не однакові. Промисловий і споживчий IIoT часто розгортаються на двох дуже різних архітектурах.

Виробники зазвичай використовують модель Пердью для сегментації своїх мереж промислових систем керування (ICS). Ця модель розділяє архітектуру IIoT

на кілька рівнів із визначеними цілями. Брандмауери мережі IIoT перевіряють і контролюють трафік через межі мережі.

- Рівень 4.5: корпоративний рівень — це корпоративна IT-мережа, де системи планування ресурсів підприємства (ERP) здійснюють високорівневе керування виробничими операціями.
- Рівень 3.5: демілітаризована зона (DMZ) розділяє IT-середовища та OT-середовища та включає системи безпеки, призначені для захисту OT-середовищ від атак через IT-мережі.
- Рівень 3: Системи виробничих операцій керують робочими процесами на виробництві.
- Рівень 2: у мережі процесів оператори контролюють фізичні процеси та керують ними за допомогою доступу людино-машинних інтерфейсів (HMI) до програмного забезпечення диспетчерського контролю та збору даних (SCADA).
- Рівень 1: у мережі керування інтелектуальні пристрої, такі як ПЛК (програмований логічний контролер) і RTU (віддалений термінальний блок), контролюють і маніпулюють фізичними пристроями.
- Рівень 0: у польовій мережі є фізичні пристрої та датчики, які виконують виробничі операції.

Навпаки, споживчі пристрої IIoT, які розгорнуті в більшій і більш різноманітній географічній зоні, можуть працювати за чотирирівневою архітектурною моделлю:

- Сенсорний рівень: пристрої IIoT збирають дані для обробки.
- Мережа або рівень збору даних: дані з однієї чи кількох систем збираються шлюзами Інтернету речей і безпечно передаються в системи обробки.
- Рівень попередньої обробки даних: IIoT-пристрої на базі Edge виконують попередню обробку, щоб зменшити обсяг даних, що надсилаються на хмарні сервери.
- Хмарний аналіз або прикладний рівень: хмарні сервери аналізують дані та надають користувачам доступ до аналітики та даних.

Архітектури промислового IIoT мають інтегровані рівні безпеки, яких може не вистачати в розгортанні споживчого IIoT. Шлюзи Інтернету речей і хмарні брандмауери можуть контролювати доступ для підвищення безпеки споживчих пристроїв Інтернету речей.

Запровадження IIoT зростає у всіх сферах, що робить безпеку IIoT важливою для всіх організацій. Однак для певних галузей і компаній безпека брандмауера IIoT особливо важлива, зокрема:

Промисловість: високі вимоги до доступності та продуктивності означають, що системи OT зазвичай працюють із застарілим програмним забезпеченням і мають обмежену підтримку вбудованих рішень безпеки. Оскільки ці системи все більше підключаються до IT-середовища, безпека брандмауера Інтернету речей є життєво важливою для блокування атак від проникнення в OT середовища та подальшого переміщення всередині організації.

Охорона здоров'я: медичний Інтернет речей (MIIoT) стрімко розвивається та включає кардіостимулятори, сканери, фітнес-трекери та подібні мережеві пристрої. Погана безпека цих пристроїв робить брандмауери IIoT необхідними для блокування спроб використання цих уразливих пристроїв.

Підприємство: на додаток до галузевих рішень, підприємства розгортають пристрої IIoT, такі як розумні системи керування будівлями, мережеві камери та принтери. Не всі пристрої можуть бути відомі або керовані IT-командою, що робить їх уразливими для експлуатації.

Виробники пристроїв: унікальні сценарії розгортання пристроїв IIoT ускладнюють захист традиційними методами. Розгортаючи вбудовані брандмауери IIoT на своїх пристроях, виробники пристроїв можуть покращити безпеку цих пристроїв і стійкість до спроб експлуатації.

Основні переваги брандмауера:

1. *Відстежує мережевий трафік*. Усі переваги безпеки брандмауера починаються з можливості відстежувати мережевий трафік. Дані, що надходять системи та виходять із них, створюють можливості для загроз для компрометації операцій. Відстежуючи та аналізуючи мережевий трафік, брандмауери

використовують попередньо встановлені правила та фільтри для захисту систем. Завдяки добре підготовленій ІТ-команді можна керувати рівнями захисту на основі того, що видно, як входить і виходить через брандмауер.

2. *Зупиняє вірусні атаки*. Ніщо не може зупинити цифрові операції швидше та сильніше, ніж вірусна атака. З сотнями тисяч нових загроз, що розробляються щодня, життєво важливо встановлювати захист, щоб системи були працездатними. Однією з найбільш очевидних переваг брандмауерів є можливість контролювати точки входу системи та зупиняти вірусні атаки. Ціна шкоди від вірусної атаки на системи може бути незмірно високою залежно від типу вірусу.

3. *Запобігає злому*. На жаль, тенденція до переходу компаній до цифрових операцій спонукає злодіїв і зловмисників робити те саме. Із зростанням крадіжки даних і злочинцями, які тримають системи в заручниках, брандмауери набувають ще більшого значення, оскільки вони запобігають несанкціонованому доступу хакерів до даних, електронних листів, систем тощо. Брандмауер може повністю зупинити хакера або завадити йому вибрати легшу ціль.

4. *Зупиняє програму-шпигун*. У світі, що керується даними, дуже необхідною перевагою є те, що шпигунське програмне забезпечення не зможе отримати доступ до систем і не потрапить у них. Оскільки системи стають більш складними та надійними, кількість точок входу, які злочинці можуть використовувати для отримання доступу до систем, також збільшується. Одним із найпоширеніших способів доступу небажаних людей є використання шпигунського та зловмисного програмного забезпечення — програм, призначених для проникнення у системи, контролю комп’ютерів і викрадення даних. Брандмауери служать важливим блоком проти цих шкідливих програм.

5. *Сприяє конфіденційності*. Головною перевагою є сприяння конфіденційності. Проактивно працюючи над захистом даних і даних клієнтів, створюється середовище конфіденційності, якому клієнти можуть довіряти. Нікому не подобається, що їхні дані викрадають, особливо коли зрозуміло, що можна було вжити заходів для запобігання вторгненню.

Недоліки традиційних брандмауерів:

1. *Обмеження поінформованості про програму*. Традиційним брандмауерам не вистачає такої глибокої здатності, як NGFW, особливо коли йдеться про програми. NGFW дозволяють користувачеві бачити, які програми використовуються в мережі, і дозволяють контролювати конкретне використання в цих програмах. За допомогою традиційного брандмауера гнучкість керування доступом так глибоко недоступна.

2. *Проблеми зі швидкістю мережі*. Швидкість є проблемою. Багато традиційних брандмауерів створюють вузьке місце в точках перевірки даних, що може уповільнити роботу та коштувати грошей. Для операцій, які очікують масштабування, додавання більше правил, політик і протоколів безпеки, це не ідеально.

3. *Логістичні недоліки*. Багато традиційних брандмауерів не здатні адаптуватися до мінливих аспектів систем і операцій компанії. Вони можуть бути громіздкими, вимагати інтенсивного керування та обслуговування, і їм важко адаптуватися до хмарних середовищ. Крім того, керування правилами політики у великій мережі може бути виснажливим і створювати надмірне та дороге навантаження на IT-відділи. Це не тільки може створити діри для вторгнення, але й може створити вузькі місця в роботі. Відсутність контролю над правилами безпеки може перешкоджати доступу до інформації та користувачів, до яких потрібно мати доступ.

4. *Відсутність можливостей еволюції*. Ландшафт загроз безпеці постійно змінюється, щодня з’являються нові загрози. Майже неможливо йти в ногу зі змінами та надавати ефективну підтримку та захист без серйозного обмеження можливостей команди чи бізнесу. Перевстановлення нових рішень у кожній системі є дорогим, трудомістким і створює можливості для вразливостей із застарілим захистом.

Переваги мережевих брандмауерів [23]:

1. *Універсальність*. Можливість постійного оновлення та адаптації безпеки мережі в режимі реального часу надає IT-команді велику гнучкість і універсальність. Хоча NGFW може мати апаратний компонент, більшість змін і

оновлень можна розгорнути з одного комп’ютера. Це дає змогу бути в курсі мінливого середовища загроз. Крім того, можна легше контролювати потік даних і користувачів, якщо бізнес змінить спосіб роботи.

2. *Контроль інтелектуального порту*. Мережеві брандмауери виходять за межі класичного однорівневого портового підходу традиційних рішень. Натомість NGFW пропонують багаторівневий захист, аналізуючи трафік на різних рівнях мережі. Крім того, NGFW додають до рівняння безпеку на рівні додатків, забезпечуючи більше контролю, кращу прозорість і можливість краще контролювати дані та інформацію, які надходять і виходять з мережі користувача. Чим розумніша система безпеки, тим ефективнішою буде її робота.

3. *Проста інфраструктура*. Однією з головних переваг NGFW є простота інфраструктури. Завдяки оптимізації безпеки мережі IT-команда може набагато легше розгортати нові політики в усій мережі з одного пристрою. Крім того, прозорість дає команді більше гнучкості в контролі того, що входить і що виходить, що є основною метою.

4. *Оновлений захист від загроз*. Історично підприємствам були потрібні незалежні брандмауери, антивіруси, системи захисту від програм-вимагачів і системи виявлення вторгнень. Великою перевагою NGFW є те, що ці заходи безпеки інтегровані в один цілісний продукт. Це не тільки легше для IT-відділу, але й підвищує рівень захисту за допомогою взаємодії компонентів. NGFW також набагато глибше завдяки глибокій перевірці пакетів (DPI), яка переглядає більше елементів даних, що надходять у системи. Результатом є більш обґрунтований та ефективніший процес прийняття рішень щодо того, що дозволити, а що заблокувати. Знову ж таки, це доповнює основну мету брандмауерів.

