ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ FORTINAC»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Пацьора Е.С.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IT – інформаційні технології

API – Application Programming Interface

BYOD – Bring Your Own Device

DHCP – Dynamic Host Configuration Protocol

CLI – Common Language Infrastructure

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

MAC – Media Access Control

NAC – Network Access Control

NBAD – Network Behavior Anomaly Detection

NOC – Network Operations Center

RADIUS – Remote Authentication in Dial-In User Service

SCADA – Supervisory Control and Data Acquisition

SIEM – Security Information and Event Management

SOC – Security Operation Center

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

ВСТУП

Актуальність дослідження. Для забезпечення безпеки функціювання інформаційної системи організації необхідно управляти активами та їх користувачами. Метою управління доступом до мережі є унеможливлення несанкціонованого доступу зловмисників та виникнення шкідливих процесів. Реалізація технології управління доступом забезпечують видимість мережевого середовища, динамічний контроль і автоматизовані реакції на загрози.

Сплеск розгортання пристроїв IoT вимагає розширеної безпеки мережі. IoT є засобом більшої цифрової трансформації, що містить в собі величезну кількість даних для зберігання, аналізу та передачі через глобальну мережу. Фахівці з кібербезпеки повинні мати можливість ідентифікувати кожного користувача та пристрій, що підключається до корпоративної мережі, а потім відповідним чином надавати або обмежувати доступ. Крім того, мережа потребує постійного спостереження, щоб забезпечити безперервну роботу з автоматичним реагуванням на загрози в міру їх виявлення.

Управління доступом є одним із важливих аспектів для забезпечення захисту інформації. Він допомагає організаціям не відставати від постійно зростаючої поверхні атак, а також використовується в галузі для опису набору функцій, мережевих протоколів, ідентифікації та перевірки пристроїв користувачів, автентифікації користувачів, а також застосування політик, які визначають, до яких мережевих ресурсів дозволено доступ користувачам.

Об'єкт дослідження – управління доступом до мережі організації.

Предмет дослідження – технологія управління доступом до мережі організації.

Мета роботи – розробити варіант технології управління доступом до мережі та рекомендації щодо застосування управління доступом до мережі організації.

Наукові завдання:

дослідити сутність проблеми захисту IoT в мережі організації;

проаналізувати загрози IoT в мережі організації;

оглянути існуючі технології управління доступом до мережі організації;

проаналізувати методи та засоби забезпечення управління доступом до мережі організації;

проаналізувати основні функції та принципи реалізації управління доступом до мережі організації;

дослідити можливості застосування програмного комплексу FortiNAC.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління доступом до мережі організації.

Практичне значення одержаних результатів полягає в розробці варіанта технології управління доступом до мережі організації на базі FortiNAC, а також рекомендації щодо застосування управління доступом до мережі організації.

Апробація результатів магістерської роботи було оприлюднено на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1. Призначення та функції IoT в мережі організації

Швидке зростання кількості пристроїв IoT і корпоративної ініціативи із використанням власного пристрою (BYOD) призвели до поширення точок доступу у мережі. З появою бездротових сенсорних мереж, вбудованих систем, датчиків, приводів та хмарних сервісів – IoT став дуже популярним. Це започаткувало еру, коли розумні об’єкти спілкуються з іншими розумними об’єктами.

Розумні пристрої збирають масу конфіденційних даних, у тому числі ідентифікаційну інформацію. Вони здатні відчувати навколишнє середовище, передавати й обробляти отримані дані, а після давати відповідь. У результаті кіберзагрози стають все більш плідними, а тактика і методи зловмисників розвиваються.

Сучасним підприємствам потрібні економічно ефективні, гнучкі та безпечні рішення для зв’язку. Збої в безпеці мережі можуть мати дорогий вплив на прибутковість компаній. Безпека мереж стала серйозною проблемою для компаній через розповсюдження вірусів та інших загроз у мережі, що поширюються через заражені або неавторизовані системи. Шкідливе програмне забезпечення може розповсюджуватися через брандмауери та системи виявлення вторгнень (IDS).

Захист контрольної площини пристроїв маршрутизації також став критично важливим для належної роботи пристроїв і мережі в цілому. Якщо площина управління мережі скомпрометована, практично неможливо гарантувати правильний робочий стан. Скомпрометована площина управління може призвести до ненавмисної маршрутизації та збою служби [1].

У сучасних цифрових підприємств бізнес-додатки розосереджені далеко від корпоративних центрів обробки даних, тому користувачі тепер мають більший доступ до корпоративних ресурсів за допомогою великої кількості кінцевих точок

з багатьох місць.

Internet of things (IoT) – інфраструктура взаємопов'язаних об'єктів, людей, систем та інформаційних ресурсів разом із сервісами, які обробляють та реагують на інформацію, що надходить як з фізичного, так і з віртуального світу [2].

IoT вже вніс значні зміни в наше повсякденне життя, очікується, що корпоративні, соціальні, технологічні та індивідуальні переваги тільки збільшяться з поширенням програм і послуг IoT. Згідно з останніми звітами, у 2021 році майже 25 мільярдів пристроїв було підключено до мережі зі швидкістю 9127 нових пристроїв щосекунди [3]. Ці пристрої генерують величезні обсяги даних, що створює нові проблеми в управлінні та використанні даних. Кількість глобальних підключень IoT зросла на 8% у 2021 році до 12,2 мільярда активних кінцевих точок.

На рис. 1.1 зображено кількість глобальних активних підключень IoT та тип підключення в мережах.

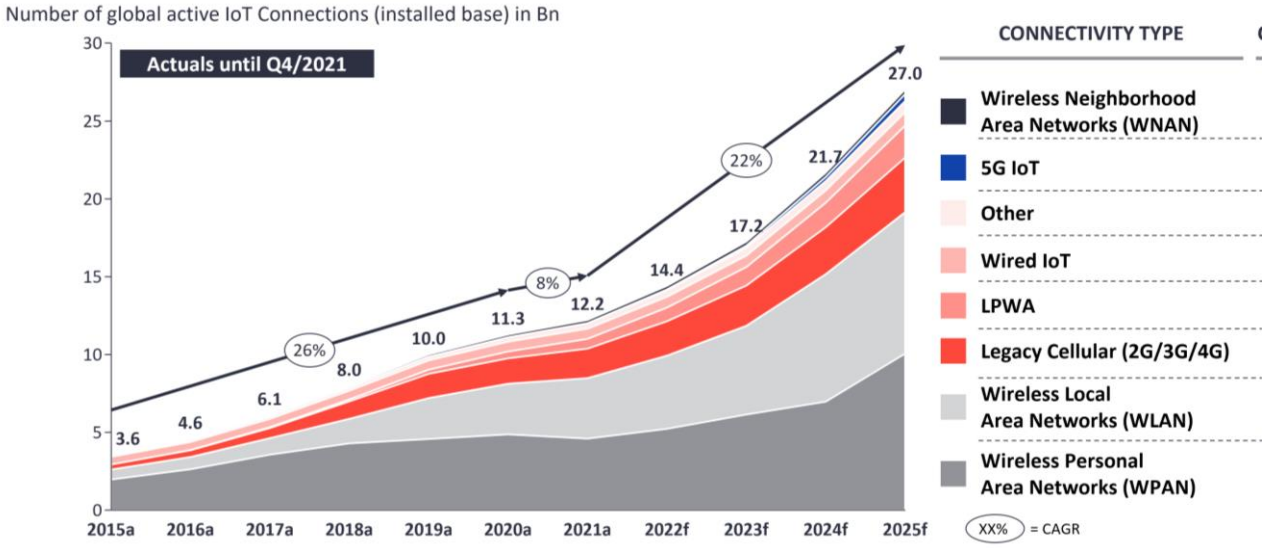


Рис. 1.1. Глобальні активні підключення IoT [4]

Реалізації IoT зазвичай базуються на технологіях датчиків і бездротового зв’язку, такі як радіочастотна ідентифікація, бездротові сенсорні мережі, Wi-Fi, бездротові сусідські мережі, 3G, 4G, 5G, стандарти зв’язку IEEE 802.15.x, LPWA, бездротова локальна мережа, бездротова мережа тіла та інші.

Комунікаційні протоколи для IoT базуються на низькому енергоспоживанні

пристроїв. Ці протоколи допомагають об’єктам автоматично ідентифікувати інші об’єкти, з якими вони спілкуються. З розвитком IPV6 стало зручно призначати унікальні цифрові ідентифікатори й доступ до різноманітної цифрової інформації та послуг.

Небезпечні IoT можуть вплинути на безпеку та конфіденційність способами, відмінними від більш традиційних інформаційних систем. Отже, для зниження неприйнятних ризиків потрібні відповідні заходи безпеки.

IoT можна розглядати як окремі електронні пристрої, так і як компоненти більших, складніших «екосистем», які потенційно включають [5]:

операційні системи та програми;

інфраструктуру мережі (персональні, локальні та глобальні мережі);

фізичний світ, з яким вони взаємодіють через датчики та приводи;

людей, які визначають, набувають, налаштовують, використовують та керують ними;

організації, які проектують та виробляють, використовують/експлуатують та керують ними.

Безпека IoT – це набір підходів і методів захисту фізичних пристроїв, мереж, процесів і технологій, які складають середовище IoT, від широкого спектру атак [6].

Двома ключовими цілями безпеки IoT є:

переконатися, що всі дані збираються, зберігаються, обробляються та безпечно передаються;

виявляти та усувати вразливості в компонентах IoT.

Мережевий периметр майже зник, оскільки поширення пристроїв, що підключаються до мережі, створило експоненціально більшу поверхню атаки. Оскільки кожен периметр пов’язаний з окремим пристроєм, кінцеві точки стали основною мішенню для зараження зловмисним програмним забезпеченням і складних експлойтів [7]. Організаціям необхідно знати, які пристрої знаходяться в мережі, для того, щоб не втратити видимість і контроль.

Пристрої організації включають:

мережеве офісне обладнання;

системи роздрібної торгівлі;

операційні технології;

датчики та пристрої IoT.

Проблема в управлінні всіма цими пристроями полягає в їх широкому розгортанні, різних рівнях керування пристроями, непослідовних елементах керування конфігурацією та відсутності підтримки стандартних протоколів зв'язку в багатьох застарілих пристроях.

На рис. 1.2 показана традиційна плоска мережева архітектура. Вона називається плоскою мережею, оскільки між пристроями немає брандмауера чи логічного розділення, тому вони можуть спілкуватися безпосередньо з усіма іншими пристроями в мережі.

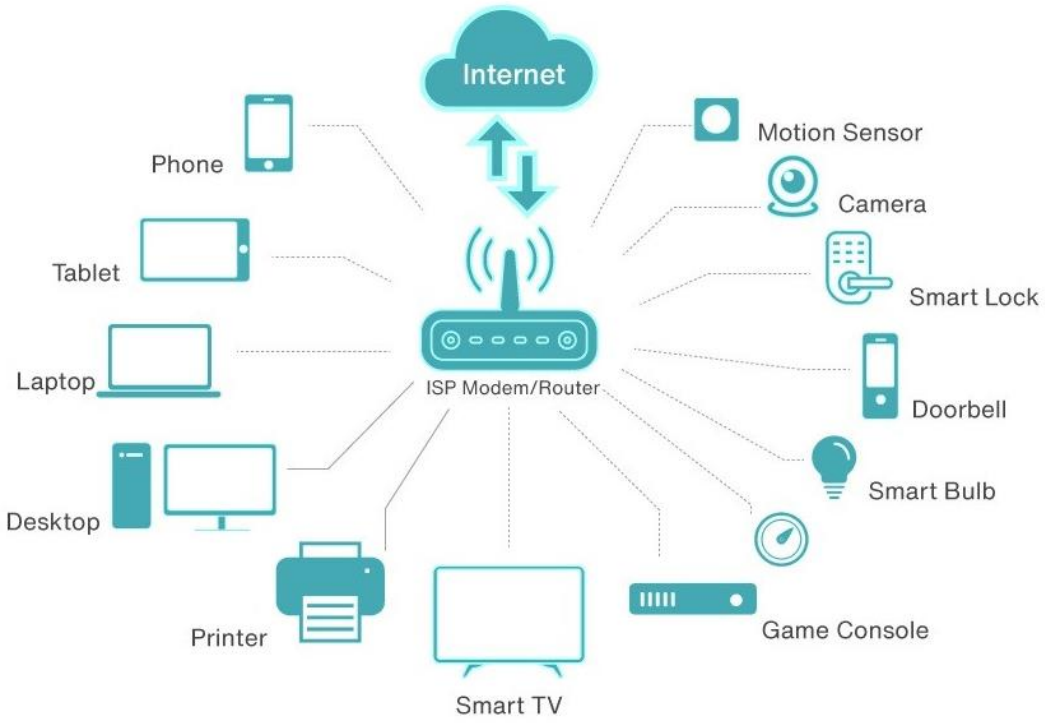


Рис. 1.2. Традиційна плоска мережева архітектура IoT [8]

Сьогодні мережева безпека є ще складнішим викликом, оскільки смарт-телевізори, смарт-лампочки, смарт-холодильники та широкий спектр інших пристроїв IoT підключаються до мереж малого бізнесу в масштабах, що іноді призводить до буквально сотень пристроїв у мережі. Всі ці нові пристрої мають

мережевий інтерфейс, накопичувач, пам'ять, процесори та операційну систему. Іншими словами, це комп'ютери, і вони так само вразливі для атак, як будь-який інший комп'ютер або смартфон.

Деякі організації використовують традиційну сегментацію мережі, але важко визначити безпечні мережеві сегменти, які можуть бути одночасно доступними для всіх авторизованих користувачів та програм і повністю недоступними для всіх інших. Сегментація на основі політик забезпечує більш динамічну та детальну стратегію сегментації мережі, яка може автоматично адаптуватися для забезпечення мінімальних привілеїв у мережі з нульовою довірою.

Традиційні моделі безпеки працюють за припущенням, що будь-чому в мережі організації слід довіряти. Але автоматичне розширення довіри пристрою чи користувачу ставить під загрозу організацію – якийсь з них може буде зламаний, навмисно чи ненавмисно.

Зловмисники, шкідливе програмне забезпечення та скомпрометовані пристрої, які обходять крайові контрольні точки безпеки, часто мають необмежений доступ до мережі через модель довіри. Опинившись усередині мережі, вони можуть використовувати переваги довіреної внутрішньої мережі для націлювання на ресурси організації. Тому IoT пристрої потрібно захищати різними законами, стандартами та правилами кібербезпеки.

1.2. Аналіз загроз IoT в мережі організації

Пристрої IoT розгортаються в мережах із феноменальною швидкістю, до 1 мільйона пристроїв щодня. Незважаючи на те, що ці пристрої створюють нові та захоплюючі способи підвищення ефективності, гнучкості та продуктивності, вони також створюють новий ризик для мережі.

Технологія IoT повністю працює в інтернеті, а отже, вона більш уразлива до атак зловмисного програмного забезпечення, оскільки вона завжди онлайн і не має захисту. Уся конфіденційна інформація зберігається в онлайн-хмарі і хакери можуть легко отримати доступ до цієї інформації. Необхідно знати, які шкідливі

програми атакують пристрої, щоб за допомогою алгоритму виявлення можна було легко знайти зловмисне програмне забезпечення на пристрої.

Є кілька багаторівневих архітектур IoT, враховуючи необхідність з'єднання багатьох різнорідних пристроїв між собою, а також з іншими цифровими платформами через більші мережі.

Різні рівні допомагають розділити більшу проблему IoT на підпроблеми, де кожну підпроблему можна віднести до іншого рівня. Кожен рівень має певні функції, надає різні технології та має визначені інтерфейси для забезпечення сумісності. Архітектура може пропонувати різні послуги на кожному рівні залежно від організаційних потреб і технічних вимог [9].

Архітектура IoT відрізняються від трьох до семи рівнів. 7-рівнева архітектура є дуже простою та включає потік даних і керування від периферійних пристроїв, що складаються з датчиків, виконавчих механізмів, машин, інтелектуальних кінцевих вузлів та інших пристроїв, до центру аналітики даних або хмарної служби.

Натомість трирівнева архітектура International Electrotechnical Commission [10] є спрощеною моделлю, яка зображена на рис. 1.3.

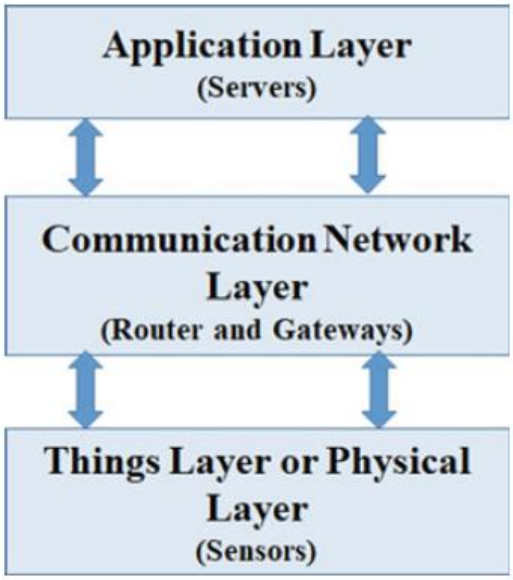


Рис. 1.3. Трирівнева архітектура IoT [9]

Ці три рівні включають прикладний рівень (сервера), рівень зв'язку (маршрутизатор і мережевий шлюз) та рівень речей або фізичний рівень (датчики).

І ці рівні складаються з величезної кількості технологій, які враховують неоднорідність пристроїв IoT і різні методи, які доступні для їх підключення до мережі.

Рівень речей або фізичний рівень

Перший рівень використовується для визначення фізичних параметрів середовища, рівень розгортає датчики для сприйняття та збору даних. Цей рівень також розпізнає інші розумні об’єкти в навколишньому середовищі.

Виробничі одиниці можуть мати об’єкти з різними характеристиками, які відповідають різним вимогам, що потребує різноманітних протоколів і архітектури IoT. Оскільки цей рівень дозволяє фізичним речам сприймати, аналізувати, обмінюватися даними та виконувати деякі бажані дії, цей рівень полегшує роботу кількох додатків, таких як розумний дім, розумне місто, розумне здоров'я чи розумна логістика.

Рівень зв’язку

Основною відповідальністю другого рівня є підключення до інших розумних об’єктів, мережевих пристроїв, периферійних пристроїв і серверів. Він також відповідає за надійну передачу та подальшу обробку даних датчиків. Після того, як тип об’єктів, які потрібно з’єднати, визначено, залежно від різних факторів, наступним кроком є з’єднання цих об’єктів, щоб вони могли спілкуватися.

Прикладний рівень

Робота третього рівня полягає в тому, щоб надавати користувачам специфічні програмні послуги. Він піклується про різні додатки, в яких можна ефективно розгортати IoT. Цей рівень систем IoT сильно відрізняється від прикладного рівня інформаційних систем. Це пов’язано з тим, що IoT включає не лише аналітику даних, зібраних із першого рівня, але й забезпечує специфічні для галузі процеси контролю. Рівень аналітичних програм збирає дані з багатьох речей і розумних об’єктів, обробляє дані, аналізує їх, а потім відображає результат.

