НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження безпечного мережевого доступу на базі платформи Cisco Identity Services Engine»

Виконав (-ла):
студент (-ка) ІІ курсу, групи ТС-71мп
Шевченко Дмитро Вікторович _____

Керівник:
Доцент, к. т. н.,
Созонник Г.Д. _____

Рецензент:

_____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2018

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Шевченку Дмитру Вікторовичу

1. Тема дисертації «ДОСЛІДЖЕННЯ БЕЗПЕЧНОГО МЕРЕЖЕВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ CISCO IDENTITY SERVICES ENGINE», науковий керівник дисертації Созонник Галина Дмитрівна, кандидат технічних наук, доцент, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації _____

3. Об’єкт дослідження: корпоративна інформаційна система організації яка захищається.

4. Предмет дослідження: комплекс питань, пов'язаний з організацією концепції захисту інформаційної безпеки корпоративної мережі, що включає метод дослідження платформи Cisco Identity Services Engine, модель сегмента мережі організації і метод моніторингу захищеності мережі через платформу Cisco ISE.

5. Перелік завдань, які потрібно розробити:

- обґрунтувати необхідність забезпечення технічних рішень з питань мережевої безпеки організації;

- здійснити пошук, кількісний і якісний аналіз наявних методів атак на мережі, описати методи рішення;
- аналіз технології захисту корпоративних мереж на базі платформи Cisco ISE
- проектування локальної мережі організації та дослідження ефективності роботи архітектури Cisco ISE
- пояснити отримані результати та оцінити доцільність використання вибраної архітектури захисту мережі

6. Орієнтовний перелік графічного (ілюстративного) матеріалу
Плакат №1 Тема роботи, мета, об'єкт та предмет дослідження
Плакат №2 Сучасні мережеві атаки та методи боротьби
Плакат №3 Архітектура Cisco ISE
Плакат №4 Організація захисту даних організації
Плакат №5 Висновки по роботі

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Строк виконання етапів роботи	Примітка
1.	Формулювання теми, мети, об’єкту та предмету дослідження у магістерській роботі	10.01.2018	Виконано
2.	Формулювання проблематики та визначення актуальності магістерської роботи. Зв’язок тематики магістерської роботи із сучасними інноваційними трендами в телекомунікаціях та інформаційному середовищі	01.02.2018 – 16.02.2018	Виконано
3.	Формування переліку наукових завдань у магістерській роботі	15.03.2018 – 16.03.2018	Виконано
4.	Обґрунтування необхідності забезпечення технічних рішень з питань мережевої безпеки організації.	17.03.2018 – 20.03.2018	Виконано

5.	Опис математичної моделі, яка використовується в магістерській роботі.	01.04.2018 – 22.04.2018	Виконано
6.	Опис виконаних наукових завдань магістерської роботи.	06.05.2018 – 18.05.2018	Виконано
7.	Аналізування технології захисту корпоративних мереж на базі платформи Cisco ISE.	19.05.2018 – 30.05.2018	Виконано
8.	Проектування локальної мережі організації та дослідження ефективності роботи архітектури Cisco ISE. Оформлення пояснювальної записки до магістерської роботи.	02.06.2018 – 29.06.2018	Виконано
	Написання розділів до магістерської роботи	1.07.2018 – 30.09.2018	Виконано
9.	Оформлення дипломної роботи.	1.10.2018 – 30.10.2018	Виконано

Студент Д.В. Шевченко

Науковий керівник дисертації Г.Д. Созонник

РЕФЕРАТ

Темою магістерської дисертації є дослідження безпечного мережевого доступу на базі платформи Cisco Identity Services Engine, його функції та моделі розгортання.

Робота містить 88 сторінок, зокрема 37 ілюстрацій, 8 таблиць та 13 джерел інформації.

Тема магістерської дисертації є актуальною, оскільки велика кількість корпоративних мереж об'єднана за допомогою Інтернет, тому очевидно, що для безпечної роботи необхідно вживати певних заходів безпеки, так як практично з будь-якого комп'ютера можна отримати доступ до будь-якої мережі будь-якої організації.

Мета дисертації полягає у висвітлення сучасних мережевих загроз та реалізація комплексного підходу до інформаційної безпеки корпоративних мереж на базі платформи Cisco Identity Services Engine.

Об’єктом дослідження є корпоративна інформаційна мережа організації яка захищається. Предметом дослідження є комплекс питань, пов'язаний з організацією концепції захисту інформаційної безпеки корпоративної мережі, що включає метод дослідження платформи Cisco Identity Services Engine.

При виконанні роботи застосовувалося моделювання корпоративної мережі у віртуалізованому середовищі VMware для визначення роботи Cisco ISE та налаштувань на надійність мережі організації.

У дисертації була запропонована методика оцінки впливу архітектури Cisco ISE на безпеку корпоративної мережі. Були надані рекомендації щодо топології мережі, та розгортання архітектури Cisco Identity Services Engine.

ABSTRACT

The topic of the master thesis is to study of secure network access based on the Cisco Identity Services Engine platform, its functions and deployment models.

The work contains 88 pages, including 37 illustrations, 8 tables and 13 sources.

Theme of master's thesis is relevant, since a large number of corporate networks are connected via the Internet, so it is obvious that for safe operation it is necessary to take certain security measures, since almost any computer can access any network of any organization.

The purpose of the thesis is to highlight modern network threats and implement an integrated approach to information security of corporate networks based on the Cisco Identity Services Engine platform.

The object of research is the corporate information network of the organization which is protected. The subject of the study is a set of issues related to the organization of the concept of information security protection of the corporate network, which includes a method of research platform Cisco Identity Services Engine.

When performing the work, we used the modeling of the corporate network in a virtualized VMware environment to determine the operation of Cisco ISE and settings for the reliability of the organization network.

The thesis proposed a methodology for assessing the impact of the architecture of the Cisco ISE in enterprise network security. Recommendations on network topology and deployment of the Cisco Identity Services Engine architecture were provided.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AAA	authentication, authorization, accounting — автентифікація, авторизація, облік
ACL	Access Control List — список контролю доступу
CA	Certification Authority — акредитований центр сертифікації ключів
DAI	Dynamic ARP Inspection — динамічне регулювання ARP запитів
dACL	Downloadable Access Control List — завантажуваний список контролю доступу
DoS	Denial of Service — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні
IPSec	IP Security — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP
IPSG	IP Source Guard — функція захисту від підміни IP адреси
MAB	MAC Authentication Bypass — перепуск автентифікації на основі MAC адрес
MAC	Media Access Control — управління доступом до середовища
MITM	Man in the middle — атака посередника, атака «людина посере
NAD	Network Access Device — мережевий пристрій доступу
SDM	Software-Defined Networking — програмно-визначені мережі
SSH	Secure Shell - «безпечна оболонка» - мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань

SSL	Secure Sockets Layer — рівень захищених сокетів
STP	Spanning Tree Protocol – Тпротокол сполучного дерева
TCP/IP	Transmission Control Protocol/Internet Protocol - систематизований стек протоколів мережі інтернет
VLAN	Virtual Local Area Network - віртуальна локальна комп'ютерна мережа
VPN	Virtual Private Network - віртуальна приватна мережа
МБ	Мережева безпека
МЕ	Міжмережевий екран

ВСТУП

Побудова об'єднаного інформаційного простору і глобальне споживання персональних комп'ютерів і, в такій же мірі, вкорінення комп'ютерних систем, подало привід знаходити рішення складних завдань в галузі захисту інформації.

Ефективність роботи системи контролю доступу, як будь-якого високотехнологічного інструмента, залежить від того, наскільки правильно його використовують.

Чи повинні всі співробітники мати однаковий доступ до всієї корпоративної інформації? Очевидно, що ні. Це нам підказує теорія інформаційної безпеки і здоровий глузд. Секретарю нема чого знати фінансові показники компанії; бухгалтер не повинен бачити в корпоративної CRM контакти і розклад керівника. База клієнтів компанії не повинна бути доступна адміністратору поштового сервера компанії; комерційний директор не повинен мати доступ до технологічної мережі управління.

Як це питання вирішувалося раніше? Користувачів ділили на групи за рівнем доступу. Для кожної групи вносили налаштування на портах підключення співробітників в мережу. Більш ефективно проводити автентифікацію користувачів при вході в мережу і застосовувати політики доступу в точці підключення до мережі. Саме тому широко використовується рішення безпечного мережевого доступу на базі платформи Cisco Identity Services Engine.

Чому саме ця платформа, і що вона нам дає? Для початку було поставлено завдання знайти таке рішення, яке б закривало більшість питань, пов'язаних з контролем доступу до корпоративної мережі. Проаналізувавши ринок запропонований різними вендорами з питань мережевої безпеки вибір однозначно перейшов на бік компанії Cisco, хоча

на ринку і є аналоги у вигляді Checkpoint, Symantec, Palo Alto Networks, але та платформа, і те рішення яке надає Cisco на сьогоднішній день є найбільш ефективним з точки зору функціоналу та можливості.

Завдяки Cisco ISE є можливість розмежувати доступ по безлічі критеріїв:

- Хто повинен мати доступ;
- З яких пристроїв;
- В який час доби;
- Через які мережеві пристрої;
- Який рівень доступу необхідний.

РОЗДІЛ 1. ОГЛЯД СУЧАСНИХ МЕРЕЖЕВИХ ЗАГРОЗ

1.1 Категорії загроз мережевої безпеки

Дротові і бездротові комп'ютерні мережі відіграють важливу роль у повсякденному житті. Фізичні особи та організації рівною мірою залежать від своїх комп'ютерів і мереж. Несанкціоноване вторгнення в мережу може призвести до надзвичайно витратних перебоїв і втрати важливих результатів роботи. Атака на мережу може мати руйнівні наслідки з втратою часу і коштів в результаті пошкодження або розкрадання інформації і ресурсів.

Зловмисники можуть отримати доступ до мережі, використовуючи вразливість програмного забезпечення, атаки, апаратні атаки, або шляхом підбору імені користувача і пароля. Зловмисники, які отримують доступ, змінюючи програмне забезпечення або експлуатуючи вразливість в програмному забезпеченні, часто іменуються хакерами [1].

Хакер, що отримав доступ в мережу, відразу стає джерелом чотирьох видів загроз:

1. Викрадення інформації;
2. Крадіжка особистої інформації;
3. Втрата даних або маніпуляція даними;
4. Припинення в обслуговуванні.

Розглянемо кожен вид загроз більше детально (рисунок 1.1).

Викрадення інформації - проникнення в комп'ютер для отримання конфіденційної інформації. Ця інформація може бути використана або продана з різними цілями. Приклад: розкрадання конфіденційної інформації, що належить організації, наприклад, відомості про науково-технічні розробки [1].

Крадіжка особистої інформації - вид розкрадання інформації, при якому відбувається крадіжка особистих даних для подальшого їх

використання з метою обману. Використовуючи ці дані, людина може отримати юридичні документи, подати заяву на кредит та здійснити несанкціоновані покупки через Інтернет [2]. Проблема крадіжки особистої інформації продовжує загострюватися, а фінансові втрати становлять мільярди доларів на рік.

Втрата даних або маніпуляція даними - проникнення в комп'ютер з метою знищення або зміни записів даних. Приклади втрати даних: передача вірусу, що затирає жорсткий диск комп'ютера. Приклад неправомірного використання даних: проникнення в систему зберігання даних з метою зміни даних, наприклад ціни виробу.

Припинення в обслуговуванні - заборона доступу правомірних користувачів до служб, для використання яких, їм має бути надане право. Приклад: атаки типу «відмова в обслуговуванні» (DoS-атаки) на сервери, мережеві пристрої і канали обміну даними по мережі.

Рисунок 1.1 Види загроз мережевої безпеки

Таким чином, навіть у невеликих мережах необхідно враховувати загрози безпеці та вразливості при плануванні впровадження мережі.

1.2 Вектор втрати даних

Вираз "вектор втрати і ексфільтрації даних" відноситься до засобів, за допомогою яких дані залишають організацію без дозволу.

Загальні типи втрати і ексфільтрації даних включають наступне:

– *Вкладення електронної пошти*: вкладення електронної пошти часто містять конфіденційну інформацію, таку як конфіденційні корпоративні, клієнтські та особисті дані. Вкладення можуть залишати організацію різними способами. Наприклад, повідомлення електронної пошти з вкладенням може бути перехоплене або користувач може випадково відправити повідомлення не тій людині.