5. *Постійна швидкість мережі*. Як уже згадувалося, традиційні брандмауери можуть дедалі більше забивати системи, коли розширюється захист. Дуже цінною перевагою є те, що можна продовжувати вдосконалювати та розширювати розгортання захисту без шкоди для швидкості мережі. Сама природа дизайну мережі сприяє найвищій потенційній пропускній здатності без шкоди для безпеки.

Простіше кажучи, системи залишаються захищеними, а швидкість операцій залишається високою.

Висновки до другого розділу

Досліджено проблематику в промислових мережах та графічно вказано концепцію моніторингу безпеки. Наведено останні тенденції у системах безпеки IIoT.

Обґрунтовано методології аналізу безпеки та категорії аналізу загроз STRIDE, які для зручності описано у таблицях. Приведено класифікацію загроз, вразливостей та методів атаки проти IIoT та IoT.

Розглянуто важливість брандмауерів для промислових мереж та описано їхні основні цілі. Проаналізовано недоліки традиційних фаєрволів, основні переваги та переваги мережевих брандмауерів.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ CISCO SECURE FIREWALL ISA 3000

3.1 Загальний опис

Cisco ISA 3000 — це надійний промисловий пристрій безпеки, встановлений на DIN-рейку, який забезпечує брандмауер, захист від загроз і послуги VPN. Термін DIN-рейки описує металеву рейку стандартного типу, яка широко використовується для монтажу автоматичних вимикачів і промислового контрольного обладнання всередині стелажів обладнання. Термін походить від оригінальних специфікацій, опублікованих Deutsches Institut für Normung (DIN) у Німеччині. Пристрій може запускати операційну систему ASA або Firepower Threat Defense.

Cisco ISA 3000 є малопотужним, безвентиляторним, з Gigabit Ethernet і виділеним портом керування. Є два SKU:

• ISA3000-4C-K9 — мідний SKU з 4x10/100/1000Base-T з портом керування.

• ISA3000-2C2F-K9 — Fiber SKU з 2x1GbE SFP і 2x10/100/1000Base-T з портом керування.

На рис.3.1 і рис.3.2 показано мідні та оптоволоконні моделі Cisco ISA 3000.

Рис.3.1. Cisco ISA 3000 Copper SKU

Рис.3.2. Cisco ISA 3000 Fiber SKU

На рис.3.3 показано деталі передньої панелі Cisco ISA 3000.

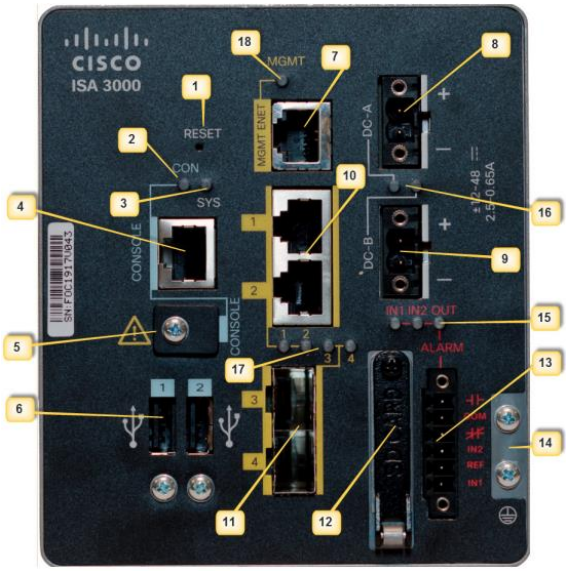

Рис.3.3. Передня панель Cisco ISA 3000

1 - скинути; 2 - світлодіоди консолі; 3 - системний світлодіод; 4 - консольний роз'єм (RJ-45); 5 - консольний роз'єм (mini-USB); 6 - роз'єми USB; 7 - інтерфейс керування; 8 і 9 - з’єднання живлення постійного струму; 10 - роз’єми RJ45 10/100/1000 BaseT 1 і 2; 11 - на ISA-3000-2C2F SKU це роз’єми SFP. на ISA-3000-4C SKU це RJ45; 12 - гніздо для знімної картки флеш-пам'яті SD на 1 ГБ; 13 - роз'єми сигналізації; 14 - точка заземлення; 15 - світлодіоди сигналізації; 16 - світлодіоди постійного струму; 17 - світлодіоди Ethernet 17 Gig; 18 - світлодіод управління

Пам'ять і зберігання. Cisco ISA 3000 має наступні характеристики:

• 8 ГБ DRAM (припаяно);

• 16 ГБ вбудованої флеш-пам'яті;

• mSATA 64Gb;

• Знімна карта флеш-пам'яті SD на 1 ГБ.

USB порти. Cisco ISA 3000 має два зовнішні роз’єми USB типу A (4-контактні). Кожен порт USB підтримує вихідне живлення 5 вольт і максимум до 500 мА.

Порт керування Ethernet. Надається порт Ethernet 10/100/1000 BaseT лише для керування. Цей порт буде єдиним портом, який можна використовувати для завантаження через мережу або для початкового налаштування та керування системою. У конфігурації цей порт має назву Management 1/1.

Консольний порт. Cisco ISA 3000 можна налаштувати через веб-інтерфейс або через консольний порт. Консольний порт – це роз’єм RJ45 або Mini USB. Для перетворення роз’єму RJ45 на роз’єм DB9 можна використовувати стандартний кабель керування.

Параметри конфігурації за замовчуванням для порту консолі RJ45 такі: 9600 бод, 8 біт даних, без паритету, 1 стоп-біт, без контролю потоку.

Якщо консольний порт USB активний (кабель вставлено та драйвери віддаленого ПК увімкнено), за замовчуванням консоль переключатиметься з RJ45 на USB, коли буде виявлено USB-кабель. Якщо підключено обидва порти, використовується консольний порт Mini USB.

Кнопка скидання повертає конфігурацію пристрою безпеки до стандартної конфігурації, встановленої на заводі. Щоб відновити конфігурацію пристрою безпеки до конфігурації за замовчуванням, встановленої на заводі, скористайтеся скріпкою стандартного розміру №1 із діаметром дроту 0,033 дюйма або менше та одночасно натисніть кнопку скидання під час подачі живлення на пристрій безпеки.

Джерело живлення. Cisco ISA 3000 постачається з резервним роз’ємом зовнішнього живлення роз'єм підтримує 12 - 48 В постійного струму. З’єднувачі –

це горизонтальна заглушка Molex із кроком 5,00 мм Eurostyle із кріпильними гвинтами.

Блок живлення не підтримує зворотну полярність, але має захист від зворотної полярності. Це означає, що якщо перевернути з'єднання + і –, система не ввімкнеться, але не буде пошкоджена.

Щоб система працювала, термінал «+» завжди має бути більшим за термінал «-». Відмінність полягає у використовуваній схемі заземлення системи.

ISA 3000 підтримує 3 основні схеми [24]:

• Ізольований вхід постійного струму, ані клеми +, ані - не прив'язані до GND шасі.

• Позитивний вхід постійного струму, негативна (-) клема підключена до заземлення шасі.

• Негативний вхід постійного струму, позитивна (+) клема прив'язана до GND шасі.

Знімна карта флеш-пам'яті SD на 1 ГБ. Cisco ISA 3000 має знімний слот для флеш-пам'яті SD (далі – SD). Це перш за все для того, щоб дозволити легке оновлення, копіювання журналів і аварійних дампів.

Пристрій не постачається зі встановленою змінною картою флеш-пам'яті SD, це додаткова запасна частина.

Порти сигналізації. Cisco ISA 3000 має порти сигналізації. Є дві умови, які генерують тривогу:

• Якщо налаштовано подвійне джерело живлення, а блок живлення несправний або відсутній.

• Коли температура ЦП знаходиться в критичному стані (нижче -40°C або вище 105°C).

Коли виконується будь-яка умова, світлодіод тривоги стає червоним, і запускається повідомлення системного журналу та перехоплення SNMP.

Температурний сенсор. Операційна система відстежує температуру процесора під час його роботи.

Якщо температура процесора знаходиться в критичному стані (нижче -40°C або вище 105°C), світлодіодний індикатор сигналізації стає червоним.

Коли температура ЦП повертається до нормального стану, світлодіодний індикатор сигналізації вимикається.

3.2 Розгортання Firepower Threat Defense за допомогою FMC

Апаратне забезпечення ISA 3000 може працювати як із програмним забезпеченням для захисту від загроз, так і з програмним забезпеченням ASA. Переключення між захистом від загроз та ASA потребує повторного створення образу пристрою.

Щоб розгорнути захист від загроз за допомогою диспетчера пристроїв, необхідно виконати такі завдання [25]:

1. ***Переглянути розгортання мережі.*** Можна керувати захистом від загроз за допомогою центру управління з інтерфейсу Management 1/1 або 6.7 і пізніших версіях через інтерфейс даних. За замовчуванням інтерфейс Management 1/1 увімкнений та налаштований на IP-адресу (192.168.45.45). Цей інтерфейс також спочатку запускає DHCP-сервер; після вибору центру керування як диспетчер під час початкового налаштування DHCP-сервер відключається.

6.7 і пізніші версії розгортання віддаленого керування.

На наступному рисунку показано рекомендоване розгортання мережі ISA 3000 з використанням зовнішнього інтерфейсу для управління. Цей сценарій ідеальний для управління філіями центральної штаб-квартири.

Загальнодоступна IP-адреса або ім'я хоста потрібно або для захисту від загроз або для центру керування.