Натомість прикладний рівень контролює параметри інтелектуальних об’єктів. Прикладом є системи диспетчерське управління і збір даних (SCADA), яке використовуються виробничими підрозділами для керування та моніторингу

промислових процесів локально або віддалено шляхом збору й обробки даних у реальному часі.

Незважаючи на те, що IoT має багато переваг, він також має багато проблем, таких як енергоефективність, інтероперабельність, безпека та конфіденційність даних. Взаємодія між розумними об’єктами стає важливою проблемою, оскільки ці об’єкти працюють у різних промислових і виробничих умовах, мають різні архітектури та розгортають різні протоколи.

Велика кількість датчиків та інтелектуальних об'єктів, які обмінюються даними один з одним через не дуже безпечну та не зашифровану мережу, призвів до виникнення вразливостей у системі безпеки з пристроями IoT, які показані на рис. 1.4.

Рис. 1.4. Загрози пристроїв IoT [9]

Ботнет – це сукупність різних систем, які разом дистанційно контролюють цільову систему та поширюють шкідливе програмне забезпечення. IoT та інші пристрої, що підключені через Інтернет, заражаються шкідливим програмним забезпеченням, дозволяючи хакерам легко контролювати їхні операції. Атаки ботнетів включають витік облікових даних, крадіжку даних, доступ неавторизованого персоналу та DoS-атаки.

Атака на відмову в обслуговуванні – це навмисна кібератака, що здійснюється на мережі, веб-сайти та Інтернет-ресурси з метою обмеження доступу до законних користувачів. Зазвичай це робиться шляхом перевантаження цільової мережі або сайту фальшивими системними запитами, запобігання доступу законних користувачів до них, іноді збій або пошкодження системи. DoS-атаки можуть тривати від кількох годин до багатьох місяців.

MITM-атака – відбувається, коли хтось сидить між двома комп'ютерами (наприклад, ноутбуком та віддаленим сервером) і перехоплює трафік. Ця людина може підслуховувати або навіть перехоплювати комунікації між двома машинами та красти інформацію. Такі атаки часто використовуються для злому об’єктів IoT.

Крадіжка особистих даних – це будь-який злочин, у якому зловмисник отримує дані іншої особи та використовує особистість жертви для шахрайства. Наприклад, дані кредитної картки, номери телефонів і адреси електронної пошти.

Соціальна інженерія – метод несанкціонованого доступу до інформації або до систем зберігання інформації без використання технічних засобів.

Постійна загроза підвищеної складності – у цьому типі атаки зловмисники неправомірно отримують доступ до мережі, а потім залишаються в мережі, не будучи виявленим протягом значного періоду часу. Вони регулярно відстежують мережеву активність і викрадають важливі дані.

Програма-вимагач – це шкідливе програмне забезпечення, яке зловмисники можуть використовувати для блокування пристрою або шифрування його вмісту, щоб вимагати викуп в обмін на відновлення доступу до робочої станції або файлів.

Віддалений запис – існування експлойтів нульового дня в пристроях IoT є добре відомим фактом для зловмисників, щоб записувати розмови людей, які використовують пристрої IoT.

Слабкі паролі – для зловмисників дуже легко зламати слабкі паролі за допомогою атаки грубої сили.

Незахищені мережеві служби – незахищені служби, що працюють на пристроях IoT, дозволяють хакерам викрадати важливі дані навіть віддалено.

Незахищені інтерфейси – це стосується нещодавнього збільшення

використання API, мобільних додатків і веб-додатків. Будь-яка вразливість у цих інтерфейсах призведе до компрометації пристроїв IoT.

Відсутність захищених механізмів оновлення – можна несвідомо встановити шкідливе програмне забезпечення від зловмисника під час оновлення свого пристрою IoT під час небезпечного процесу оновлення.

Використання застарілих компонентів – розробка програмного забезпечення з використанням застарілих компонентів, старих операційних систем, стороннього програмного забезпечення від незахищених постачальників призводить до порушення безпеки пристроїв IoT.

Недостатній захист конфіденційності – викрадення персональних даних з пристроїв IoT може призвести до порушення конфіденційності користувачів.

Небезпечна передача та зберігання даних – кожного разу, коли дані передаються через мережу, підвищується ймовірність маніпулювання цими даними. Щоб уникнути таких непередбачених ситуацій, необхідно переконатися, що дані завжди шифруються перед передачею.

Відсутність управління пристроєм – належне керування пристроями IoT є надзвичайно важливим, інакше вся мережа може бути зламана, і всі пристрої будуть скомпрометовані.

Небезпечні налаштування за замовчування – атаки на безпеку можуть мати місце, якщо хтось забуває або не має права змінити налаштування за замовчуванням.

Відсутність фізичної посилення – пристрої IoT зазвичай обробляються за допомогою технології захисту від атак. Відсутність захисту дозволяє хакерам красти важливі дані віддалено або шляхом отримання повного контролю над пристроєм IoT.

Кількість атак на пристрої IoT збільшується, а масштаби та наслідки успішної атаки можуть бути руйнівними. Наприклад, Агентство з кібербезпеки та безпеки інфраструктури (CISA) у співпраці з кількома галузевими фірмами, виявило вразливість у мільйонах пристроїв із інтелектуальною камерою, яка дозволяє зловмисникам отримати доступ до камер, переглядати відео в прямому ефірі, та

створювати ботнети [11].

Кібератаки на пристрої IoT процвітають, оскільки організації підключають все більше і більше розумних пристроїв до своїх мереж. Щоб захистити кінцеві точки, організація повинна мати повну видимість того, де знаходиться кожен пристрій, що він робить і як підключається до інших пристроїв у всій топології мережі. Організації повинні запровадити модель нульової довіри «ніколи не довіряй, завжди перевіряй», яка включає суворий контроль доступу в розподіленій мережі, щоб захистити користувачів, пристрої, кінцеві точки, хмари та інфраструктуру.

Системи IoT вимагають ефективних протоколів агрегації даних у режимі реального часу та повсюдного використання, а також доступності, гнучкості та масштабованості.

Тісно інтегровані рішення безпеки забезпечують надійне керування ідентифікацією та доступом, контролем доступу до кінцевих точок, контролем доступу до мережі та контролем доступу до програм і кінцевих точок для користувачів, які працюють з будь-якого місця.

1.3. Мета та завдання управління доступом до мережі організації

Кожен пристрій в екосистемі IoT потребує унікальної ідентифікації для реалізації правил безпеки. Пристрої можуть використовувати суворе керування, щоб ідентифікувати себе перед встановленням безпечного з'єднання з іншими пристроями та користувачами [12].

Цикл нетипового пристрою включає:

формування ідентифікаційних даних під час проектування пристрою;

реєстрацію пристрою під час виробництва;

призначення сертифікатів розгортання;

підтримку параметрів;

скасування або припинення ідентифікаційних даних пристрою.

Враховуючи широкий спектр користувачів і пристроїв, питання контролю

доступу до ресурсів і навіть ідентифікації об’єктів, що спілкуються, управління доступом та управління ідентифікацією є ключовими питаннями для забезпечення безпечних і надійних реалізацій IoT.

Управління доступом – це механізм безпеки, який забезпечує надійний доступ до ресурсів авторизованих суб'єктів. Як правило, механізм управління доступом описує, як користувачі і системи можуть спілкуватися та взаємодіяти один з одним (або іншими системами та ресурсами), що регулюється застосованими політиками [13].

На рис. 1.5 показані основні компоненти процесу управління доступом. Управління доступом, зазвичай, визначає чи дозволено суб’єкту (а саме процесу, пристрою або користувачу) виконувати, на основі певних політик, операції на об’єкті (а саме базі даних, файлам або службам).

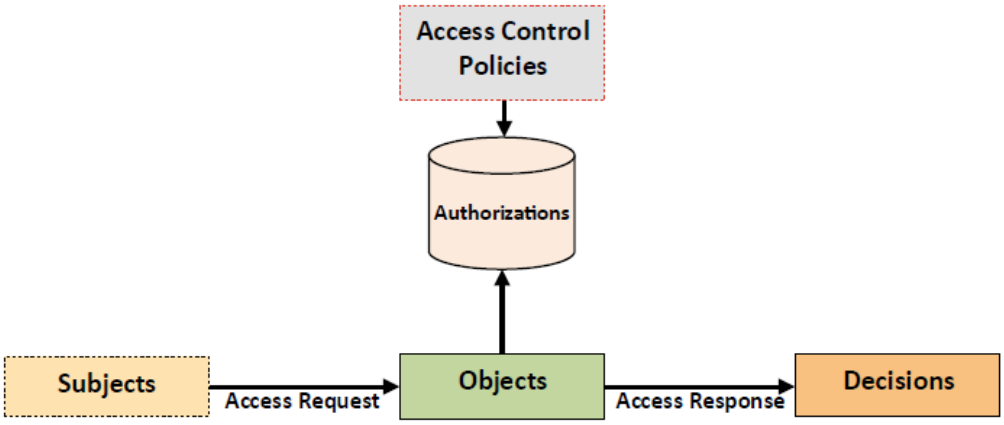


Рис. 1.5. Основні компоненти процесу управління доступом [13]

Управління доступом, як правило, зберігає такі властивості [14]:

конфіденційність: інформацію можуть переглядати авторизовані користувачі, і інформація повинна бути конфіденційною.

цілісність: авторизовані користувачі можуть лише переписувати інформацію, і інформація має бути захищена від підробки та зміни іншими.

доступність: інформація має бути доступною за запитом для використання, що стосується можливості користувача отримати доступ до ресурсу.

Управління доступом до мережі (NAC) визначається як програмне

забезпечення, яке дозволяє IT-менеджерам створювати, застосовувати, керувати та оновлювати політики безпечного доступу по всьому периметру організації.

Іншими словами, управління доступом до мережі – це комплекс технічних заходів та засобів, який забезпечує захист усіх пристроїв IoT від присутніх усередині загроз безпеці [15].

NAC може інтегрувати процес автоматичного виправлення у мережеві системи, дозволяючи мережній інфраструктурі, такій як маршрутизатори, комутатори та брандмауери, працювати разом з серверами обробки даних та з обчислювальним обладнанням кінцевих користувачів для забезпечення безпечної роботи інформаційної системи.

Перевірки стану пристрою, такі як рівень антивірусного захисту, рівень виправлення системи та конфігурація пристрою часто виконуються комерційними рішеннями NAC. Ці рішення можуть розміщати у карантин несправні пристрої, що знаходяться у сегментах мережі.

На відміну від апаратного забезпечення для управління доступом до мережі, який знаходиться в пристрої фізичної безпеки, програмне забезпечення розгортається або локально (на серверах або приватній хмарі), або через загальнодоступні хмарні ресурси для економічності, масштабованості та легкого керування [16].

NAC працює у два етапи. Перший етап – це автентифікація, авторизація користувачів і перевірка їхніх облікових даних. Більшість інструментів NAC підтримують різні методи автентифікації, включаючи паролі, одноразові PIN-коди та біометричні дані.

На другому етапі NAC забезпечує дотримання ряду факторів політики, включаючи справність пристрою, місцезнаходження та роль користувача. Більшість NAC мають можливість обмежувати доступ за ролями, надаючи користувачам доступ лише до тих ресурсів, які необхідні для виконання їхньої роботи.

Щоб повністю захистити кінцеві точки BYOD та IoT, архітектори безпеки повинні мати можливість бачити, де знаходиться кожен пристрій, що він робить і

як підключається до інших пристроїв у всій топології мережі.

З самого початку лідери безпеки зосереджувалися на управління доступом до мережі з метою захисту кінцевих точок. Розвиток NAC складається з першого, другого, третього та четвертого покоління [17].

Перше покоління NAC – це автентифікація користувачів та пристроїв на основі протоколів 802.1X. Якщо пристрій намагався підключитися до портів комутатора або точок бездротового доступу, йому потрібно було надати ім’я користувача/пароль або сертифікат, які мають бути затверджені сервером RADIUS. Цей підхід дозволяв чи забороняв доступ на рівні порту комутатора або бездротової точки доступу. Незважаючи на ефективність цього методу, його важко реалізувати та він не сумісний з усіма пристроями.

Друге покоління NAC розширилося до можливості збору інформації через SNMP за допомогою мережевих пристроїв. Це покоління також представило методи керування доступом на додаток до 802.1X, такі як карантин VLAN, керування на основі ARP і дзеркальне відображення портів.

Третє покоління NAC розширилося до автоматизації. Програмне забезпечення отримало можливість автоматично налаштовувати кінцеві пристрої відповідно до політики безпеки та можливість створювати спільну модель безпеки за рахунок інтеграції з різними системами. Наприклад, IDS або брандмауер, можуть виявляти загрози в мережі, але в кращому випадку вони лише блокують трафік через неї. Інтеграція з NAC дає можливість ізолювати шкідливі пристрої від решти локальної мережі. Ця інтеграція зазвичай використовує стандартизовані протоколи, такі як REST, Webhook і Syslog.

Четверте покоління NAC спрямоване на вирішення проблем, пов’язаних зі зниженою видимістю кінцевих точок, які виникли разом зі збільшенням поширеності IoT і BYOD. Головною особливістю цього покоління є зростаючий перехід до вдосконаленої системи цифрових відбитків пристроїв, а ще одною особливістю є автоматичні реагування NAC на відомі та нові вразливості.

Через спільність терміну «управління доступу до мережі» брандмауер вважають як продукт тієї ж функції, але є основні відмінності.

Брандмауер зазвичай розміщується між двома або більше мережами в місці конфігурації, щоб забезпечити контроль доступу для зв'язку між мережами, тоді як NAC контролює зв'язок між кінцевими точками в мережі. Наприклад, NAC може контролювати загальний доступ до файлів між двома комп'ютерами в одній підмережі, а брандмауер зазвичай цього не робить.

Політики брандмауера зазвичай створюються через такі об'єкти, як адреси та порти джерела/призначення. У NAC пристрої організовано в групи за кількома критеріями. У міру зміни поведінки та атрибутів пристроїв змінюється група, до якої поміщено пристрій. Кожна з груп може бути пов’язана з політикою безпеки з певним рівнем мережевих привілеїв. Наприклад, кінцева точка, на якій не запущено антивірус, може бути ідентифікована в режимі реального часу і поміщена в карантин мережі.

Брандмауер зазвичай контролює трафік, блокуючи невідповідний, що надходить та виходить із мережі, і зазвичай працює на основі простих наборів правил. NAC впливає на самі кінцеві точки, щоб гнучкіше контролювати трафік між пристроями в мережі.

Рішення NAC та брандмауера відіграють взаємодоповнюючі ролі, розглядаючи різні аспекти управління мережі.

Завдяки NAC організації можуть:

виявляти, ідентифікувати, профілювати та сканувати всі пристрої на наявність вразливостей;

встановлювати та забезпечувати постійний контроль мережі;

встановлювати та запроваджувати політики, які обмежують доступ до мережі лише тим, що потрібно для цього пристрою;

підтримувати автоматичне реагування та оркестровку мережі.

Управління доступом до мережі допомагають організаціям не відставати від постійно зростаючої поверхні атак, пов’язаної з поширенням кінцевих точок і пристроїв у мережі.

1.4. Огляд існуючих технологій управління доступом до мережі організації

Програмне забезпечення управлінням доступом до мережі почало набирати популярності в останнє десятиліття. Звіт Pulse Secure та Cybersecurity Insiders про безпеку кінцевих точок та IoT за 2020 рік виявив, що компаній зазнали різкого зростання кількості інцидентів [18].

Програмні платформи управління доступом до мережі запобігають неприємним сюрпризам, спричиненим інсайдерськими загрозами, обмежують неавторизованим користувачам доступ до конфіденційних ресурсів і дозволяють впевнено розширювати свій цифровий слід.

Aruba Secure Network Access Control

Aruba, яка є частиною Hewlett Packard Enterprises, пропонує продукт для наскрізного управління доступом до мережі для IoT і віддалених кінцевих точок [19].

Основні функції рішення: безагентний контроль політики та автоматичне реагування; статистика на основі штучного інтелекту, а саме автоматизовані робочі процеси та безперервний моніторинг; забезпечення доступу на основі ролей у бездротових, дротових і VPN-мережах різних постачальників; безпечний гостьовий доступ та самостійна реєстрація пристроїв.

Aruba підходить для великих підприємств із розподіленою присутністю. Він доступний як в апаратному, так і програмному забезпеченні, а основна платформа розміщена в хмарному середовищі, такому як VMware, Microsoft або Amazon Web Services.

Barracuda CloudGen Firewall

Хоча пропозиція Barracuda технічно є брандмауером, програмне забезпечення виходить далеко за межі типових можливостей брандмауера наступного покоління, і забезпечує контроль доступу до мережі [20]. Рішення інтегрується з основними загальнодоступними хмарними ресурсами через AWS, Azure та Google Cloud Platform.

Основні функції рішення: ідентифікація користувача для пріоритетного розподілу смуги пропускання або правила брандмауера з урахуванням користувачів і контроль на рівні програми; глибокий аналіз контексту програми для аналізу трафіку програми та виявлення фактичних намірів; детальний контроль програм; безпечний віддалений доступ CudaLaunch для мобільних працівників; авторитетний сервер доменних імен; контроль доступу до мережі з централізованим керуванням та локальне застосування обмежень доступу.

Організації середнього та великого розміру, які бажають повністю переробити систему безпеки, повинні розглядати Barracuda як потенційного партнера з кібербезпеки.

Cisco Identity Services Engine

Хоча Cisco визнано в усьому світі провідним постачальником кібербезпеки, його Identity Services Engine є спеціалізованим рішенням, спеціально створеним для управління доступом до мережі [21]. Це спрощує керування політикою мережевої безпеки через дротові, бездротові та VPN-з'єднання, надаючи видимість усіх користувачів і пристроїв, які потенційно мають доступ до мережі організації.

Основні функції рішення: централізоване керування службами профілювання, позиціями, гостьовими системами; керування автентифікацією та авторизацією, запровадження політики ідентифікації, що ґрунтуються на моделі, заснованій на правилах та атрибутах; інтеграція зі сховищами ідентифікаційних даних, такими як Microsoft AD, LDAP, RADIUS і одноразовий пароль RSA; програмно-визначувана сегментація мережі за допомогою тегів групи безпеки та спрощена реєстрація пристроїв; профілювання пристроїв та служб каналів.

Cisco Identity Services Engine підходять для організації, які шукають точкове рішення для контролю доступу до мережі.

Citrix Gateway

Citrix Gateway – це рішення для інфраструктури віддаленого доступу, яке дозволяє надавати безпечний доступ SSO для всіх програм, незалежно від того, де вони розміщені – у центрі обробки даних, у хмарі чи через SaaS [22]. Він розгортається в демілітаризованій зоні мережі, але також можна вибрати кілька

віртуальних пристроїв для більш складних вимог.

