ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія організації контролю доступу корпоративної мережі на прикладі рішення Cisco Identity Services Engine»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Сергій СТОРОЖУК
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
СТОРОЖУК Сергій
(прізвище, ім'я)

Керівник к.т.н., доцент ВЛАСЕНКО Вадим
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ПЕРЕЛІК ПОСИЛАНЬ

NAC - контролю доступу до мережі

ISE - Identity Services Engine

NAC - network access control

BYOD - принесіть свій власний пристрій

PAN - Policy Administration Node

MnT node - Monitoring Node

PDP – Policy Decision Point

PEP – Policy Enforcement Point

M&T – моніторинг і усунення несправностей

TACACS+ - Terminal Access Controller Access-Control System Plus

VPN - Virtual Private Network

RADIUS - Remote Authentication Dial-In User Service

ВСТУП

Актуальність дослідження. Технологія контролю доступу до мережі - це важлива складова інформаційної безпеки в сучасних організаціях. Її актуальність впровадження необхідно впроваджувати у зв’язку з збільшенням загроз кібербезпеки організацій. Зловмисники постійно шукають способи вторгнутися в мережі організацій з метою крадіжки даних, розповсюдження шкідливого програмного забезпечення та інших кібератак. Технологія контролю доступу допомагає захистити мережу та її ресурси від таких загроз.

Зараз багато працівників працюють віддалено або використовують мобільні пристрої для доступу до корпоративних ресурсів. Технологія контролю доступу дозволяє керувати цими мобільними пристроями та забезпечувати безпеку доступу до мережі навіть поза офісом.

Багато галузей, такі як фінанси, охорона здоров'я та інші, мають обов'язкові вимоги щодо захисту конфіденційності даних інших ресурсів. Технологія контролю доступу допомагає організаціям виконувати ці вимоги та дотримуватися відповідних стандартів безпеки.

Багато організацій переходять до хмарних обчислень і зберігання даних. Контроль доступу до хмарних ресурсів стає критичним для забезпечення безпеки даних і ресурсів організації.

Не тільки зовнішні зловмисники можуть становити загрозу. Інсайдери, тобто внутрішні працівники організації, також можуть бути джерелом загрози для інформаційної безпеки. Технологія контролю доступу допомагає обмежити їхні права доступу до даних і ресурсів, зменшуючи ризик витоку чутливої інформації.

Таким чином, технологія контролю доступу є важливою складовою інфраструктури інформаційної безпеки організацій і сприяє забезпеченню конфіденційності, цілісності та доступності даних та інших ресурсів. Впровадження цієї технології допомагає організаціям захищати свою інформацію

та оптимізувати управління доступом до мережі. Тому тема кваліфікаційної роботи є актуальною.

Об'єкт дослідження –контролю доступу до корпоративної мережі організації.

Предмет дослідження – технологія контролю доступу до корпоративної мережі на базі рішення Cisco Identity Services Engine.

Мета роботи – розробити варіант розгортання технології контролю доступу до мережі на базі рішення Cisco Identity Services Engine та рекомендації щодо застосування технології.

Наукові завдання:

- провести аналіз питання щодо необхідності впровадження контролю доступу до мережі організації;
- проаналізувати основні загрози корпоративній мережі організації;
- проаналізувати методи та засоби контролю доступу до мережі організації;
- розробити варіант розгортання системи контролю доступу до мережі організації на базі рішення Cisco ISE та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу контролю доступу до мережі на базі рішення Cisco Identity Services Engine.

Практичне значення одержаних результатів полягає в розробці технології розгортання системи контролю доступу до мережі організації на базі рішення Cisco ISE та рекомендації щодо застосування технології в залежності від розмірів організації, що дозволить забезпечувати необхідний рівень кібербезпеки організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ НЕОБХІДНОСТІ КОНТРОЛЮ ДОСТУПУ ДО МЕРЕЖІ НА ОСНОВІ ЗАСТОСУВАННЯ ПОЛІТИК ПРИСТРОЇВ І КОРИСТУВАЧІВ КОРПОРАТИВНИХ МЕРЕЖ

1.1. Аналіз необхідності контролю доступу до мережі організації

Контроль доступу до цифрових ресурсів є критично важливою можливістю IT-безпеки для організацій. Рішення контролю доступу до мережі (NAC) дозволяють IT-спеціалістам авторизувати або забороняти користувачам і пристроям доступ до ресурсів у мережі. NAC відіграє важливу роль у наданні доступу до ресурсів із найменшими привілеями, що є основою для стратегій Zero Trust Security. [1]

Контроль доступу до мережі обмежує доступ користувачів і пристроїв до ресурсів на основі правил, встановлених IT. Подібно до того, як дверні замки та значки безпеки не дозволяють зловмисникам отримати доступ до фізичних організаційних ресурсів, таких як будівлі та офіси, засоби контролю доступу до мережі захищають мережеві цифрові ресурси від несанкціонованого доступу.

Визначимо основні моменти, для чого необхідно впроваджувати контроль доступу до мережі організації. [1]

Безпека. Контроль доступу до мережі захищає ресурси від підробки та крадіжки зловмисниками. Рішення NAC гарантують, що лише користувачі та пристрої з відповідними дозволами можуть отримати доступ до мережі та мережевих ресурсів. Крім того, деякі рішення NAC можуть ідентифікувати суб’єктів, які можуть брати участь в атаці, і поміщати в карантин або блокувати доступ цього суб’єкта до подальшого розслідування. Ця функція може запобігти поширенню атак.

Конфіденційність. Організації керують більшими обсягами та різноманітністю даних, ніж будь-коли. Деякі з цих даних є чутливими та/або конфіденційними. Рішення для контролю доступу до мережі дозволяють

організаціям визначати, хто, що, коли та як може отримати доступ до даних у мережі, щоб зменшити ризик злому.

Відповідність. Регульованим організаціям часто доводиться дотримуватись вимог щодо конфіденційності та захисту даних, таких як Загальний регламент захисту даних (GDPR), Закон про перенесення та підзвітність медичного страхування (HIPAA) і Сарбейнса-Окслі (SOX). Рішення NAC можуть допомогти організаціям виконувати ці мандати, обмежуючи доступ до даних, зберігаючи безпечний і розділений трафік, а також забезпечуючи журналювання та звітність для аудитів.

Особливості роботи контролю доступу до мережіполягає в наступному.

Контроль доступу до мережі ґрунтується на концепції, згідно з якою різним користувачам і пристроям (суб'єктам) надаються різні типи доступу на основі їхніх потреб. Деталізація означає рівень деталізації, з яким можна визначити та застосувати суб'єкт, його потреби та пов'язані з ним дозволи доступу. Високодеталізований контроль доступу до мережі є ключовим компонентом підходів Zero Trust Security, які обмежують доступ суб'єкта лише до тих ресурсів, які необхідні для виконання їхньої роботи чи функції.

Щоб ефективно захистити ресурси, рішення для контролю доступу до мережі повинні забезпечувати декілька взаємопов'язаних можливостей, що надаються за допомогою комбінації технологій.

Технологія контролю доступу до мережі складається з наступних можливостей та функцій, які показано в таблиці 1.1.

Розглянемо приклад застосування рішення NAC, яке забезпечує безпечний доступ до ресурсів у всій організації. Наприклад, лікарня використовує рішення NAC для профілювання, захисту та керування підключенням авторизованих пристроїв IoT, виключаючи інші. Центр виконання робіт використовує рішення NAC для автентифікації кожного проводового та безпроводового пристрою, який отримує доступ до мережі (наприклад, роботів), і запроваджує узгоджені політики на основі ролей. Шкільна система використовує рішення NAC для автентифікації

учнів, викладачів, персоналу та гостей, а також для забезпечення детальної сегментації трафіку на основі визначених правил.

Таблиця 1.1.

Технології контролю доступу до мережі

Можливості	**Функція**	**Технології**
Видимість	Знати, хто і що є в мережі в будь-який момент часу	Фізичні або віртуальні збирачі даних; активні (NMAP, WMI, SNMP, SSH) і пасивні (SPAN, DHCP, NetFlow/S-Flow/IPFIX) методи виявлення; Профілювання пристроїв за допомогою AI/ML ; глибока перевірка пакетів
Аутентифікація	Переконатися з упевненістю, що користувач або пристрій є тим/тим, за кого себе видає	аутентифікація 802.1x; EAP-TLS, RADIUS, TACACS; багатофакторна аутентифікація; сертифікати
Визначення політики	Визначення правил для користувачів і пристроїв щодо ресурсів, до яких вони можуть отримати доступ, і способів доступу до ресурсів	Інструменти для написання правил, які можуть включати контекстуальні параметри, такі як роль, тип пристрою, метод автентифікації, стан пристрою, шаблони трафіку, місцезнаходження та час доби

Авторизація	Визначення відповідних правил для автентифікованого користувача або пристрою	
Примусове виконання	Дозвол, заборона або скасування доступу автентифікованого користувача чи пристрою до ресурсу на основі відповідної політики	Інтеграція та двонаправлений зв'язок із брандмауерам та іншими засобами безпеки

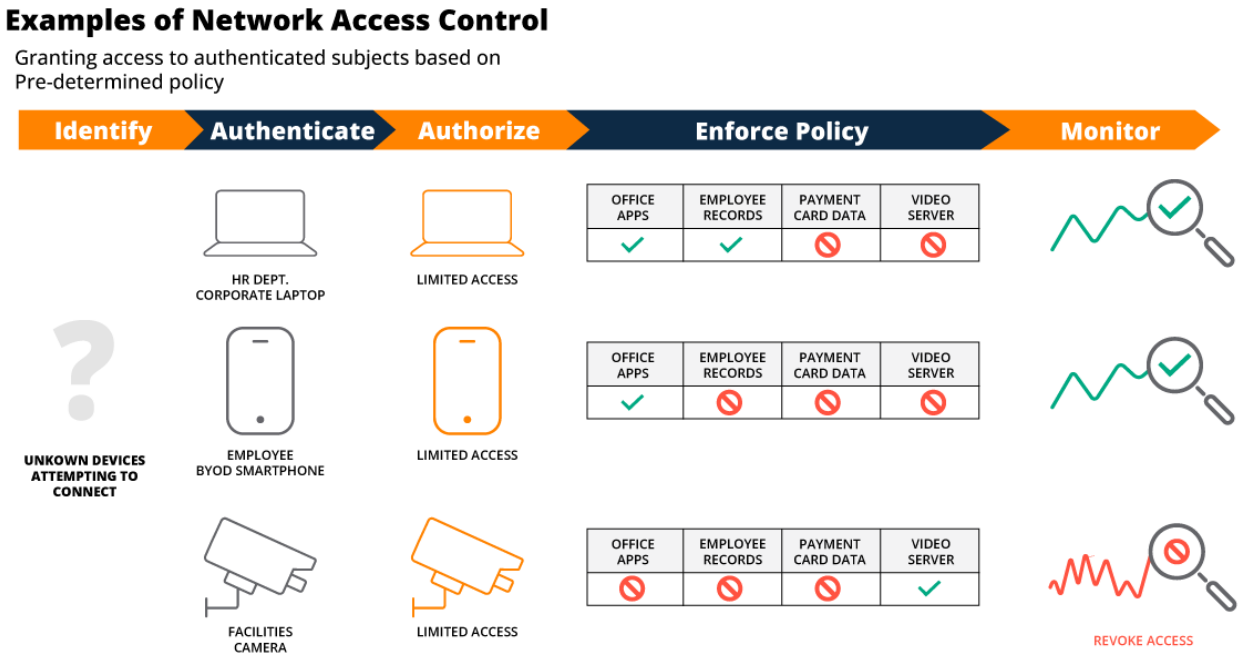

Рис 1.1. Приклад застосування контролю доступу до мережі [1]

Рішення NAC можуть вирішити кілька випадків використання безпечного підключення в організаціях:

NAC для гостей і тимчасових працівників дозволяє легко та ефективно створювати тимчасові облікові записи доступу до мережі для будь-якої кількості гостей на день для працівників ресепшн, координаторів заходів та іншого персоналу, не пов'язаного з IT. Також є можливість пропонувати налаштований портал самостійної реєстрації , який дозволяє відвідувачам створювати власні облікові дані, які потім зберігаються в системи протягом заздалегідь визначеного періоду часу та можуть бути налаштовані на автоматичне закінчення терміну дії.

NAC для власного пристрою (BYOD). Система автоматично налаштовує мобільні пристрої, дозволяючи їм безпечно підключатися до корпоративних мереж. Працівники можуть самостійно налаштувати власні пристрої, дотримуючись інструкцій щодо реєстрації та підключення. Унікальні сертифікати для кожного пристрою застосовуються, щоб гарантувати, що користувачі можуть безпечно підключати свої пристрої до мереж із мінімальною взаємодією IT.

NAC для оцінки безпеки кінцевої точки Система виконує оцінку стану кінцевої точки/пристрою, щоб переконатися, що вимоги безпеки та відповідності виконані до того, як пристрої підключаються до корпоративної мережі, що може допомогти організаціям уникнути вразливостей у своєму IT-середовищі.

NAC для пристроїв Інтернету речей (IoT). Система забезпечує повну видимість спектру пристроїв, підключених до мережі, з оцінкою ризиків і машинним навчанням для ідентифікації невідомих пристроїв і скорочення часу на ідентифікацію. Система також відстежує поведінку потоків трафіку для додаткової безпеки.

ClearPass Policy Manager профілює пристрої, які намагаються підключитися до мережі, і забезпечує доступ до мережі на основі ролей і пристроїв на основі правил, налаштованих IT-спеціалістами.

NAC для проводових пристроїв. Система забезпечує безпечний проводовий контроль доступу для таких пристроїв, як принтери та телефони VoIP, які не автентифікуються за допомогою методів 802.1x.

Хмарний NAC Хмарна система інтегрується зі звичайними хмарними сховищами ідентифікації, щоб забезпечити безперебійну хмарну адаптацію та безпечну рольову політику для користувачів і пристроїв.

Для вибору рішення NAC необхідно враховувати наступне:

1. Функціональна сумісність і функції, що не залежать від постачальника, щоб уникнути дорогих доповнень і прив'язки до постачальника.
2. Продемонстрована здатність підтримувати безпечний і розділений трафік.
3. Доступність сервісу для підтримки максимального часу безвідмовної роботи та безперервної роботи.
4. Масштабованість для підтримки сотень тисяч одночасних кінцевих точок
5. Лідерство на ринку та позначення, які визнають здатність зменшувати кіберризики.

Розглянемо нормативно- правову базу щодо контролю доступу до мережі організації.

Контроль доступу до мережі (NAC) — це технологія, яка допомагає організаціям контролювати та керувати доступом до своїх мереж. Конкретні нормативні документи, які регулюють впровадження NAC, можуть відрізнятися залежно від країни та галузі. Однак існує кілька загальних основ і правил, які часто застосовуються до NAC і безпеки мережі в цілому:

HIPAA (Закон про перенесення та підзвітність медичного страхування): якщо ваша організація має справу з медичними даними, правила HIPAA у Сполучених Штатах вимагають суворого контролю доступу для захисту інформації про пацієнтів.

PCI DSS (Стандарт безпеки даних індустрії платіжних карток): для організацій, які обробляють дані кредитних карток, PCI DSS передбачає жорсткий контроль доступу та сегментацію мережі для захисту даних власників карток.

ISO 27001: цей міжнародний стандарт для систем управління інформаційною безпекою включає вимоги до контролю доступу та безпеки мережі.

Спеціальна публікація NIST 800-53: виданий Національним інститутом стандартів і технологій (NIST) у Сполучених Штатах, цей документ містить вказівки та засоби керування інформаційною безпекою, включаючи контроль доступу.

GDPR (Загальний регламент захисту даних): GDPR, який застосовується до країн-членів Європейського Союзу, вимагає від організацій впроваджувати належні заходи безпеки, включаючи контроль доступу, для захисту персональних даних громадян ЄС.

Норми, що стосуються певної галузі, залежать від галузі, де можуть існувати спеціальні норми, які стосуються безпеки мережі та контролю доступу.

В Україні є Закон «Про захист персональних даних», який вимагає від організацій запроваджувати контроль доступу для захисту особистих і конфіденційних даних.

Політика та стандарти компанії теж є складовою контролю доступу до мережі організації. Окрім нормативних вимог, окремі організації часто мають власні внутрішні політики, стандарти та процедури контролю доступу до мережі.

Важливо розуміти конкретні нормативні вимоги, які застосовуються до вашої організації залежно від її розташування, галузі та типу даних, які вона обробляє. Відповідність цим правилам часто передбачає впровадження рішень контролю доступу до мережі та ведення документації для демонстрації відповідності під час аудитів та оцінок.

Для компаній обробка персональних даних – це будь-які дії пов’язані від збирання до знищення персональних даних. Сюди відноситься реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання, поширення (розповсюдження, реалізація, передача), знеособлення даних, тощо (стаття 2 Закону). [9]

В організаціях під час обробки даних необхідно враховувати їх категорію та застосовувати відповідні рівні безпеки.

Для організацій -це внутрішні положення або інструкції, які повинні регулювати процедуру обробки персональних даних. Такі інструкції розробляються власниками та розпорядниками персональних даних, відповідно до вимог Закону, та мають враховувати [10]:

специфіку діяльності (правові підстави);

мету обробки, обсяг даних та їх категорії;

інформаційні системи, мережі, програми, задіяні у процес обробки персональних даних;

число осіб, які мають доступ до персональних даних

форми ведення реєстру, в якому обробляються персональні дані (мануальна, електронна або змішана);

ризики, які можуть виникнути при обробці даних, як для систем, так і персоналу.