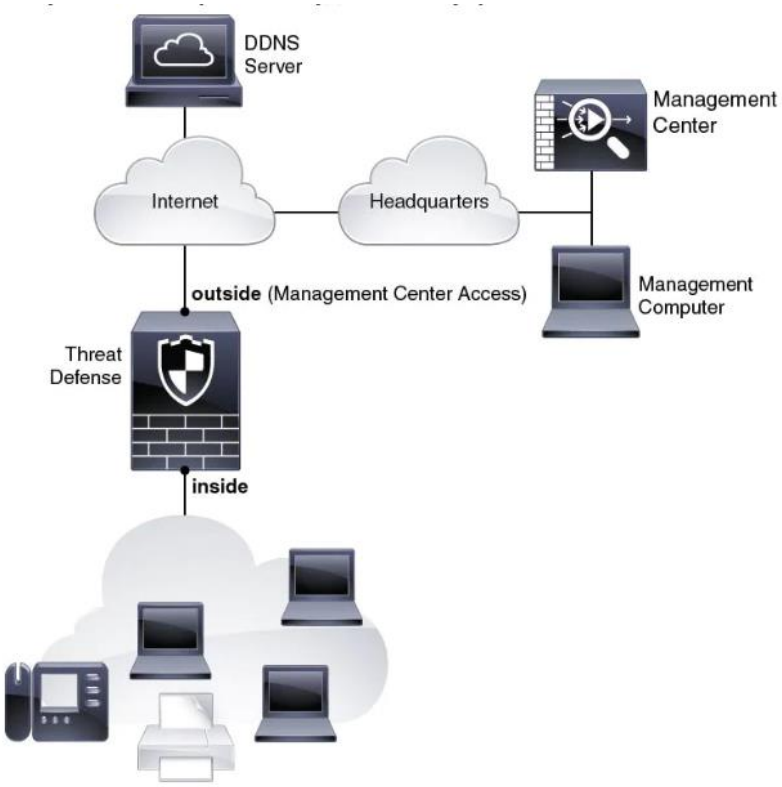

Рис.3.4. Розгортання віддаленого керування

2. Кабель пристрою. Щоб підключити сценарій віддаленого керування до ISA 3000 (рис.3.5), слід виконати такі дії:

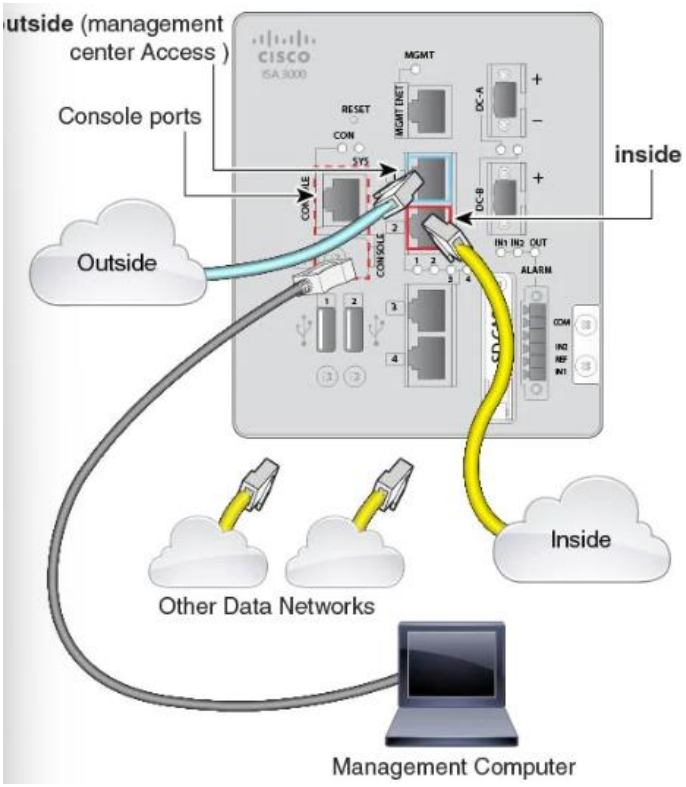

Рис.3.5. Підключення віддаленого розгортання управління

Центр керування та керуючий комп'ютер знаходяться у віддаленій штаб-квартирі і можуть підключатися до системи захисту від загроз через Інтернет.

a. Підключити керуючий комп'ютер до консольного порту. Потрібно використовувати консольний порт для доступу до CLI для початкового налаштування. Можна виконати початкове налаштування CLI у головному офісі, а потім відправити захист від загроз у віддалену філію. У філії консольне підключення не потрібне для повсякденного використання; це може знадобитися для усунення несправностей.

b. Підключити внутрішню мережу (наприклад, GigabitEthernet 1/2).

c. Підключити зовнішній інтерфейс (наприклад, GigabitEthernet 1/1) до зовнішнього маршрутизатора.

d. Підключити інші мережі до інтерфейсів, що залишилися.

3. Увімкнення пристрію. Живлення системи контролюється живленням постійного струму; немає кнопки живлення. Потрібно підключити вилку живлення до ISA 3000 після підключення його до джерела постійного струму. Потім перевірити індикатор системи на передній панелі пристрою ISA 3000; якщо він постійно горить зеленим, пристрій увімкнено. Якщо він блимає зеленим, пристрій знаходиться у фазі завантаження та POST.

4. Виконання початкового налаштування Threat Defense за допомогою інтерфейсу командного рядка. Підключення до інтерфейсу командного рядка захисту від загроз, щоб виконати початкове налаштування, включаючи налаштування IP-адреси керування, шлюзу та інших основних параметрів мережі за допомогою майстра налаштування. Виділений інтерфейс керування – це спеціальний інтерфейс із власними мережевими налаштуваннями.

a) Слід підключитись до інтерфейсу командного рядка захисту від загроз через консольний порт або через SSH до інтерфейсу управління, який за замовчуванням отримує IP-адресу від DHCP-сервера.

b) Потім увійти у систему з ім'ям користувача admin і паролем Admin123.

c) При першому вході в систему захисту від загроз буде запропоновано прийняти Ліцензійну угоду з кінцевим користувачем (EULA) та змінити пароль адміністратора. Потім буде представлено сценарій встановлення CLI.

Значення за замовчуванням або раніше введені значення відображаються у дужках. Щоб набрати раніше введені значення, потрібно натиснути клавішу Enter.

Приклад:

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ***********
Confirm new password: ***********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: ***10.10.10.15***
Enter an IPv4 netmask for the management interface [255.255.255.0]: ***255.255.255.192***
Enter the IPv4 default gateway for the management interface [data-interfaces]: ***10.10.10.1***
Enter a fully qualified hostname for this system [firepower]: ***ftd-1.cisco.com***
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: ***no***
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery

- add system policy

You can register the sensor to a Firepower Management Center and use the Firepower Management Center to manage it. Note that registering the sensor to a Firepower Management Center disables on-sensor Firepower Services management capabilities.

When registering the sensor to a Firepower Management Center, a unique alphanumeric registration key is always required. In most cases, to register a sensor to a Firepower Management Center, you must provide the hostname or the IP address along with the registration key.
'configure manager add [hostname | ip address] [registration key]'

However, if the sensor and the Firepower Management Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.
'configure manager add DONTRESOLVE [registration key] [NAT ID]'

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.
>

d) Визначити центр керування, який керуватиме цим захистом від загроз.

менеджер налаштування додати {ім'я хоста | IPv4_адреса | IPv6_адреса | НЕ ДОЗВОЛЯТИ} reg_key [nat_id].

- {ім'я хоста | IPv4_адреса | IPv6_адреса | DONTRESOLVE} — вказує або повне доменне ім'я, або IP-адресу центру керування. Якщо центр керування не адресується безпосередньо, потрібно використати DONTRESOLVE і вказати nat_id. Принаймні один із пристроїв, будь то центр керування або засіб захисту від загроз, повинен мати доступну IP-адресу, щоб встановити двосторонній канал зв'язку із шифруванням SSL між двома пристроями.
- reg_key — вказує одноразовий реєстраційний ключ на вибір, який також вказати в центрі управління при реєстрації захисту від загроз. Реєстраційний ключ не повинен перевищувати 37 символів. Допустимі символи включають буквено-цифрові символи (A-Z, a-z, 0-9) і дефіс (-).
- nat_id — вказує унікальний одноразовий рядок на вибір.

Приклад:

> configure manager add MC.example.com 123456

Manager successfully configured.

Якщо центр керування знаходиться за пристроєм NAT, вводится унікальний ідентифікатор NAT разом із реєстраційним ключем та вказується DONTRESOLVE замість імені хоста, наприклад:

Приклад:

> configure manager add DONTRESOLVE regk3y78 natid90

Manager successfully configured.

Якщо захист від загроз знаходиться за пристроєм NAT, вводится унікальний ідентифікатор NAT разом з IP-адресою або ім'ям хоста центру керування, наприклад:

Приклад:

> configure manager add 10.70.45.5 regk3y78 natid56

Manager successfully configured.

5. Вхід до Центру управління. Використовується центр керування для налаштування та моніторингу захисту від загроз. У підтримуваному браузері вводится наступна URL-адреса: https:// fmc_ip_адреса.

Ввести ім'я користувача та пароль і зайти.

6. Отримання ліцензії для Центру керування. Усі ліцензії на захист від загроз надаються центром управління. Можна придбати такі ліцензії:

- Загроза - Security Intelligence та IPS наступного покоління.
- Шкідливе програмне забезпечення — захист від шкідливих програм.
- URL-адреса — фільтрація URL-адрес.
- RA VPN – тільки AnyConnect Plus, AnyConnect Apex або AnyConnect VPN.