Основні функції рішення: сумісність із продуктами Citrix (SD-WAN), StoreFront, Workspace і XenMobile; підтримка всіх основних типів автентифікації, а також локальної автентифікації; запровадження політики доступу користувачів на основі груп та профілю автентифікації.

Citrix Gateway ідеально підходить для зрілих IT-команд, яким потрібен детальний контроль і можливості для підтримки дуже складного цифрового підприємства.

Forescout

Він інтегрується з ServiceNow, Palo Alto Networks або Check Point NGFW, а також з Splunk, QRadar і ArcSight, що створює наскрізне оркестроване рішення для контролю доступу до мережі [23].

Основні функції рішення: картографування ландшафту пристрою; оцінка ризиків та інвентаризація активів у реальному часі; застосування політики в різнорідних мережах, можливості автоматизації за допомогою модулів інтеграції plug-and-play і API; забезпечення найменш привілейований доступ на основі пристрою та ідентифікатора користувача; надання інтелектуальної інформаційної панелі із статистикою в реальному часі на основі ролей.

Forescout ідеально підходить для будь-якої компанії, яка прагне інвестувати, розвивати та захищати свій промисловий IoT.

McAfee Unified Secure Access

Програмне рішення поєднує безпеку кінцевих точок і безпеку мережі з контролем доступу користувачів та аудитом політики [24].

Основні функції рішення: визначення політики за допомогою інтегрованого централізованого McAfee ePolicy Orchestrator; інтегрування з Microsoft Network Access Protection; виявлення та контроль керованих і некерованих систем за допомогою клієнтського агента або виявлення шахрайських систем; контроль шляхом аналізу протоколів додатків, адрес джерел, призначення, портів, зміни розташування хоста та зловмисної поведінки, виявленої системою запобігання вторгненням.

McAfee Network Access легко запровадити як для малого, середнього, так і для великого бізнесу. Його можна використовувати як окреме програмне забезпечення McAfee або як об'єднання з пристроєм чи вдосконаленою платформою безпеки мережі для створення уніфікованого рішення безпечного доступу. Він найкраще підходить для віддалених співробітників і компаній з розподіленими командами.

SAP Access Control

Програмне рішення автоматизує контроль та керування мережним доступом для безперешкодного доступу користувачів. SAP Access Control приділяє особливу увагу взаємодії з користувачем, гарантуючи, що робочі процеси не перериваються, а запити на доступ і схвалення обробляються автоматично [25].

Основні функції рішення: аналіз ризиків для виявлення та усунення критичних порушень доступу; запровадження правила контролю доступу на основі ролей; автоматизоване призначення доступу в системах SAP та забезпечення сертифікації ролей з сповіщенням у разі конфліктних або конфіденційних дій.

Для компаній, які вже залежать від SAP у плануванні ресурсів підприємства через HANA чи в керуванні ідентифікаційним доступом – це ідеальне рішення для управління доступом до мережі.

Sophos NAC

Програмне рішення пропонує централізований модуль застосування політики, веб-інтерфейс керування безпекою кінцевих точок та параметри оцінки регулярного перегляду пристроїв або користувачів [26].

Основні функції: примусове застосування політик на основі агентів для влаштування пристроїв в режим самоізоляції; веб-інтерфейс для створення політики, контролю за правозастосування, звітності та сповіщень; можливості аудиту, які дозволяють IT-адміністраторам контролювати та керувати відповідністю кінцевих точок; веб-агенти та встановлені агенти для комплексної оцінки відповідності як до, так і після попереднього доступу до мережі; гнучке розгортання за допомогою поетапного підходу до звітності, виправлення та примусового застосування.

Sophos NAC сумісний із більшістю постачальників мережевого обладнання, такими як Cisco, Alcatel, HPE, Lucent, Check Point і Aruba. Незалежні професіонали, малі підприємства та організації середнього розміру повинні розглядати Sophos NAC для своїх потреб у управління доступом до мережі.

FortiNAC

Програмне рішення доступне як у версії для апаратного забезпечення, так і у версії для встановлення на віртуальній машині. Він пропонує видимість, контроль і автоматичне реагування на будь-який інцидент доступу, що виникає на периметрі мережі, незалежно від того, чи це сторонній пристрій чи IoT [27].

Головною перевагою FortiNAC є його можливості автоматизації та інтеграції. Майже всі великі постачальники – від Apple до Cisco, від Linux до Symantec і від Google Workspace до Check Point – всі вони є партнерами Fortinet. Це дозволяє користувачам створювати підключену мережу безпеки в межах свого підприємства з автоматизацією в ключових точках робочої сили.

Звіт Gartner Critical Capabilities for SD-WAN [28] за вересень 2022 року містить рекомендації щодо вибору найкращого рішення SD-WAN на основі випадків використання. Відзнаки Gartner Peer Insights Customers' Choice присуджуються постачальникам та продуктам, які високо оцінені їхніми клієнтами.

Рішення програмно-конфігурованої глобальної мережі (SD-WAN) надають організаціям додаткові переваги за рахунок використання корпоративної глобальної мережі спільно з кількома хмарними інфраструктурами, що забезпечує високу швидкість обміну даними та продуктивність додатків у периферійних мережах WAN філій.

Рішення SD-WAN користуються все більшою популярністю, оскільки організаціям потрібне швидке, масштабоване та гнучке з'єднання між різними мережевими середовищами з можливістю зменшення сукупної вартості володіння і збереженням зручності роботи для користувачів.

На рис. 1.6 зібрані дані являють собою синтез найвищого рівня програмних продуктів постачальників, які найбільше цінуються фахівцями IT-підприємства. Fortinet три роки поспіль визнавався лідером.

Рис. 1.6. Квадрант лідерів щодо SD-WAN [28]

У міру того, як кіберзагрози стають все більш витонченими, модель безпеки, орієнтована на периметр, більше не є достатньою. Крадіжка конфіденційної інформації та шкідливі програми дозволяють отримати доступ до облікових записів у корпоративній мережі. Fortinet Security Fabric дозволяє організації впроваджувати політику мережного доступу з нульовим рівнем довіри в рамках корпоративної мережі WAN.

Рішення FortiNAC забезпечують автоматичне виявлення та контроль пристроїв, підключених до корпоративної мережі WAN. Fortinet Secure SD-WAN складається з рішення FortiNAC. Саме тому в подальшому буде проаналізовано FortiNAC.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ FORTINAC

2.1. Призначення та можливості рішення FortiNAC

Як частина архітектури Fortinet Security Fabric, FortiNAC – це рішення NAC третього покоління, яке використовує вбудовані команди мережних комутаторів, маршрутизаторів і точок доступу для створення оперативної інвентаризації мережевих підключень та забезпечення управлінням доступом до мережі [30]. FortiNAC ідентифікує, перевіряє та контролює кожне з'єднання перед наданням доступу. Гнучка і масштабована архітектура дозволяє його розгортати як апаратний пристрій, віртуальний пристрій або хмарну службу, тому рішення зможе адаптуватися до унікальних потреб будь-якого мережного середовища.

На рис. 1.7 показано розгортання FortiNAC в SD-WAN.

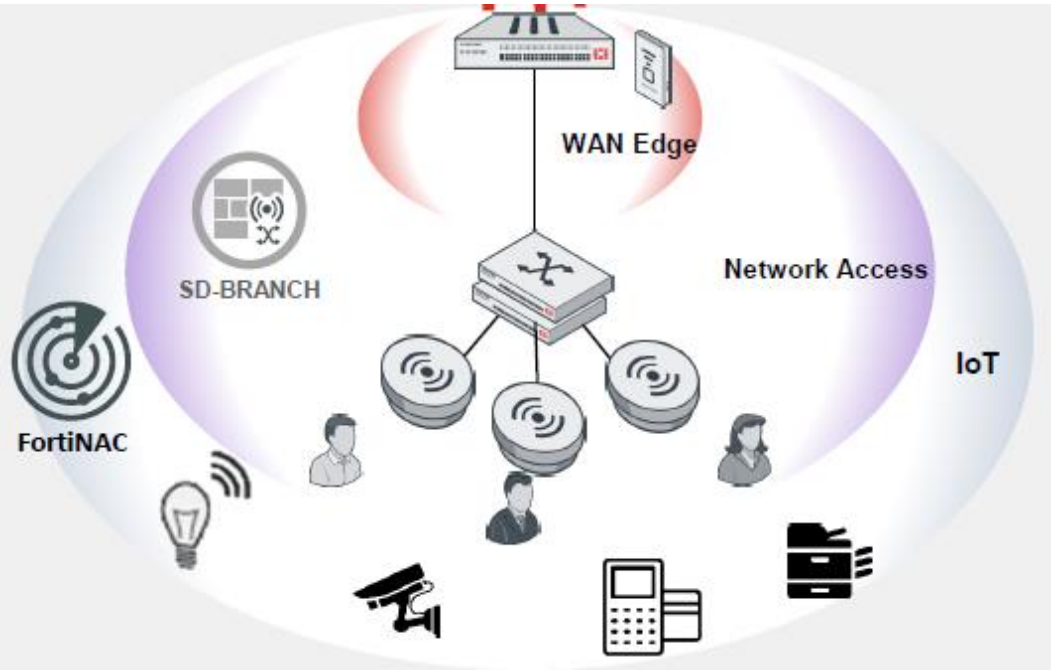


Рис. 1.7. Розгортання FortiNAC [27]

Основні переваги рішення Fortinet SD-Branch походять від покращення безпеки у філії. Глобальні політики застосовуються у всіх межах глобальної

мережі, на рівні доступу до філії та на всіх кінцевих пристроях. Він розширює як безпеку, так і продуктивність мережі до рівня доступу, поєднуючи середовища WAN та LAN. А також він автоматизує виявлення, класифікацію та захист пристроїв IoT, коли вони шукають доступ до мережі. Додатковий аудит поведінки пристрою в реальному часі можна отримати, додавши можливості управління доступом до мережі FortiNAC.

Комп'ютерна безпека NAC розширює можливості Fortinet Security Fabric за допомогою видимості, контролю та автоматичному реагуванню на все, що підключається до мережі. Він забезпечує захист від загроз IoT, поширює контроль пристроїв сторонніх виробників та керує автоматичними відповідями на широкий спектр мережевих подій. А також забезпечує сегментацію мережі на основі політик контролю доступу до конфіденційної інформації.

Автоматизовані дії безпеки на основі політики допомагають рішенням Security Fabric обмінюватися аналітичними даними в режимі реального часу, щоб стримувати потенційні загрози, перш ніж вони зможуть поширитися. FortiNAC має широкий набір політик автоматизації, які можуть миттєво активувати параметри стримування в інших елементах Fortinet Security Fabric, таких як FortiGate, FortiSwitch або FortiAP, при виявленні цільової поведінки.

Пристрої або користувачі, які порушують встановлену мережеву політику, повинні негайно ініціювати уніфіковану реакцію стримування в усій архітектурі безпеки. Це може включати автоматичне завершення з'єднання, обмеження доступу до мережі, карантинну ізоляцію та/або ряд дій щодо повідомлення операційному центру безпеки (SOC) та центру керування мережею (NOC).

Потенційні загрози стримуються шляхом ізоляції підозрілих користувачів і вразливих пристроїв, або через застосування ряду реагуючих дій. Це, у свою чергу, скорочує час стримування з кількох днів до секунд, допомагаючи підтримувати відповідність дедалі суворішим стандартам, правилам і законам про конфіденційність.

Після ідентифікації пристроїв і користувачів FortiNAC призначає відповідний рівень доступу, обмежуючи використання незв'язаного контенту. Ця

динамічна система на основі ролей групує разом додатки та дані, щоб обмежити доступ до певних груп користувачів. Отже, якщо пристрій скомпрометований, його здатність переміщатися по мережі та атакувати інші активи буде обмежена. Інтеграція з FortiNAC Security Fabric дозволяє FortiNAC впроваджувати політики сегментації та змінювати конфігурації комутаторів чи бездротових продуктів, включаючи рішення від понад 70 різних постачальників.

На рис. 1.8 показана інтеграція FortiNAC із інфраструктурою, в якій використовуються стандартні протоколи для збирання інформації.

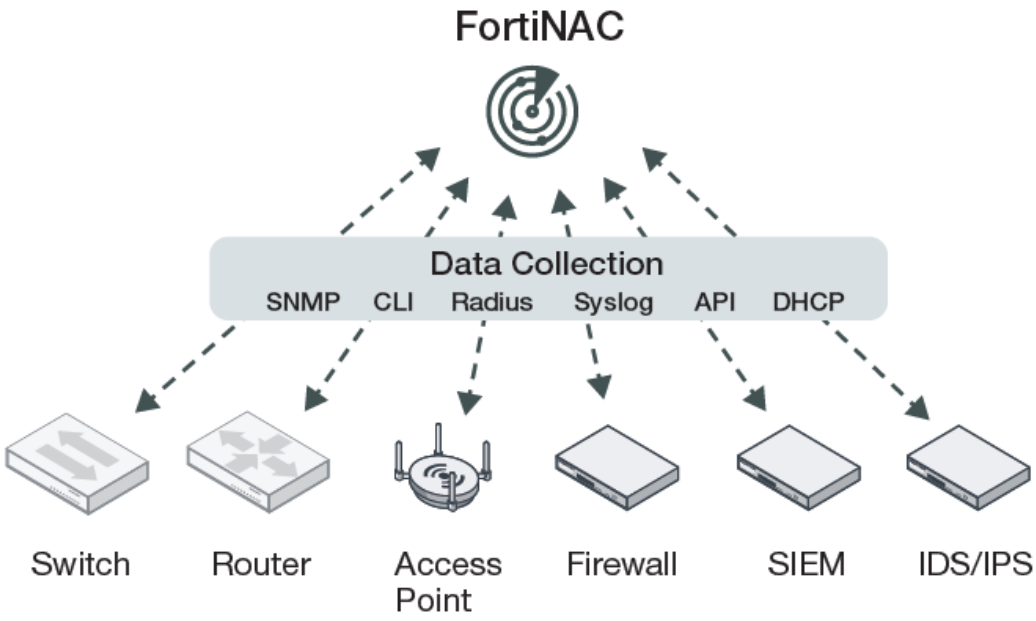


Рис. 1.8. Збір даних із різних джерел [27]

Цифрові відбитки пристроїв SNMP, CLI, RADIUS, SYSLOG, API і DHCP можна використовувати для досягнення детальної наскрізної видимості, необхідної для створення безпечного середовища.

FortiNAC перевіряє конфігурацію кінцевої точки, коли вона намагається приєднатися до мережі. Якщо конфігурація не відповідає вимогам, з'єднання блокується чи пристрій ізолюється, або йому надається VLAN з обмеженим доступом. Після цього користувачів попереджають, що їхній пристрій потрібно виправити. Доступ надається лише після вживання коригуючих заходів.

FortiNAC постійно контролює мережу, оцінюючи кінцеві точки, щоб

переконатися, що вони відповідають встановленому профілю. Рішення повторно сканує пристрої, щоб гарантувати, що підміна MAC-адреси не обійде систему безпеки доступу до мережі. Крім того, він спостерігає за аномаліями в моделях трафіку. Як тільки скомпрометована або вразлива кінцева точка виявляється як загроза, FortiNAC ініціює автоматичну відповідь в режимі реального часу.

FortiNAC також спрощує безпечний процес реєстрації гостьових користувачів, захищаючи їх від будь-яких частин мережі, що містять конфіденційні дані. За потреби користувачі можуть самостійно зареєструвати власні пристрої (ноутбуки, планшети або смартфони), перекладаючи навантаження з IT-персоналу.

Контроль може застосовуватися в точці підключення, тоді як інтеграція пристроїв безпеки дозволяє FortiNAC обробляти сповіщення безпеки та розглядати їх як тригери для автоматичного усунення загроз за допомогою настроювання робочих процесів. Дані збираються з багатьох джерел різними методами.

FortiNAC – це «зовнішнє» рішення, тобто воно не враховує трафік користувачів. Ця архітектура дозволяє централізовано розгортати рішення і керувати багатьма віддаленими розташуваннями. Видимість, контроль та реагування досягаються за рахунок інтеграції та використання можливостей мережевої інфраструктури.

2.2. Компоненти та методи рішення FortiNAC

FortiNAC забезпечує просту автоматизовану адаптацію і динамічні елементи керування доступом з можливістю налаштування. Доступ до мережі можна призначати за допомогою попередньо визначених профілів, що значно заощаджує час при наданні доступу для різноманітних потреб. Рішення контролює політики та дозволи доступу до кінцевих точок за ролями або користувачами, щоб гарантувати, що користувачі отримують лише необхідний рівень доступу. Таким чином, він захищає важливі дані та конфіденційні активи, забезпечуючи дотримання всіх застосовних галузевих норм і стандартів.

FortiNAC підтримує розширені можливості профілювання для забезпечення

довіри до пристроїв WinRM і WMI. FortiNAC також має можливості пасивного сканування для безперервної ідентифікації чутливих пристроїв, таких як автоматизована система керування та SCADA у мережах операційних технологій.

FortiNAC дізнається, де підключені кінцеві точки в мережі, використовуючи такі методи:

пастки SNMP Link State, що відправляються комутатором;

syslog MAC;

зв'язок RADIUS;

L2 Polling (читання таблиці MAC-адрес);

L3 Polling (зчитування Arp Cache).

В його компонентах є до 21 різних методів, потом він може профілювати кожен елемент на основі спостережуваних характеристик та відповідей, а також може звертатися до хмарної бази даних IoT Services FortiGuard для ідентифікаційного пошуку.

Сканування може здійснюватися активно або пасивно, а також можуть використовуватися постійні агенти, розчинні агенти або взагалі не використовуватися агенти. FortiNAC оцінює пристрій, щоб визначити, чи він відповідає затвердженим профілям, відзначивши необхідність оновлення програмного забезпечення для усунення вразливостей.

На додаток до знання всієї мережі, покращена видимість FortiNAC також може використовувати пасивний аналіз трафіку, використовуючи пристрої Fortinet FortiGate як датчики для виявлення аномальні шаблони трафіку або можливої ознаки компрометації, за якими може стежити команда SOC.

Профілювання пристроїв – це процес FortiNAC для класифікації фальшивих пристроїв та створення впорядкованого списку відомих зареєстрованих пристроїв. Крім того, профілювання можна використовувати для повторної перевірки надійності зареєстрованого пристрою [29].

Профіль пристрою – це засноване на правилах рішення FortiNAC, яке дає можливість оцінювати та класифікувати пристрої. Це набір попередньо визначених і спеціально створених упорядкованих правил. Правило складається з налаштувань

класифікації та методів оцінки.

FortiNAC оцінює пристрій за кожним правилом до тих пір, поки не буде досягнуто результату «пройдено», «не пройдено» або «неможливо оцінити» (через недостатність даних).