– *Незашифровані пристрої*: смартфони та інші персональні пристрої часто захищені тільки паролем. Співробітники іноді відправляють конфіденційну інформацію компанії на ці пристрої. У той час коли дані можуть бути зашифровані при передачі через Інтернет на пристрій, вони можуть бути незашифровані, коли вони передаються до персонального пристрою. Якщо пароль зламаний хакерами, зловмисник може отримати корпоративні дані і, можливо, навіть отримати несанкціонований доступ до мережі компанії.

– *Хмарні служби зберігання*: співробітники компанії часто відчувають спокусу передавати великі файли за допомогою хмарних служб зберігання за своїм вибором без схвалення IT-відділу компанії. Це може призвести до крадіжки конфіденційних документів кимось на кшталт "друга" соціальної мережі, з яким співробітник ділиться каталогом на сервері хмарного сховища.

– *Знімні носії*: розміщення конфіденційних даних на знімних запам'ятовуючих пристроях може представляти велику загрозу, ніж розміщення цих даних на смартфоні. Такі пристрої не тільки легко втратити або вкрасти; вони також, як правило, не мають паролів, шифрування або будь-який інший захист. Хоча такий захист для знімних пристроїв зберігання даних доступний, він відносно дорогий і часто використовується лише на папері.

– *Неправильне керування доступом*: без належних засобів управління доступом, таких як списки управління доступом на

брандмауерах, високий ризик втрати даних. Організації можуть знизити ризик втрати даних за рахунок детального налаштування управління доступом і виправлення відомих вразливостей.

1.3 Класифікація мережевих атак

Мережеві атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються великою складністю. Інші може здійснити звичайний оператор, навіть не припускаючи, які наслідки може мати його діяльність. Для оцінки типів атак необхідно знати деякі обмеження, спочатку властиві протоколу TPC/IP. Мережа Інтернет створювалася для зв'язку між державними установами та університетами на допомогу навчальному процесу та наукових досліджень. Творці цієї мережі не підозрювали, наскільки широко вона поширіться. В результаті, в специфікаціях ранніх версій інтернет-протоколу (IP) були відсутні вимоги безпеки. Саме тому багато реалізацій IP є спочатку уразливими. Через багато років, отримавши безліч рекламацій (RFC - Request for Comments), ми, нарешті, стали впроваджувати засоби безпеки для IP. Однак з огляду на те, що спочатку засоби захисту для протоколу IP були розроблені, але всі його реалізації стали доповнюватися різноманітними мережевими процедурами, послугами і продуктами, що знижують ризики, властиві цим протоколам [3].

Розглянемо найвідоміші типи атак, які зазвичай використовуються проти мереж IP:

1. *Розвідувальні атаки* – це спроба дізнатися більше про передбачувану жертву перед спробою більш складної атаки. Зловмисники можуть використовувати стандартні мережеві інструменти, такі як dig, nslookup і whois, для збору загальнодоступної інформації про ціль мережі з реєстрів DNS. Всі три інструменти є засобами командного

рядка. Інструменти nslookup і whois доступні на платформах Windows, UNIX і Linux, а dig-на системах UNIX та Linux. Запити DNS можуть виявити таку інформацію, як хто володіє певним доменом і які адреси були призначені цьому домену. Ping сканування адрес, виявлених DNS-запитів може уявити картину живих хостів в конкретному середовищі. Після створення списку активних хостів зловмисник може продовжити перевірку, запустивши сканування портів на активних хостах. Засоби сканування портів можуть циклічно перебирати всі відомі порти, щоб надати повний список всіх служб, запущених на вузлах. Зловмисник може використовувати цю інформацію для визначення найбільш простого способу використання уразливості.

2. *Парольні атаки* - були проблемою з самого початку мережевої безпеки, і вони продовжують бути домінуючою проблемою в поточній мережевої безпеки. Щороку SplashData публікує звіт про найбільш часто використовуваних паролях, які просочуються в інтернет. У 2014 році вони проаналізували 3,3 мільйона паролів і повідомили про топ-25 [10]. Пароль "password" був другим у списку. Шість з топ-11 були числовими послідовностями, що починаються з 1 і змінюються тільки по довжині послідовності (тобто 123456). Ще п'ять топ-25 були простими літеро-цифровими послідовностями (наприклад, abc123). Було кілька розумних, але все ще поганих паролів, таких як trustno1 і letmein. Решта 11 були прості слова, в нижньому регістрі. Ці топ-25 паролів, становили 2,2% від 3.3 млн. витік паролів. Зловмисники використовують кілька способів отримання паролів користувачів, в тому числі:

   2.1 Вгадування: щоб виконати вгадування пароля, зловмисник може або вручну ввести паролі або використовувати програмне забезпечення для автоматизації процесу. Дійсно погані паролі

можуть бути сприйнятливі до самотнього зловмисника, роблячи обґрунтовані здогади.

2.2 Грубої сили: атаки грубої сили виконуються за допомогою комп'ютерних програм. Програма виконує злом грубої сили, систематично пробуючи всі можливі паролі, поки він не досягне успіху. Швидкість, з якою зловмисник може отримати пароль за допомогою цього методу може залежати від швидкості комп'ютера зловмисника (скільки обчислень він може виконати в секунду), швидкість підключення зловмисника до Інтернету, а також довжина і складність пароля. Багато зломщики паролів доступні в Інтернеті, і багато з них доступні безкоштовно.

2.3 Атаки за словником: атаки за словником використовують списки слів для структурування спроб входу в систему. Списки слів можуть містити мільйони слів, включаючи слова з словника природної мови і такі слова, як назви спортивних команд, ненормативна лексика і сленг. Атаки за словником не завжди вдалі. Однак у певному сенсі, атака за словником схожа на атаку грубої сили. Це автоматизований процес, який виконується за допомогою програми підбору паролів; швидкість, з якою він дозволяє зловмиснику отримати пароль, може залежати від швидкості комп'ютера зловмисника (скільки обчислень він може виконати в секунду), швидкості підключення зловмисника до Інтернету, а також довжини і складності; і багато інструментів атаки по словнику доступні безкоштовно в Інтернеті.

3. *Атаки переповнення буфера* - Зловмисники можуть аналізувати мережеві серверні додатки на наявність дефектів. Уразливість переповнення буфера є одним з типів дефектів. Якщо служба приймає вхідні дані і очікує, що вхідні дані знаходяться в межах певного розміру, але не перевіряє розмір вхідних даних при

отриманні, вона може бути вразлива для атаки переповнення буфера. Це означає, що зловмисник може надати вхідні дані більшого розміру, ніж очікувалося, і служба прийме вхідні дані і запише їх у пам'ять, заповнивши пов'язаний буфер, а також перезаписавши сусідню пам'ять. Цей перезапис може пошкодити систему і привести до збою, в результаті чого виникає – DoS[4]. У гіршому випадку зловмисник може впровадити шкідливий код в переповнення буфера, що призведе до компрометації системи. Атаки переповнення буфера є поширеним вектором атак на стороні клієнта. Шкідливий код може бути введений у файли даних, і код може бути виконаний, коли файл даних відкритий вразливим клієнтським додатком. Наприклад, припустимо, що зловмисник відправляє такий заражений файл в Інтернет. Нічого не підозрюючи користувач завантажує документ і відкриває його за допомогою вразливого додатка. В системі користувача це породжує шкідливий процес, який може підключатися до шахрайських систем в Інтернеті і завантажувати більш шкідливі корисні для хакера дані. Брандмауери зазвичай набагато краще запобігають вхідним шкідливим підключенням з Інтернету, ніж вихідним шкідливим підключенням до Інтернету.

4. *Social Engineering* - соціальна інженерія маніпулює людьми і використовує очікувану поведінку. Соціальна інженерія часто включає в собі використання соціальних навичок, відносин або розуміння культурних норм, щоб маніпулювати людьми всередині мережі, щоб надати інформацію, необхідну для доступу до мережі. Нижче наведені приклади соціальної інженерії:
   4.1 Виклик користувачів за телефоном, стверджуючи, що це він, і переконати їх, що вони повинні встановити свої паролі для конкретних значень в рамках підготовки до оновлення сервера, який відбудеться сьогодні ввечері.

4.2 Розвиток вигаданих особистостей в соціальних мережах для отримання статусу "друга" і зловживання ним.

4.3 Відправка повідомлення електронної пошти, заманює користувача клацнути посилання на шкідливий веб-сайт ("фішинг").

4.4 Візуальний злом, коли зловмисник фізично спостерігає, як жертва вводить облікові дані (наприклад, ім'я входу робочої станції, PIN-код ATM або комбінацію фізичної блокування).

5. *Атаки типу Man-in-the-Middle* - скоріше узагальнена концепція, яка може бути реалізована в багатьох різних сценаріях, ніж конкретна атака. Як правило, в цих атаках система, яка має можливість переглядати зв'язок між двома системами, накладає себе на комунікаційний шлях між цими іншими системами. Атаки "людина посередині" - це складні атаки, які вимагають успішні атаки на IP-маршрутизацію або протоколи (такі як ARP, DNS або DHCP), що призводять до неправильного напрямку трафіку. Наприклад, коли атакуючий підмінює кеш ARP двох пристроїв з MAC-адресою NIC атакуючого[5]. Як тільки кеші ARP були успішно підмінені, кожен пристрій жертви передає всі свої пакети атакуючому при передачі іншому пристрою. Це ставить нападника в середині шляху зв'язку між двома пристроями жертви. Це дозволяє зловмиснику легко контролювати всі комунікації між пристроями жертви. Мета полягає в тому, щоб перехопити і переглянути інформацію, передану між двома пристроями жертви і потенційно ввести сеанси і трафік між двома пристроями жертви.
6. *Переадресація портів* - переадресація портів являє собою різновид зловживання довірою, коли зламаний хост використовується для передачі через міжмережевий екран трафіку, який в іншому випадку був би обов'язково відбракований. Уявімо собі міжмережевий екран

з трьома інтерфейсами, до кожного з яких підключений певний хост. Зовнішній хост може підключатися до хосту загального доступу (DMZ), але не до хосту, встановленому з внутрішньої сторони брандмауера. Хост загального доступу може підключатися і до внутрішнього, і зовнішнього хосту. Якщо хакер захопить хост загального доступу, він зможе встановити на ньому програмний засіб, що перенаправляє трафік з зовнішнього хоста прямо на внутрішній хост. Хоча при цьому не порушується жодне правило, чинне на екрані, зовнішній хост в результаті переадресації отримує прямий доступ до захищеного хосту.

7. *Сніффер пакетів* - сніффер пакетів є прикладною програмою, яка використовує мережеву карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додаткам для обробки). При цьому сніффер перехоплює всі мережеві пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправності і аналізу трафіку. Однак з огляду на те, що деякі мережеві додатки передають дані в текстовому форматі (telnet, FTP, SMTP, POP3 і т.д.), за допомогою сніффера можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі). Перехоплення логінів і паролів створює велику небезпеку, так як користувачі часто застосовують один і той же логін і пароль для безлічі додатків і систем. Багато користувачів взагалі мають один пароль для доступу до всіх ресурсів і додатків.

Хакери можуть використовувати вищезгадані інструменти атак або комбінацію інструментів для створення різних нападів. Однак, перелік не є вичерпним, так як постійно виявляються нові і нові уразливості.

Важливо розуміти, що хакери використовують різні інструменти безпеки, щоб здійснити ці напади.

1.4 Фізична безпека для мережевих пристроїв

При оцінці безпеки мережі або комп'ютера слід врахувати можливість експлуатації зловмисниками вразливостей програмного забезпечення. Але не менш значну вразливість являє собою фізична безпека пристроїв. Зловмисник може блокувати доступ до мережевих ресурсів, якщо вони можуть бути скомпрометовані на фізичному рівні.

Існує чотири класи фізичних загроз [2]:

1. Загрози для апаратного забезпечення — фізичне пошкодження серверів, маршрутизаторів, комутаторів, кабелів і робочих станцій.
2. Загрози з боку навколишнього середовища — граничні температури (занадто високі або занадто низькі) або крайні значення вологості (занадто низька або занадто висока).
3. Електричні загрози — піки напруги, недостатня напруга в мережі (провали напруги), коливання напруги (шум) і повне відключення живлення.
4. Експлуатаційні загрози — неналежне поводження з ключовими електричними компонентами (електростатичний розряд), брак важливих запасних деталей, неправильна прокладка кабелів і недостатнє маркування.