Переконатися, що обліковий запис Smart Licensing містить доступні ліцензії (рис.3.6), які потрібні.

Рис.3.6. Пошук ліцензії

Потрібно зареєструвати центр керування на сервері Smart Licensing, якщо цього ще не зроблено. Для реєстрації необхідно створити реєстраційний токен у Smart Software Manager.

7. Реєстрація захисту від загроз у Центрі управління. Слід реєструвати вручну захист від загроз у центрі керування за допомогою IP-адреси або імені хоста пристрою. У центрі керування обирається Пристрої > Керування пристроями. Потім у списку «Додати» потрібно додати пристрій (рис.3.7).

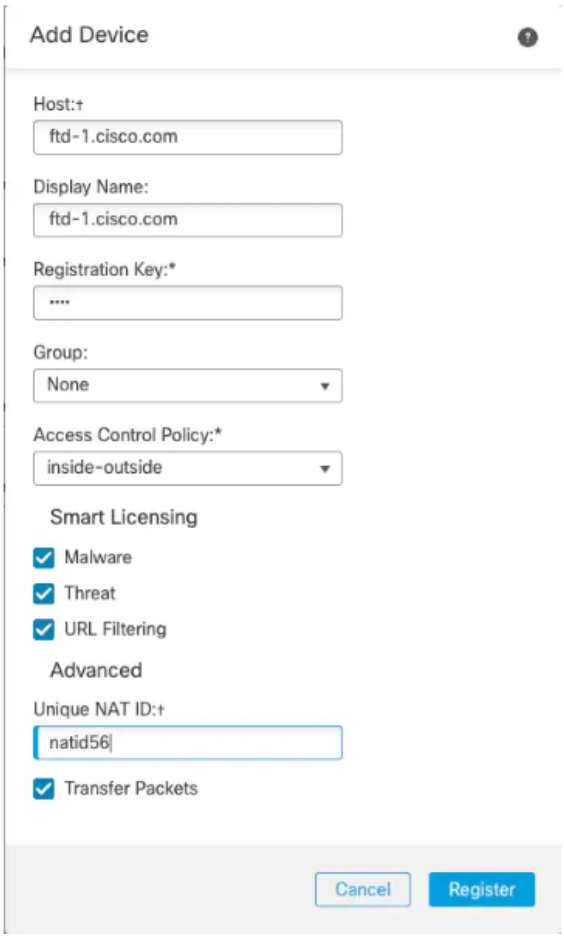

Рис.3.7. Додання пристрою

Встановити такі параметри:

•Хост — Ввести IP-адресу або ім'я хоста захисту від загроз, яку потрібно додати.

•Ім'я, що відобразится — ім'я захисту від загроз, яке має відображатися в центрі керування.

•Реєстраційний ключ —той самий реєстраційний ключ, який вказано у вихідній конфігурації захисту від загроз.

•Домен – призначити пристрій кінцевому домену, якщо багатодоменне середовище.

•Група — обрати групу пристроїв, якщо використовуються групи.

•Політика керування доступом —обрання вихідної політики. Якщо ще немає настроєної політики, яку потрібно використовувати, обирається «Створити нову політику» (рис.3.8) та «Блокувати весь трафік».

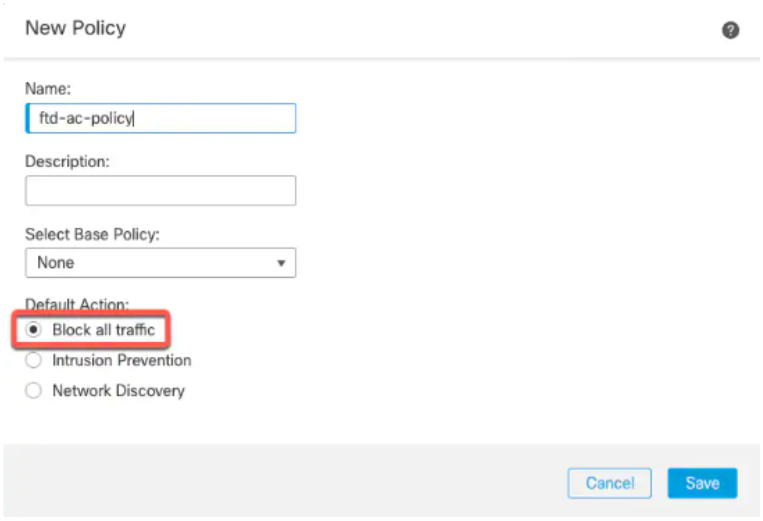

Рис.3.8. Нова політика

•Інтелектуальне ліцензування —необхідно для функцій, яку потрібно розгорнути: зловмисне програмне забезпечення, загроза та URL-адресу

•Унікальний ідентифікатор NAT —ідентифікатор NAT, який вказано у вихідній конфігурації захисту від загроз.

•Надсилання пакетів — дозволити пристрою передавати пакети до центру керування. Коли такі події, як IPS або Snort, ініціюються з увімкненою цією опцією,

пристрій відправляє інформацію про метадані події та пакетні дані до центру керування для перевірки. Якщо його вимкнути, центр керування надсилатиме лише інформацію про подію, але пакетні дані не надсилаються.

Далі реєстрація або, якщо є бажання додати інший пристрій, слід натиснути «Зареєструвати та додати інший» та підтвердити успішну реєстрацію.

Якщо реєстрація була успішною, пристрій додається до списку. У разі невдачі з’явится повідомлення про помилку. Якщо захист від загроз не реєструється, перевіряются такі пункти:

- Ping — доступ до інтерфейсу командного рядка захисту від загроз та перевірка зв'язку з IP-адресою центру керування за допомогою наступної команди:

ip_адреса системи ping

- Реєстраційний ключ, ідентифікатор NAT та IP-адреса центру керування.

8. Налаштування базової політики безпеки

Налаштування інтерфейсів. Щоб увімкнути інтерфейси захисту від загроз, слід призначити їх зонам безпеки та вказати IP-адреси. Як правило, необхідно налаштувати як мінімум два інтерфейси, щоб система пропускала значний трафік. Зазвичай це буде зовнішній інтерфейс, звернений до висхідного маршрутизатора або Інтернету, і один або кілька внутрішніх інтерфейсів для мереж організації (рис.3.9). Деякі з цих інтерфейсів можуть бути «демілітаризованими зонами» (DMZ), де розміщуються загальнодоступні активи, такі як веб-сервер.

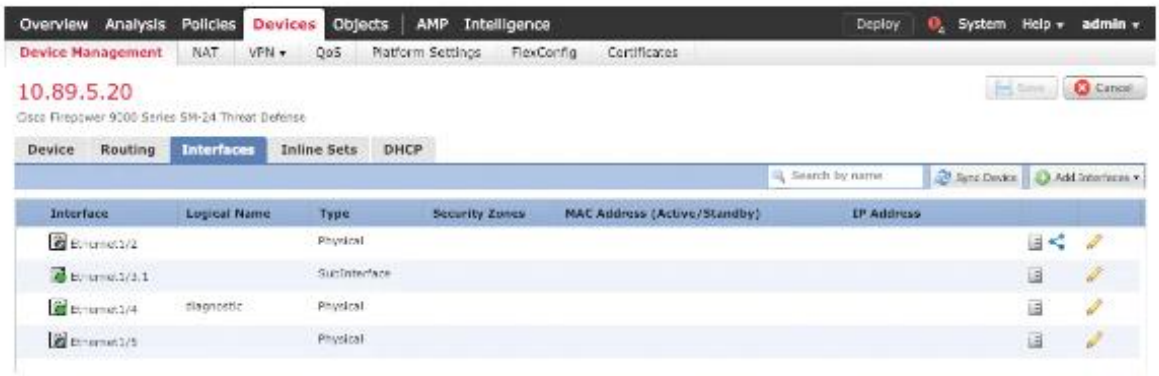

Рис.3.9. Вигляд вкладки інтерфейсів

У цьому прикладі налаштовується внутрішній інтерфейс режиму маршрутизації зі статичною адресою і зовнішній інтерфейс режиму маршрутизації з DHCP.

Обрати «Пристрої» > «Керування пристроями» та натиснути «Змінити» для брандмауера та нажати на вкладку «Інтерфейси».

Натиснути «Редагувати» для інтерфейсу, який потрібно використовувати всередині. З'явиться вкладка Загальні (рис.3.10).

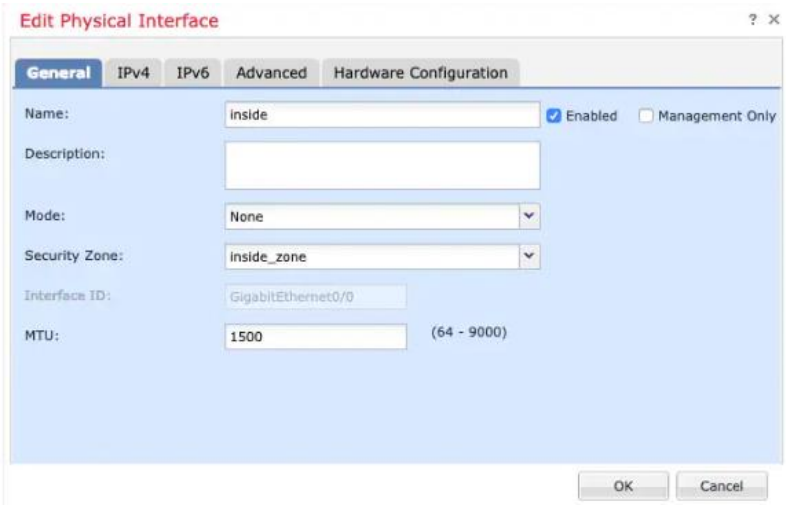

Рис.3.10. Вкладка Загальні

Додати зону з ім'ям inside_zone. Встановити прапорець «Увімкнено». «Mode» залишається встановленим на «None». У списку «Зона безпеки» обирається існуюча внутрішня зона безпеки або додається нова, натиснувши «Створити».