На рис. 1.9 зображено методи профілювання пристроїв.

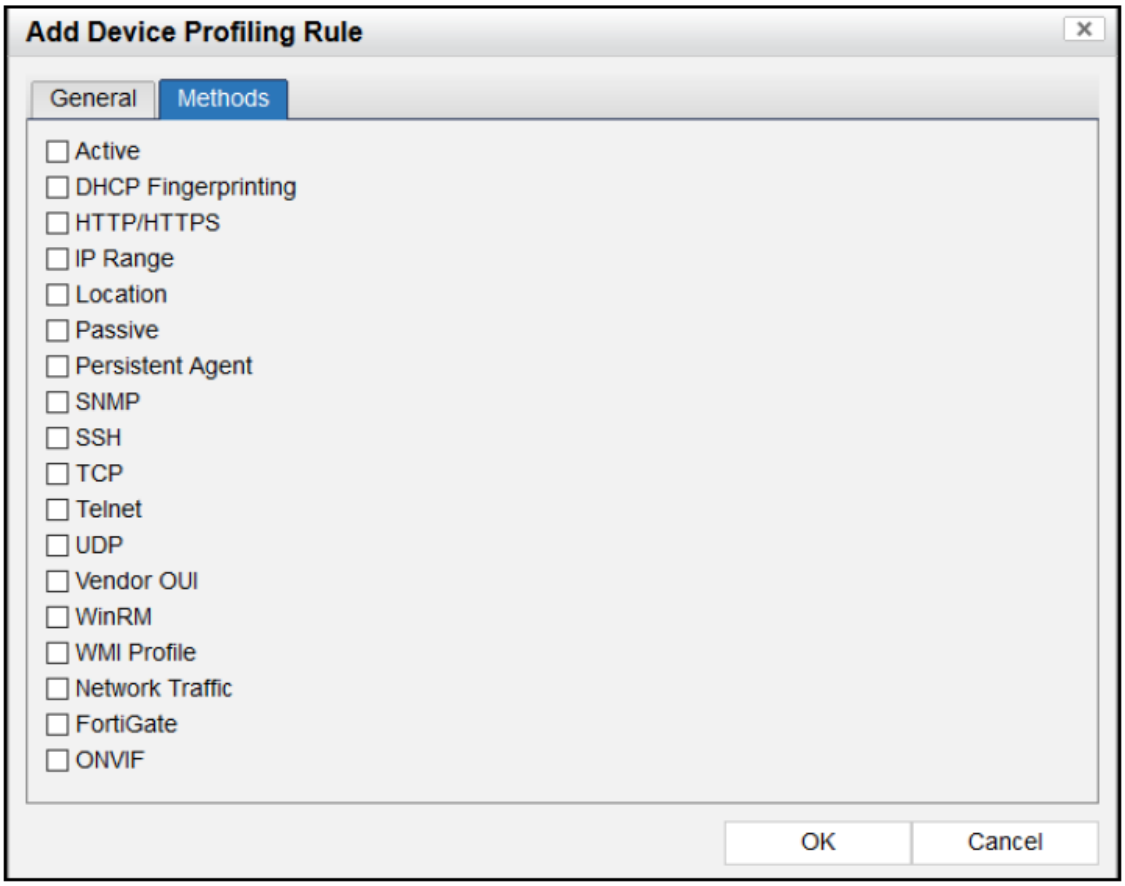


Рис. 1.9. Методи профілювання FortiNAC для класифікації пристроїв

Параметри методів профілювання класифікуються в одну з трьох пріоритетних груп: дані зібрано, дані потрібно зчитати або дані треба отримати.

Дані зібрано

Метод місцезнаходження порівнює підключене розташування пристрою з указаним об’єктом розташування.

Метод OUI постачальника порівнює OUI пристрою з базою даних OUI FortiNAC. До правила можна додати найменування, псевдонім та код постачальника, а також тип пристрою.

Дані потрібно зчитати

Активний метод оцінює ОС за допомогою бази даних виявлення ОС NMAP.

Метод HTTP/HTTPS URL проводить запит з автентифікацією чи без неї та з можливістю пошуку відповідності вмісту в результаті.

Діапазон IP порівнює IP-адресу пристрою з указаним діапазоном IP-адрес.

Метод SNMP проводить запит OID з автентифікацією V1/V2/V3 і можливістю пошуку відповідності вмісту в результаті.

Метод SSH визнає відповідність правил, надіславши запит SNMP GET для вказаного OID. До правила потрібно додати облікові дані безпеки.

Метод TCP сканує веденні в правило порти за допомогою NMAP.

Метод Telnet визнає відповідність правил, надіславши запит сеансу клієнта Telnet.

Метод UDP сканує веденні в правило порти за допомогою NMAP.

Метод WinRM проводить автентифікацію з'єднання Windows Remote Manager із можливістю виконувати команди та зіставляти вміст у результаті виконання команди. Подібно до методу SSH, за допомогою WinRM можна запускати команди PowerShell на Windows.

Профіль WMI – це метод із вбудованою фільтрацією версії Windows та автентифікація з'єднання WinRM або SSH із можливістю оцінки:

ОС, Центр безпеки Windows, серійний номер і тег ресурсу;

служби Windows;

запущені процеси;

встановлена програма.

WMI – це впровадження Microsoft Web-Based Enterprise Management, яке є галузевою ініціативою з розробки стандартної технології для доступу до інформації керування в корпоративному середовищі. WMI використовує промисловий стандарт Common Information Model для представлення систем, програм, мереж, пристроїв та інших керованих компонентів.

Методи Network Traffic та Network Flow оцінюють тип пристрою на основі інформації про сеанс FortiGate. До правила потрібно додати протокол TCP, UDP

або інший, а також додати порт призначення.

Методи FortiGate та Firewall оцінюють тип пристрою на основі відповідності політики брандмауера. Щоб використовувати цей метод, необхідно налаштувати опитування сеансу брандмауера.

Метод ONVIF визначає, чи підтримує кінцева точка певний профіль ONVIF. В правилі є профілі A, C, G, Q, S і T.

Дані треба отримати

DHCP Fingerprinting – це оцінка типу пристрою на основі цифрового відбитка DHCP у порівнянні з базою даних типів пристроїв FortiNAC. Метод надає інформацію про операційну систему та ім'я хоста. Щоб FortiNAC отримував дані цифрового відбитка, IP Helper має бути налаштовано на комутаторах/маршрутизаторах L3 для всіх виробничих VLAN, які використовують DHCP. Потрібно вказувати на IP-адресу керування (eth0) сервера FortiNAC або сервера додатків. Інтерфейс керування лише прослуховує запити DHCP і не відповідає на них.

Пасивний метод оцінює операційну систему шляхом аналізу мережевого трафіку за допомогою бази даних P0f.

Постійний агент оцінює тип пристрою на основі операційної системи, повідомленої Persistent Agent, у порівнянні з базою даних типів пристроїв FortiNAC.

Підтвердження правила – це автоматична повторна перевірка раніше профільованого пристрою. Коли пристрій спочатку профільований і відповідає правилу, інформація про правило зберігається разом із класифікованим записом пристрою з метою повторної перевірки.

Підтвердження може виконуватися під час підключення або через часовий інтервал. Помилка підтвердження правила призводить до створення події. Подію можна зіставити з дією тривоги та/або вимкненням пристрою за допомогою дії правила. FortiNAC сповіщає, якщо пристрій або хост підключається до мережі чи пристрій переміщується до нового порту.

Результати перевірки є лише інформаційними та використовуються для

перевірки правильності правила. Коли нові, невідомі пристрої підключаються до мережі, профіль пристрою класифікує їх і розміщує в FortiNAC на основі правил профілювання пристроїв.

Якщо пристрій має IP-адресу, профіль пристрою FortiNAC порівнює доступну інформацію про IP-адресу із правилами профілювання. Перевірка починається з правила, яке займає номер один, і проходить через список правил у порядку за рангом, доки не знайде відповідність одному з критеріїв правила або методів відповідності.

FortiNAC використовує численні джерела інформації та поведінки для точної ідентифікації всього в мережі. Він забезпечує докладне профілювання провідних, бездротових і навіть безголових пристроїв. Цей комплексний безагентний процес сканування автоматично виявляє кінцеві точки, класифікує їх за типом і визначає, чи є пристрій корпоративним або службовим.

2.3. Інтеграція FortiNAC до архітектури безпеки Fortinet Security Fabric

Fortinet Security Fabric — це архітектура безпеки, що забезпечує [31]:

широку видимість та захист від цифрових атак;

інтегроване виявлення нових загроз;

автоматичну реакцію на виявлені загрози та безперервну оцінку довіри до засобів захисту.

FortiNAC інтегрується із провідними сторонніми технологіями в масштабах організації, забезпечуючи управління доступом до мережі економічно ефективним.

Платформа безпеки заснована на відкритих стандартах і надає прикладний програмний інтерфейс (API) на основі передачі репрезентативного стану, що забезпечує двонаправлений зв’язок. Це розширює можливості Fortinet Security Fabric, який використовує своє з’єднання з FortiNAC для керування та контролю оновлень політик. Це також включає обмін даними про загрози та управління ними. Це особливо важливо, оскільки багато з цих елементів, підключених до рішення, знаходяться на краю корпоративної мережі, де знаходяться вразливі мобільні

пристрої та пристрої IoT.

FortiNAC має глибоку інтеграцію з іншими продуктами Fortinet, які описано в таблиці 1.1.

Таблиця 1.1.

Інтеграція FortiNAC з Fortinet Security Fabric

Продукт Fortinet	**Інтеграція**
FortiGate	Контроль FortiGate VPN від FortiNAC
	Порти FortiGate і FortiWiFi
FortiSwitch	В автономному режимі
FortiAP	В автономному режимі
FortiClient EMS	Рішення MDM як довірений пристрій для реєстрації
FortiAnalyzer	Звітність
FortiSIEM	Реагування на інцидент
FortiDeceptor	Реагування на інцидент
FortiEDR	Реагування на інцидент

FortiNAC інтегрується з Fortinet Security Fabric, щоб забезпечити видимість усіх користувачів та пристроїв, які намагаються підключитися до мережі. При підключенні до архітектури безпеки Fortinet**,** FortiNAC ідентифікує користувачів та пристрої, а потім використовує цю інформацію для надання належного доступу до мережі на основі відповідних політик.

FortiGate

Брандмауери нового покоління FortiGate; це перша лінія захисту від сучасних загроз. До складу NGFW FortiGate входить захищений веб-шлюз, який ідентифікує та блокує спроби підключення до шкідливих або підозрілих URL-адрес. FortiGate NGFWs також виконують дешифрування та перевірку пакетів на рівні захищених сокетів/безпеку на транспортному рівні.

FortiNAC інтегрується з FortiGate, забезпечуючи покращену безпеку в реальному часі пристроїв IoT у мережі. Ці опції пропонують покращену видимість і виявлення аномалій без необхідності встановлення додаткового обладнання на

кожному місці.

Він забезпечує автоматичне застосування політик брандмауера FortiGate до хостів, які підключаються до мережі. Це досягається за рахунок використання облікових повідомлень RADIUS, які надсилаються з FortiNAC до агента єдиного входу, налаштованому в брандмауері. Агент містить ідентифікатор користувача і IP-адресу хоста. За допомогою цієї інформації, брандмауер може застосовувати політику для конкретних користувачів (сегментація на основі намірів). Інтеграція з ForitGate також включає можливість FortiNAC додавати користувачів до груп користувачів.

FortiGate VPN

ForitNAC контролює доступ до мережі, використовуючи Fortinet Single Sign-On на FortiGate. Коли користувачі через VPN підключаються, доступ до мережі обмежений за замовченням. Статус доступу змінюється лише в тому випадку, якщо користувач успішно проходить аутентифікацію, запускає відповідний агент та проходить всі необхідні перевірки відповідності. Як тільки користувач і хост будуть ідентифіковані та перевірені за допомогою встановленим політикам організації, обмеження доступу до мережі можна буде зняти. FortiNAC надсилає інформацію про групу та/або теги до FortiGate, щоб налаштувати доступ користувача до мережі відповідно до правил, встановлених адміністратором у FortiNAC і FortiGate.

Порти FortiGate і FortiWiFi

FortiNAC керує кінцевими точками, безпосередньо підключеними до дротового та бездротового інтерфейсів FortiGate (порти FortiGate LAN/точки бездротового доступу FortiWiFi).

FortiSwitch та FortiAP

В автономному режимі FortiNAC забезпечує видимість мережі, а саме де підключаються кінцеві точки, та керує призначенням VLAN у точці підключення для кінцевої точки. Це досягається шляхом надсилання на пристрій відповідних команд конфігурації.

FortiClient EMS

Інтеграція складає рішення MDM, що є надійним підключенням пристрою. FortiClient прискорює процес реєстрації пристроїв, зареєстрованих у EMS. Пристрої, що підключаються до мережі, можна зареєструвати у FortiNAC за допомогою даних хоста з EMS.

FortiAnalyzer

FortiAnalyzer забезпечує централізоване ведення журналів, аналіз і звітність у Fortinet Security Fabric. Інтеграція з FortiNAC дозволяє FortiAnalzyer отримувати інформацію та звітувати про:

події;

тривоги;

дані кінцевої точки, включаючи звіти про інвентаризацію;

дані мережевої інфраструктури.

FortiSIEM та FortiEDR

Інтеграція системного журналу дозволяє FortiNAC реагувати на основі повідомлень системного журналу, надісланих із FortiSIEM. Ці повідомлення надають інформацію, яку FortiNAC може використовувати для надсилання повідомлень, наприклад, електронною поштою, або рішення може використовувати дані для вжиття заходів проти пов’язаного хоста, таких як відключення хоста або позначення його як «під загрозою».

FortiSIEM забезпечує інтелектуальну безпеку. FortiNAC надсилає подію у FortiSIEM для обробки попередження, а потім FortiSIEM наказує FortiNAC обмежити або помістити пристрій у карантин, якщо це необхідно. Вони взаємодіють між собою, збираючи всю необхідну інформацію та доставляючи її аналітику з безпеки.

FortiDeceptor

Інтеграція між FortiNAC та FortiDeceptor дозволяє автоматично ізолювати будь-який заражений пристрій від мережі на основі виявлення сповіщень FortiDeceptor. Одним із варіантів використання цієї інтеграції є протидія програмам-вимагачам з використанням токена обману SMB, щоб спонукати програми-вимагачі шифрувати підроблені файли, а потім надсилати сповіщення до

FortiNAC. FortiDeceptor використовує FortiNAC для автоматичної ізоляції зараженої кінцевої точки від мережі та запобігання пошкодженню мережі.

Зазначені вище інтеграції дозволяють FortiNAC тісно взаємодіяти з різними продуктами Fortinet Security Fabric, що одночасно покращує можливості FortiNAC і збільшує можливості Security Fabric.

2.4. Вимоги до системи для інсталяції FortiNAC

Автоматизовані заходи стримування через Fortinet Security Fabric дозволяють ще більше захистити підприємства від натиску складних атак, орієнтованих на кінцеві точки.

Крім цих основних можливостей, FortiNAC можна розгорнути як апаратний пристрій, віртуальний пристрій або хмарну службу, пропонуючи архітекторам безпеки гнучке рішення NAC третього покоління, яке можна адаптувати до унікальних потреб будь-якого середовища.

Розроблений з урахуванням масштабованості FortiNAC знижує загальну вартість володіння, оскільки не вимагає наявності сервера в кожному місці розгортання. Він також використовує існуючі інфраструктури каталогів, мережі та безпеки для захисту інвестицій та мінімізувати збої.

FortiNAC – це гнучке та масштабоване рішення, яке охоплює розгортання від середніх до дуже великих підприємств. Рішення складається із трьох елементів:

застосування та контроль;

керування;

FortiAnalyzer.

Рішення забезпечує видимість, а елемент керування надає можливості налаштування функції автоматичного реагування. Частина «керування» дозволяє спільно використовувати одночасних користувачів у розгортанні кількома серверами. FortiAnalyzer надає звіти та аналітику на основі інформації, зібраної з мережі за допомогою FortiNAC.

FortiNAC можна розгорнути на віртуальних машинах (VMWare/Hyper-

V/AWS/Azure/KVM) або як програмно-апаратний комплекс. Сервери додатків і керування можуть бути розгорнуті в різних розмірах, залежно від кількості портів. FortiNAC підходить для підтримки розподіленої архітектури, включаючи розташування SD-Branch.

FortiNAC спрощує розгортання пристроїв IoT, автоматизуючи більшу частину процесу автентифікації за допомогою спонсора. Коли новий пристрій IoT намагається підключитися до мережі, FortiNAC автоматично розміщує пристрій в ізольованій мережі, профілює пристрій і надсилає інформацію у відповідний відділ для перевірки та авторизації. Після підтвердження FortiNAC сповіщає брандмауер про тип пристрою та місце його розміщення в сегменті мережі.

FortiNAC пропонує гнучкі варіанти розгортання на основі бажаного рівня покриття та функціональності:

Начальний рівень ліцензії забезпечує просте, одноетапне рішення безпеки IoT для усунення прогалин у безпеці кінцевих точок шляхом перегляду всіх кінцевих пристроїв у мережі, автоматизації авторизації, ввімкнення мікросегментації та блокування мережі. Цей рівень підходить для організацій, яким необхідно захистити IoT та автономні пристрої, а також забезпечити блокування мережі за допомогою динамічного керування VLAN, але не потребують більш сучасних засобів керування користувачами/мережами або автоматизованого реагування на загрози.

Розширений рівень ліцензії базується на всіх функціях начального рівня з покращеною видимістю та розширеними засобами управління доступом, автоматичною ініціалізацією для користувачів, гостей і пристроїв, а також звітами та аналітикою. Звітність та аналітика можуть значно допомогти у наданні аудиторської документації відповідності. Цей рівень підходить для організацій, яким потрібна повна видимість кінцевих точок і детальний контроль, але не потрібне автоматичне реагування на загрози.

Професійний рівень ліцензії забезпечує видимість кінцевих точок у реальному часі, повний контроль доступу та автоматичне реагування на загрози, одночасно надаючи контекстну інформацію з сортованими попередженнями. Він

інтегрується з Fortinet Security Fabric. А також він використовує механізм кореляції для сортування попереджень за ступенем серйозності, підвищення точності сортування подій та представлення сповіщення аналітику. Представляючи всю інформацію в одному комплексному сповіщенні, ця ліцензія автоматизує більшу частину ручного процесу перевірки безпеки. Це значно скорочує час, які IT-аналітики витрачають на перегляд сповіщень і дослідження інформації про події.

2.5. Можливості щодо адміністрування FortiNAC

Інтерфейс FortiNAC базується на браузері. FortiNAC реєструє відомі пристрої, ізолює невідомі пристрої та визначає, де пристрої підключені до мережі. Пристроями можна керувати або контролювати на основі ролей. Існують різні способи здійснення моніторингу залежно від того, як потрібно контролювати мережу.