Документація, до якої відносяться політики безпеки персональних даних, повинна бути повною, регулярно оновлюватися й містити інформацію про:

мету, обсяг, підстави (межі повноважень) обробки персональних даних;

конфігурацію інформаційної системи (банків даних), мережі, програми тощо;

номенклатуру оброблюваних персональних даних (види та категорії), їхні локалізації та операції, що проводяться з ними;

механізм здійснення заходів безпеки (у тому числі, фізичного середовища інформаційних систем);

докладний опис критеріїв, відповідно до яких будуть доступні персональні дані;

управління доступом та список авторизованих користувачів (у числі, рівні доступу);

графік перевірок безпеки та звіти про інциденти безпеки;

особу, відповідальну за політику безпеки;

аудит безпеки (графік перевірок та звіти про інциденти безпеки);

порядок доступу до персональних даних третіх осіб;

строки збереження, процедури видалення або знищення даних;

заходи з виявлення випадків несанкціонованого доступу і/або несанкціонованої обробки персональних даних та інше. [10]

Розглянемо типи керування доступом

Існує чотири основні типи керування доступом. Кожен із них забезпечує унікальний спосіб адміністрування доступу до делікатної інформації.

Вибіркове керування доступом (DAC)

У моделях DAC кожен об'єкт у захищеній системі має власника, який на власний розсуд надає доступ до нього користувачам. DAC забезпечує індивідуальний підхід до керування ресурсами.

Обов'язкове керування доступом (MAC)

У моделях MAC користувачам надається доступ у формі дозволів. Центральний орган регулює права доступу й упорядковує їх за рівнями, які рівномірно розгортаються в усій системі. Ця модель дуже часто використовується в державних і військових установах.

Керування доступом на основі ролей (RBAC)

У моделях RBAC користувачам надається доступ залежно від їхніх функцій в організації, а не на основі ідентичностей або трудового стажу. Мета полягає в тому, щоб надавати користувачам доступ лише до тих даних, які їм потрібні для виконання робочих завдань.

Керування доступом на основі атрибутів (ABAC)

У моделях ABAC користувачам надається доступ на основі атрибутів і умов середовища, зокрема часу й розташування. ABAC – це найдеталізованіша модель керування доступом, яка допомагає зменшити кількість призначень ролей.

1.2. Аналіз загроз інформаційних систем організацій

2022 рік був одним з бурхливим для кібербезпеки організацій. Можна сказати не бракувало подій, що сприяли цьому, серед найбільш значущими були триваючі наслідки пандемії та розгортання військового конфлікту в Україні. Потрясіння зробили 2022 рік роком економічних, геополітичних та людських потрясінь, що спричинили саме такий хаос, в якому процвітають кіберзлочинці.

І вони процвітали.

IBM Security® X-Force® став свідком того, як опортуністичних зловмисників, які заробляють на безладі, використовуючи ландшафт інформаційних систем на свою користь для проникнення в в уряди та організації по всьому світу. [11]

Індекс загроз IBM Security X-Force Intelligence Index 2023 відстежує нові та існуючі тенденції та шаблони атак, а також включає мільярди точок даних, починаючи від мережевих і кінцевих пристроїв, інцидентів реагування на інциденти, вразливості вразливостей, баз даних зловмисників та багато іншого. Цей звіт показує дані досліджень з січня по грудня 2022 року.

Ці висновки є як ресурс не тільки клієнтам IBM, дослідникам кібербезпеки, політиків, засобів масової інформації та ширшої спільноти професіоналів та лідерів індустрії безпеки. професіоналів та лідерів індустрії безпеки. Сьогоднішнє нестабільне середовище з його дедалі витонченішими та зловмисними загрозами, вимагає спільних зусиль для захисту бізнесу та громадян. Більше, ніж будь-коли, фахівцям з кібербезпеки потрібно мати на озброєнні дані про загрози і знання про безпеку, щоб випереджати зловмисників в і захистити свої критичні активи.

Особливості аналізу даних у 2022 році.

У 2022 році IBM Security® X-Force® змінили підхід до аналізу частини даних. Зміни дозволили пропонувати більш глибокий аналіз і більш тісно узгоджувати його з галузевими стандартами. Це, своєю чергою, дає змогу приймати

більш обґрунтовані рішення щодо безпеки та краще захищати свою організацію від загроз.

Зміни аналізі в 2022 році включають:

- Початкові вектори доступу: Впровадження системи MITRE ATT&CK для відстеження початкових векторів доступу більш тісно пов'язує результати нашого дослідження з більш широкою галуззю кібербезпеки індустрією кібербезпеки і дозволяє нам виявити важливі тенденції на технічному рівні.

- Експлойти та компрометації нульового дня: Екстраполяція з надійної бази даних вразливостей, яка включає майже 30 років даних, допомагає надати контекст аналізу та визначити реальну загрозу, яку становлять вразливості. Цей процес також надає контекст зменшення частки вразливостей, що можуть бути використані як зброя експлойтів та атак нульових днів.

- Методи суб'єктів загроз та їхній вплив: Відокремлення кроків, які здійснюють суб'єкти загрози під час атаки, від фактичних наслідків інциденту дозволило визначити критичні етапи інциденту. Цей процес, у свою чергу, виявив області, в яких з якими повинні бути готові впоратися оперативні служби після інциденту.

Найкращі дії за цілями, що спостерігаються:

Майже у чверті всіх інцидентів виправлених у 2023 році, розгортання бекдорів (21%) було найкращим заходом для досягнення мети. Зокрема, сплеск на початку року багатоцільового шкідливого програмного забезпечення Emotet, значною мірою спричинив стрибок активності бекдорів, що спостерігається з року в рік. Незважаючи на цей сплеск активності бекдорів, програм-вимагачів, які утримували першість щонайменше принаймні з 2021 року, становило значну частку інцидентів - 17%, що посилює постійну загрозу, яку становить це шкідливе програмне забезпечення.

Вимагання було найпоширенішою атакою на організації, що спричинила найбільший вплив. У 27% випадків вимагання було явним наслідком вибору зловмисників. Жертви у виробничій сфері становили 30% інцидентів, що призвели

до вимагання, оскільки кіберзлочинці продовжували використовувати напружену ситуацію в галузі.

Фішинг був основним вектором початкового доступу: Фішинг залишається провідним вектором зараження, виявленим у 41% інцидентів, за ним слідує використання публічних додатків (26%). Зараження через шкідливі макроси втратили популярність, ймовірно, через рішення Microsoft заблокувати макроси за замовчуванням. Шкідливі ISO- та LNK-файли використовують ескалацію як основну тактику доставки шкідливого програмного забезпечення через спам у 2022 році.

Зростання хактивізму та руйнівного шкідливого програмного забезпечення: російська війна в Україні відкрила двері для того, що багато хто в спільноті кібербезпеки очікував, щоб стати демонстрацією того, як кібернетичні засоби сприяють попередній сучасній війні. Хоча на момент публікації цієї публікації найжахливіші прогнози щодо кіберпростору не справдилися, відбулося помітне відновлення хактивізму та руйнівного шкідливого програмного забезпечення. X-Force також спостерігає безпрецедентні зміни у світі кіберзлочинців із посиленням співпраці між групами кіберзлочинців і бандами Trickbot, спрямованими на українські організації.

Тож у підсумку зведемо статистику кіберзагроз у таблицю2

Таблиця 1.2

Аналіз загроз організаціям за 2023 рік

27%	**Відсоток атак з вимаганням** Зловмисники намагалися вимагати гроші у жертв у більш ніж одній чверті всіх інцидентів, на які X-Force реагувала у 2022 році. тактика, яку вони використовують, еволюціонувала за останнє десятиліття, і ця тенденція, як очікується, продовжуватиметься,

	оскільки суб’єкти загрози агресивніше прагнуть отримати прибуток.
21%	**Частка інцидентів, які призвели до розгортання бекдорів**. Розгортання бекдорів було найпоширенішою дією минулого року, що відбувалося більш ніж у кожному п’ятому зареєстрованому інциденті в усьому світі. Успішне втручання захисників, ймовірно, запобігло зловмисникам від досягнення подальших цілей, які могли включати програми-вимагачі.
17%	**Частка атак програм-вимагачів** Навіть попри хаотичний рік для деяких із найпліднішихсиндикатів програм-вимагачів, програми-вимагачі були другою за поширеністю цільовою дією, слідуючи за бекдорами та продовжуючи порушувати роботу організацій. Частка інцидентів програм-вимагачів знизилася з 21% у 2021 році до 17% у 2022 році.
41%	**Відсоток інцидентів із фішингом для початкового доступу** У 2022 році фішингові операції залишалися основним шляхом компрометації: 41% інцидентів усунула X-Force за допомогою цієї техніки для отримання початкового доступу
62%	**Відсоток фішингових атак з використанням фішингових вкладень** Зловмисники віддавали перевагу озброєним вкладенням, розгорнутим самостійно або в поєднанні з посиланнями чи фішингом через сервіс
100%	**Збільшення кількості спроб викрадення потоку на місяць**

	У 2022 році було удвічі більше спроб захоплення потоків на місяць порівняно з даними 2021 року. Спам-електронна пошта, що веде до Emotet, Qakbot і IcedID, активно використовує викрадення потоку.

Топ дій по цілям

Раніше індекс X-Force Threat Intelligence Index вивчав широку категорію найпопулярніших атак. У 2022 році X-Force зробили класифікацію за двома різними категоріями: конкретні дії, які суб'єкти загрози вживали щодо мереж жертви, або супротивні дії щодо мети, а також передбачуваний або реалізований вплив цих дій на жертву, або вплив.

Згідно з даними X-Force Incident Response, розгортання бекдорів було найпоширенішою дією проти об'єкта, що відбувалося в 21% усіх зареєстрованих інцидентів. Далі йдуть програми-вимагачі з 17% і компрометація бізнес-електронної пошти (BEC) з 6%. Шкідливі документи (maldocs), спам-кампанії, засоби віддаленого доступу та доступ до сервера були виявлені в 5% випадків кожен.

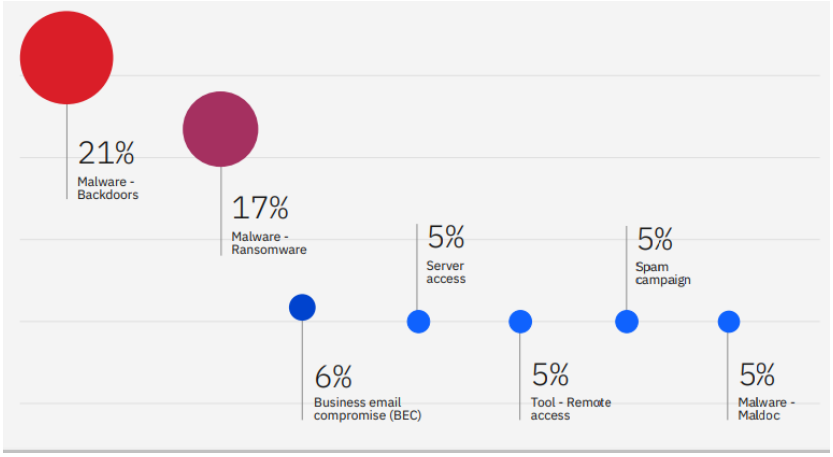

Рис. 1.2. Найпопулярніші дії щодо цілей, за якими X-Force спостерічів у 2023 році [11]

Відповідно до проведеного аналізу, організації, які не впроваджують контроль доступу до мережі (NAC), можуть бути вразливими до різних загроз і ризиків безпеки. NAC служить критичним компонентом безпеки мережі, контролюючи та керуючи доступом до мережі, і його відсутність може призвести до таких загроз:

Несанкціонований доступ:

Без NAC неавторизованим користувачам або пристроям легше отримати доступ до мережі організації. Це можуть бути шахрайські пристрої, гостьові пристрої або скомпрометовані пристрої, які намагаються підключитися.

Внутрішні загрози:

Співробітники або інші особи з законним доступом до мережі можуть зловживати своїми привілеями, навмисно чи ненавмисно, що призведе до витоку даних або несанкціонованої діяльності в мережі.

Поширення шкідливих програм і вірусів:

Шкідливе програмне забезпечення, таке як віруси, хробаки та трояни, може потрапити в мережу через незахищені пристрої. NAC гарантує, що в мережі допускаються лише належним чином налаштовані та оновлені пристрої, що знижує ризик розповсюдження зловмисного програмного забезпечення.

Порушення даних:

Відсутність NAC може полегшити зловмисникам використання вразливостей і отримати доступ до конфіденційних даних. Це може призвести до витоку даних із фінансовими, юридичними та репутаційними наслідками.

Зловживання мережею:

Користувачі без NAC можуть брати участь у зловживаннях мережею, наприклад, надмірному споживанні пропускної здатності, одноранговому обміні файлами або іншим діям, які можуть погіршити продуктивність мережі та вплинути на продуктивність.

Відсутність видимості:

NAC забезпечує мережевим адміністраторам видимість усіх пристроїв, які підключаються до мережі. Без цього мережеві адміністратори можуть мати обмежений або взагалі відсутній доступ до пристроїв і користувачів у мережі, що ускладнює виявлення інцидентів безпеки та реагування на них.

Питання відповідності та регулювання:

Багато галузей і організацій підпадають під нормативні вимоги, які передбачають певні заходи безпеки, зокрема NAC. Невиконання NAC може призвести до невідповідності, що призведе до юридичних і фінансових санкцій.

Перевантаження мережі:

Неконтрольований доступ може призвести до перевантаження мережі, уповільнити важливі бізнес-операції та викликати розчарування серед користувачів.

Неефективний розподіл ресурсів:

Без NAC ресурси можуть бути неефективно розподілені між пристроями та користувачами, яким вони не потрібні, що призведе до неоптимальної продуктивності мережі та потенційної неефективності витрат.

Складність реагування на інциденти:

У разі інциденту безпеки відсутність NAC може ускладнити заходи з реагування на інцидент, оскільки ідентифікація та ізоляція уражених пристроїв стає складнішою.

Таким чином, NAC відіграє вирішальну роль у підвищенні безпеки мережі, підтримці відповідності та забезпеченні ефективного керування мережею. Організації, які не впроваджують NAC, піддаються більшому ризику різних загроз безпеці та операційних проблем. Тому організаціям доцільно розглянути можливість впровадження рішень NAC, щоб зменшити ці ризики та підвищити загальну безпеку мережі.

1.3. Аналіз технологій контролю доступу до мережі організації

Gartner визначає контроль доступу до мережі (NAC) як технології, які дозволяють організаціям впроваджувати політики контролю доступу до корпоративної інфраструктури як орієнтованими на користувача пристроями, так і пристроями Інтернету речей (IoT). Політики можуть базуватися на автентифікації, конфігурації кінцевої точки (положенні) або ролі/ідентифікації користувачів. NAC також може впроваджувати політики після підключення на основі інтеграції з іншими продуктами безпеки.

Аналітичне агентство Gartner опублікувало «магічний квадрант», присвячений рішенням для контролю доступу до мережі (Network Access Control, NAC), які почали активно розвиватися.

Основним стимулом для впровадження продуктів цього класу є популярність концепції BYOD (Bring Your Own Device), застосування якої без забезпечення ефективного захисту особистих пристроїв співробітників може створити значний ризик безпеки підприємств і стабільної роботи корпоративної мережі. Для більш надійного контролю мобільних пристроїв свого персоналу багато організацій інтегрують NAC з рішеннями управління Enterprise Mobility Management (EMM), що дозволяє блокувати доступ до мережі з технічними пристроями, на яких не встановлено програмний агент EMM.

Ще одна важлива тенденція розвитку NAC — їх інтеграція з іншими компонентами системи безпеки, включаючи міжмережеві екрани наступного покоління, рішення класів Advanced Threat Defense (ATD) і Security Information And Advanced Management (SIEM). Наприклад, система NAC може передавати ідентифікаційні дані користувача мережевому екрану для застосування наступних відповідних політик доступу, а контекстна інформація може спільно використовувати NAC з рішеннями SIEM/ATD, в яких вона відображається в IP-адресі пристрою для безпеки фахівців, що відповідають за реагування на попередження.

Тож розглянемо найбільш популярні технології контролю доступу до мережі організації (рис. 1.3).

1. *CISCO ISE,* надійне рішення безпеки.

Враховуючи широкий набір функцій безпеки, як-от запобігання вторгненням і можливості VPN, він забезпечує багаторівневу систему захисту для захисту середовища організації.

ISE надає багато даних кінцевої точки та покращення безпеки. Найкраще використовувати для впровадження NAC і TrustSec. Навігація різними меню може бути важкою, доки ви не звикнете до системи.

2. *Платформа Forescout*

У сучасному світі організації страждають від нестачі некерованих пристроїв, таких як мережеві пристрої, як-от пристрої IOT і некеровані пристрої вводу/виводу,

які підключені до Інтернету. Атака в реальному часі тепер відбувається з некерованого пристрою. І якщо організації не знають їхні активи в мережі/середовищі, що є великою проблемою для повної видимості організації, яка є ключовою частиною витоку, це призводить до злому багатьох організацій. Рішення NAC можна використовувати для виявлення некерованих активів.