Встановити IPv4 (рис.3.11): для цього потрібно обрати «Використовувати статичну IP-адресу» у списку, що розкривається, і ввести IP-адресу та маску підмережі 192.168.1.1/24.

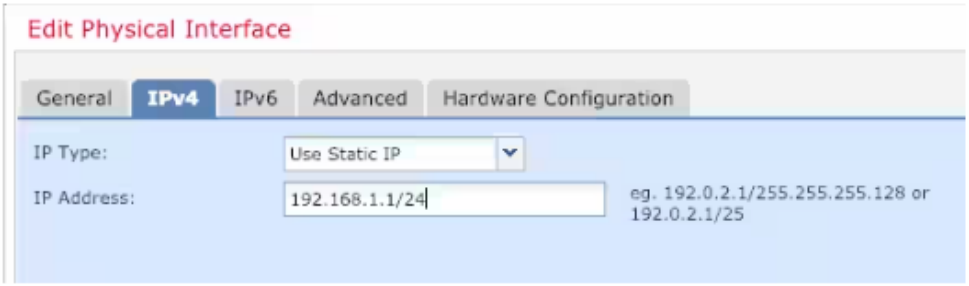

Рис.3.11. Налаштування IPv4

На IPv6 встановити прапорець «Autoconfiguration» для автоматичного налаштування без збереження стану та підтвердити. Слід відредагувати інтерфейс (рис.3.12), який потрібно використовувати зовні. З'явиться вкладка «Загальні».

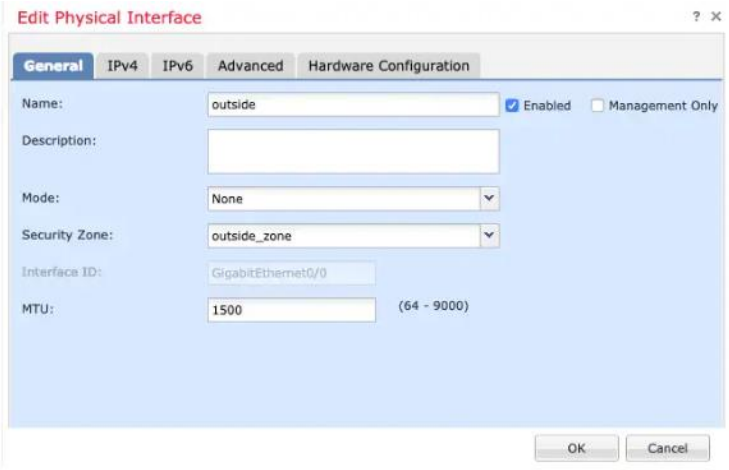

Рис.3.12. Редагування інтерфейсу

а. Ввести ім'я – outside. Встановити прапорець «Увімкнено». Залишити «Mode» встановленим на «None». У розкривному списку «Зона безпеки» додати зону з ім'ям outside_zone.

У вкладці IPv4 (рис.3.13) — обрати «Використовувати DHCP» та налаштувати такі необов'язкові параметри:

•Отримати стандартний маршрут за допомогою DHCP — повинен отримувати стандартний маршрут від DHCP-сервера.

•Метрика маршруту DHCP - призначає адміністративну відстань для вивченого маршруту в діапазоні від 1 до 255. Адміністративна відстань за замовчуванням для вивчених маршрутів дорівнює 1.

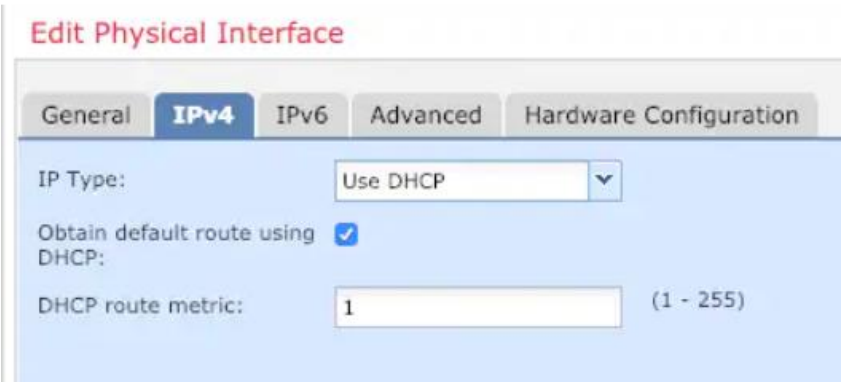

Рис.3.13. Налаштування IPv4

IPv6 — прапорець на «Autoconfiguration» для автоматичного налаштування без збереження стану. Зберігти.

Налаштування DHCP-серверу. Увімкнути DHCP-сервер, якщо потрібно, щоб клієнти використовували DHCP для отримання IP-адрес від захисту від загроз.

Обирається «Пристрої» > «Керування пристроями» та натискається «Змінити» для пристрою. Обирається DHCP > DHCP-сервер. Додається сервер (рис.3.14).

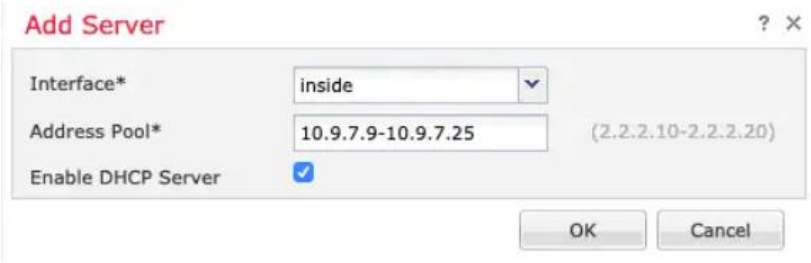

Рис.3.14. Додавання серверу

- Інтерфейс — обрати зі списку.
- Пул адрес — встановити діапазон IP-адрес від найнижчого до найвищого, які використовуються DHCP-сервером. Діапазон IP-адрес повинен знаходитися в тій же підмережі, що і вибраний інтерфейс, і не може включати IP-адресу самого інтерфейсу.
- Увімкнути DHCP-сервер — увімкнути DHCP-сервер на вибраному інтерфейсі. Зберігти.

Додати маршрут за замовчуванням

Маршрут за замовчуванням зазвичай вказує на вищестоящий маршрутизатор, доступний із зовнішнього інтерфейсу.

Обрати «Пристрої» > «Керування пристроями» та натиснути «Змінити» для пристрою.

Обрати «Маршрутизація» > «Статичний маршрут» , натиснути «Додати маршрут» (рис.3.15) та вказати такі параметри:

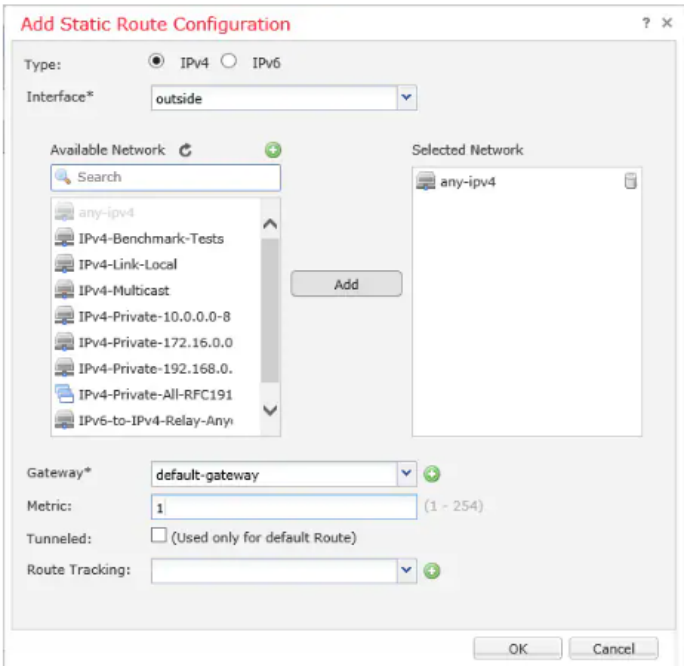

Рис.3.15. Додавання маршруту

- Тип — IPv4
- Інтерфейс — зовнішній.
- Доступна мережа — any-ipv4
- Метрика —за замовчуванням дорівнює 1.

Маршрут додається (рис.3.16) до статичної таблиці маршрутів.

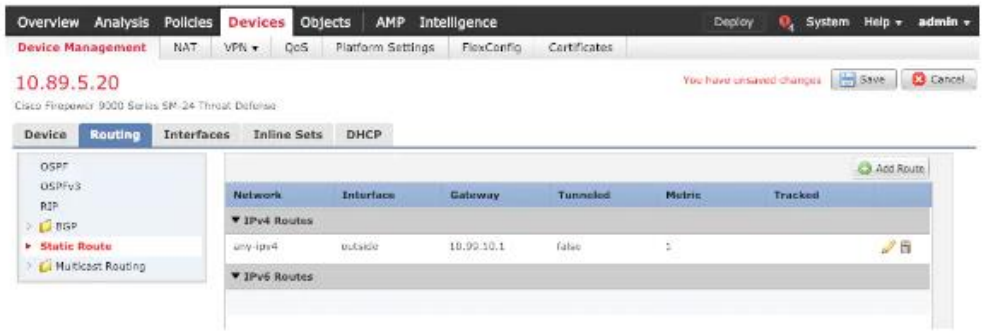

Рис.3.16. Доданий маршрут

Зберегти.