Fortinet – це гнучка модульна платформа безпеки, яка дозволяє налаштовувати рішення відповідно до потреб організації.

На рис. 1.10 показана повністю запущена інформаційна панель FortiNAC.

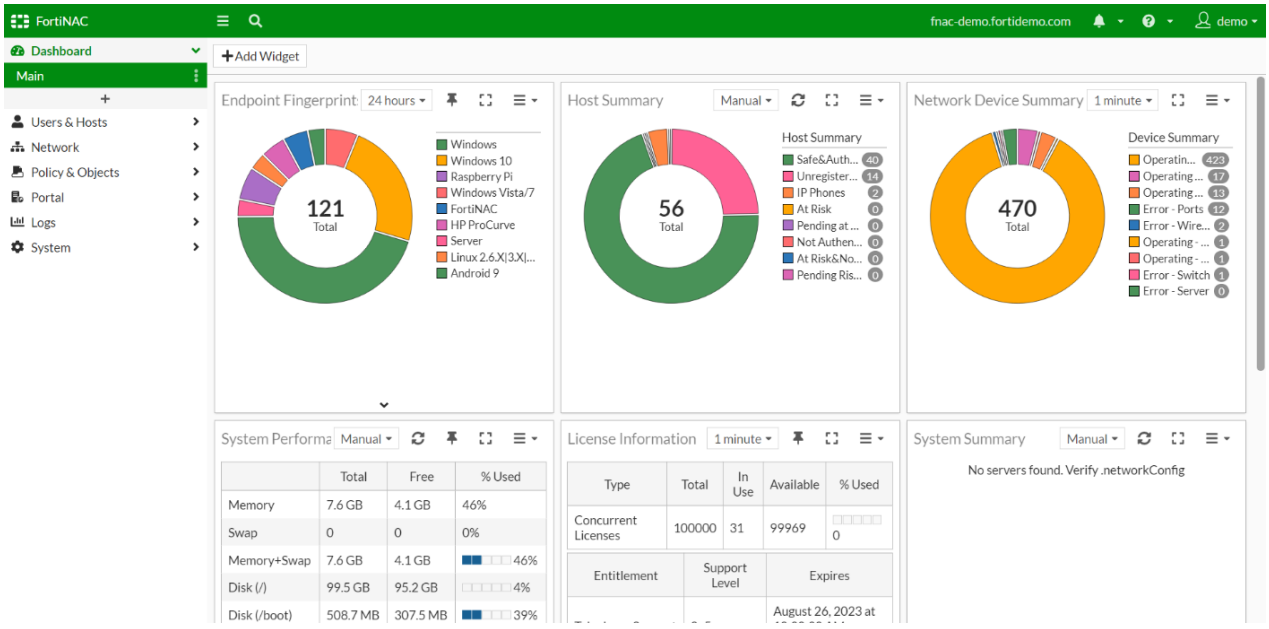


Рис. 1.10. Інформаційна панель FortiNAC

Інформаційна панель

Інформаційна панель FortiNAC відіграє важливу роль у отриманні інформації про всі пристрої підключених до мережі. Оскільки деякі IT-фахівці можуть мати дуже велику кількість пристроїв, інформаційна панель необхідна для отримання загального уявлення про всю мережеву активність.

На інформаційну панель можна добавити додаткові віджети, що збирають інформацію по всій мережі: перелік системи, тривоги, очікувані завдання, мережеві пристрої, RADIUS, доступ до хосту логічної мережі, продуктивність системи, останні хости, цифрові відбитки кінцевої точки, перелік хостів, опис безпеки, активність хостів, опис користувача та результати сканування.

FortiNAC зберігає параметри інформаційної панелі для кожного адміністратора, тому погляди одного адміністратора на той самий пристрій можуть без конфліктів виглядати інакше. Якщо адміністратор не має визначених інформаційних панелей, за замовчуванням для всіх користувачів створюється панель із назвою «main», але це ім’я можна змінити.

Профілі адміністратора – це шаблони, призначені адміністраторам для визначення того, що користувач може робити у FortiNAC. Кожен адміністратор повинен мати профіль адміністратора. Профіль адміністратора можна призначити кільком адміністраторам.

На рис. 1.11 зображено основні функції використання FortiNAC.

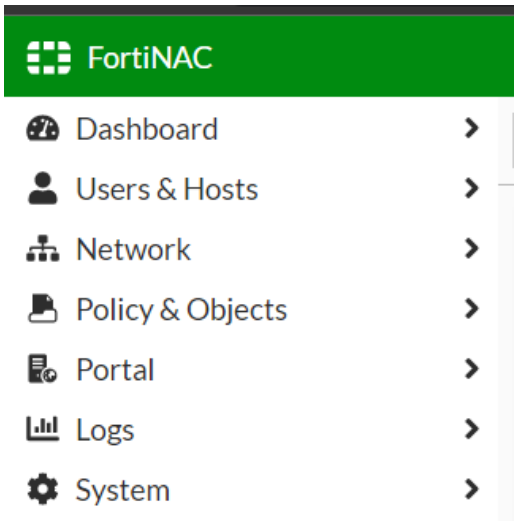


Рис. 1.11. Основні компоненти FortiNAC

Основні компоненти розташовані вздовж лівої частини вікна та містять наступні параметри: інформаційна панель, користувачі і хости, мережа, політика безпеки і об’єкти, портал, журнали та система.

Користувачі та хости

Панель «користувачі та хости» містить елементи керування обліковими записами та пристроями, які показані на рис. 1.12.

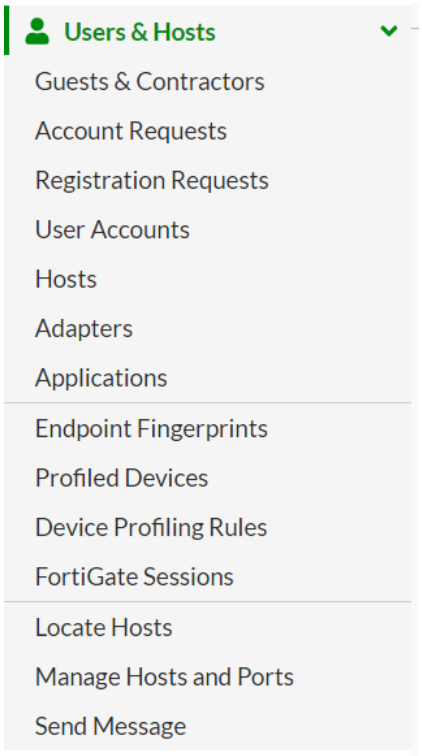


Рис. 1.12. Основні компоненти в панелі користувачів та хостів

Панель гостей та підрядників забезпечує контрольований доступ до мережі для гостей або віддалених учасників конференцій. Менеджер гостей відповідає цим вимогам, надаючи набір інструментів для створення обмежених мережевих облікових записів для гостей і підрядників, заснованими на ролях, і надають доступ протягом певного періоду часу. Крім того, гостів і підрядників можна сканувати, щоб переконатися, що вони мають оновлене антивірусне програмне забезпечення та не становлять загрози для мережі.

Облікові записи користувачів використовуються, щоб додавати, видаляти, змінювати, знаходити та керувати користувачами (гості, підрядники і

адміністратори) у мережі.

Перегляд хостів використовується, щоб додавати, видаляти, змінювати, знаходити та керувати хостами, підключеними до мережі.

Перегляд адаптера використовується, щоб знаходити адаптери, підключені до мережі, і керувати ними.

Перегляд програми є частиною вікна, яке містить параметри меню для користувачів, адаптерів, хостів і програм.

FortiNAC постійно збирає записи ідентифікаційних даних, коли хости підключаються до мережі. Ці записи використовуються для швидкої ідентифікації та класифікації нових пристроїв. Список цих збігів ідентичності пристрою відображається в меню цифрових відбитків кінцевої точки.

Панель «мережа» зображено на рис. 1.13.

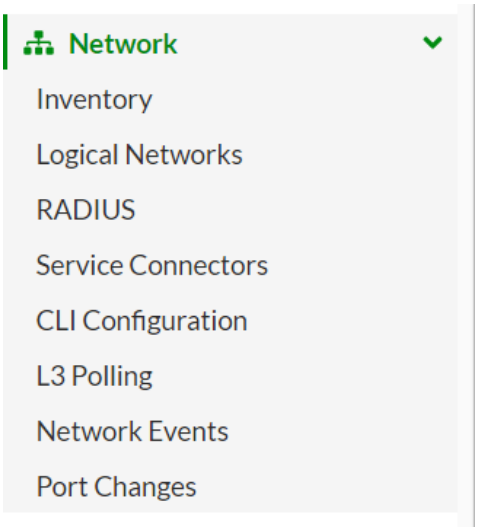


Рис. 1.13. Основні компоненти в панелі мережі

Інвентаризація надає огляд керованої мережі.

Логічні мережі використовуються, щоб відокремити політики доступу до мережі від певних значень пристрою. Кожна логічна мережа має значення доступу, яке перетворюється на фізичне значення пристроїв мережної інфраструктури. FortiNAC використовує це значення для забезпечення відповідного доступу до мережі.

Сервер RADIUS забезпечує зовнішню автентифікацію для користувачів,

підключених до мережевих пристроїв, керованих FortiNAC.

Службові з’єднувачі діють як головна панель для створення та зміни з’єднань і автентифікації між FortiNAC або різними службами.

Конфігурація CLI – це набір команд, які зазвичай використовуються через інтерфейс командного рядка. Вікно конфігурації CLI дозволяє створювати окремі набори команд, називати їх і потім повторно використовувати для керування портами, VLAN або доступом хоста до мережі.

Функція L2 Polling використовується FortiNAC, щоб дізнатися, де хости підключені в мережі на основі їх MAC-адрес.

L3 Polling запускає перетворення IP-адреси на MAC-адресу. На основі отриманої інформації FortiNAC визначає MAC-адреси, пов’язані з IP-адресами для хостів та інших пристроїв у мережі.

Перегляд мережевих подій відображає вміст журналу підключень: список історичних мережевих подій хоста/користувача.

На рис. 1.14 показана панель «політика безпеки та об'єкти».

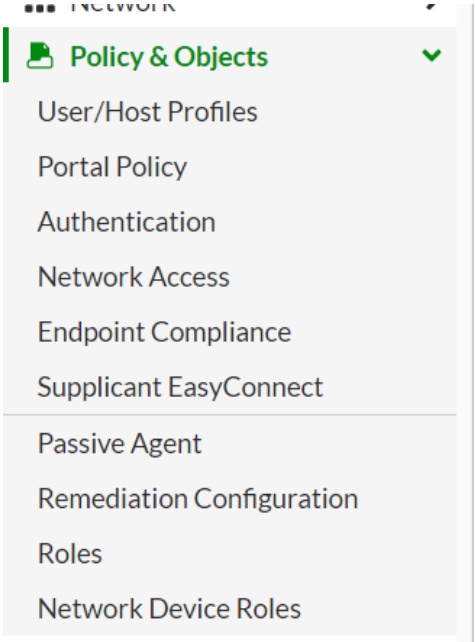


Рис. 1.14. Основні компоненти в панелі політики безпеки та об’єктів

Профілі користувачів/хостів використовуються для зіставлення наборів хостів і користувачів із політиками доступу до мережі, політиками відповідності

кінцевих точок, політиками Supplicant EasyConnect, політиками порталу або правилами безпеки.

Політика порталу складається з одного профілю користувача/хоста та однієї конфігурації порталу.

Політика автентифікації складається з одного профілю користувача/хоста та однієї конфігурації автентифікації. Конфігурація автентифікації призначає обробку, яку отримують користувачі та хости під час підключення до мережі.

Політика доступу до мережі складається з одного профілю користувача/хоста та однієї конфігурації доступу до мережі. Конфігурація доступу до мережі визначає VLAN, CLI або групову політику VPN, які застосовуються до хоста, якому потрібен доступ до мережі. Якщо користувач або хост збігається з вибраним профілем користувача/хоста, їм надається доступ до мережі, визначений у конфігурації.

Відповідність кінцевої точки – це набір функцій, що використовується для забезпечення того, щоб вузли, що підключаються до мережі, відповідали вимогам щодо використання мережі. Якщо не створити політики, коли вузли підключаються до мережі або користувачі вводять свої облікові дані, вони будуть автоматично зареєстровані без застосування політики.

Реєстрація пасивного агента дозволяє створювати індивідуальні конфігурації, які реєструють і сканують хости, пов’язані з користувачами мережі, які містяться у LDAP або Active Directory.

Конфігурація виправлення використовується, щоб налаштувати конфігурації сканування адміністратора, які пов’язані з такими параметрами, як заборона доступу для гостей або інших користувачів за часом доби або днем тижня.

Ролі можна використовувати для фільтрації конкретних користувачів або хостів під час застосування політик доступу до мережі, політик відповідності кінцевих точок і політик Supplicant EasyConnect.

Ролі мережевих пристроїв дають змогу зіставляти ролі пристроїв і місця підключення до конфігурацій мережного доступу. Ці ролі застосовуються лише до хостів, керованих в інвентарі, таких як принтер та пристрої.

Панель «мережева активність RADIUS» відображає активність

автентифікації RADIUS у мережі. Ця активність відстежується шляхом періодичного створення моментального знімка, який підраховує останні відповіді щодо прийняття та відхилення доступу, та відбувається з 5-хвилинними інтервалами. Для відхилених запитів автентифікації кількість помилок відстежується з унікальної причини. Це дозволяє адміністратору побачити, чи є якісь проблеми з автентифікацією в мережі, особливо, якщо щодня реєструються тисячі хостів.

Вікно конфігурації порталу використовується для налаштування вмісту та макета сторінок порталу, з якими користувачі мережі стикаються, коли їхні пристрої чи хости незареєстровані.

Програма FortiNAC розділена на два основні компоненти, перший – це адміністративні компоненти, а другий – компоненти кінцевого користувача. Основною частиною програми для кінцевого користувача є портал. Портал – це серія настроюваних веб-сторінок, які направляють кінцевого користувача, членів організації клієнта, через процес автентифікації, сканування та реєстрації свого пристрою в мережі.

На рис. 1.15 показано панель «журнали».

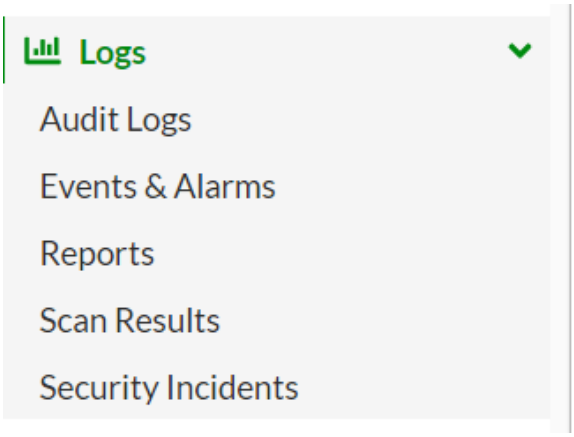


Рис. 1.15. Основні компоненти в панелі журнали

Журнал аудиту відстежує всі зміни, внесені до елемента в системі. Адміністратори бачитимуть зміни в журналі аудиту щоразу, коли дані додаються, змінюються чи видаляються. Користувачі можуть бачити, що було змінено, коли

було внесено зміни та хто вніс зміни.

Події відображає вміст журналу подій. Журнал подій – це контрольний журнал важливих інцидентів у мережі та FortiNAC. Якщо переглядати подію, вона містить таку інформацію, як ім’я користувача, IP-адреса, MAC-адреса або місцезнаходження.

Тривога відображає усі останні аварійні сигнали, що відбулися в системі. Він складається з стовпців, які вказують наскільки серйозним є тривога. Всього декілька рівнів: критичний, незначний, попередження, інформаційний.

Звіти використовуються, щоб переглядати стандартні та створювати спеціальні звіти на основі інформації в базі даних. Дані можна виводити у форматах HTML, CSV, EXCEL, XML, RTF і PDF. Шаблони звітів включають: реєстрацію гостей, реєстрацію та результати сканування.

Перегляд результатів сканування відображає результати, які зберігаються в базі даних FortiNAC щодо розчинного агента, постійного агента та сканування системи.

Інциденти безпеки інтегрується з такими рішеннями безпеки, як FireEye, Fortinet і Palo Alto Networks, щоб корелювати сповіщення безпеки. Вхідна інформація нормалізується в узгоджений формат подій безпеки та надає додаткову інформацію про вихідні хости.

Інциденти безпеки ізолюють, обмежують або блокують скомпрометовані кінцеві точки та скорочують час стримування загрози за допомогою:

автоматизації дій щодо події на основі політик;

надання інформації в сповіщеннях безпеки;

визначення пріоритетів подій безпеки;

відстеження загрози в IT-доменах і автоматизація дій для мінімізації часу стримування загрози.

Інший компонент FortiNAC є «система».

Керування сертифікатами надає користувачам можливість керувати сертифікатами з різними схемами кодування та форматами файлів. Перегляд керування сертифікатами показує сертифікати, які наразі встановлено у Fortinet.

Користувачі можуть створювати та встановлювати сертифікати сервера для інтерфейсу адміністратора.

Групи дозволяють об’єднувати подібні елементи. Створюючи групи, позбавляється необхідність окремо налаштовувати та керувати елементами в межах групи.

Видимість функцій надає можливість увімкнути або вимкнути структурні зміни видимості стилю FortiNAC.

Використання панель графіки дає можливість додавати, змінювати та видаляти заплановані завдання у Fortinet. Завдання – це дія, виконання якої заплановано на визначений час і зазвичай пов’язане з певною групою. Існує два типи планування: фіксований день і повторюваний.

Будь-які призначені активні завдання відображатимуться у верхньому правому куті сторінки FortiNAC під новою піктограмою сповіщення дзвіночка. Кожне завдання має повідомлення, піктограму, яка показує, кому воно призначено. Дії, які можна виконати, відображаються за допомогою кнопок у верхній частині сторінки FortiNAC. Можна створювати завдання, редагувати завдання, позначати завдання як виконані або взагалі видаляти їх.

Перегляд налаштувань надає доступ до параметрів глобальної конфігурації системи, таких як властивості старіння для видалення хостів і користувачів із бази даних або параметри електронної пошти для надсилання електронних листів користувачам і адміністраторам.

FortiNAC спрощує IT-операції, надаючи адміністраторам можливість створювати політики безпеки, які автоматизують контроль доступу до мережі. Крім того, політики доступу до мережі гарантують безпеку конфіденційних ресурсів, відстежуючи, яким користувачам дозволено доступ, деталізуючи, які користувачі вже могли отримати доступ до цих ресурсів, і гарантуючи, що конфіденційна інформація залишається конфіденційною.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ FORTINAC

3.1. Розроблення варіанта технології управління доступом до мережі організації на базі FortiNAC

FortiNAC забезпечує моніторинг всієї корпоративної мережі. Це дозволяє рішенню реєструвати відомі пристрої, ізолювати невідомі пристрої та бачити, де пристрої підключені до мережі. Пристроями можна керувати або контролювати їх на основі ролей.