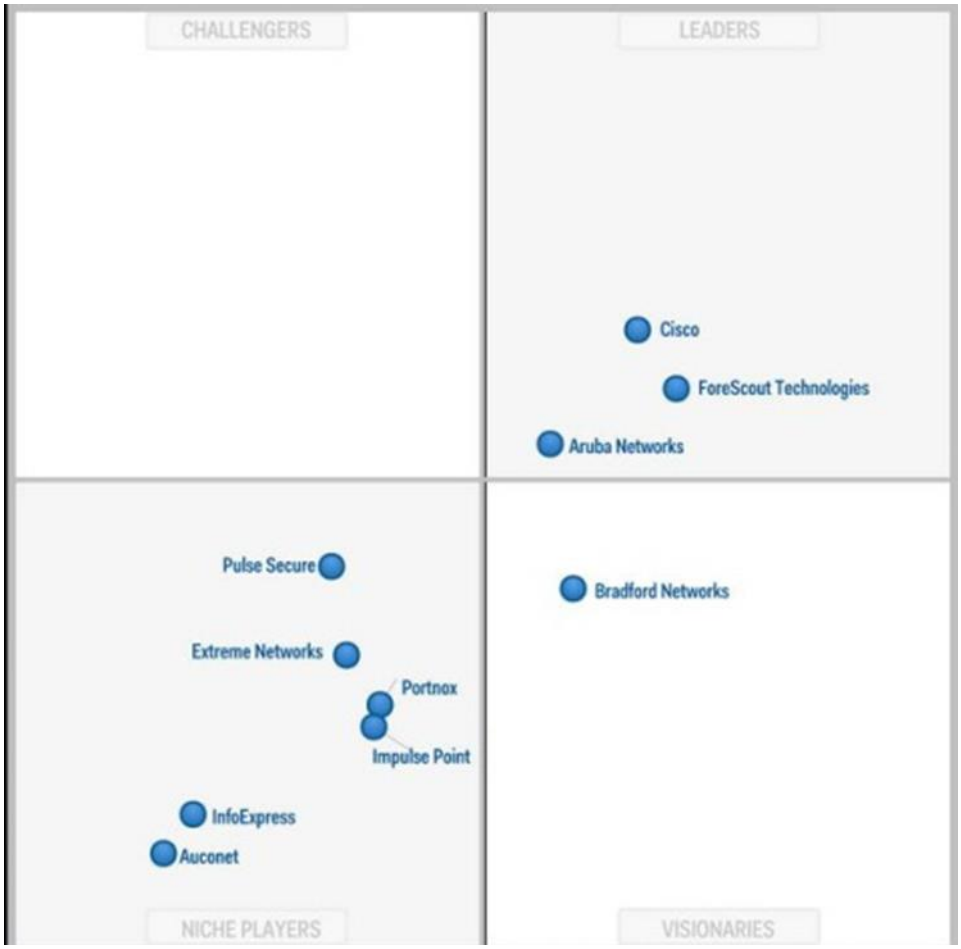

Рис. 1.3. Технології контролю доступу до мережі організації [7]

3. *Aruba clear pass* — це найкраще рішення для запобігання несанкціонованому доступу до Мережі та захисту Мережі від загроз. Це дуже корисно для керування мережею та захисту від шкідливих програм та інших мережевих загроз. ми можемо створити кілька політик для доступу до мережі та зловживання мережею. Це дуже добре для керування всіма точками доступу з однієї консолі.

Aruba clear pass є рішенням для запобігання несанкціонованому доступу до мережі та захисту мережі та захисту від загроз. Це повна допомога для керування мережею та захисту від шкідливих програм та інших мережевих загроз. ми можна створити кілька політик для доступу до мережі та зловживання мережею. Це дуже добре для керування всіма точками доступу з єдиної консолі.

4. FortiNAC - це зручний інструмент безпеки мережі, який надає корисну інформацію про всі активи, підключені до мережі, як проводові та безпроводові. Було доведено, що це вигідно нашого бізнесу, оскільки тут маємо справу з конфіденційними даними або запускаємо кілька хмарних екземплярів. Налаштування FortiNAC для доступу до систем, а також віддаленого доступу з дому було простим. За допомогою кількох команд можна встановити VPN-з'єднання, підключити два або декілька пристроїв.

Висновки до1 розділу

1. Проведено аналіз технології контролю доступу до мережі організації, в результаті якого визначено важливу роль у наданні доступу до ресурсів із найменшими привілеями.

2. Проведено аналіз загроз інформаційній системі організації на основі звіту IBM Security® X-Force®. Визначено основні загрози, які можуть бути зупинені шляхом впровадження рішень контролю доступу до мережі організації.

3. Проведено вибір рішення на основі досліджень Gartner, який визначає контроль доступу до мережі (NAC) як технології, які дозволяють організаціям впроваджувати політики контролю доступу до корпоративної інфраструктури як орієнтованими на користувача пристроями, так і пристроями Інтернету речей (IoT). Для подальшого дослідження було обрано технологію CISCO ISE, надійне рішення безпеки.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ДОСТУПУ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1. Архітектура рішення Cisco Identity Services Engine

В залежності від потреб організації для контролю доступу до мережі можна використовувати різні моделі.

NAC для гостей/підрядників

Незалежно від того, чи здійснюють облік підрядники, відвідувачі чи партнери, організації використовують рішення NAC, щоб переконатися, що особи, які не є працівниками, мають права доступу до мережі, які відрізняються від привілеїв працівників. Такі моделі використовують рішення Cisco Identity Services Engine.

NAC для BYOD

Експоненційне зростання мобільних пристроїв звільнило робочу силу від робочого столу та дало їм можливість працювати віддалено зі своїх мобільних пристроїв. NAC для BYOD забезпечує відповідність усіх пристроїв, які належать працівникам, перед доступом до мережі. Такі моделі використовують рішення Cisco Identity Services Engine.

NAC для Інтернету речей

Пристрої IoT, будь то на виробництві, в охороні здоров’я чи в інших галузях, зростають експоненціально та служать додатковими точками входу для зловмисників, щоб проникнути в мережу. NAC може зменшити ці ризики в пристроях IoT, застосовуючи певні політики профілювання та доступу для різних категорій пристроїв. Такі моделі використовують рішення захист від загроз Cisco IoT.

NAC для реагування на загрози

Постачальники NAC можуть обмінюватися контекстною інформацією (наприклад, ідентифікатором користувача або типом пристрою) із сторонніми компонентами безпеки. Вони можуть реагувати на сповіщення про кібербезпеку, автоматично запроваджуючи політики безпеки, які ізолюють скомпрометовані кінцеві точки. Такі моделі використовують рішення швидкого стримування загроз Cisco.

NAC для медичних приладів

Оскільки все більше медичних пристроїв з'являється в мережі, дуже важливо ідентифікувати пристрої, які входять до конвергентної мережі. Рішення NAC можуть допомогти захистити пристрої та медичні записи від загроз, покращити безпеку охорони здоров'я та посилити захист від програм-вимагачів. Такі моделі використовують рішення Cisco Identity Services Engine.

Рішення NAC допомагають організаціям контролювати доступ до своїх мереж за допомогою таких можливостей:

Керування життєвим циклом політики: забезпечує виконання політик для всіх операційних сценаріїв, не вимагаючи окремих продуктів або додаткових модулів.

Профілі та видимість: розпізнає та створює профілі користувачів та їхні пристрої до того, як шкідливий код може завдати шкоди.

Гостьовий доступ до мережі: керуйте гостями через настроюваний портал самообслуговування, який включає реєстрацію гостей, автентифікацію гостей, спонсорування гостей і портал керування гостьовими.

Перевірка стану безпеки: оцінює відповідність політиці безпеки за типом користувача, типом пристрою та операційною системою.

Реагування на випадки: пом’якшує мережеві загрози шляхом застосування політик безпеки, які блокують, ізолюють і відновлюють несумісні машини без уваги адміністратора.

Двонаправлена інтеграція: інтеграція з іншими рішеннями безпеки та мережевими рішеннями через відкритий/RESTful API.

Cisco Identity Services Engine (ISE) — це система керування мережевим доступом на основі ідентичності та застосування політик (рис.2.1). Ця система функціонує як механізм загальної політики, яка забезпечує контроль доступу до кінцевої точки та адміністрування мережевих пристроїв організацій.

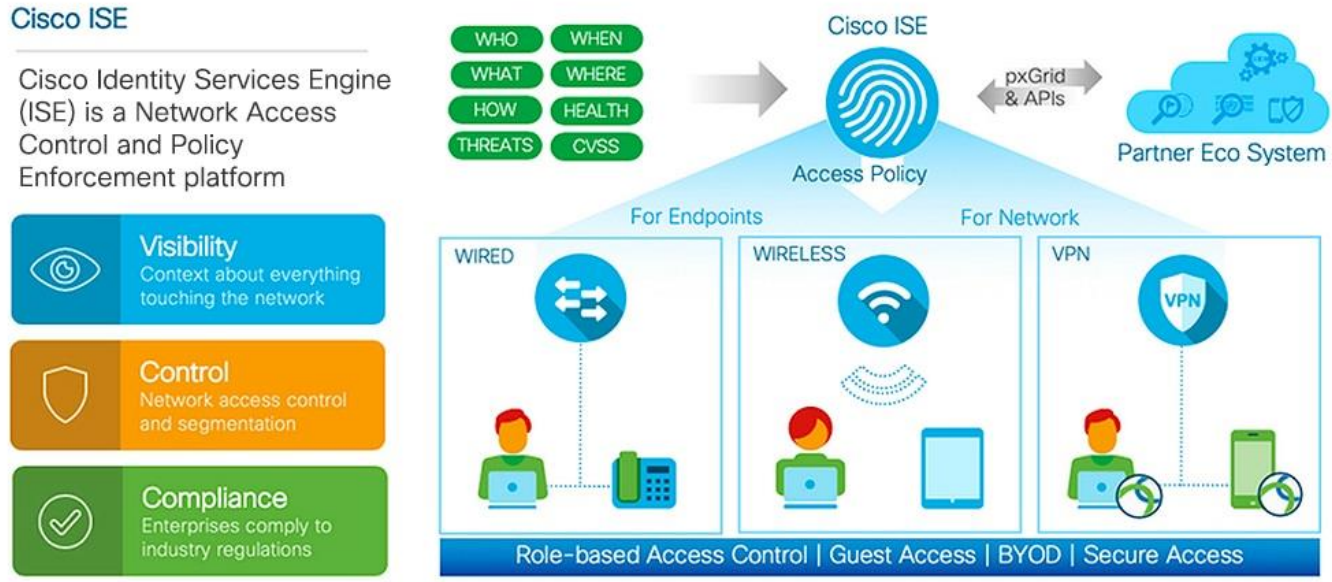

Рис.2.1. АрхітектураCisco Identity Services Engine

Технологія Cisco ISE використовується, щоб забезпечити відповідність, підвищити безпеку інфраструктури та оптимізувати роботу служби.

Адміністратор Cisco ISE може збирати контекстні дані в реальному часі для мережі, включаючи користувачів і групи користувачів (хто?), тип пристрою (що?), час доступу (коли?), місце доступу (де?), тип доступу (проводовий) , безпроводовий доступ або VPN) (як?), а також мережеві загрози та вразливості (рис.2.1).

Адміністратор Cisco ISE використовувє цю інформацію для прийняття рішень щодо управління мережею. Це також дає можливість зв’язати ідентифікаційні дані з різними мережевими елементами, щоб створити політики, які регулюють доступ до мережі та її використання.

2.2. Призначення та функції технології Cisco ISE

Програмне забезпечення на основі технології Cisco ISE надає основні функції та можливості щодо управління пристроями в мережі організації:

Адміністрування пристроїв: Cisco ISE використовує протокол безпеки TACACS+ для контролю та аудиту конфігурації мережевих пристроїв. Це полегшує детальний контроль того, хто може отримати доступ до якого мережевого пристрою, і змінювати відповідні налаштування мережі. Мережеві пристрої можна налаштувати для запиту Cisco ISE для автентифікації та авторизації дій адміністратора пристрою. Ці пристрої також надсилають облікові повідомлення до Cisco ISE для реєстрації таких дій.

TACACS (система контролю доступу до контролера доступу до терміналу) — це протокол безпеки, який забезпечує централізовану перевірку користувачів, які намагаються отримати доступ до маршрутизатора або NAS. TACACS+ надає окремі послуги автентифікації, авторизації та обліку. Ви можете використовувати TACACS+ Vendor-Specific Attributes (VSA) для керування авторизацією адміністратора. TACACS+ VSA дозволяють швидко змінювати ролі, домени доступу та групи користувачів адміністраторів через ваш каталог замість того, щоб змінювати параметри брандмауера.

Підтримувані операції TACACS+.

Автентифікація TACACS — це дія визначення користувача (або сутності). Традиційна автентифікація використовує ім’я користувача та фіксований пароль. Однак фіксовані паролі мають обмеження. Багато сучасних механізмів автентифікації використовують «одноразові» паролі або запит виклик-відповідь.

TACACS+ розроблено, щоб підтримувати все це та бути достатньо потужним, щоб працювати з будь-якими майбутніми механізмами.

Авторизація — це дія, яка визначає, що користувачеві дозволено робити. Авторизація TACACS+ не просто надає відповіді «так» чи «ні», але також може налаштувати послугу для конкретного користувача. Сервер TACACS+ може відповідати на ці запити, дозволяючи службу, але встановлюючи часові обмеження на оболонку входу, або вимагаючи списки доступу IP для з'єднання PPP.

Облік - є третьою дією після автентифікації та авторизації. Але знову ж таки, ні автентифікація, ні авторизація не потрібні. Облік — це дія запису того, що користувач робить і/або зробив. TACACS+ Accounting може служити двом цілям: Його можна використовувати як інструмент аудиту для служб безпеки. Його також можна використовувати для обліку використаних послуг, наприклад у платіжному середовищі.

Відіграючи центральну роль у світі бізнесу в результаті розвитку цифрових технологій, системи віддаленого доступу мають багато переваг, таких як забезпечення стабільності робочих процесів, підвищення ефективності та оптимізація витрат. Однак слід також зазначити, що ця модель керування доступом створює деякі труднощі з точки зору кібербезпеки. Ключем до мінімізації цих проблем або навіть до того, щоб вони не постраждали так часто, є використання модуля TACACS+ / RADIUS Access Management.[12]

Віддалена автентифікація дозволяє зберігати імена користувачів і паролі у вашій IT-мережі в одному місці на центральному сервері. Протоколи TACACS+ і RADIUS також пропонують унікальну інфраструктуру для налаштування відповідних імен користувачів і паролів. Ви можете налаштувати зміни на кожному окремому мережевому пристрої за допомогою обох протоколів, коли користувач додається чи видаляється, або коли користувач змінює пароль.

Крім того, скажімо, ви вносите лише одну зміну в конфігурацію на сервері. Без необхідності втручатися в роботу інших компонентів системи пристрої

продовжують отримувати доступ до сервера для автентифікації. Хоча найвідомішою функцією TACACS+ і RADIUS є аутентифікація, слід зазначити, що функції авторизації та обліку також досить ефективні.

Термінал Access Controller Access-Control System Plus (TACACS+) і Remote Access Dial In User Service (RADIUS) є двома поширеними протоколами безпеки для доступу до IT-мереж. TACACS+ використовується для адміністративного доступу до мережевих пристроїв, таких як маршрутизатори та комутатори, або пристроїв у мережі. RADIUS, з іншого боку, призначений для автентифікації та реєстрації віддалених користувачів мережі, які бажають отримати доступ до вашої IT-мережі. Обидва протоколи безпеки забезпечують керування автентифікацією, авторизацією та обліком (AAA) для пристроїв, які підключаються до IT-мережі та використовують її.

Забезпечуючи керування AAA, що складається з етапів автентифікації, авторизації та обліку, TACACS+ / RADIUS Access Management — це процес із 9 кроків, який класифікується як Автентифікація та адміністрування. Мережевий адміністратор, мережевий фахівець, магістральний спеціаліст беруть активну роль у цьому робочому процесі з 9 кроків. Крім того, Active Directory (AD) сприяє безперебійній роботі керування доступом, забезпечуючи завершення етапу полегшеного протоколу доступу до каталогу (LDAP) на завершальній фазі процесу. Тепер розглянемо принцип роботи з 9 кроків.[12]

Автентифікація

1-й крок : користувач ініціює сеанс CLI на цільовому пристрої. Після цього користувач вводить ім'я користувача та пароль.

2-й крок : цільовий пристрій надсилає ім’я користувача та пароль диспетчеру доступу TACACS+.

3-й крок : якщо ім’я користувача та пароль правильні, генерується успішна відповідь.

4-й крок : цільовий пристрій надсилає відповідь користувачеві.

5-й крок : між користувачем і цільовим пристроєм встановлюється сеанс CLI. Після цього кроку користувач може вводити команди для керування пристроєм.

Авторизація

6-й крок : користувач вводить команду на екрані CLI, і ця команда надсилається на цільовий пристрій.

7-й крок : цільовий пристрій надсилає відповідну команду диспетчеру доступу модуля TACACS+.

8-й крок : TACACS+ Access Manager перевіряє, чи має відповідний користувач привілей виконувати цю команду. Після перевірки він або приймає, або відхиляє. Записує цю команду разом із відповіддю.

9-й крок : якщо TACACS+ Access Manager відповідає повідомленням про прийняття, цільовий пристрій виконує команду та надсилає відповідь користувачеві. Якщо відповіддю є повідомлення про відхилення, цільовий пристрій надсилає користувачеві повідомлення про помилку.

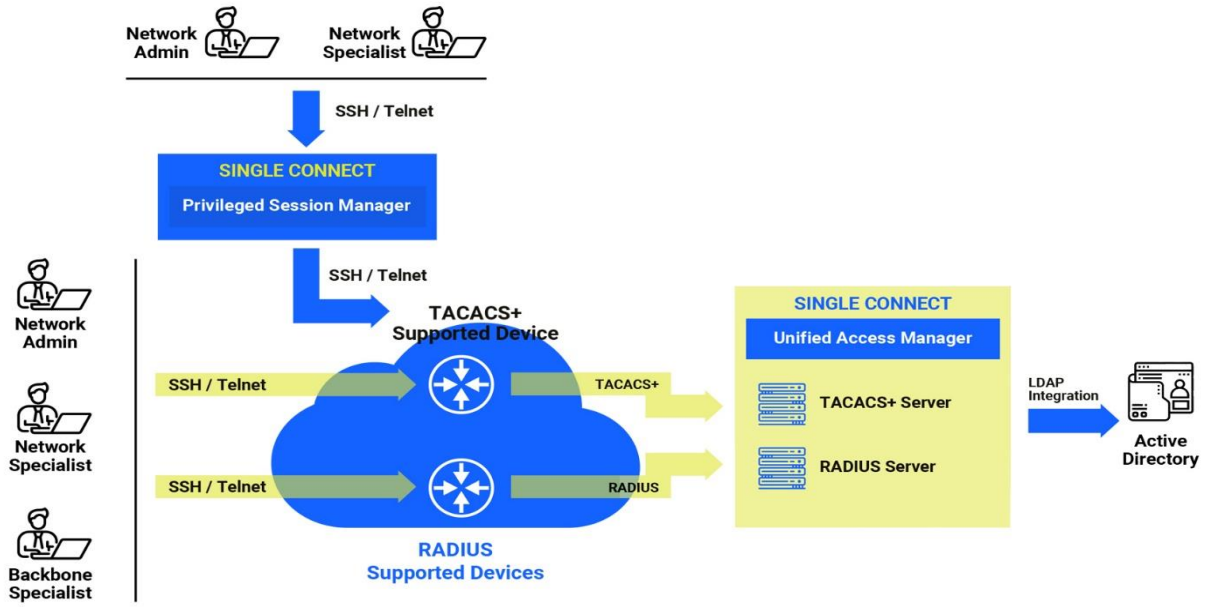

Рис. 2.2. Основні кроки AAA [12]

Основні переваги модуля TACACS+ / RADIUS Access Management таким чином:

За допомогою автономного рішення AAA не потрібна додаткова платформа для заміни застарілих серверів Cisco ACS.