Налаштувати NAT. Типове правило NAT перетворює внутрішні адреси на порт на IP-адресі зовнішнього інтерфейсу. Цей тип правила NAT називається перетворенням адреси порту інтерфейсу (PAT).

Обрати «Пристрої» > «NAT» та натиснути «Нова політика» > «NAT захисту від загроз».

Дати назву політиці, обрати пристрої, для яких потрібно використовувати політику, і натиснути «Зберегти» (рис.3.17).

Рис.3.17. Нова політика

Політика додана до центру управління. Але все ще потрібно додати правила до політики. З'явиться діалогове вікно «Додати правило NAT» (рис.3.18). У ньому налаштувати основні параметри правила:

Рис.3.18. Правило NAT

- Правило NAT — Автоматичне правило NAT.
- Тип — «Динамічний».

На сторінці «Об'єкти інтерфейсу» додати зовнішню зону в області «Доступні об'єкти інтерфейсу» до області «Об'єкти інтерфейсу призначення» (рис.3.19).

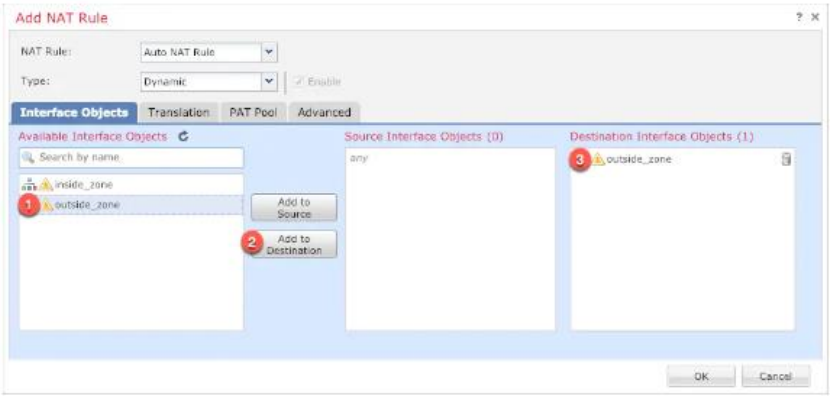

Рис.3.19. Додавання до області «Об'єкти інтерфейсу призначення»

На сторінці «Переклад налаштувати такі параметри» (рис.3.20):

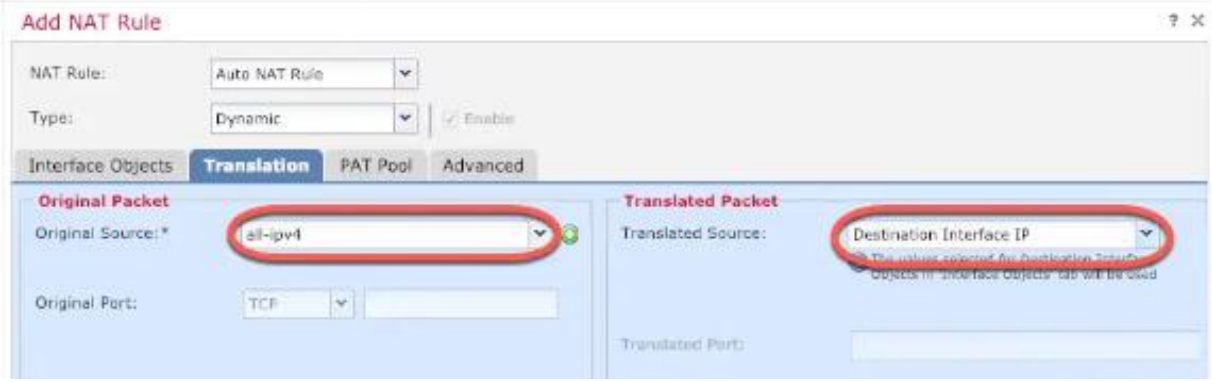

Рис.3.20. Налаштування вихідного і перекладеного джерел

- Вихідне джерело —додати об'єкт мережі для всього трафіку IPv4 (0.0.0.0/0).
- Перекладене джерело — обрати IP-адресу цільового інтерфейсу.

Натиснути «Зберегти», щоб додати правило.

Правило зберігається у таблиці «Rules» (рис.3.21).

Рис.3.21. Створене правило

Натиснути кнопку «Зберегти» на сторінці NAT , щоб зберегти зміни.

Дозволити трафік зсередини назовні. Якщо було створено базову політику контролю доступу «Блокувати весь трафік» під час реєстрації захисту від загроз, необхідно додати до політики правила, що дозволяють трафік через пристрій. Наступна процедура додає правило, що дозволяє трафік із внутрішньої зони у зовнішню зону.

Обрати «Політика» > «Політика доступу» > «Політика керування доступом» та натиснути «Змінити» для політики керування доступом, призначеної для захисту від загроз.

Натиснути «Додати правило» і вказати такі параметри (рис.3.22):

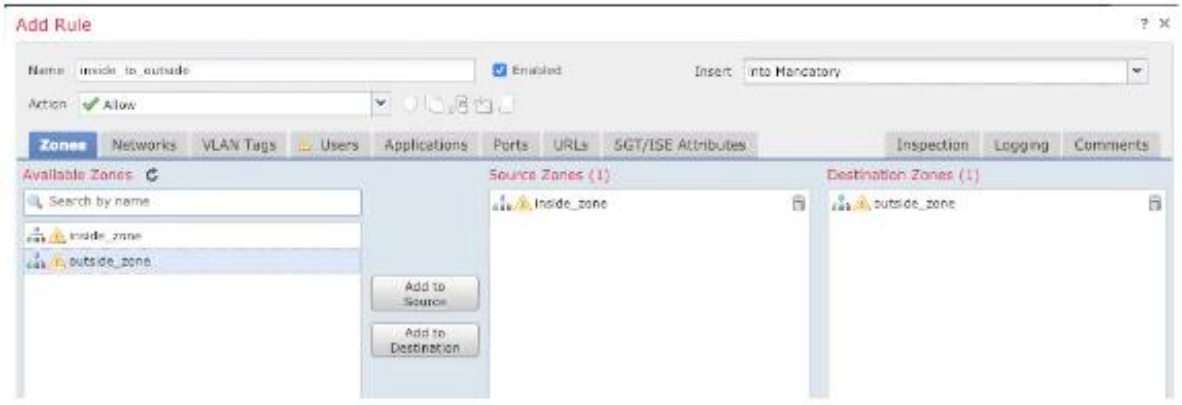

Рис.3.22. Налаштування трафіку з середини назовні

- Name —inside_to_outside.
- Вихідні зони — обрати внутрішню зону з доступних зон і натиснути «Додати до джерела».
- Зони призначення — обрати зовнішню зону з доступних зон та натиснути «Додати до місця призначення».

Інші налаштування залишити як є.

Натиснути «Додати».

Правило додається до таблиці «Rules» (рис.3.23).

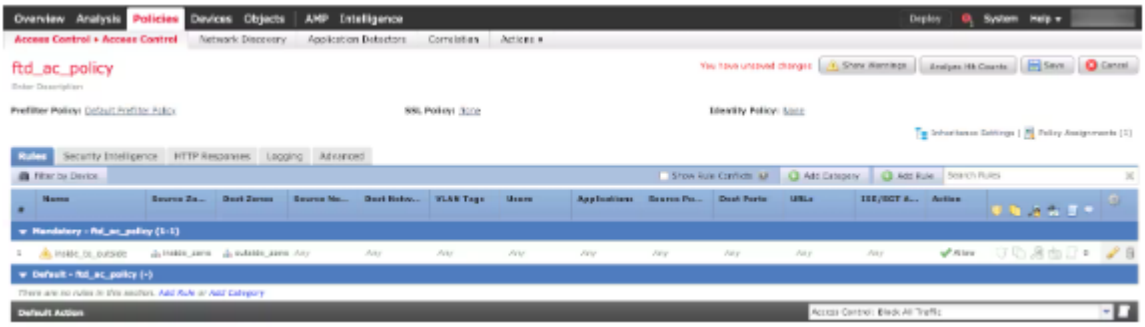

Рис.3.23. Додане правило

Натиснути «Зберегти».

Розгорнути конфігурацію

Розгорнути зміни захисту від загроз; жодна із змін не буде активною на пристрої, поки їх не розгорнути.

Натиснути «Розгорнути» у верхньому правому кутку (3.24).

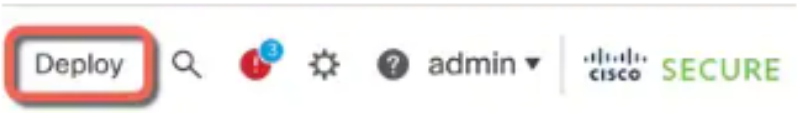

Рис.3.24. Розгортання

Або натиснути «Розгорнути все» (рис.3.25), щоб виконати розгортання на всіх пристроях, або натиснути «Розширене розгортання» (рис.3.26), щоб виконати розгортання на вибраних пристроях.