Деякі з цих проблем необхідно вирішувати за допомогою організаційних політик. Інші проблеми вирішуються за рахунок грамотного керівництва і управління в організації.

Планування фізичної системи безпеки в цілях обмеження збитку для обладнання:

– Блокування устаткування та запобігання несанкціонованого доступу через двері, стелю, фальшпол, вікна, вентиляційні та каналізаційні шахти.

– Моніторинг і управління доступом до серверної шафи за допомогою електронної системи обліку.

– Використання камер безпеки.

– Не можна покладатися на надійність електромережі. Слід передбачити різні способи захисту від проблем з електроживленням.

1.4 Висновки з розділу 1

1. Були розглянуті сучасні мережеві загрози, до них відносяться: викрадення інформації, крадіжка особистої інформації, втрата даних або маніпуляція даними, припинення в обслуговуванні. В наш час потрібно бути завжди на крок попереду зловмисних хакерів, які можуть спричинити перелічені загрози.
2. Вектор атаки - це шлях за допомогою якого зловмисник може отримати доступ до сервера, сайту або мережі. Багато атак відбувається поза межами корпоративної мережі. Але атаки також можуть виходити і з внутрішньої мережі.
3. До основних категорій засобів нападу на мережу відносять: IP-спуфінг, модифікація даних, відмова в обслуговування, парольні атаки, атаки типу MITM та переадресація портів.
4. Фізичний захист IT інфраструктури підприємства також є дуже важливим. Доступ до серверної кімнати відкритий тільки для

авторизованого персоналу. Центр повинен бути під захистом служби охорони та обладнаний системою відео моніторингом.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ АРХІТЕКТУРИ CISCO ISE У ЯКОСТІ МЕХАНІЗМУ КОНТРОЛЮ ДОСТУПУ ДО МЕРЕЖІ

2.1 Нові виклики безпеки

У міру зміни корпоративного IT-ландшафту організації стикаються з новими викликами IT-безпеки. Кожні кілька місяців з'являється нова історія про те, як великі компанії стають жертвами атак і тим самим втрачають величезні обсяги особистих даних та інтелектуальної власності.

Зловмисники не обмежуються окремими особами або невеликими групами хакерів. Організована злочинність і навіть національні уряди часто причетні до нападів. Сьогоднішні зловмисники надзвичайно розумні і хитрі і мають велике допоміжне фінансування і ресурси. Ці зміни включають поширення пристроїв Інтернету речей (IoT), переміщення робочого навантаження в хмарні ресурси, а також розширення використання віртуалізованих служб[13]. Крім того, співробітники хочуть використовувати Bring your Own Device (BYOD) сервіси і отримувати доступ до корпоративних ресурсів в будь-який час і в будь-якому місці.

Всі ці тенденції мають потенціал для підвищення гнучкості і прибутковості організації, але приносять з собою новий набір проблем. Ці проблеми включають в себе зниження видимості того, хто підключений до мережі, які пристрої використовуються і звідки. І якщо ви не бачите пристрою, ви не можете контролювати його, що може збільшити вразливість мережі. Будь-яка спроба вручну пом'якшити ці проблеми збільшує експлуатаційні витрати (OPEX) надання IT-ресурсів[14].

Як організації можуть організовано і ефективно вирішувати ці проблеми? Що для цього необхідно зробити?

Організації вимагають контролю над активами. IT-фахівці повинні мати можливість легко бачити, хто підключений, як підключений і які кінцеві пристрої вони використовуються.

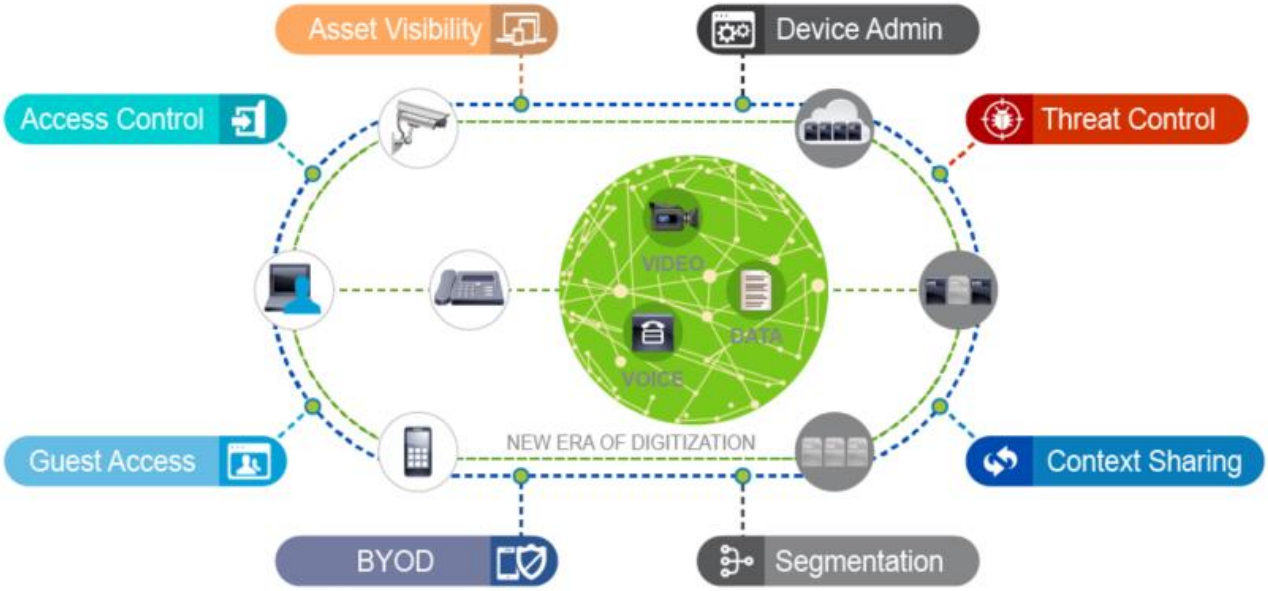


Рисунок 2.1 Нова ера оцифрування

Спроможність застосовувати відповідні рівні доступу для користувачів і кінцевих вузлів, в залежності від того, хто вони, і як вони підключаються, включаючи доступ співробітників і кінцевих пристроїв, а також гостьовий доступ та доступ BYOD, та сегментування ресурсів відповідним чином - покращує можливості управління доступом до мережі.

IT-персонал повинен мати під рукою ресурси для більш легкого контролю і стримування загроз. Ці загрози можуть виходити від кінцевих точок, які використовують застарілі або не залатані операційні системи, або без відповідного, сучасного програмного забезпечення для захисту від вірусів, серед багатьох інших векторів атак.

Організації також повинні мати можливість контролювати доступ до мережевих пристроїв - маршрутизаторів, комутаторів, брандмауерів, контролерів і інших пристроїв, складових мережевої інфраструктури.

Крім того, IT-фахівці можуть часто отримувати вигоду з обміну різною інформацією про безпеку у контексті користувача між різними мережевими службами, навіть від різних постачальників.

Cisco Identity Services Engine (ISE) є централізованим інструментом управління доступом до мережі і платформою застосування політик[10]. Він надає централізоване управління політиками для управління доступом до мережі і політиками використання з одного розташування.

Cisco ISE збирає ключову інформацію про доступ користувача та пристрої і використовує цю інформацію для управління доступом до мережі кінцевого користувача і доступом пристрою адміністративної мережі, незалежно від типу з'єднання[13]. Дротові, бездротові та віддалені користувачі можуть підключатися безпосередньо або через VPN. Незалежно від того, підключені вони віддалено або безпосередньо до корпоративних ресурсів, користувачі можуть отримати однаковий уніфікований доступ і управління.

Cisco ISE також надає гостьові та корпоративні можливості управління мобільністю, які передбачають доступ до Інтернету, мережі та файлів компанії. Цей продукт має можливість налаштувати автоматичні правила, щоб надавати доступ співробітникам. Ця автоматизація допомагає підтримувати загальну корпоративну безпеку і забезпечувати своєчасний доступ гостей і підрядників.

Cisco ISE може також використовувати зібрану інформацію для забезпечення нормативної відповідності до різного уряду і галузевих стандартів. Ця інформація може також використовуватися серед пристроїв партнера Cisco Eco system, щоб збільшити можливості для сервісів включаючи інформацію про безпеку та управління подіями (SIEM), управління мобільними пристроями (MDM), аналіз поведінки мережі (NBA), системи запобігання вторгнень (IPS), і багато іншого[10].

Зібрана інформація багато в чому пов'язана з "контекстом" конкретного сеансу зв'язку.

2.2 Аналіз механізму контролювання безпечного доступу

В області Cisco ISE контекст відноситься до "Хто, що, коли, де і як" будь-якої спроби з'єднатися. Хто є цим користувачем? Що він намагається зробити? Коли він намагаються з'єднатися? Де він знаходяться? І як намагається встановити зв'язок? Можна надати різні рівні доступу, які залежать від будь-якого або всіх цих критеріїв.

Як Cisco ISE збирає цю інформацію?

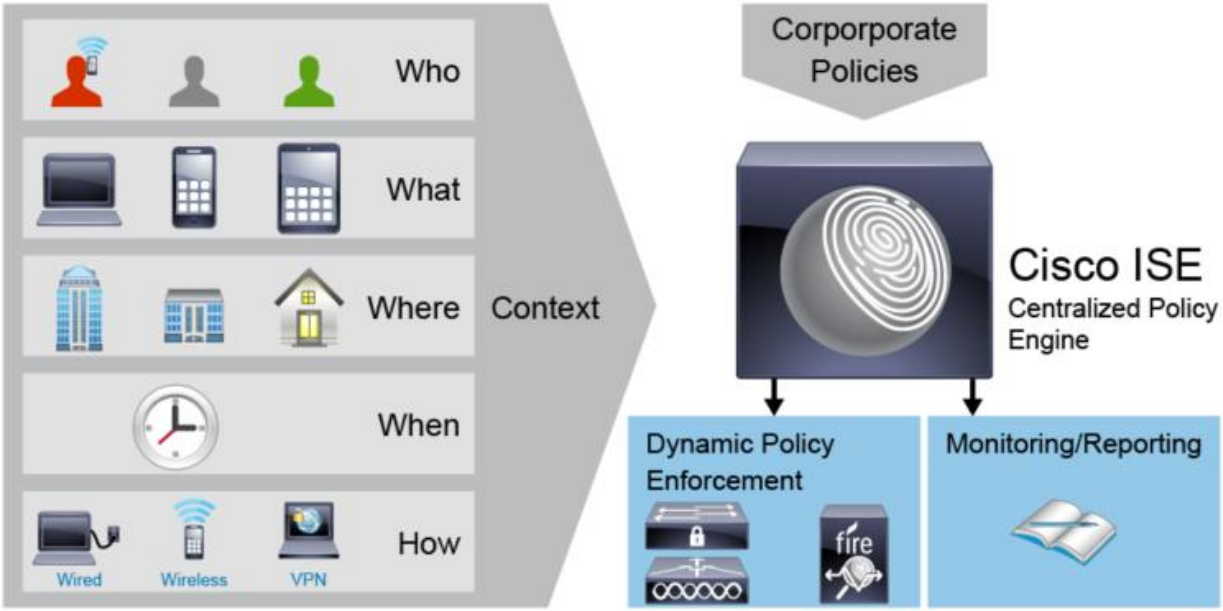


Рисунок 2.2 Опис контексту з точки зору Cisco ISE

Cisco ISE збирає контекстні дані від мережі через DHCP і NetFlow, наприклад. Він збирає контекстні дані про посвідчення користувача через інтеграцію Active Directory і Lightweight Directory Access Protocol (LDAP).

Він також збирає контекст від інтегрованих партнерів при оцінці стану або відповідності. З встановленим контекстним посвідченням, Cisco ISE в змозі об'єднати ці непорівнянні частини даних до єдиного розташування та зробити більш повністю проінформоване рішення щодо доступу.