Повна видимість із детальними журналами аудиту

Розподіл обов'язків і принцип найменших привілеїв

Повна відповідність міжнародним нормам, таким як GDPR та ISO27001, з груповими політиками Active Directory, поширеними на мережеву інфраструктуру

Прямий контроль доступу до цільових пристроїв

Багатофакторна аутентифікація

Позбудьтеся слабких і/або прострочених паролів

Визначте часові обмеження доступу

Обмежені привілеї для кожного корпоративного відділу, ізольованого від мережі

Спрощення керування за допомогою імен користувачів і паролів Active Directory (AD).

Автоматично блокувати обліковий запис користувача після закінчення терміну роботи

Підтримка мережевих пристроїв на основі відкритого протоколу

Підтримка конфігурації пари значень атрибутів

Підтримка 250 000 пристроїв в одному екземплярі

Гостьовий і безпечний безпроводовий доступ: Cisco ISE дозволяє надавати безпечний доступ до мережі для відвідувачів, підрядників, консультантів і клієнтів. Такий доступ дозволяє використовувати веб-портали та мобільні портали для підключення гостей до мережі та внутрішніх ресурсів організації. Дозволяє визначити права доступу для різних типів гостей і призначити адміністраторів для створення та керування обліковими записами гостей.

Кожному обліковому запису користувача при створенні надається ім’я та пароль, призначається малюнок, створюється персональна папка для розміщення документів користувача. Ім’я персональної папки складається зі слова. Документи всіх користувачів можуть зберігатися у папці Спільні документи. Для користувачів,

що працюють на комп'ютерах однорангової мережі або таких, що не підключені до мережі, визначені три типи облікових записів:

•обліковий запис адміністратора комп'ютера;

•обліковий запис користувача з обмеженими правами;

•обліковий запис гостя.

Налаштування ОС може здійснювати лише користувач з правами адміністратора. Найменші права має користувач з обліковим записом гостя.

Облікові записи створюються окремо на кожному комп'ютері, що входять до складу робочої групи. Для домену визначено більше типів облікових записів. Найбільші права надаються Адміністратору домену. Для інших облікових записів у складі домену можна встановити більш гнучкі права доступу, наприклад, дозволити створення та зміну файлів тільки в окремих папках, встановити доступ до певних ресурсів мережі і тільки у визначений інтервал часу, обмежити розмір місця на диску для персональної папки користувача тощо.

Якщо облікові записи створюються на сервері, що виконує функції контролера домену, ці записи автоматично стають доступними на всіх комп'ютерах домену. Це дає змогу користувачеві використовувати свої налаштування на будь-якому комп'ютері мережі. Адміністратор домену може об'єднати облікові записи у групи з однаковими правами доступу до ресурсів мережі.

Концепція принесіть свій власний пристрій (BYOD): Cisco ISE дозволяє вашим співробітникам і гостям безпечно використовувати свої особисті пристрої в корпоративній мережі. Кінцеві користувачі функції BYOD можуть використовувати налаштовані шляхи для додавання своїх пристроїв і надання попередньо визначених автентифікацій та рівнів доступу до мережі.

BYOD розшифровується як «принеси свій власний пристрій», і найпоширенішим значенням BYOD є те, що працівники використовують власні особисті пристрої для підключення до мережі організації та доступу до того, що їм потрібно для виконання роботи. Це включає дані та інформацію, які можуть бути потенційно чутливими або конфіденційними.

Пристрої, які використовуються для BYOD, можуть включати смартфони, планшети, персональні комп'ютери, ноутбуки або USB-накопичувачі. Це дає працівникам більше свободи у використанні пристроїв, які полегшують виконання повсякденних завдань, що, зрештою, економить гроші роботодавців. Однак BYOD потрібно ретельно керувати, зосереджуючись на підтримці безпеки та продуктивності.

Принесіть свій пристрій (BYOD) — це можливість для співробітників підвищити свою продуктивність, а якщо вона виконується з використанням відповідних протоколів безпеки, політика «принесіть свій пристрій» забезпечує поєднання гнучкості та безпеки.

Працює BYOD наступним чином.

Встановлення системи безпеки BYOD

У контексті наведеного вище значення BYOD, як і у випадку з усіма мережами, першим кроком є переконатися, що кожен раз, коли користувач підключається до вашої системи, незалежно від пристрою, який він використовує, він робить це безпечним способом. Тому необхідно:

Використовувати надійні паролі та шифрування даних для кожного пристрою, який підключається.

Визначати типи конфіденційних даних (якщо такі є), які можна зберігати на локальних пристроях, а не на пристрої користувача.

Вирішіти, які мобільні інструменти безпеки BYOD або програмне забезпечення для керування даними встановити на кожному пристрої BYOD.

Виберіть відповідні функції блокування на основі часу, щоб користувачі не могли брати участь у тривалих сесіях, які дають можливість хакеру, який захопить їхній пристрій, підключитися до вашої мережі.

Вирішіть, як ваша організація може стерти конфіденційну інформацію з пристрою користувача, якщо це необхідно.

Видимість активів: Cisco ISE надає вам видимість і контроль над тим, хто і що є у вашій мережі постійно, через безпроводові, проводові та VPN-з'єднання.

Cisco ISE використовує зонди та датчики пристроїв, щоб прослухати спосіб підключення пристроїв до мережі. База даних профілів Cisco ISE класифікує пристрій. Це забезпечує видимість і контекст, необхідні для надання належного рівня доступу до мережі.

VPN (Virtual Private Network) – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером. Дані в ньому надійно зашифровані: ваш інтернет-провайдер не дізнається вашої локації та вебресурсів, які ви відвідали. [13]

Оновлена IP-адреса зазвичай створюється з іншого міста або країни. Наприклад, ви можете увійти в систему з Києва, перебуваючи в Україні, але ваша IP-адреса буде вказувати, що ви, наприклад, у Лондоні, Великій Британії.[13]

VPN-сервіси дозволяють користуватися ресурсами, доступ до яких заборонено за географічним принципом або на підставі рішень органів влади. Завдяки VPN можна вільно відвідувати заблоковані сайти, достатньо лише вибрати та завантажити додаток на свій комп'ютер або мобільний пристрій.

[13] надають рекомендаації коли варто користувати VPN.

Під час користування незахищеними загальнодоступними мережами Wi-Fi, щоб захистити свої дані.

Коли необхідний захищений доступ до інтернет-мережі та систем під час організації віддаленої роботи.

Щоб захистити себе від вебсайтів, програм і сервісів, які хочуть відстежувати ваші дії.

Щоб оператор або провайдер не міг відслідковувати ваших дій в інтернеті.

Щоб отримати доступ до заблокованих окупантом інформаційних ресурсів.

Як обрати VPN

При виборі VPN зверніть увагу на такі критерії:

Захист. Краще обрати VPN, в якому є шифрування військового класу (наприклад, AES-256), асортимент протоколів безпеки (OpenVPN, L2TP, IKEv2,

WireGuard та інші), захист від витоків через DNS, технологія TrustedServer, яка видаляє всі ваші дані при кожному перезапуску, та функцію автоматичного аварійного відключення (kill switch).

Підтримка операційних систем. Переконайтесь, що VPN підтримує операційні системи, якими ви користуєтесь: Android, iOS, Windows та інші потрібного покоління.

Кількість одночасних активних пристроїв. Головне, щоб вам вистачило.

Вартість. VPN бувають платні та безкоштовні. Платні можуть мати кращий рівень захисту, вищу швидкість з'єднання, підтримку більшої кількості операційних систем. [13]

При виборі VPN перевірте репутацію сервісу у пошуковику – чи не було фактів витоку або продажу даних користувача.

Не використовуйте російських VPN, вони, ймовірно, можуть надсилати дані російським спецслужбам.

Кілька варіантів VPN-сервісів, які рекомендують фахівці [13]:

ExpressVPN

Surfshark

PrivateInternetAccess

CyberGhostVPN

NordVPN

ProtonVPN

Безпечний доступ: Cisco ISE використовує широкий спектр протоколів автентифікації, щоб надати мережевим пристроям і кінцевим точкам безпечний доступ до мережі. До них належать, але не обмежуються, 802.1X, RADIUS, MAB, веб-методи аутентифікації, EasyConnect і зовнішні агенти.

RADIUS (Remote Authentication Dial-In User Service) — це клієнт-серверний протокол і програмне забезпечення, яке дозволяє серверам віддаленого доступу зв'язуватися з центральним сервером для автентифікації користувачів, які

підключаються за телефоном, і авторизувати їхній доступ до потрібної системи чи служби.

RADIUS дозволяє організації підтримувати профілі користувачів у центральній базі даних , яку можуть спільно використовувати всі віддалені сервери. Наявність центральної бази даних забезпечує кращу безпеку, дозволяючи компанії налаштувати політику, яку можна застосувати в одній адміністрованій точці мережі. Центральна база даних також спрощує відстеження використання для виставлення рахунків за доступ до мережі або постачальника послуг Інтернету та ведення статистики мережі. Створений колишнім мережевим постачальником Livingston Enterprises у 1991 році RADIUS є фактичним галузевим стандартом, який використовують провідні компанії-виробники мережевих продуктів. Інженерна робоча група Інтернету прийняла протокол RADIUS як проект стандарту в 2000 році, як зазначено в RFC 2865 .

Спочатку RADIUS був розроблений для підтримки великої кількості користувачів, які віддалено підключаються до Інтернет-провайдерів (ISP) або корпоративних мереж через пули модемів або інші послідовні лінії зв'язку «точка-точка». RADIUS зараз широко використовується для віддаленого доступу через різні типи мереж, включаючи бездротові мережі, мережі Ethernet та інші типи віддаленого доступу користувачів через Інтернет.

ISE 2.1 представив нову функцію під назвою Easy Connect , де логіни Microsoft Active Directory (AD) використовуються для пасивного відображення інформації користувача на існуючі мережеві сеанси, ініційовані за допомогою обходу автентифікації MAC (MAB). Це схоже на сценарій централізованої веб-автентифікації (CWA) або CWA Chaining, де ISE поєднує активний сеанс автентифікації MAB або 802.1X з ідентифікатором, отриманим із веб-автентифікації. ISE використовує ідентифікацію та членство в групах з пасивної ідентифікації (PassiveID), які використовуються як умови для призначення політики.

Переваги Easy Connect порівняно з 802.1X:

Для автентифікації користувача не потрібен заявник 802.1X

Для довіреного транспортування облікових даних не потрібна інфраструктура відкритих ключів (PKI).

Може використовуватися як основний ідентифікатор користувача або доповнювати інший активний ідентифікатор, наприклад MAB або 802.1X

Сегментація: Cisco ISE використовує контекстні дані про мережеві пристрої та кінцеві точки для полегшення сегментації мережі. Теги груп безпеки, списки контролю доступу, протоколи доступу до мережі та набори політик, які визначають авторизацію, доступ і автентифікацію, є деякими способами, за допомогою яких Cisco ISE забезпечує безпечну сегментацію мережі.

Положення або відповідність: Cisco ISE дозволяє перевірити відповідність, також відому як положення, кінцевих точок, перш ніж дозволити їм підключитися до вашої мережі. Ви можете гарантувати, що кінцеві точки отримають відповідні агенти позиції для послуг позиції.

Стримування загроз: якщо Cisco ISE виявляє атрибути загрози або вразливості з кінцевої точки, надсилаються адаптивні політики керування мережею для динамічної зміни рівнів доступу кінцевої точки. Після оцінки та усунення загрози або вразливості кінцевій точці повертається початкова політика доступу.

Інтеграція екосистеми безпеки: функція pxGrid дозволяє Cisco ISE безпечно обмінюватися контекстно-залежною інформацією, даними політики та конфігурації тощо з підключеними мережевими пристроями, сторонніми постачальниками або партнерськими системами Cisco.

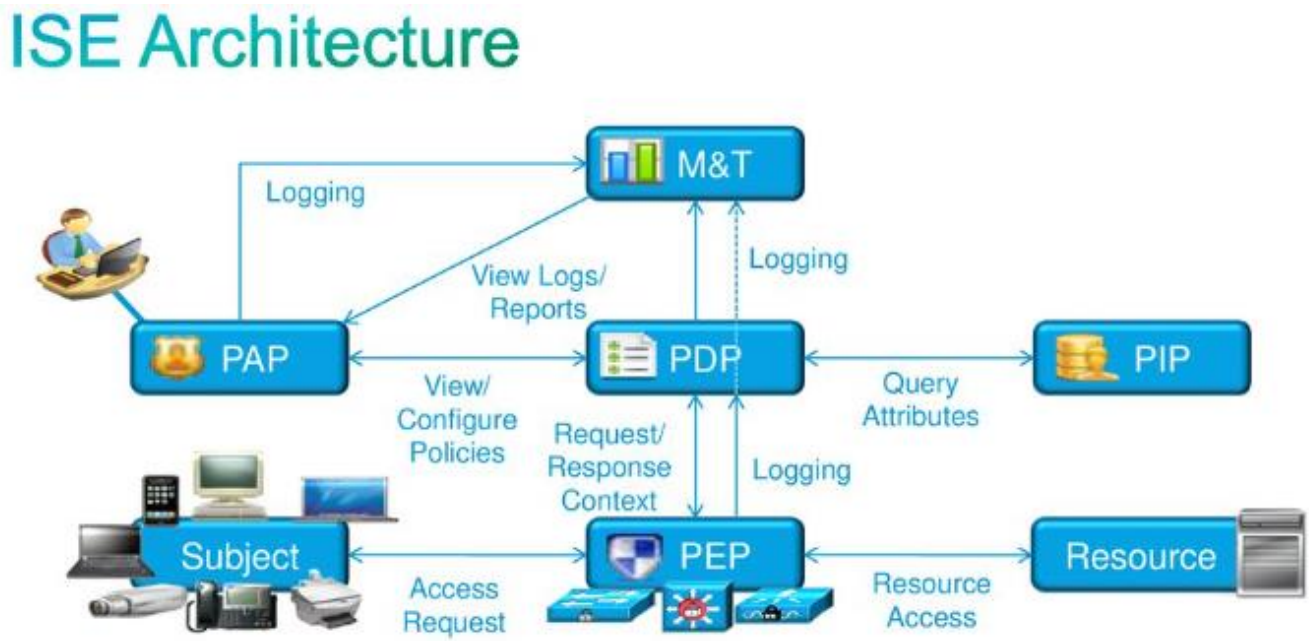

Рис. 2.2. Архітектура Cisco ISE[2]

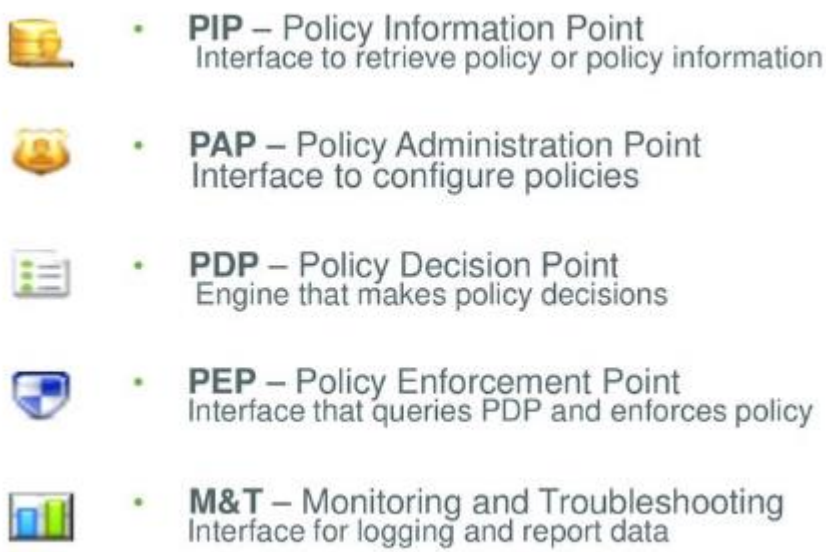

Рис 2.4 Архітектура ISE вузлів [4]

PIP – Policy Information Point. Це Інтерфейс пошуку або інформація про розділ.

PAP – Policy Administration Point. Інтерфейс для налаштування політик.

PDP – Policy Decision Point. Движок, який приймає рішення щодо політик.

PEP – Policy Enforcement Point. Інтерфейс, який запитує PDP і забезпечує дотримання політик.

M&T – моніторинг і усунення несправностей. Інтерфейс для реєстрації та звітування даних.