Сценарій застосування FortiNAC може складатися з динамічного профілювання пристроїв, як показано на рис. 1.16.

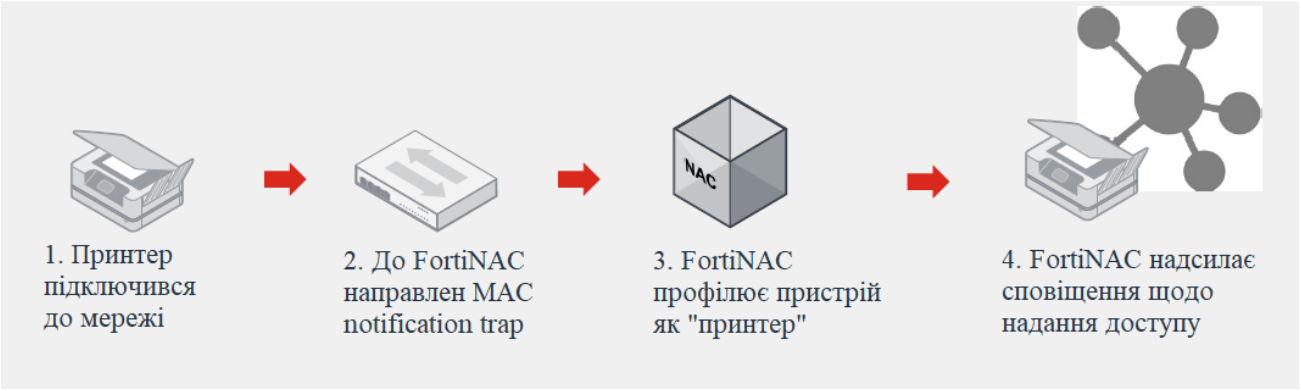


Рис. 1.16. Динамічне профілювання пристроїв

У середовищі, де FortiNAC контролює велику кількість пристроїв та портів, на комутаторах, які підтримують сповіщення MAC SNMP, рекомендується використовувати MAC Notification Trap замість стандартних перехоплень linkUp і linkDown для підвищення продуктивності.

Перехоплення сповіщень MAC спрацьовує за такими умовами:

додавання – пристрій вперше генерує трафік;

видалення – MAC видаляється з адресної таблиці;

змінювання – пристрій, MAC-адреса якого вже розпізнано на порту,

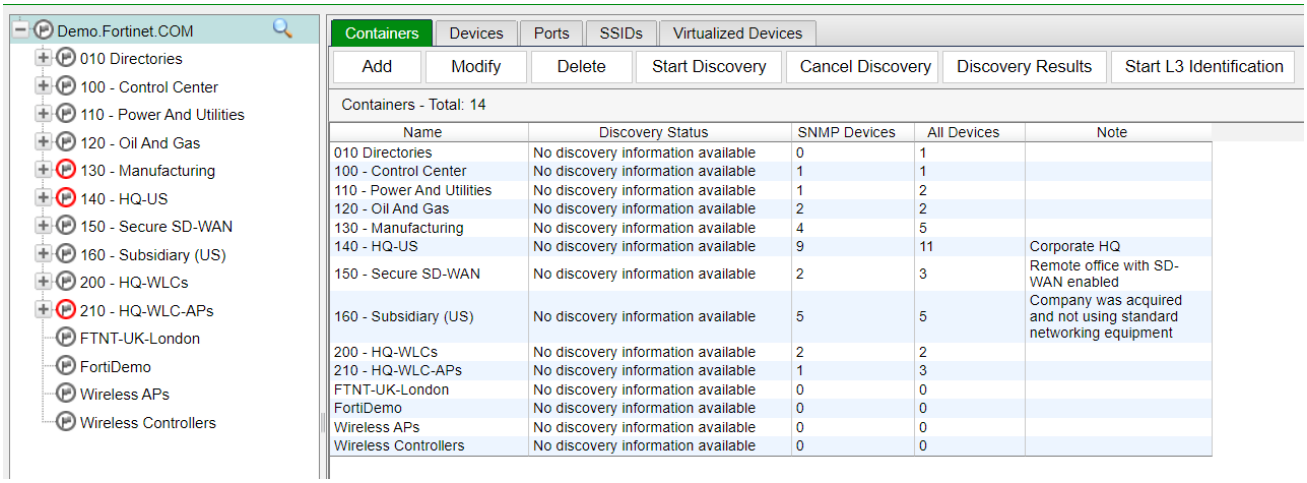
переміщується, потім підключається до іншого порту та генерує трафік.

Підключити FortiNAC до відомих пристроїв можна кількома способами. Однак слід почати з комутаторів, маршрутизаторів і контролерів, оскільки ці пристрої контролюють мережу та надають FortiNAC інформацію про інші пристрої, що підключені до мережі. Їх можна імпортувати із файлів .csv або FortiNAC може автоматично їх виявити.

Виявлення – це автоматизований процес, запущений адміністратором FortiNAC. Рішення шукає діапазони IP-адрес для пристроїв, якими можна керувати за допомогою SNMP. Модель кожного пристрою створюється у FortiNAC у міру виявлення, і її можна переглянути в панелі «мережеві пристрої». Після виявлення кожен пристрій необхідно налаштувати, щоб FortiNAC мав правильні паролі CLI та конфігурації VLAN.

У FortiNAC є багато варіантів перегляду пристроїв, а саме через панель «інвентаризація», «перегляд хоста» та «інформаційна панель».

Інвентаризація надає огляд керованої мережі, що знаходиться в панелі «мережа» і зображено на рис. 1.17. Вона складається з FortiNAC і контейнерів, створених користувачами. Створені користувачами контейнери містять керовані мережеві пристрої. Значки пристроїв змінюються на червоні, якщо зв’язок втрачено. Панель зверху справа відображає вкладки контейнерів, пристроїв, портів і SSID.



Name	Discovery Status	SNMP Devices	All Devices	Note
010 Directories	No discovery information available	0	1	
100 - Control Center	No discovery information available	1	1	
110 - Power And Utilities	No discovery information available	1	2	
120 - Oil And Gas	No discovery information available	2	2	
130 - Manufacturing	No discovery information available	4	5	
140 - HQ-US	No discovery information available	9	11	Corporate HQ
150 - Secure SD-WAN	No discovery information available	2	3	Remote office with SD-WAN enabled
160 - Subsidiary (US)	No discovery information available	5	5	Company was acquired and not using standard networking equipment
200 - HQ-WLCs	No discovery information available	2	2	
210 - HQ-WLC-APs	No discovery information available	1	3	
FTNT-UK-London	No discovery information available	0	0	
FortiDemo	No discovery information available	0	0	
Wireless APs	No discovery information available	0	0	
Wireless Controllers	No discovery information available	0	0	

Рис. 1.17. Огляд керованої мережі

Більшість мереж також мають серію пристроїв, якими не можна керувати за допомогою SNMP, наприклад принтери, камери безпеки або системи сигналізації. Цей тип пристроїв називають пристроями з можливістю ping. Пристрої без SNMP можна імпортувати в базу даних, вручну або автоматично зареєструвати за допомогою профілювання пристроїв.

Зареєструвати персональний комп'ютер в FortiNAC як пристрої можна вручну, підключивши його до мережі. Але після підключення вони створюються як фальшиві хости. Якщо шахрайським хостам заборонено доступ до мережі, вони вимикаються. Для реєстрації вручну потрібно перейти в панель «хости» або «адаптери», що знаходиться в «користувачі та хости», далі потрібно обрати пристрій і натиснути «зареєструвати як пристрій».

На рис. 1.18 показано вікно редагування пристрою.

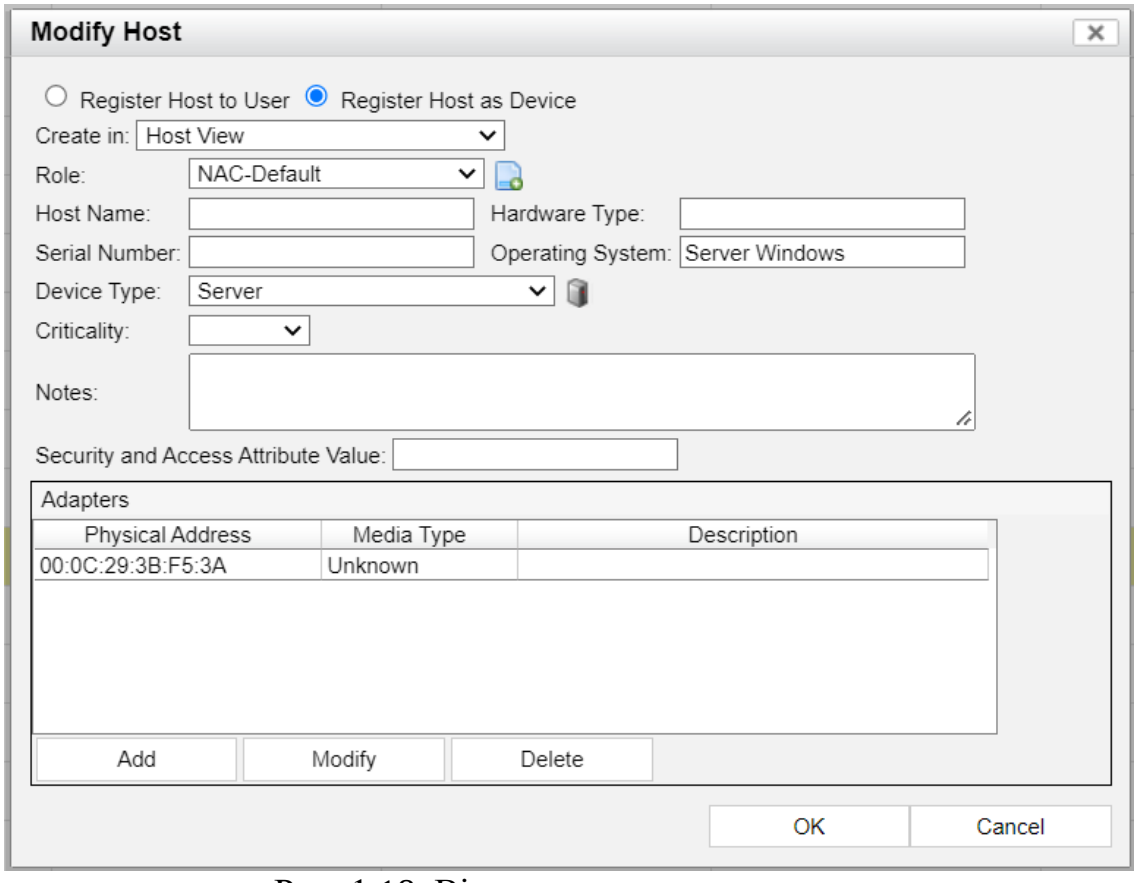


Рис. 1.18. Вікно редагування пристрою

У вікні реєстрації пристрою є кілька налаштувань: місце розташування, тип

пристрою, роль, назва хоста, тип обладнання, операційна система та адаптер пристрою.

Профілі користувачів/хостів використовуються для зіставлення наборів хостів/користувачів із політиками доступу до мережі, політиками відповідності кінцевих точок, політиками Supplicant EasyConnect, політиками порталу або правилами безпеки. Профілі користувача/хоста можна повторно використовувати в різних політиках.

Наприклад, політики доступу до мережі використовуються для призначення VLAN, у якій розміщено хост. Кожна політика доступу до мережі має певний профіль користувача/хоста та конфігурацію доступу до мережі, яка містить VLAN, конфігурацію CLI або групу VPN. Коли хосту потрібен доступ до мережі, FortiNAC переглядає політики доступу до мережі, починаючи з першої у списку, і перевіряє, чи збігається профіль. Якщо ні, перевіряється наступна політика доступу до мережі, доки не буде знайдено збіг.

На рис. 1.19. показано вікно додавання профілю користувач/хост.

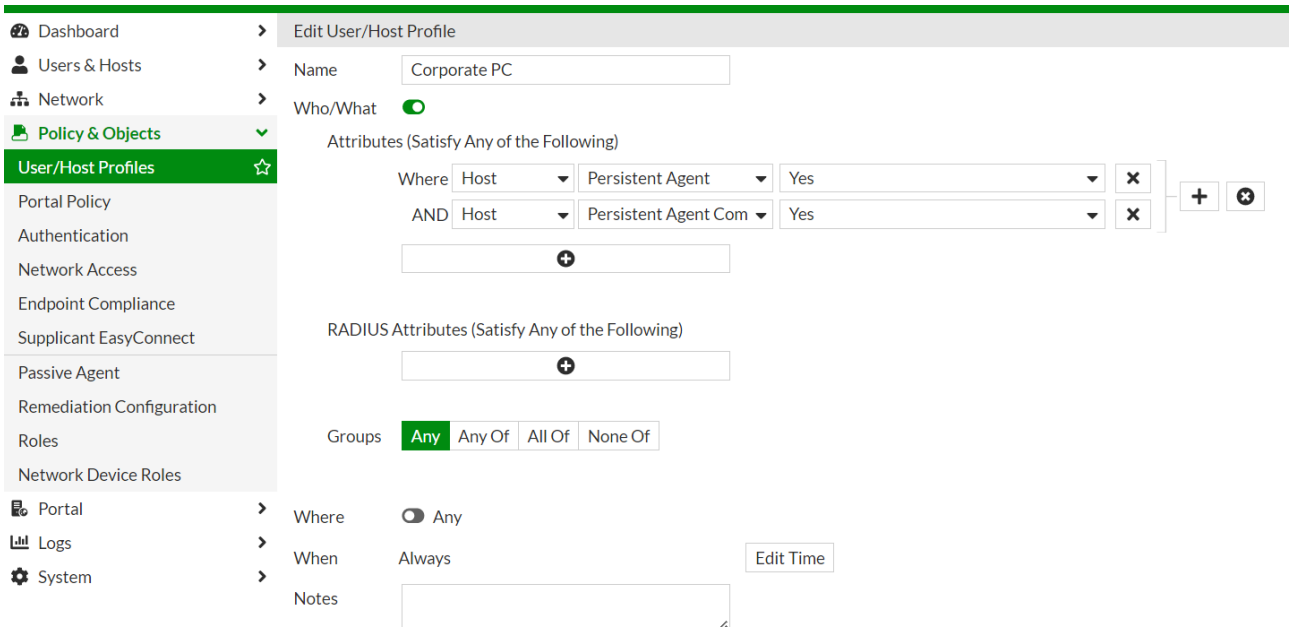


Рис. 1.19. Вікно додавання профілю

Для створення нового профілю йому призначається назва, місце розташування; фільтр профілю, який базується на даних адаптера, хоста чи

користувача; фільтр атрибуту RADIUS, що використовуються для зіставлення кінцевих точок до та після автентифікації; параметр часу, в якому хост може знаходиться в мережі протягом зазначеного періоду часу.

Сценарії входу можна використовувати для автоматичної реєстрації персонального комп'ютера під час входу користувачів в мережу. Для цього потрібно створити одну або кілька політик безпеки.

В меню «політика та об'єкти» в панелі «відповідність кінцевої точки» створюється політика безпеки, що показано на рис. 1.20. В вікні можна ввести найменування, конфігурацію відповідності кінцевої точки або визначати профіль користувача/хоста.

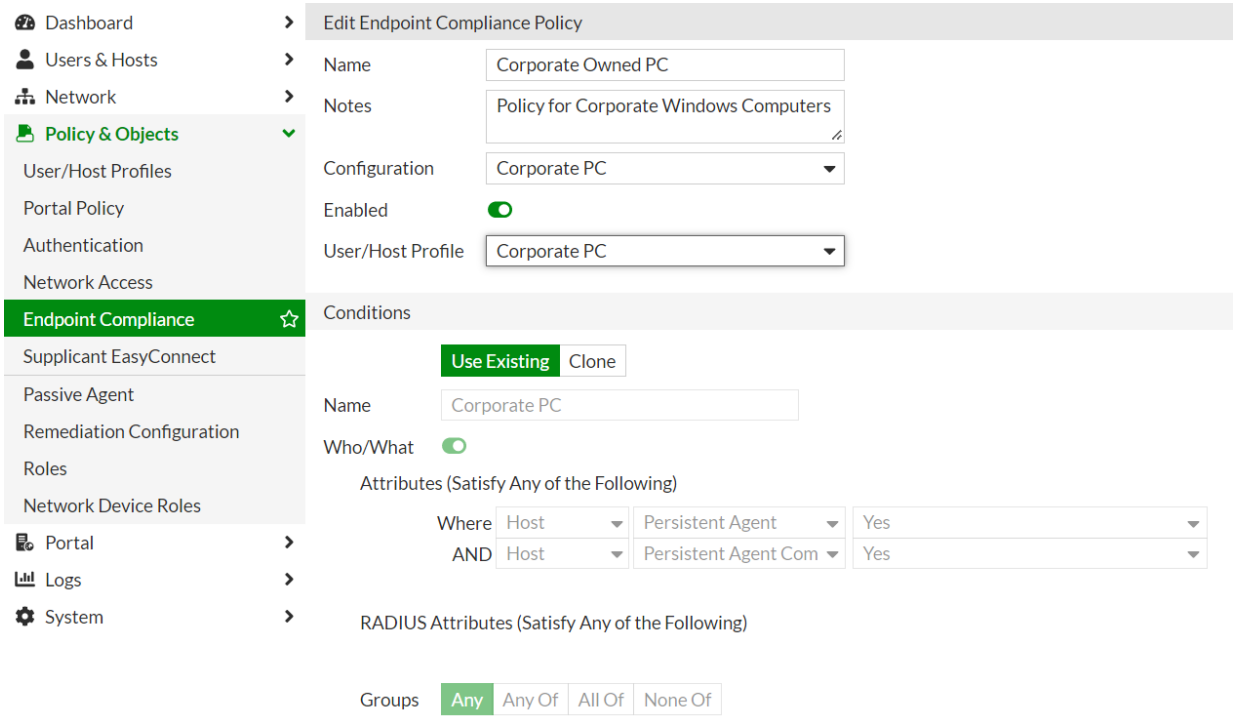


Рис. 1.20. Вікно редагування політики безпеки

FortiNAC має можливість зберігати та використовувати набори команд CLI. Ці набори команд можуть бути дуже потужними під час керування пристроями та мають кілька варіантів реалізації. В прикладі, CLI реалізується за роллю, призначеною пристрою, і портом, до якого він підключається. Ролі мережевих пристроїв дозволяють контролювати доступ до мережі на основі комбінацій пристроїв і місць підключення. Кожну створену роль можна застосувати до

окремих пристроїв.