Рішення безпечного доступу знижує ризики безпеки, забезпечуючи всебічну видимість в контексті: хто підключається, через який пристрій і звідки? Коли і як вони з'єднуються? Ця контекстна видимість забезпечує виняткове управління доступом.

Система безпечного доступу використовує засновані на стандартах моделі ідентичності такі як IEEE 802.1X і управління VLAN. Також існує ще багато розширених можливостей ідентифікації, таких як гнучка аутентифікація, завантажуванні списки управління доступом (DACL), масштабований груповий доступ (SGA), профілювання пристрою, оцінки положення, управління гостьовим доступом та інші [10]. Велика частина цієї функціональності досягнута за допомогою тісної інтеграції між Cisco ISE і пристроями доступу до мережі (NADs).

2.3 Дослідження розгортання Cisco ISE

Рисунок 2.3 надає огляд типового розгортання Cisco ISE. Різні кінцеві точки підключаються до мережевого приладу доступу (NAD), наприклад комутатор Ethernet, брандмауер або точка бездротового доступу (AP) та відповідний контролер бездротової локальної мережі (WLC) [12].

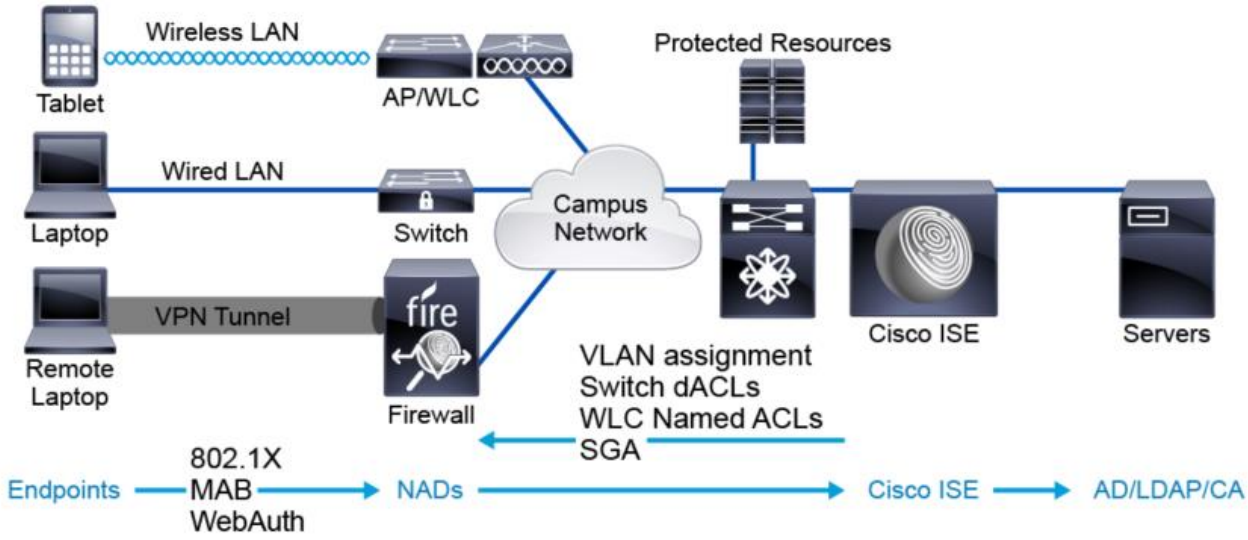


Рисунок 2.3 Розміщення елементів в архітектурі Cisco ISE

NAD - це пристрій, до якого користувачі підключаються для доступу до мережі. Таким чином, це ключова точка застосування політики для вирішення безпечного доступу. Для radius-аутентифікації, Cisco ISE часто виступає в якості RADIUS-сервера, і мережеві пристрої доступу виступають у якості radius-клієнтів [12].

Для виконання підключення та отримання доступу можна налаштувати метод авторизації. Корпоративні користувачі часто проходять автентифікацію за допомогою протоколу IEEE 802.1X, а користувачі-гості, як правило, проходять перевірку автентичності з допомогою системи WebAuth [13]. Спеціальні пристрої, такі як принтери або портативні сканери, можуть не підтримувати ці методи перевірки автентичності. Ці пристрої можуть використовувати аутентифікацію по MAC-адресам. Тобто при підключенні пристрою до інтерфейсу заздалегідь вірно налаштованого комутатора відбувається аутентифікація підключеного девайсу.

Ці запити аутентифікації централізовано управляються Cisco ISE, який може аутентифікувати ці запити локально або використовувати внутрішні сервіси. Ця служба включає Microsoft Active Directory [13], або систему на основі імені користувача і пароля LDAP. Також Cisco ISE включає певний сервіс зовнішнього центру сертифікації.

Cisco ISE дозволяє або забороняє запити автентифікації. Якщо приходить запит на автентифікацію, Cisco ISE передає інформацію назад до NADs для управління рівнями доступу для користувача. Наприклад, Cisco ISE може сказати комутатору або WLC промаркірувати трафік того чи іншого користувача з певним ідентифікатором VLAN по технології IEEE 802.1Q. ISE передає DACL до комутатора або до WLC для управління, до чого може звернутися кожен користувач. Альтернативно, Cisco ISE може працювати з NAD для розгортання SGA при управлінні доступом користувачів.

2.4 Дослідження функцій Cisco ISE

Cisco ISE надає централізовану платформу політики на основі посвідчень для управління доступом з урахуванням контексту через дротову, бездротову і VPN-інфраструктуру. Cisco ISE об'єднує аутентифікацію, авторизацію і облік (AAA), TACACS+, відстеження стану, профілювання і управління гостьовими функціями в єдиному уніфікованому пристрої, забезпечуючи єдину точку для управління політикою, моніторингу і усунення проблем [6].

- AAA
- Профілювання
- Управління гостьовим доступом
- Централізація політик
- Моніторинг
- Деталізований аудит
- TACACS+
- pxGrid
- Впровадження MDM
- Звіт в режимі реального часу

Комутована, бездротова і маршрутизуюча інфраструктура надає будівельний блок застосування політик. Ці NAD гарантують, що кінцеві пристрої можуть отримати доступ до відповідних ресурсів.

Функції Cisco ISE центрального моніторингу збирають ідентифікаційні дані та інформацію про кінцевий вузол і використовують цю інформацію з іншими компонентами в архітектурі. Додаткова функціональність доступна як програмні елементи, встановлюються на кінцевих точках, таких як Cisco AnyConnect Mobility client, Cisco Network Admission Control (NAC) і інтеграція управління мобільними пристроями (MDM).

Cisco ISE також підтримує TACACS + для адміністрування пристрою, pxGrid для обміну інформацією з іншими платформами та інтеграції з Cisco Software Defined Network (SDN) рішення - архітектура цифрової мережі (Cisco DNA).

Табл. 2.1 – Порівняння TACACS+ та RADIUS

	RADIUS	TACACS+
Базовий протокол	UDP	TCP
Підтримка сервісів	Authentication, Accounting	Authentication, Authorization, Accounting
Безпека	Шифрує тільки пароль	Шифрує все тіло пакета
Підтримка типу аутентифікації	Clear text (ASCII, PAP) CHAP	Clear text (ASCII, PAP) CHAP ARAP
Можливість перенаправлення запиту	+	-

2.4.1 Аналіз послуг AAA RADIUS

Інтегровані сервіси RADIUS включають AAA служби, які зазвичай використовується для доступу до мережі кінцевого користувача. Посвідчення користувачів можуть бути перевірені окремо від внутрішньої бази даних Cisco ISE, внутрішньою Microsoft Active Directory службою або серверами LDAP.

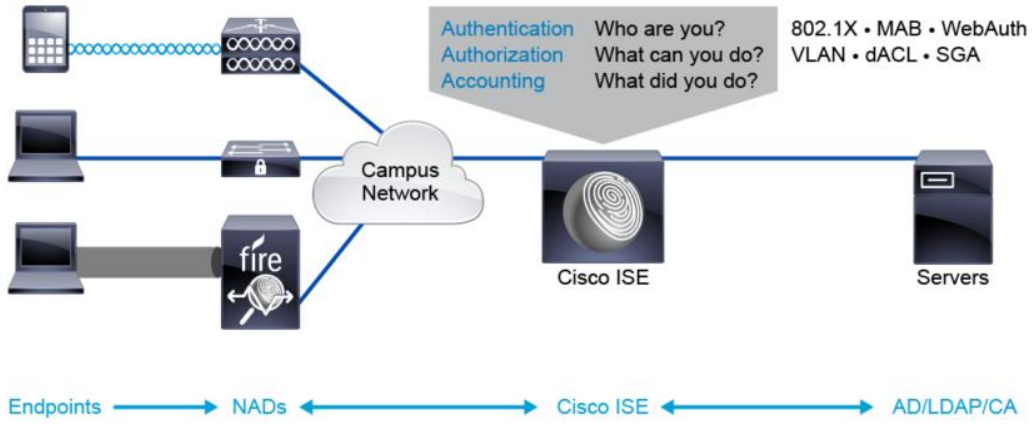


Рисунок 2.4 Служби AAA RADIUS

Три основні методи автентифікації:

1. Аутентифікація 802.1X для типових кінцевих точок: цей заснований на стандартах метод аутентифікації для дротяних і бездротових з'єднань під час корпоративного доступу співробітника.

2. Обхід автентифікації MAC (MAB) для пристроїв, яким не вистачає можливості 802.1 X: ці пристрої включають спеціальні елементи, такі як IP-камери, принтери, портативні сканери і багато іншого.

3. Веб-аутентифікація для гостьового доступу.

Автентифікація визначає, чи може користувач отримати доступ до мережі. Після того, як сервіс RADIUS Cisco ISE перевіряє ідентичність користувача і обробляє атрибути облікового запису, він може застосувати профіль авторизації до сеансу зв’язку. Cisco ISE передає цю політику авторизації до NAD у відповіді RADIUS Access-Accept. Ця політика авторизації визначає, які дії може виконувати користувач. Accounting відстежує дії користувачів, коли і де вони увійшли в систему, до чого вони отримали доступ і багато іншого.

2.4.2 Аналіз послуг AAA TACACS+

Інтегровані сервіси TACACS+ створюють можливість підтримки AAA, які зазвичай використовується для адміністративного доступу до мережевих пристроїв. Ідентичність користувачів може бути перевірена також, або через внутрішню базу даних Cisco ISE, або внутрішню базу Microsoft Active Directory чи базу серверів LDAP.

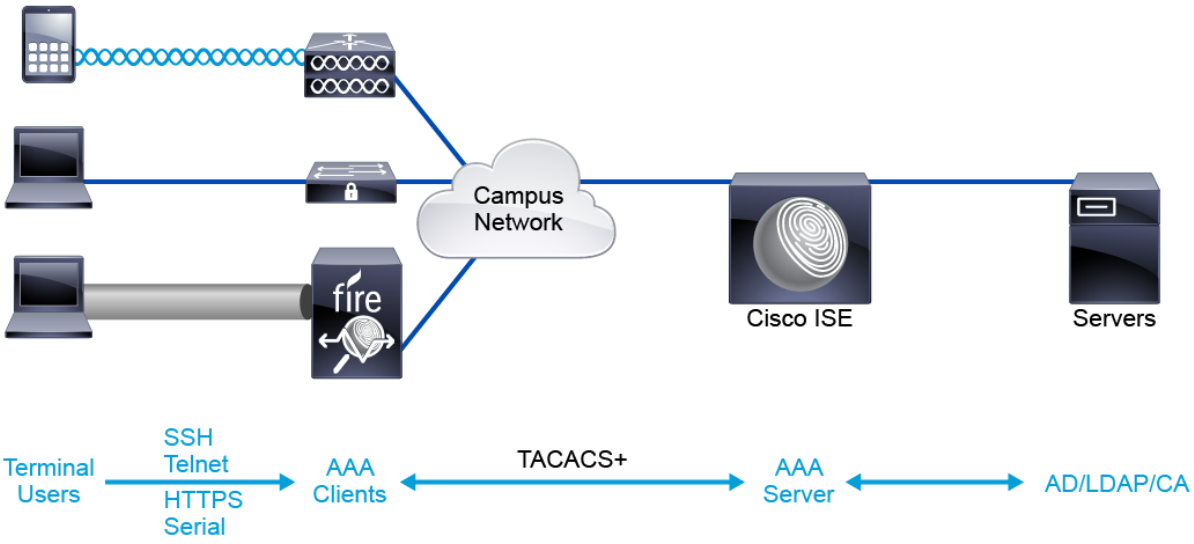


Рисунок 2.5 Служби AAA TACACS+

Мережеві адміністратори підключаються до мережевих пристроїв за допомогою SSH, Telnet, HTTP / HTTPS або через пряме підключення послідовного порту зі свого ноутбука чи іншого пристрою до пристрою.