Cisco ISE надає автентифікованим користувачам доступ до певних сегментів мережі або певних програм і служб або до того й іншого на основі результатів автентифікації, які визначили в мережі адміністратори (рис2.3). [3]

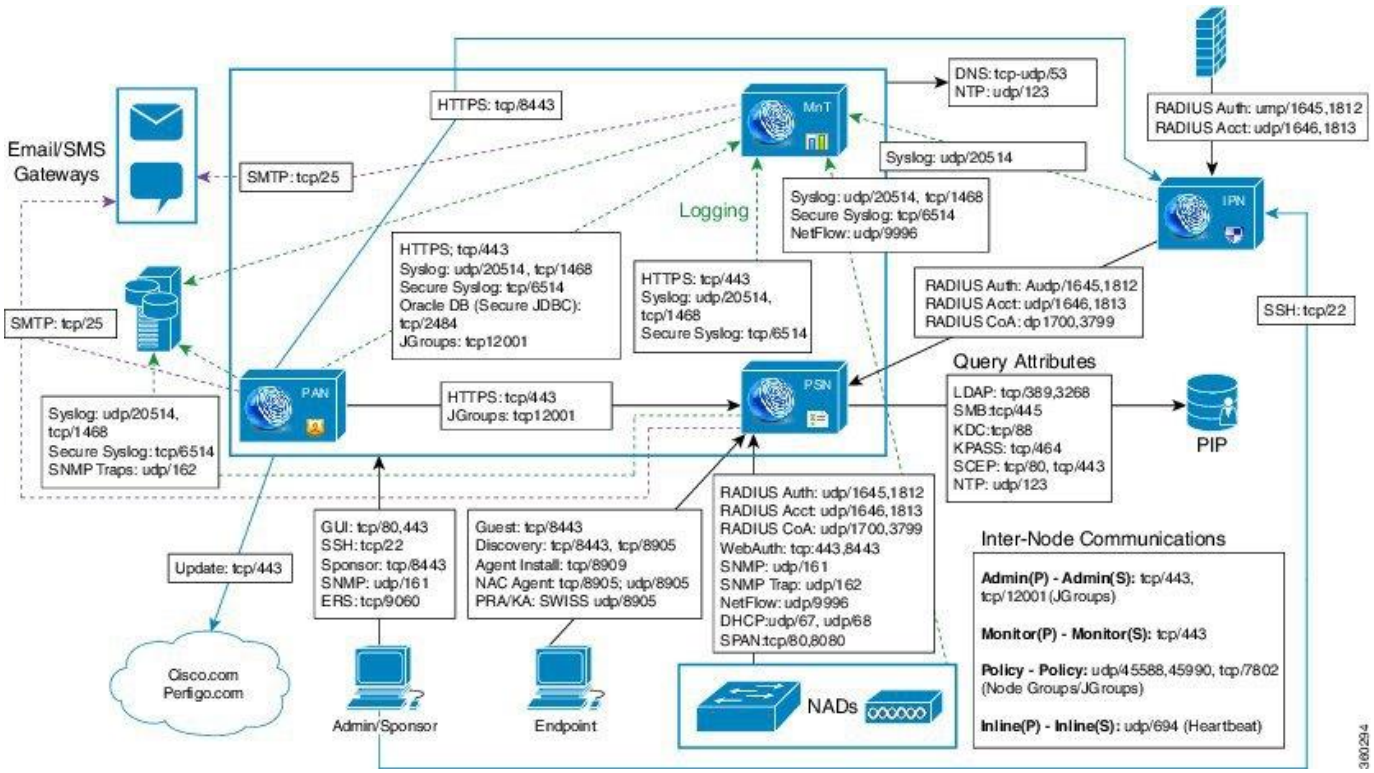

Рис 2.3. Доступ до певних сегментів мережі [3]

2.3. Вимоги до розгортання рішення Cisco ISE

Використання сценаріїв розгортання Cisco ISE вимагають розуміння відповідних термінів. Розглянемо чотири з них, які зазвичай використовуються:

Сервіс: сервіс — це певна функція, яку надає персона, наприклад доступ до мережі, профайлер, положення, доступ до групи безпеки, моніторинг і усунення несправностей тощо.

Вузол: вузол — це окремий екземпляр, який запускає програмне забезпечення Cisco ISE. Cisco ISE доступний як пристрій, а також як програмне

забезпечення, яке можна запускати на VMware. Кожен екземпляр (пристрій або VMware), який запускає програмне забезпечення Cisco ISE, називається вузлом.

Персона: Персона вузла визначає послуги, які надає вузол. Вузол Cisco ISE може приймати будь-яку з наступних персон: адміністрування, служба політики, моніторинг і pxGrid. Параметри меню, які доступні через портал адміністратора, залежать від ролі та персон, які приймає вузол Cisco ISE.

Модель розгортання: визначає, чи є ваше розгортання розподіленим, автономним або високодоступним у автономному режимі, що є базовим двовузловим розгортанням.

Розглянемо вузли в розподілених розгортаннях Cisco ISE

Вузол Cisco ISE може взяти на себе функції адміністрування, служби політики або моніторингу.

Вузол Cisco ISE може надавати різні послуги на основі персони, яку він приймає. Кожен вузол у розгортанні може взяти на себе функції адміністрування, служби політики та моніторингу. У розподіленому розгортанні можна використовувати таку комбінацію вузлів у своїй мережі:

Основний вузол адміністрування політики (первинний PAN) і вторинний вузол адміністрування політики (вторинний PAN) для високої доступності.

Первинний вузол моніторингу (первинний вузол MnT) і вторинний вузол моніторингу (вторинний вузол MnT) для високої доступності.

Пара вузлів перевірки працездатності або один вузол перевірки працездатності для основного автоматичного перемикання після відмови PAN.

Один або кілька вузлів служби політики (PSN) для перемикання сеансу після відмови

Налаштування вузлу Cisco ISE полягає в наступному.

Після інсталяції вузла Cisco ISE на ньому запускаються всі служби за замовчуванням, що надаються особами адміністрування, служби політики та

моніторингу. Цей вузол знаходиться в автономному стані. Необхідно увійти на портал адміністратора вузла Cisco ISE, щоб налаштувати його. При цьому немає можливості редагувати особи чи служби автономного вузла Cisco ISE. Однак можливо редагувати персони та служби основного та вторинного вузлів Cisco ISE. Тому необхідно спочатку налаштувати основний вузол ISE, а потім зареєструвати вторинні вузли ISE на основному вузлі ISE.

Після першого входу до вузла, необхідно змінити пароль адміністратора за замовчуванням і встановити дійсну ліцензію.

Для реєстрації вторинного вузола Cisco ISE необхідно зареєструвати вузли Cisco ISE до основної PAN, щоб створити багатовузлове розгортання. Вузли в розгортанні, відмінні від основної PAN, називаються вторинними вузлами. Під час реєстрації вузла ви можете вибрати персони та служби, які мають бути ввімкнені на вузлі. Зареєстрованими вузлами можна керувати з основної PAN (наприклад, керувати особами вузлів, послугами, сертифікатами, ліцензіями, застосовувати виправлення тощо).

Коли вузол зареєстровано, основний PAN надсилає конфігураційні дані на вторинний вузол, а сервер додатків на вторинному вузлі перезапускається. Після повної реплікації даних подальші зміни конфігурації, зроблені на первинній PAN, реплікуються на вторинний вузол. Час, необхідний для реплікації змін на вторинному вузлі, залежить від різних факторів, таких як затримка мережі, навантаження на систему тощо.

Перед тим як починати необхідно переконайтеся, що основний PAN і вузол, який реєструється, можуть зв’язуватись через DNS один з одним. Якщо вузол, який реєструється, використовує ненадійний самопідписаний сертифікат, вам буде запропоновано попередження про сертифікат разом із деталями сертифіката. Якщо ви приймаєте сертифікат, він додається до надійного сховища сертифікатів основного PAN, щоб увімкнути зв’язок TLS із вузлом.

Під час реєстрації вузла з увімкненими службами сеансу (такими як доступ до мережі, гостьовий режим, положення тощо) ви можете додати його до групи вузлів.

Cisco ISE підтримує декілька сценаріїв розгортання.

Cisco ISE можна розгорнути в інфраструктурі підприємства, підтримуючи проводові, безпроводові та віртуальні приватні мережі (VPN) 802.1X.

Архітектура Cisco ISE підтримує як автономні, так і розподілені (також відомі як висока доступність або резервування) розгортання, де одна машина бере на себе основну роль, а інша резервна машина бере на себе другорядну роль. Cisco ISE має різні конфігурації, служби та ролі, які дозволяють створювати та застосовувати служби Cisco ISE там, де це необхідно в мережі. Результатом є комплексне розгортання Cisco ISE, яке працює як повністю функціональна та інтегрована система.

Вузли Cisco ISE можна розгорнути з одним або декількома особами служби адміністрування, моніторингу та політики. Кожна особа виконує різну, але життєво важливу роль у загальній топології керування політикою мережі. Встановлення Cisco ISE за допомогою особи адміністратора дозволяє налаштовувати мережу та керувати нею з централізованого порталу для підвищення ефективності та простоти використання.

Розподілене розгортання Cisco ISE, це розгортання, яке має більше одного вузла Cisco ISE, називається розподіленим розгортанням. Для підтримки відновлення після відмови та підвищення продуктивності можливо налаштувати розгортання з кількома вузлами Cisco ISE розподіленим способом. У розподіленому розгортанні Cisco ISE діяльність з адміністрування та моніторингу централізована, а обробка розподілена між PSN. Залежно від потреб у продуктивності ви можете масштабувати розгортання. Кожен вузол Cisco ISE у розгортанні може взяти на себе будь-який із цих персонажів — адміністрування, служба політики та моніторинг.

Висновки до розділу 2

1. Проведено аналіз основних можливостей рішення Cisco ISE щодо управління пристроями в мережі організації. Це дозволило визначити особливості адміністрування на основі протоколу TACACS+, види користувачів та функції адміністратора, застосування концепції BYOD, визначити види інструментів для надання належного рівня доступу до мережі.

2. Представлено архітектуру Cisco ISE, на основі якої визначено вимоги до розгортання рішення Cisco ISE.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ УПРАВЛІННЯ ДОСТУПОМ ДО МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CISCO ISE

3.1. Розроблення варіанта розгортання системи управління доступом до мережі організації на базі рішення Cisco ISE

В другому розділі було розглянуто архітектуру, складові та функції Cisco Identity Services Engine (ISE).

В даному розділі буде розроблено питання щодо розгортання Cisco ISE.

Cisco ISE можна розгорнути в інфраструктурі підприємства, підтримуючи дротові, бездротові та віртуальні приватні мережі (VPN) 802.1X.

Архітектура Cisco ISE підтримує як автономні, так і розподілені (також відомі як висока доступність або резервування) розгортання, де одна машина бере на себе основну роль, а інша резервна машина бере на себе другорядну роль. Cisco ISE має різні конфігуровані особи, служби та ролі, які дозволяють створювати та застосовувати служби Cisco ISE там, де це необхідно в мережі. Результатом є комплексне розгортання Cisco ISE, яке працює як повністю функціональна та інтегрована система.

Вузли Cisco ISE можна розгорнути з одним або декількома особами служби адміністрування, моніторингу та політики. Кожна особа виконує різну, але життєво важливу роль у загальній топології керування політикою мережі. Встановлення Cisco ISE за допомогою особи адміністратора дозволяє налаштовувати мережу та керувати нею з централізованого порталу для підвищення ефективності та простоти використання.

1. Розподілене розгортання Cisco ISE

Розгортання, яке має більше одного вузла Cisco ISE, називається розподіленим розгортанням. Для підтримки відновлення після відмови та підвищення продуктивності ви можете розподілено налаштувати розгортання з кількома вузлами Cisco ISE. У розподіленому розгортанні Cisco ISE діяльність з адміністрування та моніторингу централізована, а обробка розподілена між PSN.

Залежно від ваших потреб у продуктивності ви можете масштабувати розгортання. Кожен вузол Cisco ISE у розгортанні може взяти на себе будь-яку з цих персон — адміністрування, службу політики та моніторинг.

Після встановлення Cisco ISE на всіх ваших вузлах, як описано в Посібнику з встановлення апаратного забезпечення Cisco Identity Services Engine , вузли переходять у автономний стан. Потім потрібно визначити один вузол як основний номер PAN. Визначаючи свій основний номер PAN, ви повинні ввімкнути адміністрування та моніторинг на цьому вузлі. Додатково можна ввімкнути персоналізацію служби політики на основній PAN. Після того, як ви виконаєте завдання визначення персон на первинному PAN, ви можете зареєструвати інші вторинні вузли в основному PAN і визначити персони для вторинних вузлів.

Усі налаштування системи Cisco ISE та конфігурації, пов’язані з функціональністю, слід виконувати лише на первинній PAN. Зміни конфігурації, які ви виконуєте на основній PAN, реплікуються на всі додаткові вузли у вашому розгортанні.

У розподіленому розгортанні має бути принаймні один MnT. Під час налаштування основного PAN ви повинні ввімкнути функцію моніторингу. Після того, як ви зареєструєте вузол MnT у своєму розгортанні, ви зможете редагувати основний PAN і за потреби вимкнути особу моніторингу.

2. Реплікація даних від основного до вторинного вузла Cisco ISE

Коли ви реєструєте вузол Cisco ISE як вторинний вузол, Cisco ISE негайно створює канал реплікації даних від основного до вторинного вузла та починає процес реплікації. Реплікація — це процес обміну даними конфігурації Cisco ISE від основного до вторинних вузлів. Реплікація забезпечує узгодженість даних конфігурації, доступних у всіх вузлах Cisco ISE, які є частиною вашого розгортання. клацніть відповідний перемикач, щоб увімкнути або вимкнути реплікацію динамічно виявлених кінцевих точок на всіх вузлах у вашому розгортанні Cisco ISE:

Повна реплікація зазвичай відбувається, коли ви вперше реєструєте вузол Cisco ISE як вторинний вузол. Інкрементна реплікація відбувається після повної реплікації та забезпечує відображення будь-яких нових змін, таких як додавання, модифікація або видалення конфігураційних даних у PAN, у вторинних вузлах. Процес реплікації гарантує, що всі вузли Cisco ISE у розгортанні синхронізовані. Ви можете переглянути статус реплікації в стовпці «Статус вузла» в розділі «Розгортання» .вікно порталу адміністратора Cisco ISE. Коли ви реєструєте вузол Cisco ISE як допоміжний вузол або виконуєте ручну синхронізацію з PAN, стан вузла відображає помаранчевий значок, що вказує на те, що виконується запитана дія. Після завершення синхронізації стан вузла стає зеленим, що вказує на те, що вторинний вузол синхронізовано з PAN.

3. Скасування реєстрації вузла Cisco ISE

Щоб видалити вузол із розгортання, необхідно скасувати його реєстрацію. Коли ви скасовуєте реєстрацію вторинного вузла з основної PAN, стан скасованого з реєстрації вузла змінюється на автономний, а зв’язок між основним і вторинним вузлом втрачається. Оновлення реплікації більше не надсилаються на скасований реєстр автономний вузол.

Після скасування реєстрації PSN дані кінцевої точки втрачаються. Якщо ви хочете, щоб PSN зберігав дані кінцевої точки після того, як він стане автономним вузлом, ви можете виконати одну з таких дій:

Отримайте резервну копію від основної PAN, і коли PSN стане автономним вузлом, відновіть цю резервну копію даних на ньому.

Змініть особу PSN на адміністрування (вторинний PAN), синхронізуйте дані з вікна розгортання на порталі адміністратора, а потім скасуйте реєстрацію вузла. Тепер цей вузол матиме всі дані. Потім ви можете додати додатковий номер PAN до наявного розгортання.

Розглянемо варіанти розгортання ISE.

У невеликому розгортанні ви можете мати всього 2 вузли ISE, обидва з яких запускають усі три необхідні персони ISE. Нижче наведено приклад невеликого розгортання ISE. Обидва вузли, ймовірно, будуть розміщені в центрах обробки даних і, ймовірно, спілкуватимуться з мережами кампусу/філій через WAN (глобальну мережу) для всіх служб автентифікації. Це означатиме, що збій глобальної мережі призведе до втрати служби автентифікації для тих сайтів, які постраждали.