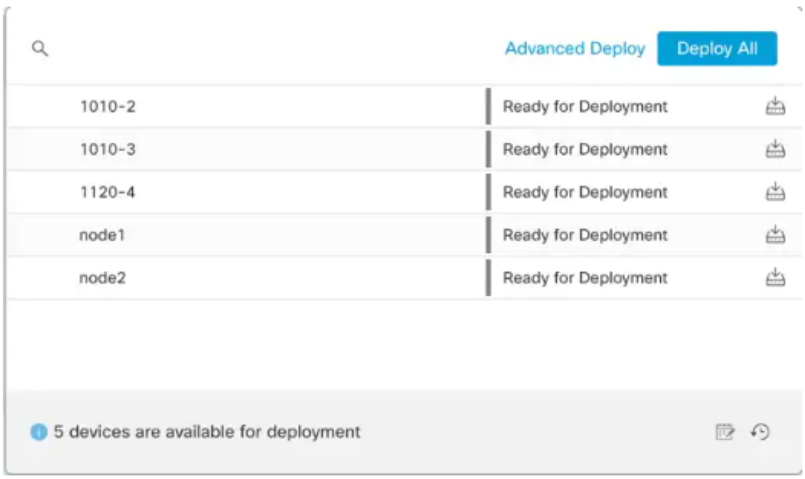

Рис.3.25. Розгорнути все

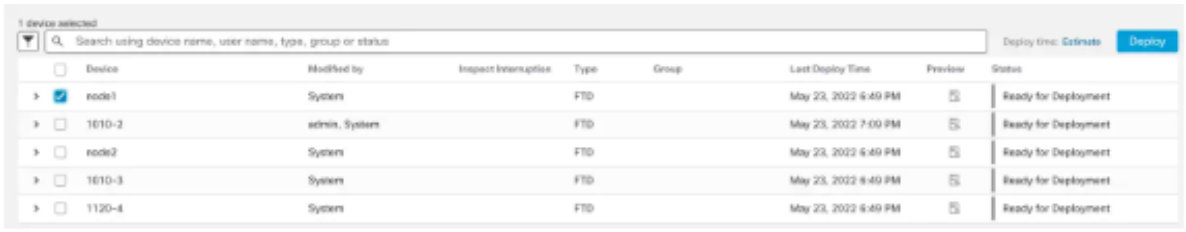

Рис.3.26. Розширене розгортання

Переконатися, що розгортання було успішне. Клацнути значок праворуч від кнопки «Розгорнути» у рядку меню, щоб переглянути стан розгортань (рис.3.27).

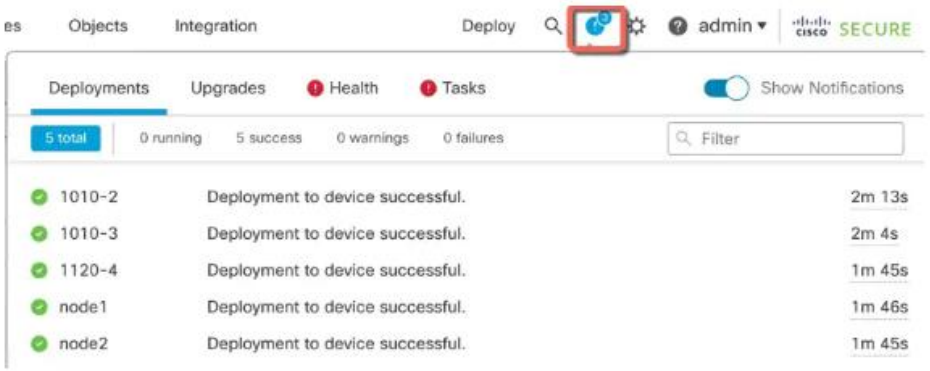

Рис.3.27. Статус розгортання

Доступ до інтерфейсу командного рядка Threat Defense. Використовувати інтерфейс командного рядка (CLI) для налаштування системи та усунення основних проблем системи. Не можна налаштовувати політики через CLI. Можна отримати доступ до CLI, підключившись до консольного порту.

Можна підключитися по SSH до інтерфейсу управління пристроєм захисту від загроз. Також можна підключитися до адреси на інтерфейсі даних, якщо відкрити інтерфейс SSH-з'єднань. Доступ SSH до стандартних інтерфейсів даних вимкнено.

Щоб увійти до інтерфейсу командного рядка, слід підключити керуючий комп'ютер до консольного порту, або порт RJ-45 або порт mini-USB. Обов'язково встановити всі необхідні драйвери послідовного USB-порту для операційної системи.

Увійти в інтерфейс командного рядка захисту від загроз, використовуючи ім'я користувача адміністратора та пароль, які було встановлено при початковому налаштуванні (за замовчуванням Admin123).

Вимкнути брандмауер. Важливо правильно завершити роботу системи. Просте вимкнення живлення може призвести до серйозного пошкодження файлової системи. Слід пам’ятати, що у фоновому режимі постійно працює безліч процесів, і відключення або відключення живлення не дозволяє коректно завершити роботу системи брандмауера. Шасі ISA 3000 не має зовнішнього вимикача живлення. Можна вимкнути пристрій за допомогою сторінки керування пристроєм у центрі керування або за допомогою інтерфейсу командного рядка.

Вимкнути брандмауер за допомогою Центру керування. Важливо правильно завершити роботу системи. Просте вимкнення живлення або натискання вимикача може призвести до серйозного пошкодження файлової системи. Слід пам’ятати, що у фоновому режимі постійно працює безліч процесів, і вимкнення або ввімкнення живлення не дозволяє коректно завершити роботу брандмауера. Можна коректно завершити роботу системи за допомогою центру керування:

Обрати «Пристрої» > «Керування пристроями» .

Поруч із пристроєм, який потрібно перезапустити, клацнути значок редагування.

Перейти на вкладку «Пристрій».

Клацнути піктограму вимкнення пристрою у розділі «Система».

Якщо з'явиться запит, підтвердити, що потрібно вимкнути пристрій.

Потрібно слідкувати за процесом вимкнення. Якщо немає змоги контролювати пристрій, зачекати приблизно 3 хвилини, щоб переконатися, що система вимкнулась.

- Консоль — якщо є консольне підключення до брандмауера, потрібно слідкувати за системними підказками під час вимкнення брандмауера. З’явиться наступне запрошення:

Firepower Threat Defense is stopped.

It is safe to power off now.

To restart the device, you must Power cycle to the device.

Тепер можна вимкнути живлення, щоб фізично відключити живлення від корпусу, якщо це необхідно.

Вимкнути брандмауер у CLI.

Підключитися до консольного порту, щоб отримати доступ до інтерфейсу командного рядка захисту від загроз, а потім відключити захист від загроз.

Приклад:

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd...                                          [  OK  ]
Clearing static routes
Unconfiguring default route                                     [  OK  ]
Unconfiguring address on br1                                    [  OK  ]
Unconfiguring IPv6                                              [  OK  ]
Downing interface                                               [  OK  ]
Stopping xinetd:
Stopping nscd...                                                [  OK  ]
Stopping system log daemon...                                   [  OK  ]
Stopping Threat Defense ...
Stopping system message bus: dbus.                              [  OK  ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted
filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped
/usr/sbin/acpid (pid 3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
```