Мережеві пристрої діють як клієнти AAA. Вони збирають облікові дані користувача і передають їх до AAA-сервера через протокол TACACS+ або RADIUS. Припускаючи, що облікові дані дійсні, користувач автентифікується для доступу до мережевого пристрою. Кожна дія, яку користувач намагається виконати, має пройти дозвіл на AAA-сервері.

Accounting відстежує дії користувачів, коли і де вони увійшли в систему, до чого вони отримали доступ і багато іншого[6].

2.4.3 Відповідність стану та інтеграція MDM

Оцінка стану дозволяє перевіряти і підтримувати можливості безпеки кінцевих користувачів. Можна налаштувати початкову перевірку автентичності RADIUS для надання тільки обмеженого клієнтського доступу. Після початкового доступу клієнта ISE має можливість перевірити версії операційної системи, захист від вірусів та інше. Якщо пристрій задовольняє цим критеріям, підвищений доступ може бути наданий за допомогою обміну повідомленнями зміни авторизації (CoA)[10]. Якщо пристрої несумісні, можна ввімкнути функції виправлення.

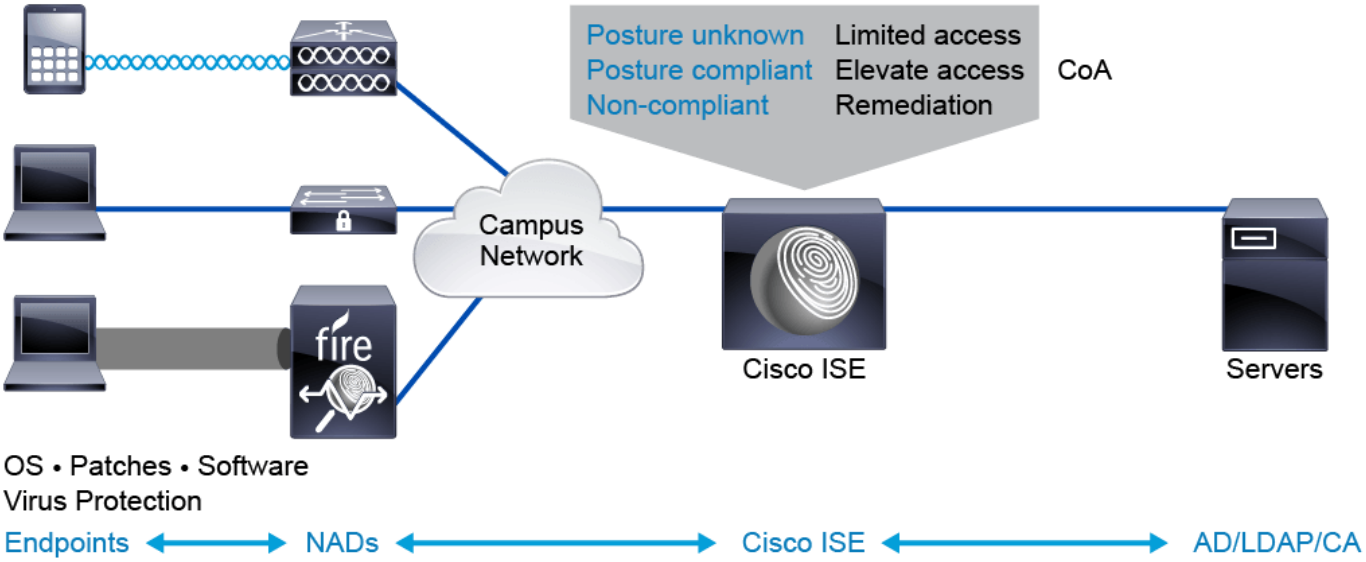


Рисунок 2.6 Оцінка стану кінцевого обладнання

Ця функція допомагає забезпечити відповідність кінцевих пристроїв певним стандартам безпеки і може бути покращена шляхом інтеграції зі сторонніми рішеннями MDM. Cisco ISE інтегрується з платформами MDM для забезпечення кращого положення і контролю пристроїв.

Можна використовувати відомості про профіль і положення для визначення політики авторизації. Авторизація в загальному випадку покладається на заснованому на стандартах механізмі CoA.

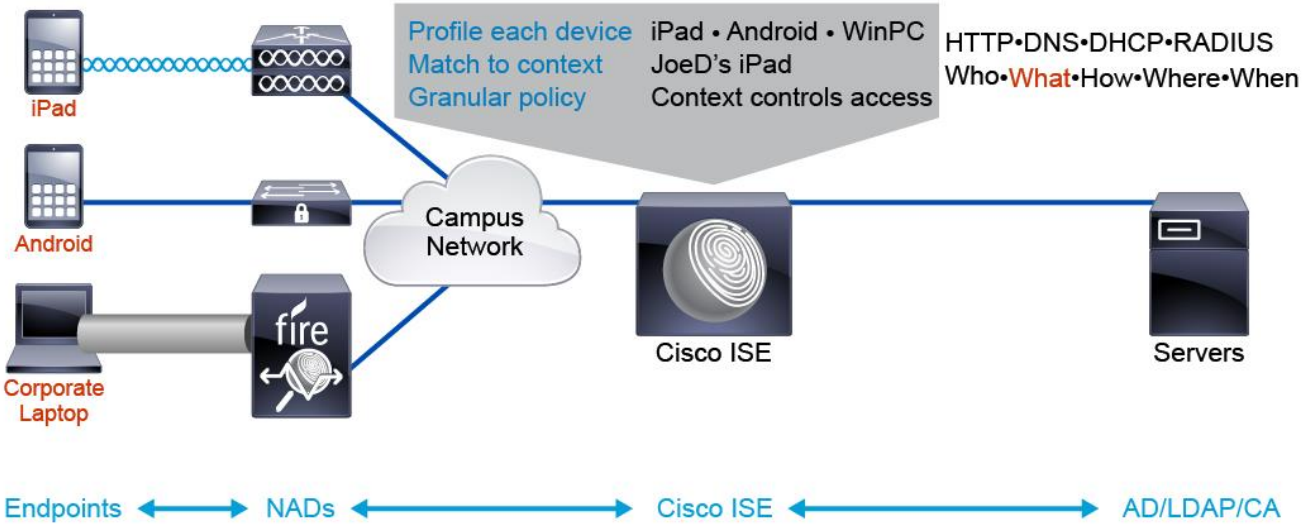
Використовуючи CoA, сервери RADIUS повідомляють NADs для підвищення або пониження рівнів авторизації кінцевої точки після обміну початковою аутентифікацією та авторизацією.

2.4.4 Профілювання

Головна ціль профілювання – класифікація кінцевих пристроїв, профіль визначає групу ідентичності пристрою, яка являє собою атрибут, що використовується для визначення умови в політики автентифікації та авторизації.

Початковий доступ: сервіси профілювання дозволяють Cisco ISE визначати тип пристрою кінцевого обладнання і його можливості. Після початкової аутентифікації пристрою можуть бути поміщені у "невідому" категорію.

Класифікація / профілювання: потім служба профілювання досліджує ключові характеристики, такі як взаємодія зі службами HTTP, DNS, DHCP і RADIUS. Таким чином, він може визначити тип пристрою і помістити його в певну категорію, таку як Android, Apple або iPad. Внутрішня база даних кінцевих вузлів зберігає результати профілювання для спрощення подальшої авторизації та категоризації.



Риунок 2.7 Профілювання клієнтів у системі Cisco ISE

Відповідність пристрою до іншого контексту: Cisco ISE тепер знає усе, що пов’язано з контекстом, і підбирає що це або хто це, яким чином під єдналось, де і коли.

Більш чіткі політики: тепер можна використовувати цей контекст для створення дуже детальних політик. Коли користувач "JoeD" входить в систему, використовуючи свій особистий iPad з громадського кафе, він може мати обмежений доступ. Але коли він входить в систему, використовуючи свій корпоративний ноутбук зі свого робочого столу в офісі, він отримує підвищений рівень доступу.

2.4.5 Адаптація пристроїв

Портал самостійної реєстрації дозволяє користувачам відповідати за адаптацію своїх пристроїв. Цей портал простий для кінцевих користувачів, з мінімальним втручанням, виконаний для того, щоб забезпечити більш граціозний досвід користувача (UX):

- Резервування пристрою, що намагається пройти авторизацію автоматизує параметри конфігурації клієнтського пристрою, такі як ідентифікатор набору бездротових служб (SSID), попередні ключі, розширюваний протокол аутентифікації (EAP) і більше.
- Дає можливість легко управляти чорним списком аби стерти втрачені або вкрадені пристрої і відновити їх в міру необхідності.
- Забезпечує автоматичну ініціалізацію сертифікатів з унікальним ідентифікатором пристрою (UDI), MAC-адресою та іншими атрибутами.
- Інтеграція з провідними платформами MDM забезпечує відповідність кінцевих пристроїв користувачів корпоративним

вимогам. Ці вимоги можуть включати в себе перевірку "кореневого" пристрою і правильності рівнів виправлень і оновлень вірусів. Крім того, можливість додавання, видалення і зміни локальних додатків контролюється і може бути обмежена, що дозволяє контейнеризації корпоративних даних.

Гостьова мережа використовується для самостійної реєстрації співробітників і гостьового доступу. Після підготовки корпоративні користувачі підключаються до захищеного корпоративного SSID. Оскільки гості ідентифікуються за їх обліковими даними, вони як і раніше мають обмежений доступ через вихідний SSID гостя.

2.4.6 Управління гостьовим доступом

Cisco ISE надає повну систему для управління гостьовим циклом. Гостьові користувачі можуть отримати доступ до мережі протягом обмеженого часу з допомогою організованого облікового запису або автономного входу і гостьового порталу. Адміністратори можуть налаштовувати гостьові портали і політики в залежності від конкретних потреб підприємства. Приклад схематично вказаний на рисунку 2.8.

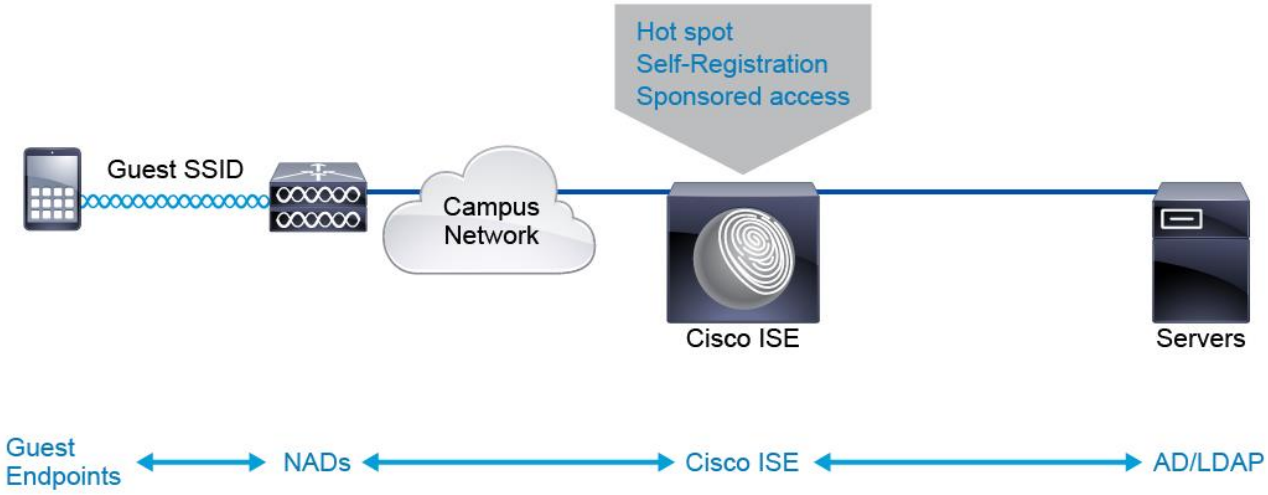


Рисунок 2.8 Доступ гостьовим користувачам до мережі

2.4.7 Централізоване управління та моніторинг

Cisco ISE надає центральний інтерфейс для управління, моніторингу та налаштування сервісів AAA, профілювання, відстеження стану, гостьового управління і сервісів BYOD.