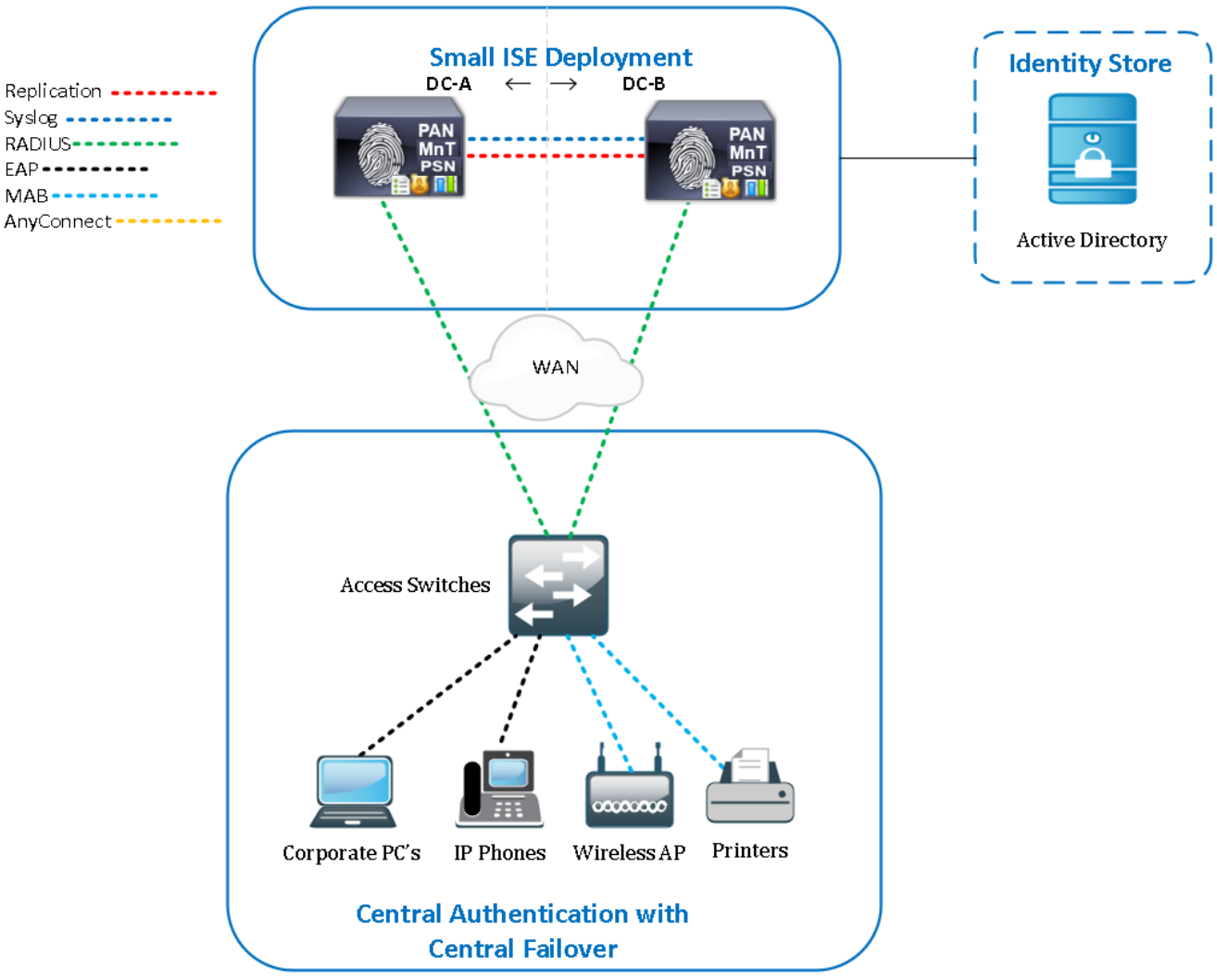

Рис.3.1. Схема невеликого розгортання ISE

У середньому розгортанні ви можете мати всього 7 вузлів ISE. На двох вузлах працюватимуть і особи PAN, і MnT, а до 5 вузлів працюватимуть як спеціальні особи PSN. Нижче наведено приклад середнього розгортання ISE. Вузли PAN/MnT, ймовірно, будуть розміщені в центрах обробки даних. У цій моделі ми звільнили PSN для розміщення в будь-якій мережі на ваш вибір. Деякі PSN можна розмістити поруч із PAN/MnT у центрі обробки даних, тоді як деякі можна розмістити в критичних місцях кампусу/філії. Це дозволить автентифікації критично важливих розташувань кампусу/філії зберегтися в разі збою WAN.

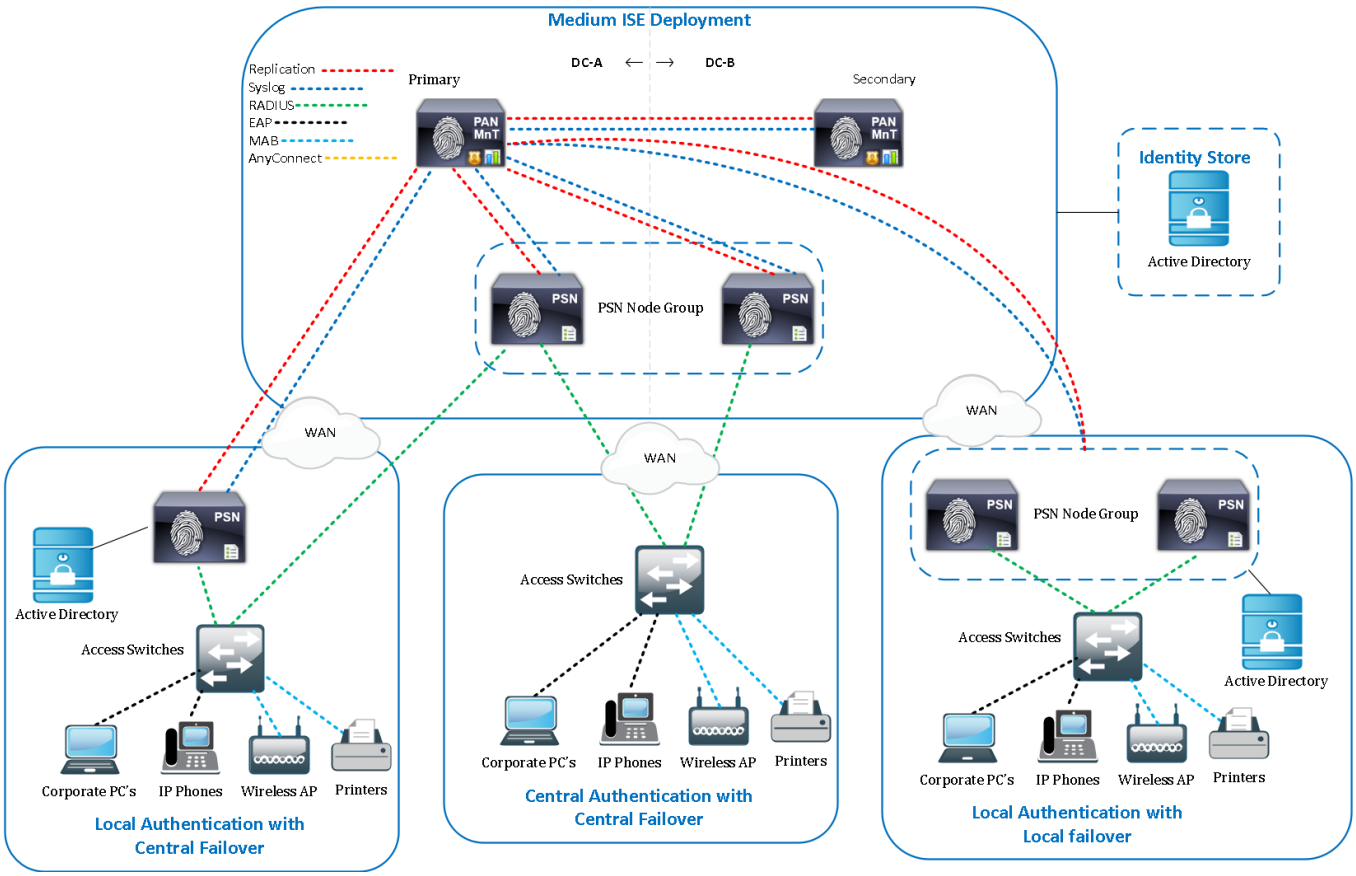

Рис.3.2. Схема середнього розгортання ISE

У великому розгортанніу вас може бути 54 вузли ISE. Два вузли керуватимуть особою PAN, 2 вузли керуватимуть особою MnT і до 50 вузлів працюватимуть як виділені особи PSN. Нижче наведено приклад великого розгортання ISE. Вузли PAN/MnT, ймовірно, будуть розміщені в центрах обробки даних. У цій моделі ми звільнили PSN для розміщення в будь-якому місці мережі

за вашим вибором і значно збільшили масштаб/гнучкість розгортання. Деякі PSN можна розмістити поряд із PAN/MnT у центрі обробки даних як пул інтерфейсу з балансувальником навантаження, а деякі можна розмістити в критичних місцях кампусу/філії. Це дозволить автентифікації критично важливих розташувань кампусу/філії зберегтися в разі збою WAN. Використання балансувальників навантаження, однак не обов'язкове,

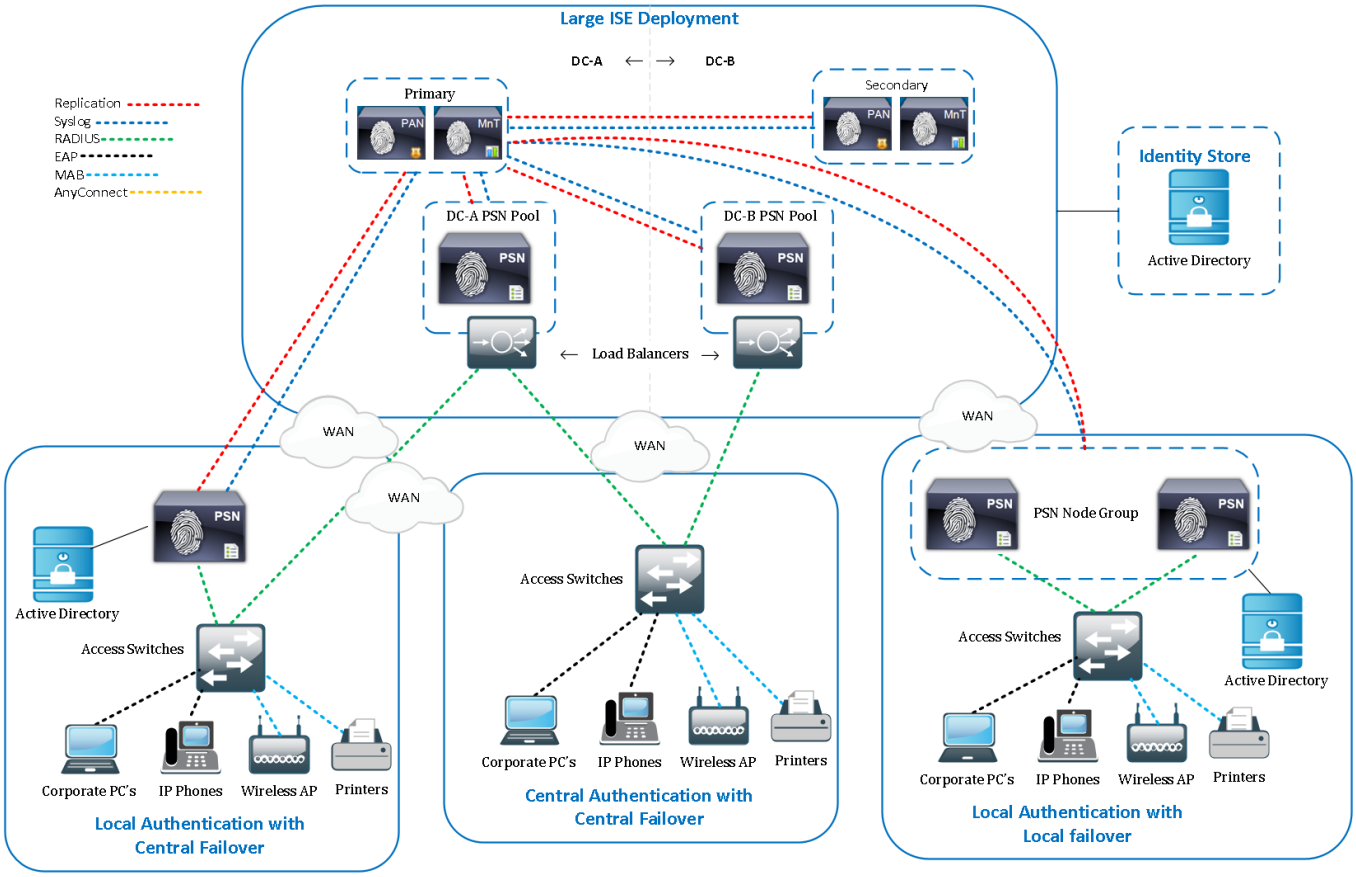

Рис.3.3. Схема великого розгортання ISE

Ви можете побачити, як розгортання Cisco ISE можна підібрати відповідно до ваших потреб у розгортанні, масштабуючи від дуже маленьких (1 або 2 вузли) до величезних (54 вузли).. Наступна блок-схема може бути використана як довідка, яка допоможе спростити вибір моделі розгортання Cisco ISE для випадку використання 802.1X.

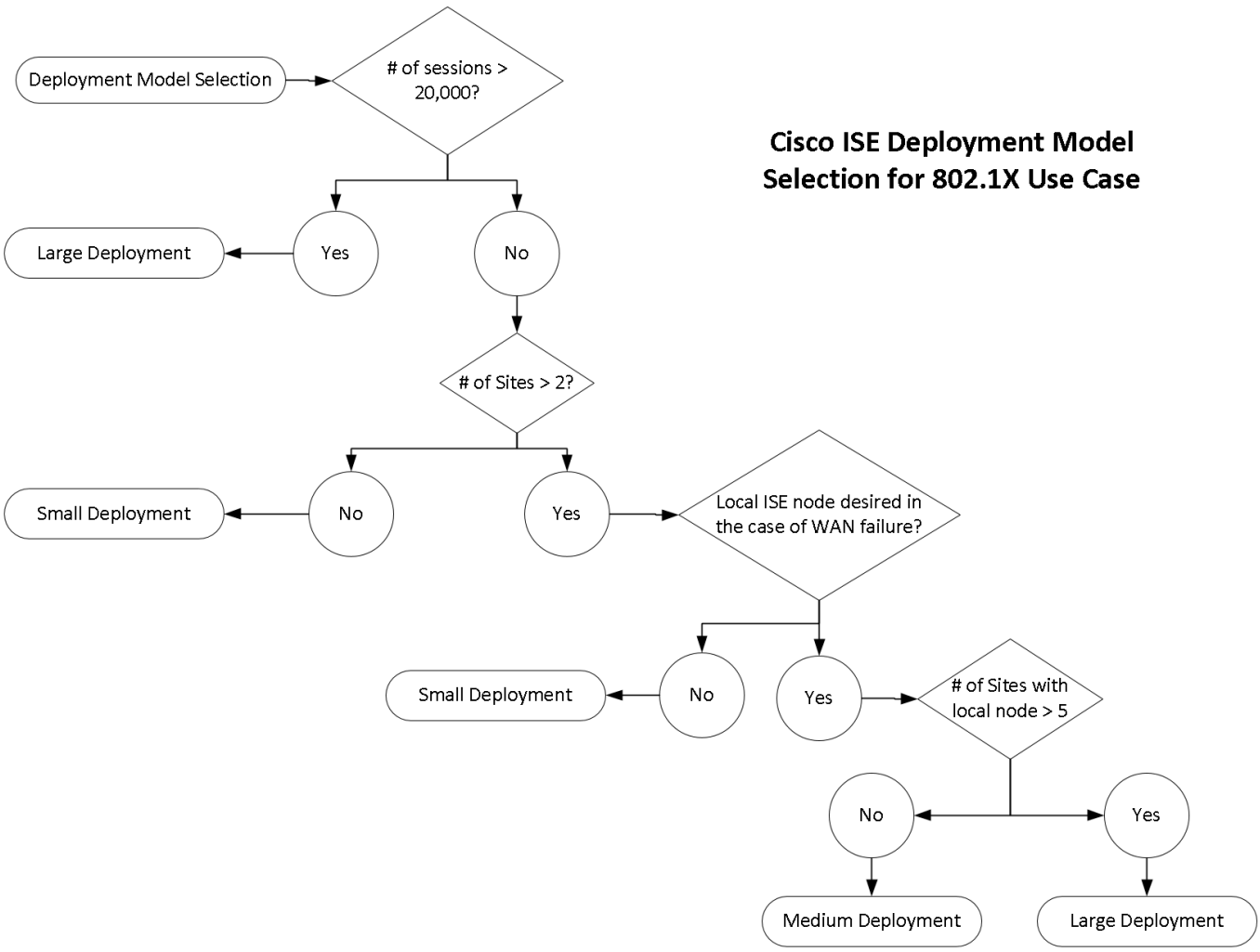

Рис.3.3. Технологія вибору типу розгортання ISE

3.2. Технологія управління доступом до мережі організації на базі рішення Cisco ISE

Перейдемо до опису конфігурацію політики Cisco ISE

Cisco ISE — це рішення для керування мережевим доступом на основі політики, яке пропонує набори політик доступу до мережі, що дозволяє вам керувати кількома різними випадками використання доступу до мережі, як-от безпроводове, проводове, гостьове та клієнтське забезпечення. Набори політик (як для доступу до мережі, так і для адміністрування пристроїв) дозволяють логічно групувати політики автентифікації та авторизації в одному наборі. Ви можете мати кілька наборів політик на основі області, наприклад наборів політик на основі

розташування, типу доступу та подібних параметрів. Коли ви встановлюєте ISE, завжди визначається один набір політик, який є набором політик за замовчуванням, і набір політик за замовчуванням містить у собі попередньо визначену та аутентифікацію за замовчуванням,

Під час створення наборів політик ви можете налаштувати ці правила (настроєні з умовами та результатами), щоб вибрати служби доступу до мережі на рівні набору політик, джерела ідентифікації на рівні політики автентифікації та дозволи мережі на рівнях політики авторизації. Ви можете визначити одну або кілька умов, використовуючи будь-які атрибути зі словників, що підтримуються Cisco ISE, для різних постачальників. Cisco ISE дозволяє створювати умови як окремі елементи політики, які можна повторно використовувати.

Служба доступу до мережі, яка буде використовуватися для кожного набору політик для зв'язку з мережевими пристроями, визначається на верхньому рівні цього набору політик. Послуги доступу до мережі включають:

Дозволені протоколи — протоколи, налаштовані для обробки початкового запиту та узгодження протоколу

Служба проксі — надсилає запити на зовнішній сервер RADIUS для обробки

У робочому центрі адміністрування пристроїв ви також можете вибрати відповідну послідовність сервера TACACS для свого набору політик. Використовуйте послідовність серверів TACACS, щоб налаштувати послідовність проксі-серверів TACACS для обробки.

Набори політик налаштовані ієрархічно, де правило верхнього рівня набору політик, яке можна переглянути в таблиці «Набір політик», застосовується до всього набору та збігається перед правилами для решти політик і винятків. Після цього правила набору застосовуються в такому порядку:

Правила політики автентифікації

Винятки з місцевої політики

Винятки з глобальної політики

Правила політики авторизації

Нова модель політики

Усі політики доступу до мережі та набори політик, включаючи автентифікацію, авторизацію та винятки, об’єднані разом у вікні « Набори політик» у Cisco ISE 2.3 і пізніших версій. Кожен набір політик — це контейнер, визначений на верхньому рівні ієрархії політик, у якому налаштовуються всі відповідні політики автентифікації та авторизації та правила винятків політики для цього набору.