Для налаштування гостя в панелі «роль», спочатку потрібно в панелі «мережа» обрати «логічні мережі», щоб відокремити політики доступу до мережі від значень, специфічних для пристрою. Кожна логічна мережа має значення доступу, яке перекладається на фізичне значення пристроїв мережевої інфраструктури. Після створення логічної мережі можна призначити значення доступу для окремих пристроїв, а потім призначити конфігурацію в панелі «доступ до мережі».

На рис. 1.21 показано вікно редагування політики доступу до мережі.

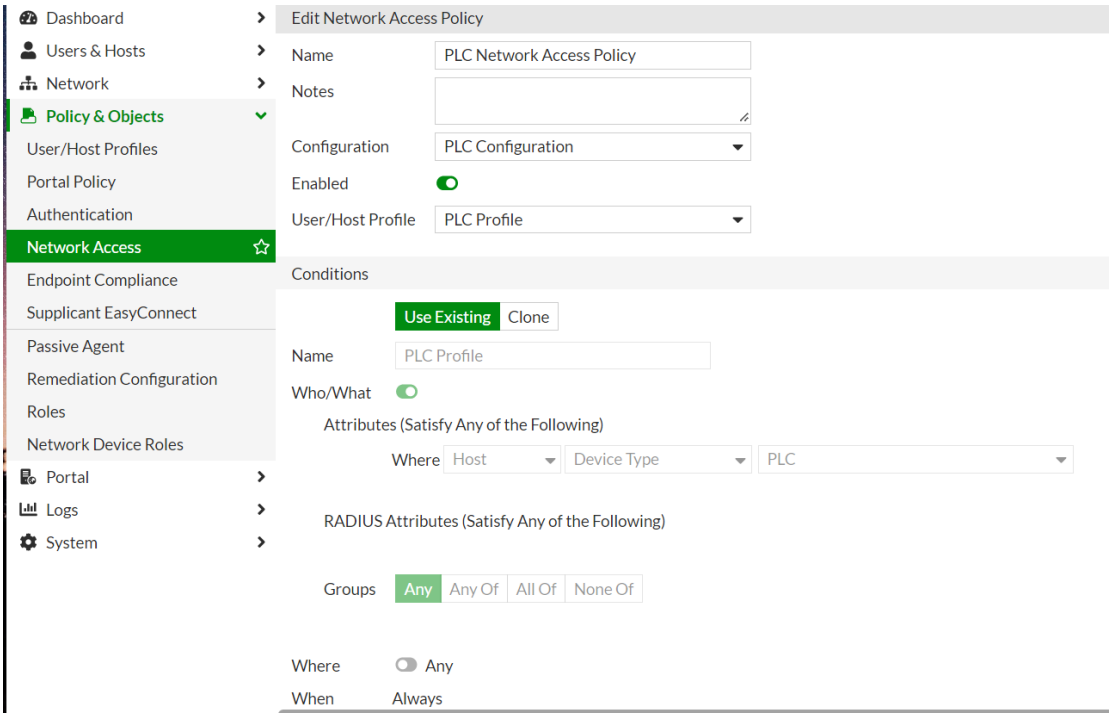


Рис. 1.21 Редагування політики доступу до мережі

Під час реєстрації кожному пристрою у FortiNAC призначається роль NAC за замовчуванням. Лише ті пристрої, які зареєстровані та налаштовані для керування в панелі «інвентаризація», можуть використовувати доступ на основі ролей. Ролі можна призначати користувачам, хостам, мережевим пристроям і портам.

Меню «правила профілювання пристрою», що заходиться в панелі «користувачі/хости» відображає стандартний набір правил. Меню можна

використати, щоб змінити стандартні правила або створити власний набір правил.

На рис. 1.22 зображено вікно редагування правила профілювання пристрою.

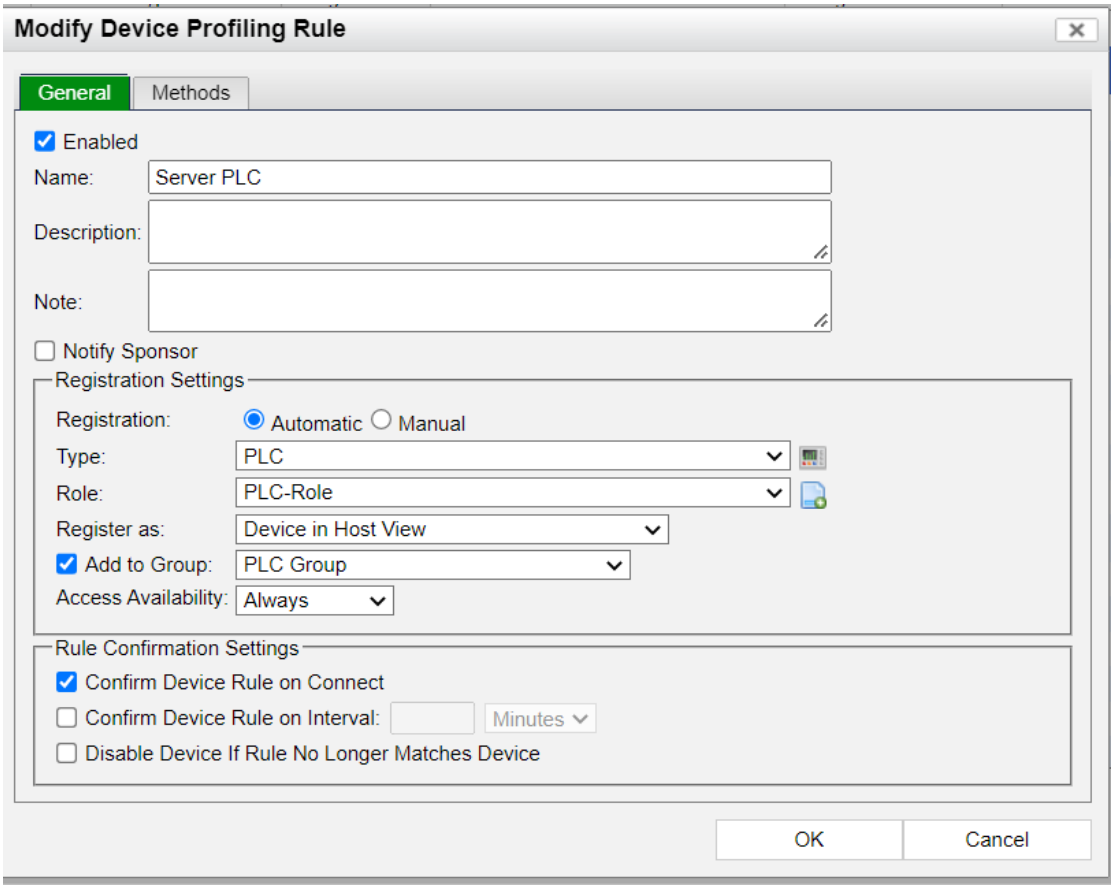


Рис. 1.22. Вікно редагування правила профілювання пристрою

Для прикладу було обрано програмований логічний контролер, тому що він підтримує IoT та є незахищеним в мережі організації, також він входить до сегменту управління процесами.

В вікні можна включити пристрій, обрати ім’я, опис та нотатки. Якщо вибрана функція «повідомити спонсора», адміністратори з дозволом на керування пристроями, пов’язаними з цим правилом, отримають сповіщення, коли новий пристрій відповідає правилу.

Параметри реєстрація включають ручну або автоматичну реєстрацію, тип пристрою, тип доступу на основі ролей; місце розміщення у FortiNAC, додавання пристрою до групи та час доступу до мережі. В прикладі створений профіль пристрою було додано до типу, ролі і групи PLC.

Параметри підтвердження правил включають: під час підключення пристрою або за інтервалом підключення або вимкнення пристрою, якщо правило більше не відповідає.

На вкладці «методи» можна обрати один або кілька методів для ідентифікації пристрою, як показано на рис. 1.23.

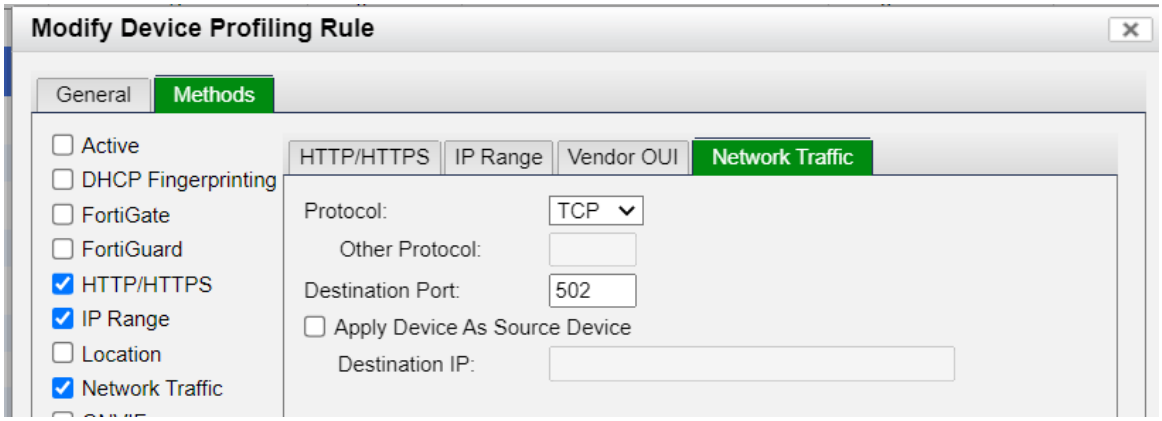


Рис. 1.23. Вікно методів профілювання пристрою

Для прикладу були вибрані HTTP/HTTPS, IP Range, Vendor OUI та Network Traffic.

Метод HTTP/HTTPS – URL-запит з автентифікацією або без неї і є необхідним для налаштування безпечного з'єднання HTTP. В вікні налаштування потрібно вибрати протокол, порт і посилання. Якщо необхідно можна вказати облікові дані користувача.

Метод IP Range – порівнює IP-адресу пристрою з указаним діапазоном IP-адрес.

Метод Vendor OUI визначає відповідність правил за допомогою OUI постачальника. До цього правила можна додати код постачальника, назву постачальника, псевдонім постачальника, який існує в базі даних постачальників FortiNAC, та тип пристрою. Але якщо обрати тип пристрою, пов'язаний із пристроєм для підключення, він має збігатися з типом пристрою постачальника в базі даних FortiNAC.

Метод Network Traffic оцінює тип пристрою на основі інформації про сеанс

FortiGate. У вікні налаштування треба встановити протокол TCP, UDP або інший. В прикладі обрано TCP та порт 502, що є одним із основних протоколів у мережах TCP/IP.

Для підтвердження правила профілювання пристрою потрібно перейти до панелі «користувачі/хости» та «адаптери», знайти MAC-адреси фальшивого пристрою, який повинний відповідати правилу, натиснути на нього та обрати правило, яке потрібно перевірити.

Коли пристрої реєструються, підключаються та від'єднуються від мережі, збираються дані для всіх цих транзакцій. Крім того, події та тривоги генеруються залежно від активності пристрою. Журнали та звіти відображають активність пристрою.

Керування подіями дозволяє вказати, які події генерувати та чи реєструвати записи подій на іншому сервері. Можна обмежити кількість генерованих подій, вибравши групу для кожної. Повідомлення створюються лише тоді, коли подія відбувається в межах зазначеної групи. Можна ввімкнути подію на короткий проміжок часу, наприклад, щоб знайти певний хост, коли він підключається до мережі.

На рис. 1.24 зображено події FortiNAC.

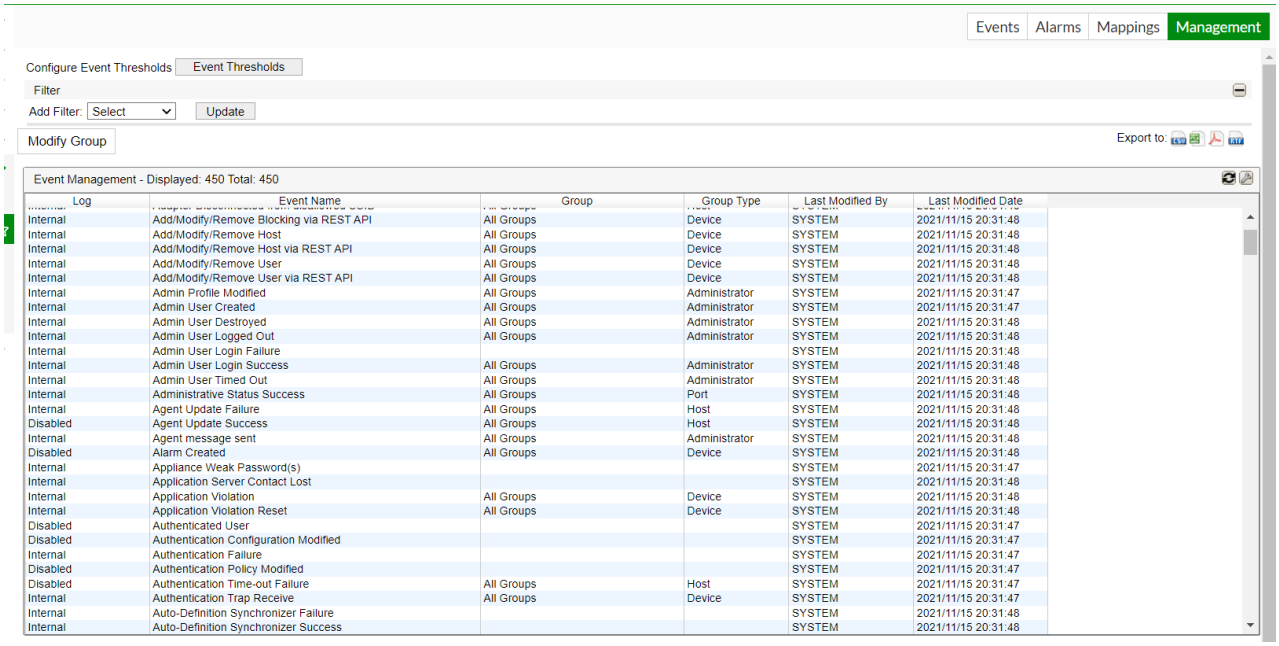


Рис. 1.24. Керування подіями

Панель «інциденти безпеки» дозволяє створювати правила безпеки, які запускатимуться на основі визначених адміністратором шаблонів подій безпеки для генерування сигналів безпеки. Правила безпеки можна націлити на генерування тривоги лише для певних хостів або користувачів. В панелі також можна автоматично ізолювати або блокувати скомпрометовані хости.

На рис. 1.25 зображено вікно «зміни правила безпеки».

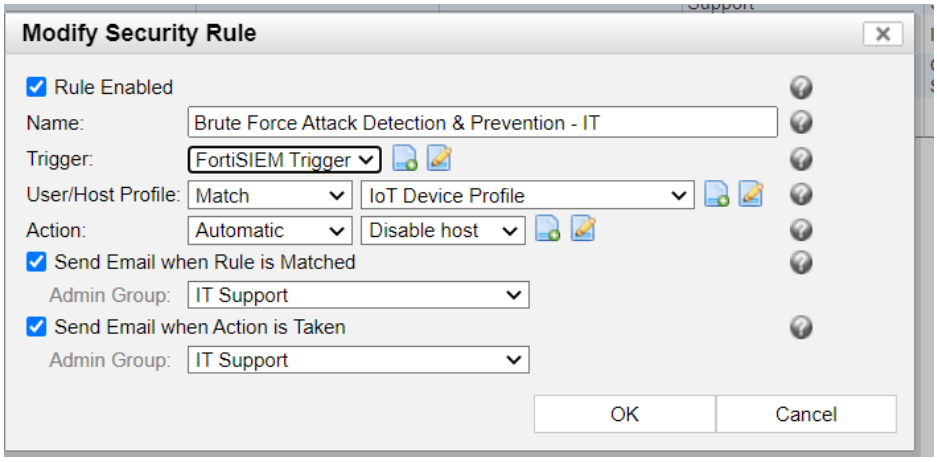


Рис. 1.25. Зміна правила безпеки

Після налаштування мережевих пристроїв необхідно створити правила безпеки. Правила безпеки містять тригери, які корелюють вхідні події від мережевих пристроїв і створюють тривогу. Для цього потрібно перейти в меню «журнали», а потім в панель «інциденти безпеки».

У вікні можна ввести назву; визначити тригер, який активує правило; вказати чи має правило відповідати профілю хоста, вибраному в розкривному меню; призначити автоматично чи вручну дію правилу безпеки, та вказати, щоб створена подія автоматично надсилала електронний лист вибраній групі адміністраторів, коли створюється новий сигнал тривоги.

Інциденти безпеки інтегруються з такими рішеннями, як FireEye, Fortinet і Palo Alto Networks, щоб корелювати сповіщення безпеки. Вхідна інформація нормалізується в узгоджений формат подій безпеки та надає додаткову інформацію про вихідні хости.

3.2. Технологія управління додатками FortiNAC

В FortiNAC є головна панель для створення та зміни з'єднань і автентифікації між рішенням та різними службами.

На рис. 1.26 показано головне меню «інтеграція з додатками», що знаходиться в панелі «мережа».