Функції адміністрування та моніторингу розширюють можливості відстеження активності клієнтів, ведення мережевої політики, управління мережними ресурсами і діагностики проблем клієнтів[10]. Централізований аудит та звіт користувачів в режимі реального часу легко доступні.

Cisco ISE надає інформаційну панель для спрощення створення політики, видимості, звітності та нормативної відповідності.

Адміністрування і моніторинг всіх компонентів Cisco ISE, навіть з розподіленим розгортанням, виконані через з'єднання веб-браузера з єдиним централізованим інтерфейсом.

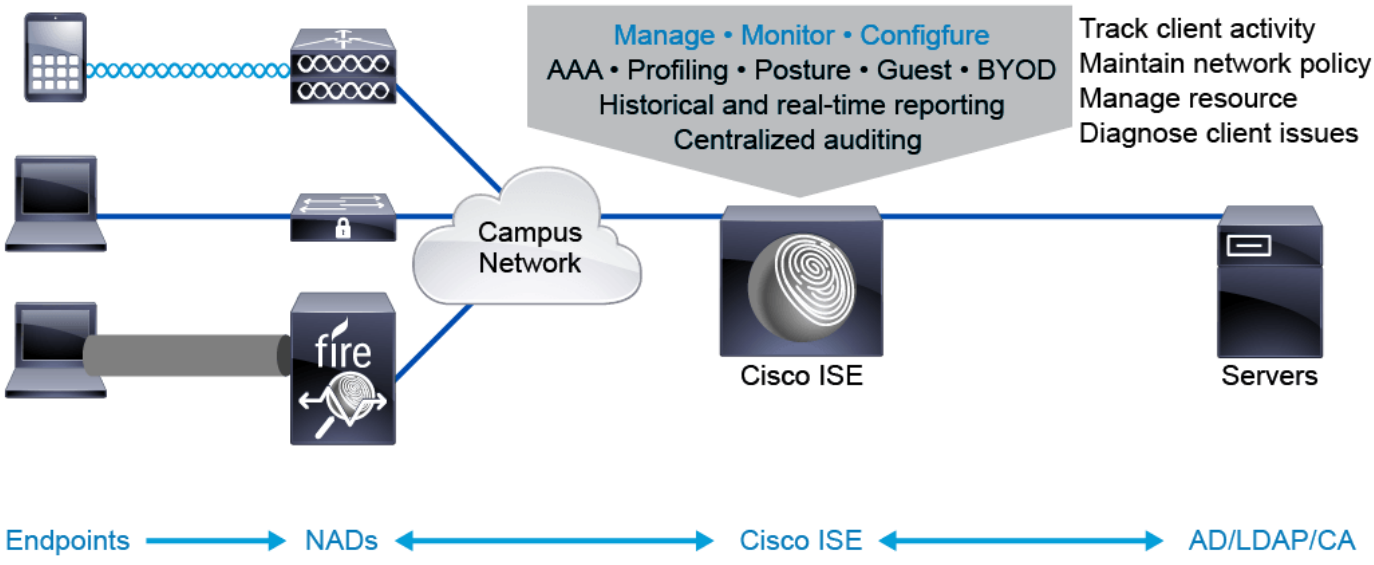


Рисунок 2.9 Опис функції моніторингу Cisco ISE

2.5 Моделі розгортання Cisco ISE

2.5.1 Вузли Cisco ISE

Вузол Cisco ISE являє собою програмне забезпечення Cisco ISE. ПЗ може бути у вигляді фізичного пристрою або у вигляді віртуальної машини в середовищі VMware.

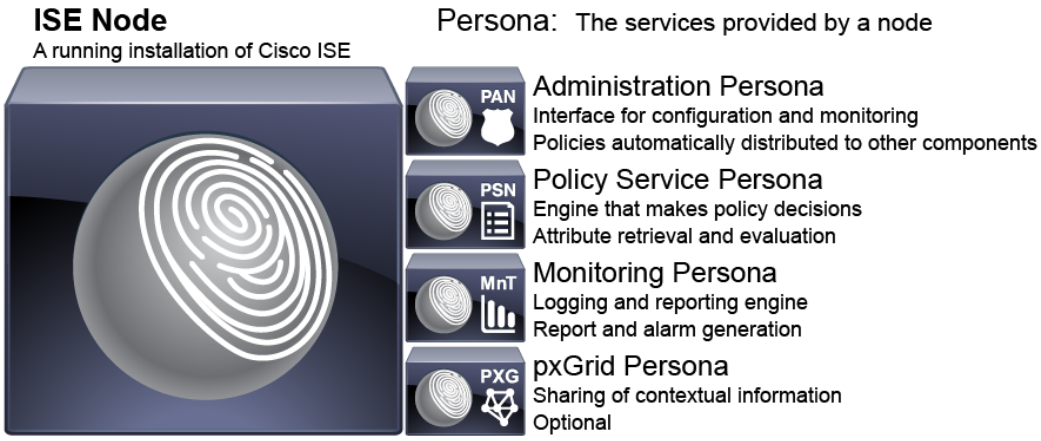


Рисунок 2.9 Вузли Cisco ISE

Існує чотири основних набори сервісів Cisco ISE, які організовані в personas, як показано на рисунку 2.9. З точки зору перекладу будемо їх окреслювати як – персони Cisco ISE. Ці персони відповідальні за різні функції в архітектурі Cisco ISE. Їх можна розмістити на одному вузлі або розподілити між декількома вузлами.

Чотири персони Cisco ISE:

- Персона адміністрування (PAN): ця частина є центром управління, має користувацький інтерфейс для ліцензування та конфігурації політик. Вміщає у собі усе управління та усі налаштування[11]. Адміністратор відправляє конфігурації на інші вузли розподіленого розгортання і часто називається вузлом адміністратора.
- Персона сервісу політики (PSN): механізм прийняття рішень політики, обробляє весь пов'язаний з Cisco ISE мережевий обмін

повідомленнями, а саме - DHCP, протокол NetFlow і RADIUS, і так далі. Вузли, що реалізують цю персону, називаються вузлами служби політики. Вирішує усі питання пов’язані з доступом та AAA[11].

- Персона моніторингу (MnT): ця персона є двигуном для збору і кореляції журналів та звітів. Генерує звіти і сигнали тривоги для системи Cisco ISE. Вузли, що реалізують цей образ, називаються вузлами моніторингу[11]. Максимум персон в архітектурі – 2.
- pxGrid персона: ця персона включає спільне використання контекстної інформації від каталогу сеансу Cisco ISE до інших мережевих систем, таких як Cisco Adaptive Security Appliance (ASA). Інфраструктуру pxGrid можна використовувати для обміну даними політики та конфігурації між вузлами[11]. Ці дані включають мітки спільного використання і об'єкти політики між Cisco ISE і сторонніми постачальниками для не пов'язаних обмінів інформацією ISE, таких як інформація про загрозу. Для служб pxGrid потрібна додаткова ліцензія.

2.5.2 Модель комунікації вузлів

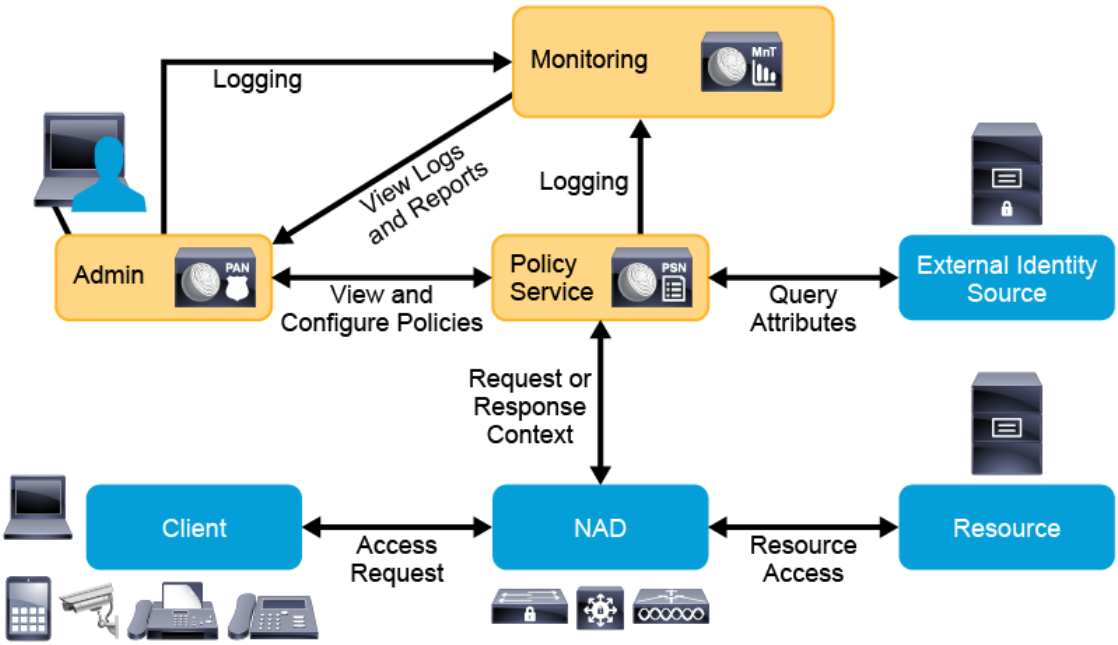


Рисунок 2.10 Характеристика комунікації вузлів Cisco ISE

Рисунок 2.10 ілюструє зв'язок між різними компонентами Cisco ISE і представляє логічний зв'язок, тому що вузли можуть, або не можуть працювати на тому ж пристрої або віртуальному пристрої:

- Клієнт - це пристрій, який намагається отримати доступ до мережі.
- Клієнт з'єднується з комутатором NAD, WLC або між мережевим екраном або концентратором VPN.
- Клієнт отримує запит на автентифікацію, який надсилається протоколом RADIUS до PSN.
- Використовуючи конфігурацію, надану вузлом Admin, PSN обробляє облікові дані клієнта. Потім на основі відповідності політики вузол приймає рішення про авторизацію.
- PSN може запросити будь-яке зовнішнє джерело посвідчень- Microsoft Active Directory, LDAP або сервер сертифікатів.

- PSN передає рішення NAD для здійснення різних функцій, таких як VLAN, dACLs або SGTs.
- На основі цього рішення клієнт може перейти крізь NAD до необхідних мережевих ресурсів.
- Вся реєстрація, така як обмін автентифікацією системного журналу від PSN, передається вузлу моніторингу для кореляції та обробки.
- Вузол Admin є вікном адміністратора Cisco ISE в інфраструктурі. У той час як вузол моніторингу виконує функцію ведення журналу, можна переглянути інформацію про реєстрацію через GUI вузла Admin. Точно так само, в той час як PSN керує операціями політики виконання, адміністратор переглядає і налаштовує ці політики через GUI вузол Admin.

2.6 Дослідження служб сертифікації

Інфраструктура відкритих ключів (PKI) призначена для надійного розповсюдження інформації про відкритий ключ. Ця система автентифікації базується на приватних та відкритих ключових парах. Аутентичність відкритого ключа гарантується CA.

Cisco ISE підтримує паролі та автентифікацію користувачів на основі сертифікатів. Деякі методи автентифікації використовують змішаний підхід. Змішані підходи використовують декілька типів облікових даних для досягнення двоспрямованої автентифікації між клієнтом та сервером, такими як паролі, одноразові паролі (OTP) та сертифікати.

Для майже всіх методів EAP, таких як розширений протокол перевірки транспортного рівня (EAP-TLS) та розширений протокол перевірки автентичності - Microsoft Challenge Handshake Authentication

Protocol Version 2 (PEAP-MSCHAPv2), клієнт перевіряє мережу, перевіряючи дійсність сервера сертифікатів аутентифікації Cisco ISE.

Для PEAP-MSCHAPv2 мережа перевіряє клієнта за допомогою імен користувача та паролів. Тому потрібно лише сертифікати для серверних пристроїв, таких як Cisco ISE.