На основі умов можна визначити кілька правил як для автентифікації, так і для авторизації. Тепер можна легко отримати доступ до умов і додаткових пов’язаних конфігурацій і повторно використовувати їх безпосередньо з нового інтерфейсу набору політик . Порядок, у якому збігаються набори політик, визначається порядком, у якому вони відображаються в новому інтерфейсі набору політик . Перевірка починається з першого рядка таблиці Policy Set і продовжується, доки не буде знайдено збіг. Якщо відповідності не знайдено, використовується системний набір політик за замовчуванням. Така ж логіка використовується для зіставлення та вибору правильної автентифікації, а потім правильних правил авторизації. Перевірку починають зверху кожного Таблиця набору політик і кожне правило перевіряється, доки не буде знайдено збіг. Правило за замовчуванням використовується, якщо немає інших правил.

Нова модель політики представляє всі політики, які також можна було додати в попередніх версіях за допомогою старого інтерфейсу користувача, але пропонує набагато більш спрощений і вдосконалений інтерфейс, за допомогою якого можна логічно керувати доступом до мережі.

Зміни в політиці автономної автентифікації та авторизації

Під час роботи з автономними правилами автентифікації правила з ISE 2.2 і попередніх версій перетворюються на нову модель політики. Існує два окремі сценарії на основі дозволених протоколів, призначених правилам автентифікації.

Якщо всім «зовнішнім частинам» у системі призначено той самий дозволений протокол, включаючи частину за замовчуванням, тоді всі вихідні правила автентифікації перетворюються таким чином:

Усі «зовнішні частини» перетворюються на єдиний набір політики в новій моделі політики. Новий набір політик називається за замовчуванням, і на рівні набору політик не визначено жодних умов і буде призначено уніфікований дозволений протокол. Усі внутрішні частини перетворюються на правила як частину політики автентифікації в новому наборі правил за замовчуванням.

Таблиця 3.1.

Параметри конфігурації набору політик

Назва поля	**Правила використання**
Статус	Виберіть статус цієї політики. Це може бути одне з наступного: Увімкнено: ця умова політики активна. Вимкнено: ця умова політики неактивна і не буде оцінюватися. Лише моніторинг: ця умова політики не буде оцінюватися.
Назва набору політики	Введіть унікальну назву для цього набору правил.
Умови	У новому рядку політики клацніть піктограму плюс (+) або в існуючому рядку політики клацніть піктограму Редагувати, щоб відкрити Conditions Studio.
Опис	Введіть унікальний опис політики.
Дозволені протоколи або послідовність сервера	Виберіть дозволений протокол, який ви вже створили, або натисніть знак (+), щоб створити новий дозволений протокол , створити нову послідовність радіусів або створити послідовність TACACS.
Умови	У новому рядку винятків клацніть піктограму плюс (+) або в наявному рядку винятків клацніть піктограму Редагувати, щоб відкрити Conditions Studio.
Оновлення	Звернення – це інструмент діагностики, який показує, скільки разів збігалися умови. Наведіть курсор на піктограму, щоб переглянути час останнього оновлення, скинути на нуль і переглянути частоту оновлень.

Назва поля	Правила використання
Дії	Натисніть значок шестерінки ⚙ в стовпці «Дії», щоб переглянути та вибрати різні дії: Вставити новий рядок вище: вставте нову політику над політикою, з якої ви відкрили меню «Дії». Вставити новий рядок нижче: вставте нову політику під політикою, з якої ви відкрили меню «Дії». Дублювати вище: вставте дублікат політики над політикою, з якої ви відкрили меню «Дії», над оригінальним набором. Дублювати нижче: вставте дублікат політики під політикою, з якої ви відкрили меню «Дії», під оригінальним набором. Видалити: видалити набір правил.
Перегляд	Клацніть піктограму стрілки, щоб відкрити вікно «Набір» певного набору політик і переглянути підполітики автентифікації, винятків і авторизації.

Правила автентифікації

Кожен набір політик може містити кілька правил автентифікації, які разом представляють політику автентифікації для цього набору. Пріоритет політик автентифікації визначається на основі порядку цих політик, як вони відображаються в самому наборі політик (зі сторінки перегляду «Установити» в області «Політика автентифікації»).

Cisco ISE динамічно вибирає службу доступу до мережі (або дозволений протокол, або послідовність сервера) на основі параметрів, налаштованих на рівні набору політик, а потім перевіряє джерела ідентифікації та результати на рівнях політики автентифікації та авторизації. Ви можете визначити одну або кілька умов, використовуючи будь-який атрибут зі словника Cisco ISE. Cisco ISE дозволяє створювати умови як окремі елементи політики, які можна зберігати в бібліотеці, а потім повторно використовувати для інших політик на основі правил.

Метод ідентифікації, який є результатом політики автентифікації, може бути одним із наведених нижче.

– Заборонити доступ — користувачу заборонено доступ і автентифікація не виконується.

– База даних ідентифікаційних даних — єдина база даних ідентифікаційних даних, яка може бути будь-якою з наведених нижче.

Внутрішні користувачі

Гостьові користувачі

Внутрішні кінцеві точки

Активна Директорія

База даних Lightweight Directory Access Protocol (LDAP).

Сервер токенів RADIUS (сервер RSA або SafeWord)

Профіль автентифікації сертифіката

– Послідовності джерел ідентифікаційних даних — послідовність баз даних ідентифікаційних даних, яка використовується для автентифікації.

Набір політик за замовчуванням, реалізований під час початкової інсталяції Cisco ISE, включає стандартні правила автентифікації та авторизації ISE. Набір правил за замовчуванням також включає додаткові гнучкі вбудовані правила (які не є правилами за замовчуванням) для автентифікації та авторизації. Ви можете додавати додаткові правила до цих політик, а також видаляти та змінювати вбудовані правила, але ви не можете видалити правила за замовчуванням і ви не можете видалити набір політик за замовчуванням.

Потік політики автентифікації

У політиках автентифікації можна визначити кілька правил, які складаються з умов і результатів. ISE оцінює умови, які ви вказали, і на основі результатів оцінки призначає відповідні результати. База даних ідентифікаційних даних вибирається на основі першого правила, яке відповідає критеріям.

Ви також можете визначити послідовність джерела ідентифікаційної інформації, що складається з різних баз даних. Ви можете визначити порядок, у якому Cisco ISE шукатиме ці бази даних (рис 3.5). Cisco ISE отримуватиме доступ до цих баз даних послідовно, доки автентифікація не буде успішною. Якщо в

зовнішній базі даних є кілька екземплярів одного користувача, автентифікація не вдається. У джерелі ідентифікаційної інформації може бути лише один запис користувача.

Як рекоменація -необхідно використовувати лише три або щонайбільше чотири бази даних у послідовності джерела ідентифікаційної інформації.

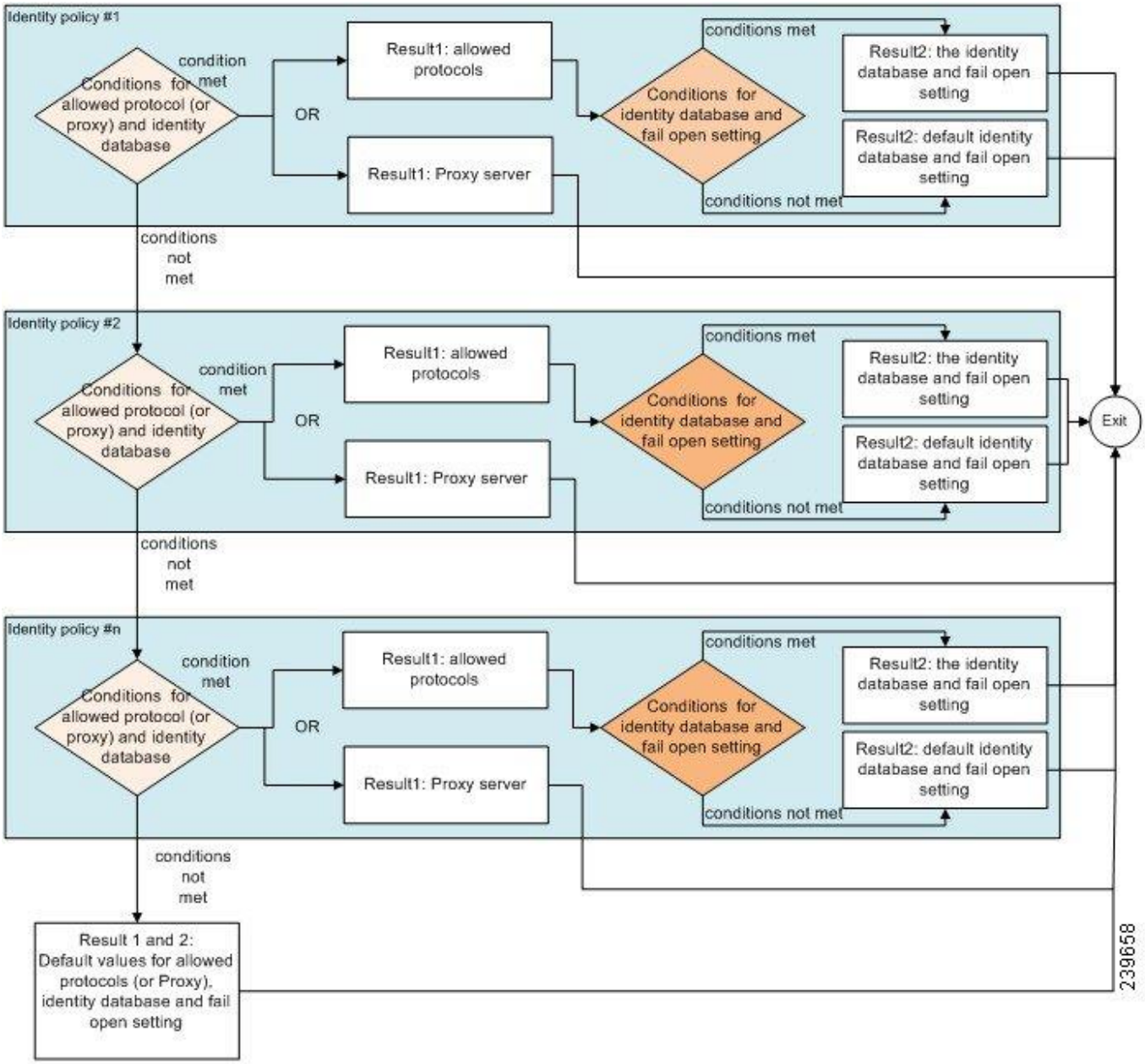

Рис.3.5. Потік політики автентифікації

Перейдемо до технології додавання пристроїв до групи мережевих пристроїв з відповідними політиками.

Для цього необхідно в ISE GUI, перейти до Адміністрування/ Ресурси мережі /Групи мережевих пристроїв/ Натисніть ДОДАТИ

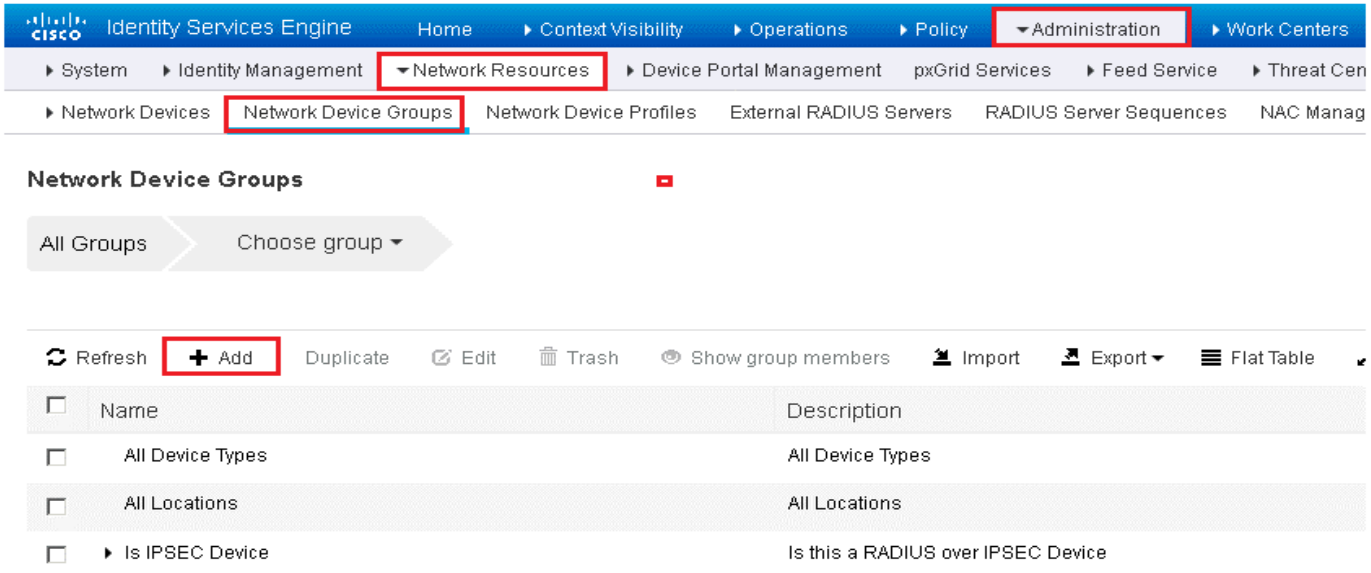

Рис.3.6. Меню ISE на початку додавання пристроїв

Додавати пристрої необхідно виду груп пристроїв, які для прикладу подано на рис.3.7.

Name	Description	Parent Group
Wired	Wired Access Switch	All Access Device Type
Wireless	WLCs	All Access Device Type
VPN	VPN Access Device	All Access Device Type
HQ	HeadQuaters	All Location
Branch1	Branch1	All Location
R&D	Research & Development LAB	All Location

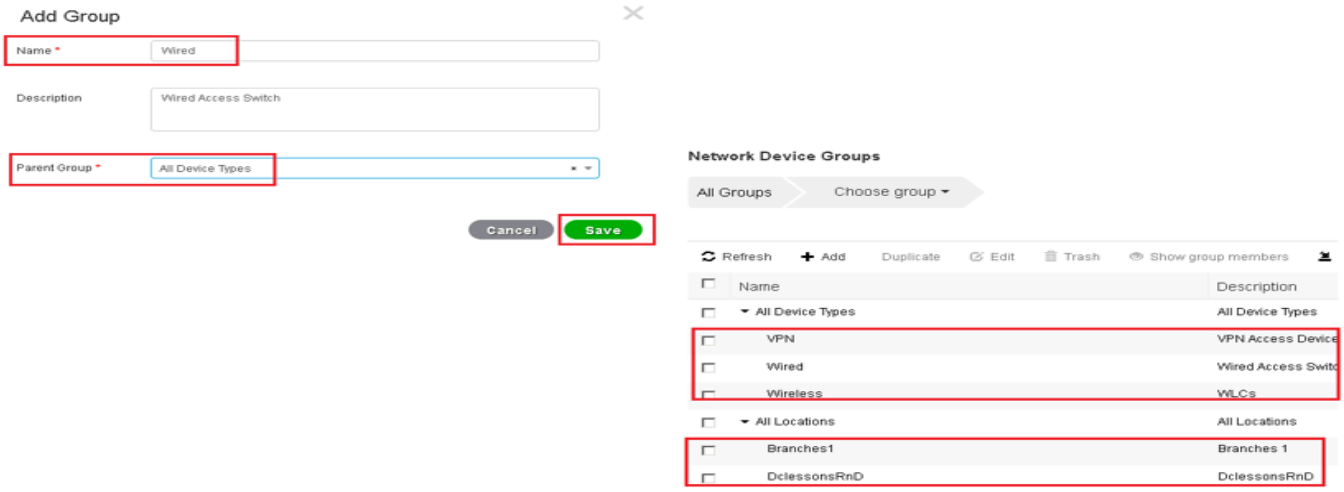

Рис. 3.7. Додавання пристроїв до відповідних груп

Наступним кроком буде визначення фактичного NAD (рис.3.8), який буде членом груп, які ми щойно створили. Для цього в консолі Адміністрація /Ресурси мережі/| Мережеві пристрої / Натисніть ДОДАТИ. Для комутатора доступу дотримуйтеся наведеної нижче процедури, щоб додати комутатор у NAD. Після чого натиснути надіслати.

Attribute	Value
Name	3k-access
Description	Access Switch
IP address	10.1.100.1/32
Model Name	NR
Software Version	NR
Network Device Group	
Location	HQ
IPSEC	No
Device Type	Wired
Radius Authentication Setting	Checked
Shared Secret	XXXXXXX
TACACS Authentication Setting	UnChecked
SNMP Setting	UnChecked
Advance TrustSec Setting	UnChecked

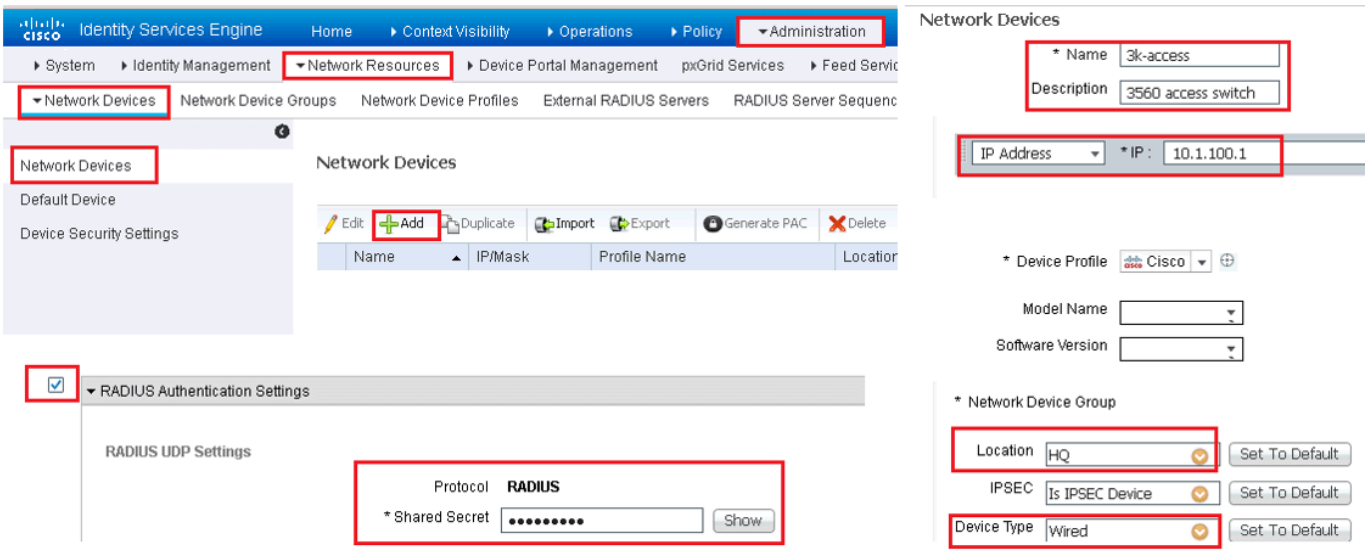

Рис.3.8 . Визначення фактичного NAD

Після того, як додано необхідні комутатори, необхідно перевірити WLC і додати ці мережеві пристрої до Cisco ISE.