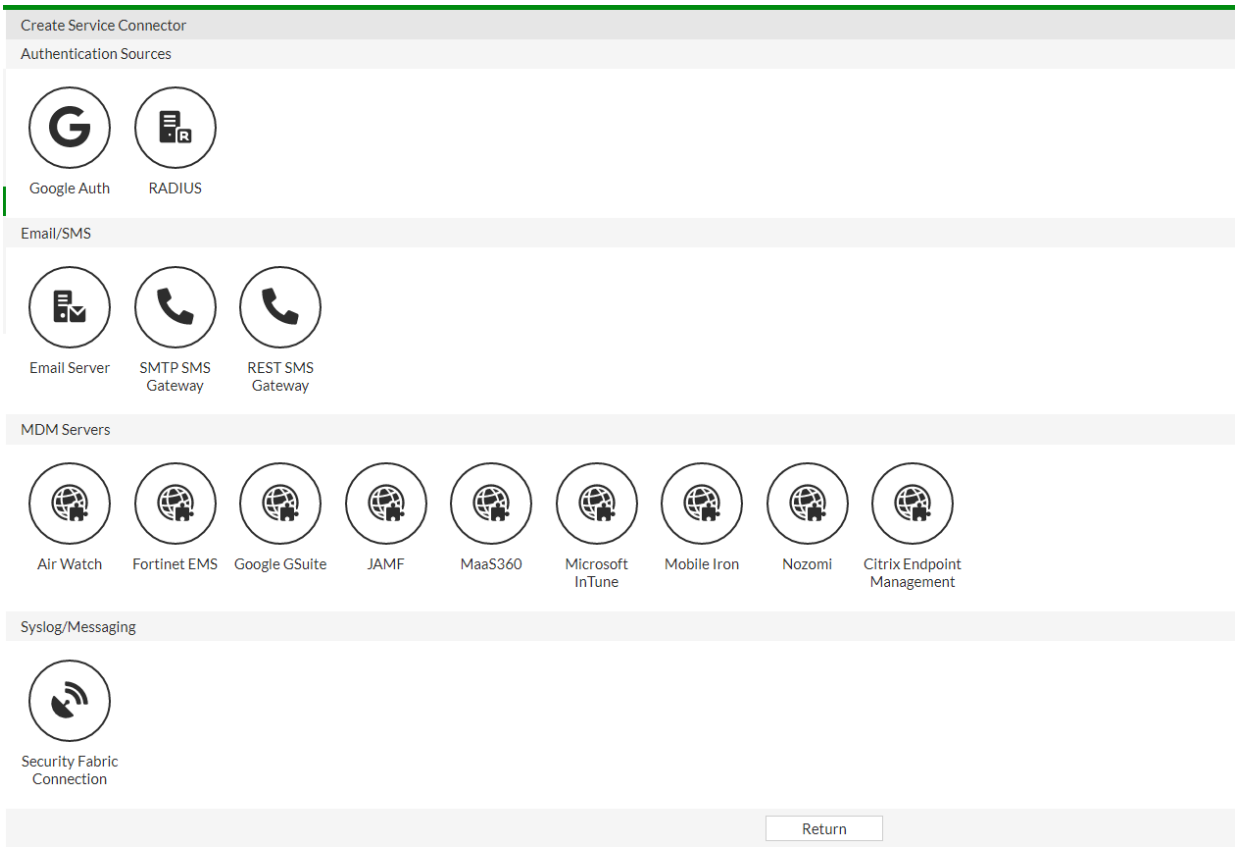


Рис. 1.26. Створення інтеграції з додатками

Сервіси MDM дозволяють налаштувати з'єднання або інтеграцію між FortiNAC і системою керування мобільними пристроями. Вони працюють разом, обмінюючись даними через API для захисту мережі. FortiNAC використовує дані в базі даних MDM і реєструє хости, коли вони підключаються до мережі.

Список серверів MDM включає: Air Watch, Fortinet EMS, Google GSuite, JAMF, MaaS360, MicrosoftInTune, Mobile Iron, Nozomi, Citrix Endpoint Management.

Увімкнення автентифікації дозволяє адміністратору визначати, чи будуть хости, які підключаються до мережі, проходити примусову автентифікацію. Хостів

можна повторно автентифікувати через певний період часу. Це об’єднує параметри підключення для автентифікації за допомогою облікового запису Google і налаштування серверів RADIUS для автентифікації користувачів.

Аутентифікація Google дозволяє користувачам проходити автентифікацію за допомогою облікового запису Google. Після налаштування параметрів користувач входить у мережу, використовуючи свій обліковий запис Google. Після автентифікації користувача його ім’я, адреса електронної пошти та домен передається FortiNAC для перевірки з наданою інформацією.

RADIUS – це мережевий протокол, який забезпечує централізований доступ, авторизацію та керування обліковим записом для підключення та використання мережевої служби.

Сервер RADIUS забезпечує зовнішню автентифікацію для користувачів, підключених до мережевих пристроїв, керованих FortiNAC. Цей тип сервера часто використовується в бездротовому середовищі, але також використовується в дротовому середовищі, що підтримує автентифікацію 802.1x.

Системний журнал/повідомлення використовує Fortinet Security Fabric, що забезпечує інтелектуальну архітектуру, яка об’єднує окремі рішення безпеки в єдине ціле для виявлення, моніторингу, блокування та усунення атак на всій поверхні атаки. Він забезпечує широкий захист і видимість для кожного сегмента мережі та пристрою, будь то апаратне, віртуальне чи хмарне.

Електронна пошта/SMS використовується для надсилання сповіщень, та включає: Email Server; SMTP SMS Gateway та REST SMS Gateway, що дозволяє автоматично надсилати й отримувати текстові SMS-повідомлення з будь-якої програми надсилання електронної пошти.

FortiNAC має можливість надсилати SMS-повідомлення адміністраторам, гостям або користувачам. Ці повідомлення використовуються для надання гостям імен користувачів і паролів, сповіщення адміністраторам про спрацьовування тривоги або сповіщення користувача про спрацьовування тривоги на основі його хоста.

3.3. Розроблення рекомендацій щодо застосування технології управління доступом до мережі організації

З розвитком BYOD та IoT, особливо в промислових середовищах – програмне забезпечення для управління доступом до мережі стало обов'язковим компонентом у інструментарії захисту інформації. Він гарантує, що доступ через ці пристрої залишається безпечним, навіть якщо вони працюють у домашній мережі чи загальнодоступній Wi-Fi.

Ключовим елементом належного проектування мережі є підтримка комплексних послуг безпеки для всіх аспектів роботи мережі. Багаторівневий підхід до безпеки також потрібен для захисту мережі, центрів обробки даних, мережевих пристроїв, служб і програм від зовнішніх або навіть внутрішніх атак.

Традиційні стратегії контролю доступу за своєю суттю довіряють користувачу або пристрою в мережі. Це поняття довіри часто базується на місцезнаходження користувача або пристрою: якщо вони в мережі, їм довіряють. Але оскільки периметр мережі продовжує зникати, захистити мережеві ресурси стає все важче. Тепер користувачі отримують доступ до корпоративної мережі з домашніх офісів і мобільних пристроїв. Корпоративні ресурси також дедалі частіше розміщуються в різних місцях за межами традиційної мережі, наприклад у приватних і публічних хмарах.

Щоб подолати обмеження традиційного контролю доступу, організаціям потрібне рішення NAC, яке забезпечує:

постійну перевірку користувачів і пристроїв;

ретельну сегментацію мережі для створення зон контролю, що допомагає обмежити вплив злому та встановити більше контрольних точок;

доступ із найменшими привілеями для користувачів і пристроїв, тому користувачам надається лише той доступ, який їм необхідний для виконання своїх ролей, що допомагає обмежити вплив скомпрометованої особи чи пристрою.

NAC є ключовим рішенням для контролю доступу до кінцевих систем на основі ідентифікації користувача і оцінки стану, та відіграє важливу роль у

розробці централізованої багаторівневої архітектури безпеки, яка дозволяє серверу NAC діяти як точка прийняття рішень. Впровадження рішень NAC є важливим кроком до інтеграції окремих продуктів безпеки в мережу шляхом використання функцій каталогів, серверів AAA, пристроїв мережної інфраструктури та програмного забезпечення безпеки кінцевих точок у процесі динамічного надання доступу до мережі для кожного користувача та кінцевого пристрою. Більшість рішень NAC включають функції автентифікації, відповідності кінцевих точок, виправлення та застосування політик у процесі перевірки ідентифікації користувача та стану безпеки хостів перед наданням доступу до мережі. NAC вносить інформацію про ідентифікацію та відповідність вимогам до сегментації та управління доступом, його положення в центрі мережі робить його центральним менеджером безпеки.

Рекомендації щодо застосування технології управління доступом до мережі організації:

Забезпечення захисту пристроїв IoT та мереж, до яких вони підключені, має включати принципи нульової довіри, у тому числі жорстке керування контролем доступу. У корпоративних мережах, де поширені пристрої IoT дуже важливо, щоб фахівці з кібербезпеки могли:

зрозуміти, які пристрої IoT розгортаються, переглядаючи та профілюючи кожен пристрій, що підключається до мережі;

управляти доступом до мережі, включаючи не тільки те, які пристрої підключаються до мережі, але й те, до яких областей мережі можуть отримати доступ пристрої IoT;

відстежувати пристрої IoT, коли вони підключені до мережі, щоб гарантувати постійний доступ та захист пристроїв від компрометації;

автоматично вживати негайних дій у разі компрометації пристрою або інших проблем безпеки.

Фахівці з кібербезпеки повинні мати можливість відстежувати все обладнання мережевої інфраструктури в різних місцях, у тому числі на крайніх межах мережі. Надійний захист починається з повного огляду внутрішніх

пристроїв (ПК, смартфонів, ноутбуків, серверів, пристроїв IoT, медичних пристроїв, POS-терміналів, контролерів HVAC, зчитування бейджів, IP-камер), а також будь-яких інших пристроїв на базі IP-пристроїв за допомогою єдиного, інтегрованого представлення топології мережі.

Технології управління доступом до мережі організації повинна включати такі основні функції:

NAC повинний бачити та оцінювати повний набір кінцевих точок (включаючи IoT) до того, як вони підключаться до мережі. Він також повинен класифікувати користувача пристрою. Знання про ризики пристрою та користувача має продовжуватися після підключення.

NAC також повинний вміти визначати критичні уразливості пристроїв, такі як застарілі версії програмного забезпечення або невстановлені оновлення, включаючи сканування пристроїв у VPN-з'єднаннях.

Після ідентифікації пристрою та користувача рішення має підтримувати сегментацію на основі намірів для автоматичного застосування політик безпеки на основі визначеної інформації про пристрій/користувач.

NAC має інтегруватися з іншими рішеннями в ширшій архітектурі безпеки, включаючи сторонні продукти, щоб активно обмінюватися актуальною інформацією про потенційні загрози та застосовувати засоби контролю у розширеній організації.

NAC повинний забезпечувати автоматичне реагування на загрози в режимі реального часу, щоб допомогти негайно локалізувати підозрілі пристрої, перш ніж відбудеться серйозне пошкодження чи зараження.

NAC має забезпечувати самообслуговування користувачів, автоматичну адаптацію пристроїв, а також підказки щодо самостійного виправлення, якщо пристрій не відповідає мінімальним стандартам безпеки.

NAC повинний підтримувати динамічні атрибути (як суб’єкти, так і об’єкти) і давати можливість оновлювати та/або змінювати їх у будь-який час, а користувачі можуть персоналізувати сценарії на основі подій.

NAC має забезпечувати масштабовану архітектуру, яка зможе доступно

підтримувати численні місця на підприємстві та необмежену кількість пристроїв. Він повинен запропонувати гнучке розгортання з фізичними, віртуальними та хмарними варіантами.

NAC має співіснувати та підключатися до існуючої цифрової екосистеми, включаючи апаратне забезпечення, додатки для підвищення продуктивності, програми безпеки та інфраструктуру безпеки.

NAC повинен підтримувати доступ користувачів за межами безпосередньої корпоративної мережі, бажано обмежувати доступ за часом і ретельно відстежувати використання мережі.

NAC особливо корисний для роботи з неавторизованими точками доступу. Несанкціоновані точки доступу варіюються від простої неприємності до реальної загрози безпеці у корпоративній мережі. Лише одне незахищене підключення, може стати вразливою точкою доступу для всієї мережі.

NAC займає особливе місце в плані безпеки мережі, оскільки, на відміну від брандмауера, який забезпечує захист периметра, NAC стежить за внутрішньою частиною корпоративної мережі. NAC є лише частиною плану безпеки, а не повним заходом безпеки. Він не замінює брандмауер і не захищає від витоку даних через електронну пошту, принтери або USB-накопичувачі. Однак більшість зломів і крадіжок даних відбуваються за брандмауерам, що робить NAC критичним компонентом багаторівневої політики безпеки.

ВИСНОВКИ

Пристрої або користувачі, що підключаються до корпоративної мережі, становлять потенційну загрозу безпеці організації. Управління доступом до мережі – це набір інструментів, процесів і протоколів обмеження доступу неавторизованих користувачів і пристроїв, які зловмисники можуть використовувати для несанкціонованого доступу. Реалізація технології управління доступом забезпечують видимість мережевого середовища, динамічний контроль і автоматизовані реакції на загрози.

Встановлено, що управління доступом є одним із важливих аспектів для забезпечення захисту інформації. Він допомагає організаціям не відставати від постійно зростаючої поверхні атак, а також використовується в галузі для опису набору функцій та мережевих протоколів, ідентифікації та перевірки пристроїв користувачів, автентифікації користувачів і застосування політик, які визначають, до яких мережевих ресурсів дозволено доступ користувачам.

Проаналізовано призначення та функції IoT в мережі організації. Швидке поширення пристроїв IoT призвело до того, що в організацій виникла потреба покращувати уявлення про те, що підключено до їхніх мереж. Необхідно знати кожен пристрій та кожного користувача, який отримує доступ до корпоративних мереж.

Проаналізовано загрози IoT в мережі організації. IoT більш уразливий до атак зловмисного програмного забезпечення, оскільки пристрої IoT завжди онлайн і не мають надійного захисту. Інтегрована стратегія безпеки потрібна для захисту від загроз, спрямованих на пристрої IoT.

Визначено тему та завдання управління доступом до мережі організації. NAC забезпечує видимість мережевого середовища для примусового виконання та динамічного контролю політики. Незалежно від того, чи підключаються пристрої до мережі чи поза нею, рішення NAC може автоматично реагувати на зламані пристрої чи аномальну активність.

Оглянуто існуючі технології управління доступом до мережі організації. Сьогодні доступно кілька типів програмних рішень для управління доступом до мережі. До них належать спеціалізовані платформи, повний пакет рішень для кібербезпеки, рішення з відкритим кодом, а також готові комерційні рішення. Програмне рішення залежить від розміру організації, характеру цифрового сліду та кількості пристроїв, що працюють у корпоративній мережі.

Проаналізовано призначення рішення FortiNAC та його основні компоненти щодо управління доступом до мережі. FortiNAC забезпечує видимість для всіх адміністраторів, щоб бачити все, що підключено до корпоративної мережі, а також надає можливість контролювати пристрої та користувачів, включаючи динамічне автоматичне реагування.

Запропоновано варіант технології управління доступом до мережі організації на базі FortiNAC.

Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління доступом до мережі організації.

Таким чином, застосування технології управління доступом до мережі на базі рішення FortiNAC та запропоновані рекомендації фахівцям з кібербезпеки мають забезпечити ефективний захист корпоративних мереж від несанкціонованого доступу зловмисників та виникнення шкідливих процесів в них.

ПЕРЕЛІК ПОСИЛАНЬ

1. James Aweya. Designing Switch/Routers. Architectures and Applications. CRC Press, 2022. 336 p.
2. ISO/IEC 20924:2021. Information technology – Internet of Things (IoT) – Vocabular [Електронний ресурс] – Режим доступу: https://www.iso.org/standard/82771.html
3. Emerging IoT Technologies Report. 2022 [Електронний ресурс] – Режим доступу: https://iot-analytics.com/product/emerging-iot-technologies-report-2022/
4. State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. 2022. [Електронний ресурс] – Режим доступу: https://iot-analytics.com/number-connected-iot-devices/
5. ISO/IEC 27400:2022 – Cybersecurity – IoT security and privacy – Guidelines [Електронний ресурс] – Режим доступу: https://www.iso27001security.com/html/27400.html
6. Internet of Things (IoT) Security: Challenges and Best Practices. 2022. [Електронний ресурс] – Режим доступу: https://www.apriorit.com/dev-blog/513-iot-security
7. Lawrence Miller. Zero Trust Access. Fortinet Special Edition. New Jersey: Hoboken, 2022. 45 p.
8. Business network segmentation: a must in the IoT era. 2020. [Електронний ресурс] – Режим доступу: https://www.hikvision.com/ar/newsroom/blog/business-network-segmentation--a-must-in-the-iot-era/
9. Sandeep Saxena, Ashok Kumar Pradhan. Internet of Things. Security and Privacy in Cyberspace. Springer Nature Singapore, 2022. 293 p.
10. International Electrotechnical Commission. IoT 2020: Smart and secure IoT platform. Switzerland: Geneva, 2020. 193 p.
11. Cybersecurity and Infrastructure Security Agency. The Internet of Things. 2019. 1–6 p.

12. Omar Dib, Khalifa Toumi. Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions. 2020. 40 p.

13. Shantanu Pal. Internet of Things and Access Control. Springer Nature Switzerland, 2021. 205 p.

14. Andrei Tchernykha, Uwe Schwiegelsohnb, El-ghazaliTalbic, Mikhail Babenkod. Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Volume 36. 1–9 p.

15. What is NAC and why is it important for network security. 2022. [Електронний ресурс] – Режим доступу: https://www.networkworld.com/article/3654479/what-is-nac-and-why-is-it-important-for-network-security.html

16. Maanak Gupta, Smriti Bhatt, Asma Hassan, Alshehri, Ravi Sandhu. Access Control Models and Architectures for IoT and Cyber Physical Systems. Springer Nature Switzerland, 2022. 173 p.

17. Understanding Network Access Control. 2021. [Електронний ресурс] – Режим доступу: https://docs.genians.com/release/en/intro.html

18. Zero Trust Progress Report. 2022. [Електронний ресурс] – Режим доступу: https://www.cybersecurity-insiders.com/portfolio/2020-zero-trust-progress-report-pulse-secure/

19. Secure Network Access Control for modern IT [Електронний ресурс] – Режим доступу: https://www.arubanetworks.com/products/security/network-access-control/

20. Barracuda CloudGen Firewall [Електронний ресурс] – Режим доступу: https://www.barracuda.com/products/cloudgenfirewall

21. Cisco Identity Services Engine (ISE) [Електронний ресурс] – Режим доступу: https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html

22. Citrix Gateway [Електронний ресурс] – Режим доступу: https://www.citrix.com/downloads/citrix-gateway/

23. Forescout. Network Access Control (NAC) [Електронний ресурс] – Режим

доступу: https://www.forescout.com/solutions/network-access-control/

24. McAfee Unified Secure Access [Електронний ресурс] – Режим доступу: https://www.mcafee.com/

25. SAP Access Control [Електронний ресурс] – Режим доступу: https://www.sap.com/products/financial-management/access-control.html

26. Sophos NAC Advanced [Електронний ресурс] – Режим доступу: https://www.sophos.com/en-us/products/zero-trust-network-access

27. FortiNAC. Data Sheet. Fortinet Inc, 2022. 11 p.

28. Magic Quadrant for SD-WAN. 2022. [Електронний ресурс] – Режим доступу: https://www.gartner.com/doc/reprints?id=1-2B4JI935&ct=220913&st=sb

29. FortiNAC. Device Profiler Configuration. Fortinet Inc, 2022. 65 p.

30. Fortinet. Network Access Control (NAC) [Електронний ресурс] – Режим доступу: https://www.fortinet.com/products/network-access-control

31. Fortinet Security Fabric [Електронний ресурс] – Режим доступу: https://www.itc.by/data-security/fortinet-security-fabric/

32. Пацьора Е.С. Управління доступом до мережі в еру IoT. Всеукраїнська наукова-практична конференція «Актуальні проблеми кібербезпеки». ДУТ ННІЗІ, м. Київ, 27 жовтня 2022. С. 139–140.

33. Пацьора Е.С. Важливі елементи щодо рішення безпеки IoT. Всеукраїнська наукова-практична конференція «Актуальні проблеми кібербезпеки». ДУТ ННІЗІ, м. Київ, 27 жовтня 2022. С. 204–207.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)