Однак, для EAP-TLS, клієнт перевіряє мережу, перевіряючи сертифікат сервера Cisco ISE, а мережа перевіряє клієнта, перевіряючи сертифікат клієнта. Тому потрібно створювати та поширювати сертифікати для кожного клієнтського пристрою, крім сервера автентифікації.

Перевірка сертифіката сервера

1. Використовується в PEAP, EAP-TLS, PEAP-TLS та EAP-FAST.
2. Клієнт вимагає кореневого сертифіката CA або явного відношення до надійності до сертифіката сервера.
3. Самописний сертифікат Cisco ISE не рекомендується.

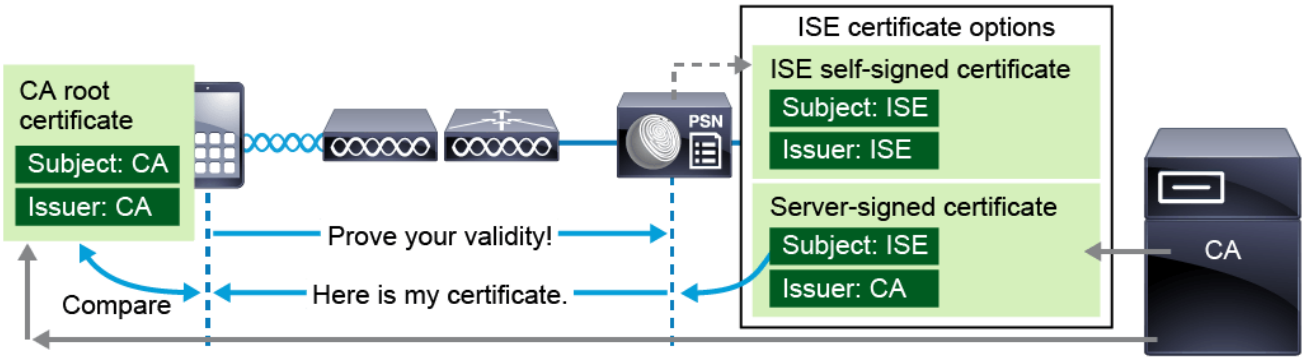


Рисунок 2.11 Відпрацювання служби сертифікатів

Для рішень на основі 802.1X / EAP необхідно налаштувати інфраструктуру відкритого ключа з сервером CA. Є можливість розгорнути власну службу сертифікації або підписати контракт із сторонньою службою PKI.

У CA ви створюєте сертифікат для кожного сервера автентифікації, наприклад Cisco ISE. Цей процес дозволяє Cisco ISE довести свою автентичність клієнтам. Cisco ISE постачає сертифікат із власним

підписом, який ви можете використовувати, але краще уникати його використання та розгортання сертифікатів за допомогою CA. Таким чином, ви досягнете більш безпечного та масштабованого рішення.

Тим часом ви поширюєте копію кореневого сертифіката сервера CA для кожного клієнта. Припускаючи завершення всієї іншої конфігурації, ви готові для автентифікації клієнтів.

Для майже всіх методів автентифікації EAP клієнт запитує сертифікат сервера Cisco ISE. Cisco ISE виступає як серверна сторона та пред'являє клієнтові сертифікат ідентифікації. Клієнт порівнює цей сертифікат сервера зі збереженою копією кореневого сертифіката. Якщо сертифікат дійсний, автентифікація продовжується. Якщо клієнт визначає, що сертифікат недійсний, аутентифікація припиняється. Ви не хочете, щоб клієнт виявив облікові дані на ненадійному сервері.

Перевірка сертифіката клієнта:

1. Використовується в EAP-TLS, PEAP-TLS та EAP-FAST
2. Сервер повинен мати кореневий сертифікат CA
3. Аутентифікація клієнта виконується після автентифікації сервера

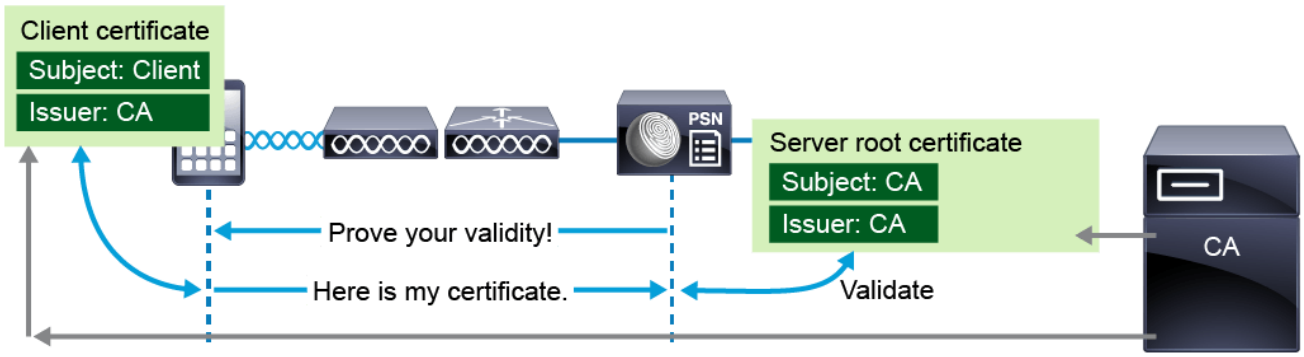


Рисунок 2.12 Перевірка сертифіката клієнта

Для деяких методів EAP клієнти можуть використовувати сертифікати для підтвердження своєї ідентичності, включаючи EAP-TLS, PEAP-TLS та, можливо, EAP-FAST. Звичайно, ви повинні отримати доступ

до своєї служби сертифікації для створення сертифікатів клієнта, а потім поширювати їх клієнтам. Починаючи з версії 1.3, Cisco ISE може служити як CA. Ви також повинні поширювати кореневий сертифікат сервера CA на Cisco ISE.

Під час автентифікації Cisco ISE вимагає, щоб клієнт довів свою ідентичність. Клієнт надає свій сертифікат, і Cisco ISE порівнює цей сертифікат із збереженим копією кореневого сертифіката CA. Cisco ISE витягує відкритий ключ кореневого сертифіката CA і використовує його для перевірки підпису CA у отриманому сертифікаті ідентифікації клієнта.

Профілі автентифікації сертифікатів

- Увімкнути додаткову функцію автентифікації клієнта

1. Виконується після сеансу TLS
2. Після перевірки сертифіката клієнта

- Профілі аутентифікації сертифікатів включають таку інформацію:

1. Поле сертифіката, яке слід використовувати як основне ім'я користувача
2. Необхідно провести бінарне порівняння сертифіката

2.7 Політики Cisco ISE

Cisco Identity Services Engine (ISE) використовує ієрархічну систему політики для управлінням доступом до мережі. Політика – це набір умов та результат спрацювання. Умови складаються з атрибута, оператора та значення. Існує два типи політик: проста, та основана на правилах.

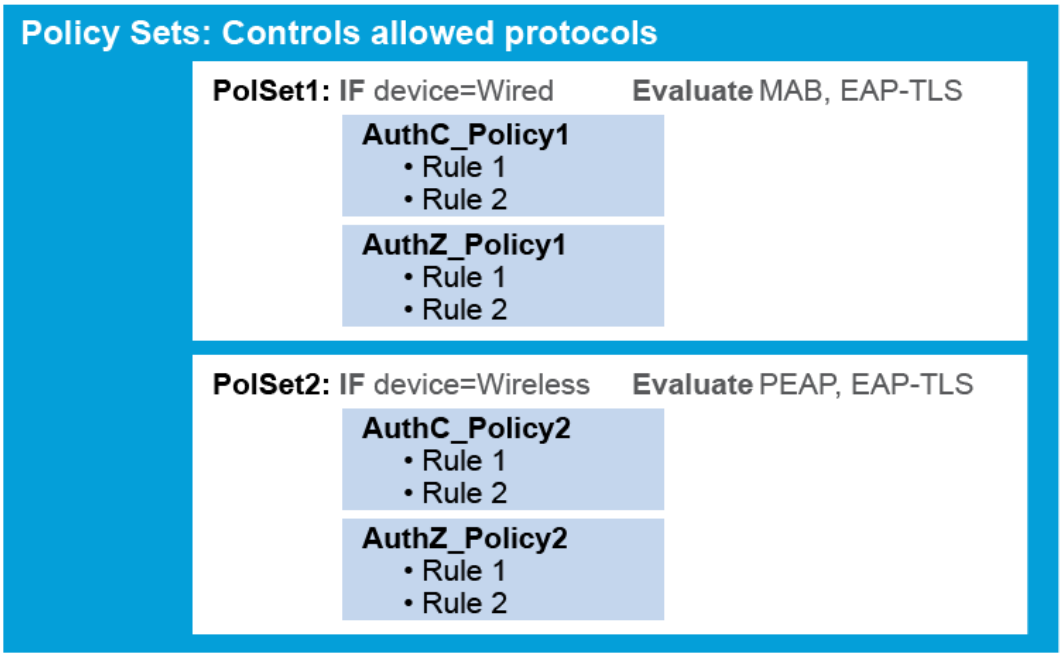


Рисунок 2.13 Приклад політики Cisco ISE

На рисунку 2.13 наведено приклад політики Cisco ISE, а набори політики знаходяться на вершині цієї ієрархії. Набір політики містять три основні, взаємопов'язані функції:

- Служить як контейнер для логічного групування правил автентифікації та авторизації.
- Використовує логічні умови для спрямування користувачів до відповідної групи правил для аутентифікації та авторизації мережі.
- Обмежує сеанс дозволу на набір дозволених протоколів (або проксі на зовнішньому сервері RADIUS).

При створенні політики може знадобитися групова політика автентифікації та авторизації на основі деяких критеріїв, виконаємо це завдання, створивши набори правил. Наприклад, групування може базуватися на наступному:

- Сценарій використання: бездротовий зв'язок, проводове з’єднання або гість. Є можливість згрупувати набір правил

автентифікації та авторизації, які базуються на випадку використання, як показано на рисунку. Проводові з’єднання використовують інший набір політик, ніж бездротові користувачі.

- Місцезнаходження: регіон, кампус або будинок. Є можливість створити різні набори політики для різних розташувань у організації. Можливо, компанія прагне, щоб користувачі в основному кампусі автентифікувались використовуючи різні ресурси, ніж ті, що знаходяться в віддаленому кампусі. Можна використовувати будь-які критерії, відповідні вашій організації.

Як показано на малюнку, створюється політика, встановлена шляхом налаштування трьох основних елементів: ім'я, умови та результуючий набір дозволених протоколів. Розглянемо на набір політик PolSet1. Якщо користувач намагається отримати доступ до мережі за допомогою проводового комутатора Ethernet, вибирається PolSet1. Таким чином, вони будуть обмежені набором дозволених протоколів для автентифікації; в цьому випадку їм дозволяється використовувати лише MAC Authentication Bypass (MAB) або протокол розширення перевірки автентичності (Layer Security) (EAP-TLS). Вони будуть автентифіковані на основі правил, що містяться в AuthC_Policy1, і мають право на доступ до певних ресурсів за допомогою політики авторизації AuthZ_Policy1.

Набори політики обробляються "зверху вниз", як і типовий список доступу (ACL). Оскільки PolSet1 перераховано першим то спочатку перевіряються його умови. Якщо ці умови не виконуються (не провідний користувач), то перевіряється PolSet2.

Політика PolSet2 перевіряє, чи використовують користувачі бездротові пристрої. Якщо так, тоді користувач може автентифікувати лише через протокол захищеного розширюваного аутентифікації (PEAP) або EAP-TLS. Вони автентифікуються за правилами AuthC_Policy2 і авторизовані на основі правил у AuthZ_Policy2.