Для цього необхідно увійти в WLC | Натисніть WLAN | Перевірте три мережі WLAN, налаштовані з ідентифікатором, як показано на рис 3.9, він використовуватиметься для користувачів Employee, Guest і Hotspot. Клацніть кожну мережу WLAN і встановіть її статус Увімкнено та ЗАСТОСУВАТИ до конфігурації.

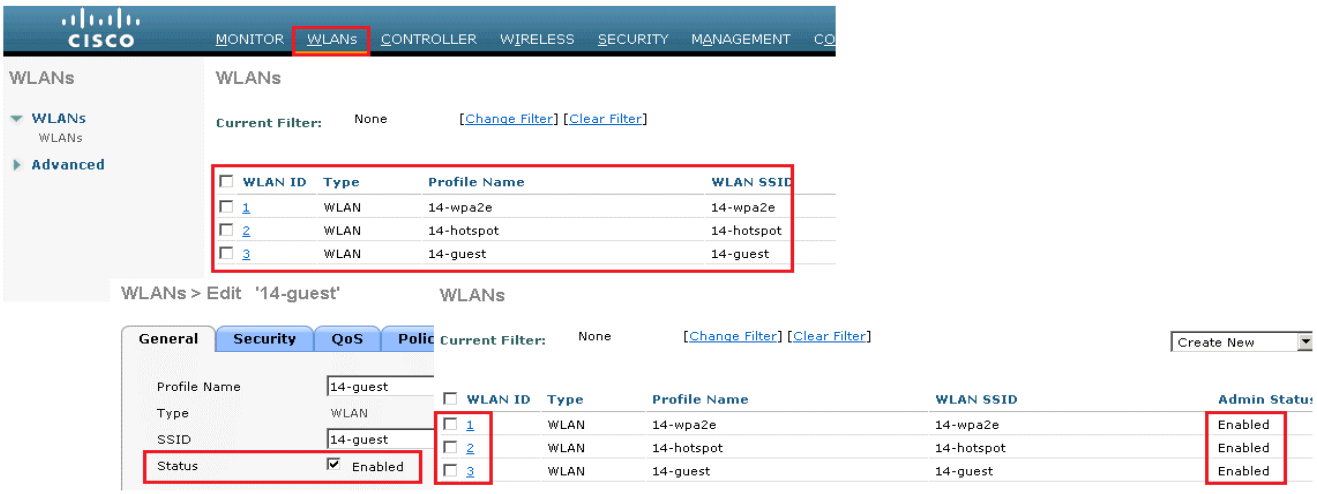

Рис. 3.9 Застосування конфігурацій

Перейдемо налаштування безпеки, для цього в консолі обираємо Безпека/ AAA/ RADIUS /Автентифікація . Переконайтеся, що RADIUS-сервер налаштовано. Зніміть прапорець у полі «Керування» та виконайте те саме для «Обліку», як показано на рис. 3.10. Після цього необхідно переконатись, натиснувши в консолі Wireless / і дізнатись, що ваш модуль AP виявлено.

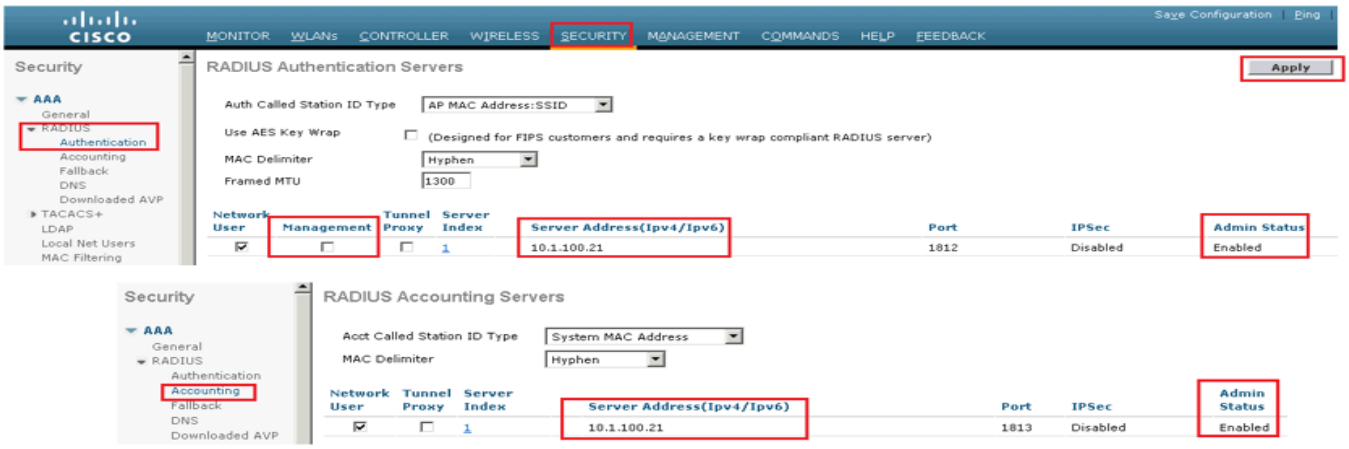

Рис.3.9. Налаштування безпеки

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

Cisco Identity Services Engine надає широкі можливості щодо управління доступом до мережі, а саме такі можливості:

Впровадження в корпоративну IT-інфраструктуру засобів аутентифікації і авторизації користувачів і кінцевих пристроїв, підключених до проводових мереж, безпроводових мереж і мереж VPN, забезпечення дотримання узгодженої політики в масштабах всього підприємства.

Запобігання несанкціонованого доступу до мережі для захисту корпоративних активів.

Управління повним життєвим циклом гостьового доступу за рахунок надання запрошуючим особам (Спонсорам) коштів для дозволу доступу їх гостей, що дозволяє знизити поточне навантаження на IT- фахівців.

Підтримка налаштованих порталів і можливість публікації web-сторінок для спрощення роботи як нових, так і досвідчених користувачів відповідно до прийнятих в організації процесів.

Забезпечення повномасштабного моніторингу шляхом виявлення, класифікації та управління підключеними до мережі кінцевими пристроями для надання відповідних сервісів і рівнів доступу.

Усунення вразливостей на комп'ютерах користувачів шляхом регулярної перевірки та коригування їх стану, що дозволяє нейтралізувати такі мережеві загрози, як віруси, черв'яки і шпигунські програми.

Забезпечення дотримання політик безпеки за рахунок блокування та ізоляції невідповідних корпоративним стандартам комп'ютерів в карантинній області, а також їх оновлення без залучення адміністратора.

Підтримка вбудованої консолі моніторингу, звітності та усунення неполадок для спрощення роботи фахівців служби підтримки та адміністраторів.

Підвищення точності профілювання підключених до мережі пристроїв за рахунок методів активного сканування пристрою. Цей механізм дозволяє підвищити точність профілювання пристроїв, для якого раніше використовувалися тільки кошти аналізу мережевого трафіку, за рахунок сканування певних атрибутів пристрою (відповідно до політики).

Управління доступом кінцевих пристроїв до мережі за допомогою сервісу захисту кінцевих пристроїв (EPS). Сервіс EPS дозволяє адміністратору пов'язувати кінцеві пристрої і дії, які необхідно виконати при підключенні пристрою (перенесення в нову VLAN, повернення в вихідну VLAN або повна ізоляція пристрою від мережі), за допомогою єдиного інтерфейсу.

Cisco Identity Services Engine надає ряд додаткових основних можливостей, які необхідно використовувати та розуміти фахівцім з кібербезпеки.

Протокол AAA

Використання стандартного протоколу RADIUS для аутентифікації, авторизації та обліку (AAA).

Протоколи аутентифікації

Підтримує широкий діапазон протоколів аутентифікації, включаючи PAP, MS-CHAP, Extensible Authentication Protocol (EAP) -MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST) та EAP-Transport Layer Security (TLS).

Модель політики

Підтримує модель політики на основі правил і умов для створення гнучких і важливих для бізнесу політик контролю доступу. Дозволяє задавати політики шляхом вилучення атрибутів із заздалегідь визначених баз, в яких містяться дані про облікові дані користувачів і кінцевих пристроїв, оцінці стану, протоколах аутентифікації, результати профілювання і т. д. Атрибути можна створити динамічно і зберегти для використання в подальшому.

Контроль доступу

Підтримує безліч різних механізмів контролю доступу, включаючи завантажуємі списки контролю доступу (dACL), призначення мереж VLAN, перенаправлення по URL-адресам і додавання міток SGA, що дозволяє використовувати розширені можливості мережевих пристроїв Cisco.

Профілювання

У базі даних платформа містяться зумовлені шаблони пристроїв для різних кінцевих пристроїв, таких як IP-телефони, принтери, IP-камери, смартфони і планшети. Адміністратори можуть створювати власні шаблони пристроїв. Їх можна використовувати для автоматичного виявлення, класифікації і зв'язування визначених адміністраторами ідентифікаційних даних при підключенні кінцевих пристроїв до мережі. Крім того, адміністратори можуть задавати політики авторизації на основі типу пристрою.

Платформа Cisco Identity Services Engine збирає відомості про атрибути кінцевих пристроїв з використанням засобів пасивної мережевої телеметрії, шляхом активного сканування кінцевих пристроїв, а також шляхом взаємодії з сенсорами пристроїв, що функціонують на комутаторах Cisco Catalyst.

Засоби профілювання пристроїв, розміщені на комутаторах Cisco Catalyst, є одним з елементів технології профілювання Cisco ISE. Вони дозволяють комутаторам швидко зібрати відомості про кінцеві пристрої, підключені до них, і передати зібрані відомості по протоколу RADIUS платформі Cisco ISE для класифікації пристроїв і призначення відповідних політик. Технологія профілювання з використанням сенсорів на комутаторах дозволяє здійснити ефективний збір відомостей про кінцеві пристрої в рамках розподіленої IT-інфраструктури, а також забезпечує масштабованість платформи, спрощує розгортання і дозволяє підвищити ефективність класифікації пристроїв.

Управління життєвим циклом гостьового доступу

Платформа забезпечує управління повним життєвим циклом гостьового доступу, при якому користувачі зі статусом «Гість» можуть отримати

контрольований доступ до мережі протягом обмеженого часу при підтримці адміністратора або шляхом самостійної реєстрації на порталі гостьового доступу. Дозволяє адміністраторам налаштовувати портали і політики з урахуванням конкретних потреб організації.

Оцінка стану кінцевих пристроїв

Проводить оцінку стану кінцевих пристроїв для всіх типів користувачів, що підключаються до мережі. Функціонує з використанням або постійно встановленого на пристрої агента, або з використанням тимчасово завантаженого web-агента. В процесі оцінки стану кінцевих пристроїв оцінюється відповідність кінцевого пристрою вимогам політик безпеки, таким як наявність останніх виправлень для операційних систем і наявність пакета антивірусного програмного забезпечення з найостаннішими і актуальними антивірусними базами. Розвинена система оцінки стану кінцевих пристроїв дозволяє виконувати перевірку файлових змінних (версія, дата і т. д.), реєстру (розділ, значення і т. д.) і додатків. Щоб гарантувати відповідність кінцевого пристрою політикам компанії, платформа Cisco ISE забезпечує регулярне автоматичне оновлення клієнта і проводить повторну оцінку стану пристрою.

Сервіс захисту кінцевих пристроїв

Дозволяє адміністраторам оперативно вживати коригувальні заходи (розміщення в карантин, вихід із карантину і повне блокування) до крайових пристроїв, що не відповідає вимогам політик безпеки. Це дозволяє знизити ризики і підвищити рівень захищеності всієї IT-інфраструктури.

Централізоване управління

Дозволяє адміністраторам централізовано налаштовувати сервіси профілювання, оцінки стану, гостьового доступу і авторизації і керувати ними за допомогою єдиної web-консолі з графічним інтерфейсом, значно спрощуючи адміністрування за рахунок узгодженого управління всіма сервісами.

Моніторинг і усунення неполадок

Включає інтегрований компонент моніторингу, звітності та усунення неполадок, доступний за допомогою графічного web-інтерфейсу і призначений для спрощення роботи співробітників служби підтримки та операторів мереж. Пропонує засоби формування комплексної звітності для всіх сервісів, реєстрації всіх дій, а також відстеження в режимі реального часу всіх користувачів і кінцевих пристроїв, що підключаються до мережі, за допомогою панелі моніторингу.

Висновки до розділу 3

1. В роботі запропоновано три види схем розгортання ISE в організації на основі представленого алгоритму розрахунку вузлів в інформаційні системі організації.

2. Розроблено технологію управління доступом до мережі організації на базі рішення Cisco ISE на базі потік політики автентифікації. Такі політики створюються на основі відповідних груп користувачів.

3. В практичній частині показано основні кроки щодо підключення пристроїв до інфраструктури організації, відповідно до прийнятих політик та налаштування протоколу автентифікації.

4. Розроблено рекомендації щодо застосування технології управління доступом до мережі організації на базі рішення Cisco ISE , які покращують розуміння необхідності використання модулів даного рішення.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи отримано наступні результати:

1. Проведено аналіз технології контролю доступу до мережі організації, в результаті якого визначено важливу роль у наданні доступу до ресурсів із найменшими привілеями.

2. Проведено аналіз загроз інформаційній системі організації на основі звіту IBM Security® X-Force®. Визначено основні загрози, які можуть бути зупинені шляхом впровадження рішень контролю доступу до мережі організації.

3. Проведено вибір рішення на основі досліджень Gartner, який визначає контроль доступу до мережі (NAC) як технології, які дозволяють організаціям впроваджувати політики контролю доступу до корпоративної інфраструктури як орієнтованими на користувача пристроями, так і пристроями Інтернету речей (IoT). Для подальшого дослідження було обрано технологію CISCO ISE, надійне рішення безпеки.

4. Проведено аналіз контролю доступу до мережі організації відіграє важливу роль у наданні доступу до ресурсів із найменшими привілеями.

5. В роботі запропоновано три види схем розгортання технології ISE в організації на основі представленого алгоритму розрахунку вузлів в інформаційні системі організації.

6. Розроблено технологію управління доступом до мережі організації на базі рішення Cisco ISE на базі потоку політик автентифікації. Такі політики створюються на основі відповідних груп користувачів.

7. В практичній частині показано основні кроки щодо підключення пристроїв до інфраструктури організації, відповідно до прийнятих політик та налаштування протоколу автентифікації.

8. Розроблено рекомендації щодо застосування технології управління доступом до мережі організації на базі рішення Cisco ISE , які покращують розуміння необхідності використання модулів даного рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Контроль доступу до мережі URL: https://www.arubanetworks.com/faq/what-is-network-access-control/ (дата звернення: 01.10.2024).
2. Identity Services Engine URL: https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_overview.html (дата звернення: 02.10.2024).
3. Архітектура ISE URL: https://smbitsolutions.wordpress.com/2012/07/12/cisco-identity-services-engine/ (дата звернення: 11.10.2024).
4. Доступ до певних сегментів мережі URL: https://www.routexp.com/2020/03/cisco-ise-cisco-identity-services-engine.html
5. http://blog.51sec.org/2019/12/ise-studying-notes.html (дата звернення: 30.09.2024).
6. Розгортання ISE URL: https://www.linkedin.com/pulse/cisco-ise-device-administration-model-mohammad-ahmadvand/ (дата звернення: 01.10.2024).
7. Дослідження Gartner URL: https://www.gartner.com/reviews/market/network-access-control (дата звернення: 05.10.2024).
8. Держспецз'язок. Рекомендації захисту URL: https://cip.gov.ua/ua/statics/cyber-protection (дата звернення: 10.10.2024).
9. Закону України «Про захист персональних даних».
10. Основні питання щодо захисту персональних даних URL: https://ecpl.com.ua/news/top-10-pytan-u-sferi-zakhystu-personal-nykh-danykh/ (дата звернення: 03.11.2023).

11. IBM Security X-Force Threat Intelligence Index 2023 URL: https://www.ibm.com/reports/threat-intelligence-action-guide (дата звернення: 03.11.2024).

12. Що таке TACACS+ / RADIUS Access Management? Як це працює? https://krontech.com/what-is-tacacs-radius-access-management-how-does-it-work (дата звернення: 03.11.2024).

13. Безпечне використання VPN URL: https://cip.gov.ua/ua/faqs/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення: 15.11.2024).

14. Політики безпеки URL: https://www.dclessons.com/configure-ise-policy-set (дата звернення: 15.11. 2024).

15. Сторожук С.С. Необхідність застосування технології контролю доступу корпоративної мережі Атаки на ланцюг поставок supply chain. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Київ, 2024. С. 163-165 (дата звернення: 05.11.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)