```
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

To restart the device, you must Power cycle to the device.
```

Після того, як захист від загроз відключиться і на консолі з'явиться повідомлення «Зараз безпечно відключити живлення», можна вимкнути живлення, щоб фізично відключити живлення від корпусу, якщо це необхідно.

3.3 Рекомендації щодо забезпечення безпеки, вибору та налаштування брандмауера

Підприємства у виробничій, енергетичній, транспортній та інших галузях трансформують свою діяльність у вигляді цифровізації. Ця глибша інтеграція між IT, хмарними та промисловими мережами створює безліч проблем з безпекою, які тепер ставлять під загрозу цілісність, безперервність та безпеку виробництва.

У міру того, як промислові організації підключають більше пристроїв, розширюють можливості віддаленого доступу та створюють нові програми, підхід «повітряний зазор» для захисту промислових мереж від кіберзагроз стає недостатнім. Операційні технології (OT) мають особливі потреби у захисті від загроз, що потребують надійного рішення та ідеального розуміння промислових протоколів.

Пристрої промислової безпеки Cisco Secure Firewall ISA3000 задовольняють ці потреби завдяки перевіреному корпоративному брандмауеру, захисту від вторгнень і політикам мережевої безпеки нового покоління програмного забезпечення брандмауера Cisco. Розроблені спеціально для розгортання в

найсуворіших промислових середовищах, ці промислові брандмауери є основою для безпечної промислової роботи та дотримання нормативних вимог.

Переваги [26]:

• Зменшення ризику за допомогою обізнаності про програми: контролювання трафіку промислової мережі, щоб забезпечити безвідмовну роботу та цілісність. ISA3000 розуміє пропрієтарні та стандартні протоколи OT.

• Захист комп'ютерів OT від шкідливих програм: блокує зловмисний трафік, поки не пізно. ISA3000 використовує аналіз загроз Talos для постійного аналізу файлів і виявлення прихованих загроз.

• Розширення IT-безпеки на OT: застосування узгоджених політик безпеки в OT та IT. ISA3000 є частиною сімейства Cisco Firepower і використовує ті самі інструменти керування.

• Спрощення відповідності і зменшення обсягу аудиту: створення безпечної промислової мережі, яка відповідає нормативним вимогам. ISA3000 допоможе відповідати стандартам NERC-CIP, ISA99, IEC 62443, CFATS, ANSI/AWWA G430 та іншим.

Ключові риси:

- Міцний промисловий дизайн. Створено для екстремальних температур, вібрацій, ударів, стрибків напруги та електричних перешкод. Сертифіковано для розгортання в найбільш вимогливих галузях.
- Надійна і довговічна робота. Без вентилятора, з конвекційним охолодженням, без рухомих частин. Подвійні входи живлення, апаратний обхід і дизайн високої доступності.
- Видимість і контроль трафіку OT/IT. Провідні можливості брандмауера Cisco плюс широка підтримка промислових протоколів для контролю комунікацій промислових процесів.
- Розширене виявлення загроз. Використовує провідні в галузі правила, розроблені Cisco Talos, включаючи тисячі промислових правил і правил для захисту від використання вразливостей.

- Конвергентний робочий процес безпеки IT/OT. Повна інтеграція з портфоліо безпеки Cisco, включаючи Cyber Vision, Identity Services Engine (ISE), Stealthwatch і SecureX, що забезпечує скоординований захист.
- Простий у використанні та управлінні. На пристрої або централізоване керування для швидкого надання кількох пристроїв, розгортання узгоджених політик безпеки в OT та IT і моніторингу статусу загроз, надаючи актуальні звіти.

Випадки використання:

- Створення промислової DMZ. Захист невеликих розподілених промислових об’єктів. ISA3000 є ідеальним міжмережевим екраном DMZ для підключення комунальних підстанцій, трубопровідних мереж, блоків дистанційного керування або вуличних шаф. Він фільтрує трафік, що проходить через WAN, і керує VPN-з’єднаннями, щоб забезпечити безперебійну та безпечну розподілену роботу.
- Безпечне виробництво з сегментацією мережі. Запобігання будь-яким загрозам або зловмисникам від безперешкодного переміщення через мережу. ISA3000 розділяє різні частини мережі у виробничих клітинах, зонах або підстанціях, щоб стримувати атаки та захищати критично важливі для бізнесу процеси.
- Захист вразливих активів від зловмисних дій. Блокування загроз та експлойтів для вразливого контрольного обладнання та заощадження часу простою. ISA3000 використовує аналіз загроз від Cisco Talos для виявлення зловмисної діяльності або шкідливого трафіку та захисту промислових активів, які неможливо виправити.
- Підключити машини з дублікатами IP-адрес. Увімкнути зв’язок між різними машинами та осередками без зміни IP-адрес. ISA3000 перетворює IP-адреси та захищає зв’язок, тож не потрібно змінювати повторювані адреси та легко підключати попередньо зібрані системи.

Брандмауери забезпечують покращену та розширену форму безпеки. Ось кілька корисних порад щодо ефективного управління брандмауерами [25]:

1. Потрібно тримати брандмауер завжди увімкненим. Першим очевидним кроком є постійне увімкнення захисту брандмауером. Якщо виконується якась конкретна робота, наприклад, встановлюється програмне забезпечення або усуваються неполадки, можна тимчасово відключити брандмауер, але ця практика не завжди рекомендується, оскільки вона може призвести до катастрофічних наслідків у разі використання шкідливого програмного забезпечення.

2. Програмне/апаратне забезпечення брандмауера має бути ізольовано. Необхідно захищати брандмауер від прямих атак, особливо прямих атак, коли брандмауер є апаратним пристроєм. Це означає, що не потрібно дозволяти обмін даними між брандмауером і неавторизованими джерелами.

3. Оновлення ОС. Оновлення до останньої версії програмного забезпечення для брандмауера є обов'язковим.

4. Чітке визначення «основи правил». Коли пакет досягає брандмауера, він перевіряє його на відповідність базі правил. Таким чином, найкраще помістити найчастіше використовуване правило вгорі, щоб брандмауеру не доводилося зіставляти всі правила в базі правил. Це, у свою чергу, зменшить навантаження на нього.

5. Відхилення підозрілих запитів на обхід брандмауера. Заперечувати, заперечувати та заперечувати. Це правило, яке слід дотримуватися, коли є сумніви у справжності запиту. Завжди можна дозволити заблоковане з'єднання пізніше, коли це необхідно або після автентифікації.

6. Блокування доступу до VPN

7. Регулярне сканування вразливостей брандмауера. Впровадження практики тестування та аудиту брандмауера на наявність уразливостей. Це допоможе оновлювати захист брандмауера за необхідності.

8. Заблокувати і всю країну, якщо відбувається атака. Легке блокування всіх атак з певної країни, наприклад, з Китаю.

9. Регулярне оновлення брандмауера. Необхідно оновлювати програмне забезпечення брандмауера, щоб бути впевненим, що не залишилось жодних лазівок, які можуть поставити під загрозу безпеку. Застаріле програмне

забезпечення для забезпечення безпеки практично марне, оскільки атаки на систему безпеки відбуваються щодня.

10. Спостереження за доступом користувачів до налаштувань брандмауера. У корпоративних мережах спільні брандмауери зазвичай використовуються для забезпечення першої лінії захисту мережі, але власник мережі повинен контролювати, хто має доступ до налаштувань брандмауера і який тип доступу, оскільки не хочеться, щоб хтось змінив конфігурацію. навмисно чи ненавмисно зробити їх уразливими.

Нижче наведено найважливіші фактори, які слід враховувати при наголошенні на важливості брандмауерів.

Відстежує мережевий трафік: Для забезпечення безпеки систем захист брандмауера починається з ефективного моніторингу мережного трафіку на основі попередньо встановлених правил та фільтрів. Наступні способи безпеки використовуються для моніторингу мережного трафіку. Джерело або призначення вхідного мережного трафіку заборонено. Це найбільш поширена функція більшості брандмауерів, і вона включає перевірку джерела трафіку. Багато брандмауерів також можуть фільтрувати дані між внутрішньою мережею та Інтернетом залежно від джерела або пункту призначення вхідного мережного трафіку. Наприклад, можна заборонити співробітникам переглядати невідповідні веб-сайти. Більш сучасні брандмауери можуть сканувати мережевий трафік на наявність небажаного контенту та зупиняти трафік на основі цього. Наприклад, брандмауер у поєднанні зі сканером вірусів може захистити мережу від заражених вірусами даних. Інші брандмауери функціонують разом із службами електронної пошти, щоб блокувати небажані повідомлення. При фільтрації мережного трафіку в Інтернеті та з Інтернету також важливо розуміти, що робить брандмауер, хто намагався проникнути у мережу та хто намагався отримати доступ до забороненого контенту в Інтернеті. Майже всі брандмауери мають ту чи іншу функцію створення звітів.

Зупиняє атаки вірусів та шпигунських програм: щодня створюються сотні тисяч нових кіберзагроз, включаючи шкідливі програми, віруси та інші атаки, такі як електронні бомби, відмова в обслуговуванні та шкідливі макроси, тому дуже

важливо захищати комп'ютери. У міру того, як системи стають більш складними та потужними, кількість точок входу, які злодії можуть використовувати для отримання доступу до них, збільшується. Один з найбільш поширених способів отримання доступу небажаними людьми - це шпигунське та шкідливе ПЗ, призначене для злому мереж, керування пристроями та крадіжки даних. Брандмауери мають вирішальне значення у боротьбі зі шкідливим програмним забезпеченням.

Захищає систему від злому: кіберзагрози швидко змінюються та широко поширюються. Брандмауери утримують хакерів від доступу до даних, електронної пошти, систем та іншої важливої інформації. Брандмауер може повністю перешкодити хакеру отримати доступ, або змусити його вибрати більш вразливу мету.

Сприяє конфіденційності: наявність брандмауера захищає дані та створює безпечну атмосферу конфіденційності, у той час як система без нього допускає будь-яке підключення до мережі від будь-кого. Без брандмауера неможливо було б ідентифікувати загрози, що входять. Як наслідок, злочинці можуть отримати доступ до пристроїв, поставивши під загрозу конфіденційність. Щоб захистити мережу та особисту інформацію, що зберігається на комп'ютері, від кіберзлочинів, дуже важливо використовувати сучасні заходи безпеки.

Висновки до третього розділу

Приведено основні апаратні характеристики та графічно зображено усі деталі технології Cisco Secure Firewall ISA3000.

Наведено покроковий опис підключення апаратної частини та показано практично налаштування політики безпеки брандмауера із розгортанням Firepower Threat Defense.

Надано рекомендації щодо забезпечення безпеки, вибору та налаштування брандмауера. Приведено поради щодо ефективного управління брандмауерами.

ВИСНОВКИ

В магістерській роботі отримано наступні наукові на науково-практичні результати:

1. Досліджено поняття мережі промислових IoT та проілюстровано підмножину комунікаційних технологій і протоколів IoT та IIoT. Розглянуто загальні протоколи та архітектура IIoT, такі як: Message Queuing Telemetry Transport, протокол обмеженого застосування та SCADA (мережа керування, інфраструктура зв'язку, мережа процесу).

2. Зазначено проблеми безпеки та специфічні вразливолсі: комунікаційна інфраструктура, сервер додатків, сервер бази даних, людино-машинний інтерфейс, програмний логічний контролер та віддалений термінальний пристрій. Представлено підмножину варіантів використання IoT та IIoT і проведено їх порівняльний аналіз із наведеною таблицею відмінностей.

3. Доведено, що аналіз загроз системи особливо важливий, оскільки причиною багатьох вразливостей є потоки архітектурного проектування. Виправлення цих вразливостей на ранніх етапах зменшить витрати в процесі та зменшить вектор атаки. Обґрунтовано методології аналізу безпеки та категорії аналізу загроз STRIDE, які для зручності описано у таблицях.

4. Розглянуто важливість брандмауерів для промислових мереж та описано їхні основні цілі. Проаналізовано недоліки традиційних фаєрволів, основні переваги та переваги мережевих брандмауерів.

5. Наведено апаратні характеристики технології Cisco Secure Firewall ISA3000. Дана технологія вважається надійним промисловим пристроєм безпеки, встановленому на DIN-рейці, який забезпечує брандмауер, захист від загроз і послуги VPN.

6. Обґрунтовано, що зазначені рекомендації щодо забезпечення безпеки мереж IIoT із використанням технології Cisco Secure Firewall ISA3000 можуть бути використані у сфері забезпечення інформаційної безпеки промислових мереж.