2.7.1 Політика автентифікації та авторизації

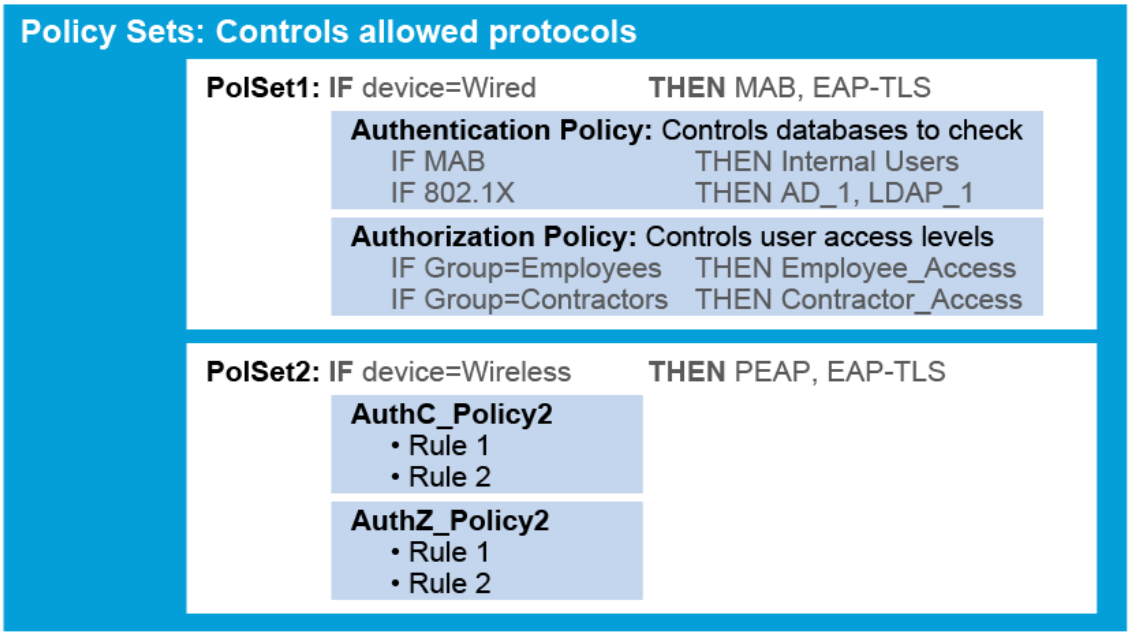


Рисунок 2.14 Приклад політики автентифікації та авторизації архітектури Cisco ISE

Набори політик є найвищим рівнем політики системи Cisco ISE. Вони спрямовують користувачів на набір політик і обмежують їх набір дозволених протоколів. Другий рівень цієї ієрархії складається з фактичних правил аутентифікації та авторизації.

Правила автентифікації контролюють, які бази даних перевіряти на облікові дані користувачів, так зване джерело ідентичності або послідовність джерела ідентифікації. Кожен набір політики може мати лише одну політику автентифікації, однак ця політика може мати кілька правил.

На рисунку політика перевірки автентичності PolSet1 має два правила, і, як ACL, ці правила обробляються зверху вниз. Розглянемо перше правило. Якщо користувач намагається здійснити автентифікацію за допомогою MAB, його облікові дані перевіряються на одному джерелу ідентифікації - базі даних внутрішнього користувача Cisco ISE. Якщо ця

умова не виконується, то перевіряється друге правило. Якщо використовується 802.1X, то застосовується послідовність джерел ідентифікації. По-перше перевіряється, Active Directory з ім'ям AD_1, після чого перевіряється база LDAP з ім'ям LDAP_1.

Незалежно від MAB або 802.1X, облікові дані користувачів перевіряються на відповідну базу даних. Якщо дані дійсні, користувач аутентифікується – тобто ми знаємо, хто є користувачем. Але які дії дозволено виконати користувачеві?

Політика авторизації визначає, які ресурси користувач може отримати. Знову ж таки, можна мати лише одну політику авторизації (і деякі політики виключення авторизації, які незабаром будуть описані). Ця політика може мати кілька правил, які обробляються зверху вниз.

У політиці авторизації PolSet1 рівень доступу визначається членством у групі Active Directory. Якщо ви є членом групи працівників, то вам надається відповідний рівень доступу працівників. Якщо ви є членом групи підрядників, то ваші права обмежуються лише доступом до меншого набору ресурсів.

Поглянемо на цей процес з точки зору користувача, який намагається отримати доступ до своєї мережі:

- Послуги доступу до мережі вибрані на рівні встановлених політик.
- Джерела ідентифікації вибираються на рівні політики автентифікації.
- Права на мережу вибрані на рівні політики авторизації.

2.7.2 Автентифікація та її компоненти

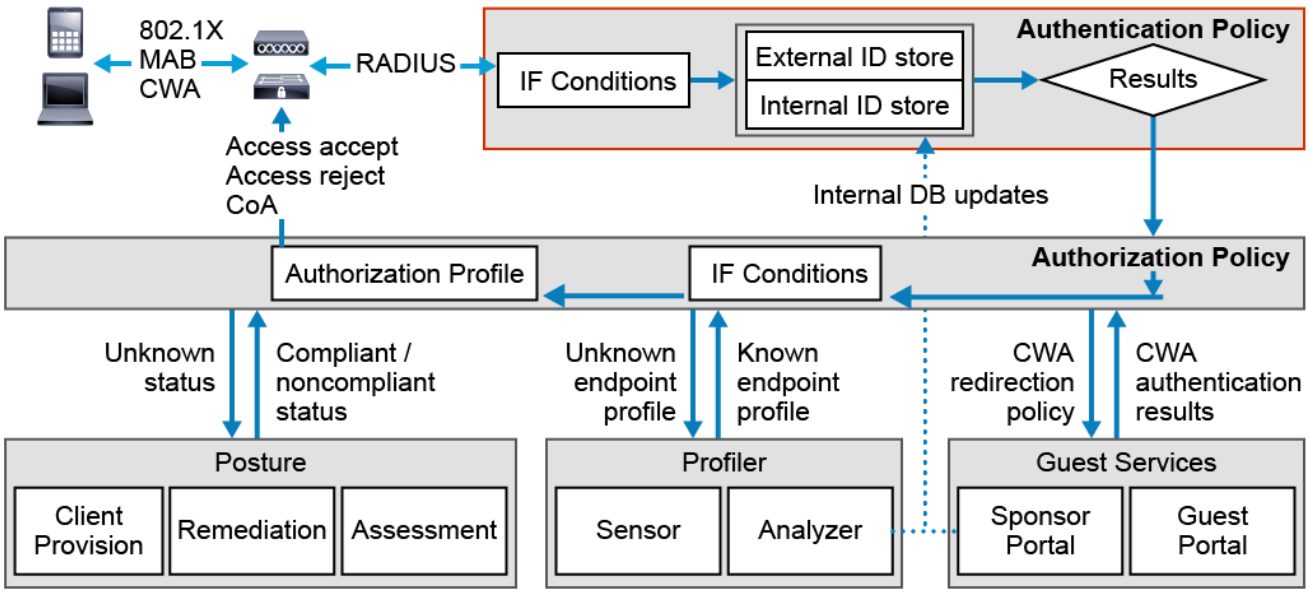


Рисунок 2.15 Схема компонентів політики автентифікації

На рисунку 2.15 показано взаємозв'язок між різними службами Cisco ISE, пов'язаними з автентифікацією, авторизацією, профілюванням та гостьовими службами. Ця підтема зосереджена на аутентифікації. Запити автентифікації обробляються відразу після того, як кінцева точка намагається отримати доступ до мережі за допомогою пристрою доступу до мережі (NAD). Cisco ISE оцінює контекстну інформацію, яка пов'язана з конкретним з'єднанням кінцевого пристрою та порівнює її з умовами політики автентифікації. Коли він знаходить відповідність, вибирається певний зовнішній або внутрішній ідентифікатор (або вибрано послідовність ідентифікаторів). Облікові дані користувача перевіряються на адресу схощива особистих даних. Звичайно, якщо недійсні облікові дані призводять до невдалої автентифікації, доступ зазвичай відхиляється. Дійсні облікові дані призводять до успішної автентифікації.

Потім політика авторизації обробляється поряд з іншими службами, як показано на рисунку.

2.7.3 Компоненти політики автентифікації

Пам’ятатимемо, що набір політик визначає протоколи, які Cisco ISE повинна використовувати для аутентифікації пристроїв. Політика автентифікації визначає джерела посвідчень, які вона повинна використовувати для автентифікації. Політика автентифікації складається зі списку правил. Кожне правило автентифікації складається з трьох компонентів:

1. Ім'я.
2. Набір умов.
3. Результуюче джерело ідентифікації.

Ім'я - це будь-яке довільне ім'я, яке має сенс для адміністраторів, можливо, відповідне деякій корпоративній угоді про імена.

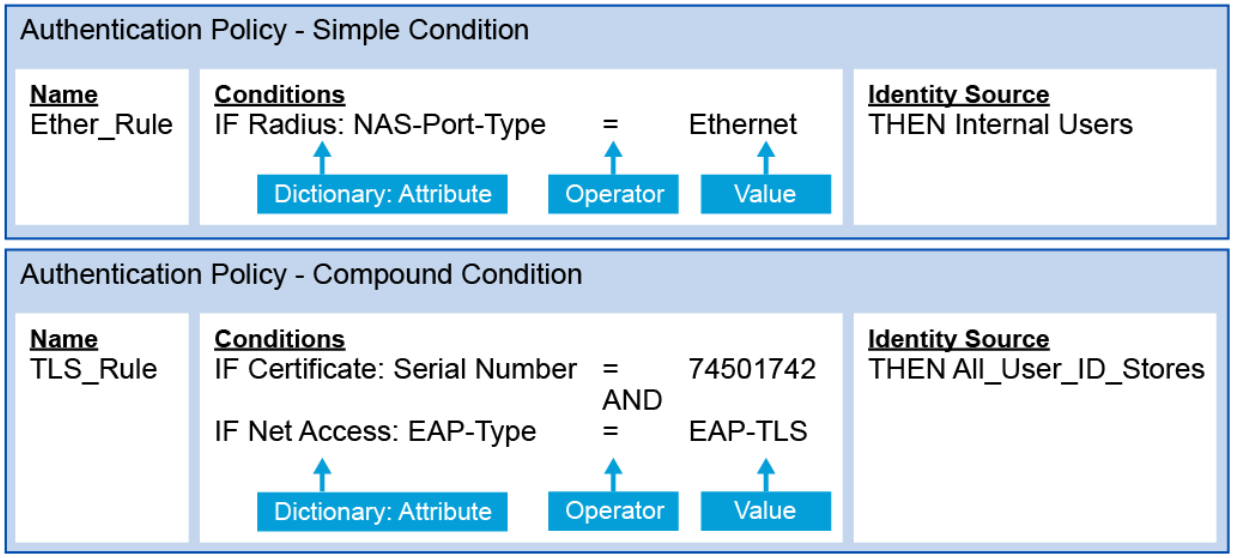


Рисунок 2.16 Приклад компонентів політики Cisco ISE

Умова складається з операндів (атрибут), оператор (рівне, не дорівнює, більше і т. д.), і значення. Можна створити складні умови, що складаються з одного або декількох простих умов, З'єднаних оператором AND або OR. Cisco ISE оцінює умови політики і потім застосовує вказаний

результат на основі того, чи повертає оцінка політики значення true або false.

Cisco ISE дозволяє вам створювати умови як окремі, повторно використовувані елементи політики, на які можна послатися від іншої заснованої на правилах політики.

У верхній частині рисунка 2.14 показано досить просте правило з ім'ям *Ether_Rule*. Стан умови: якщо Radius NAS-Port-Type = Ethernet. Якщо ця умова виконана, результатом є те, що база даних внутрішнього користувача Cisco ISE використовується для пошуку облікових даних.

Існує ще одне правило з ім'ям *TLS_Rule*. Це правило зв'язується з умовами логічним оператором AND. Якщо серійний номер сертифікату = 74501742 і тип аутентифікації EAP доступу до мережі = EAP-TLS, то послідовність серверів може бути використана для перевірки користувача на облікові дані. Перевіряються фактичні сервери, що визначені в послідовності джерел ідентифікації з ім'ям All_User_ID_Stores.

Зверніть увагу, що атрибут має формат *DICTIONARY: dictionary-attribute*. Слово сертифікат - це словник. Всередині цього довідника знаходиться список атрибутів, пов'язаних з сертифікатами.

Розглянемо ці словники, джерела посвідчень та послідовності джерел посвідчень.

Словники

- Основний елемент політики.
- Набір параметрів, що визначають атрибути сеансу.
- Атрибути, зазначені в умовах, що визначають застосовність політики.

Словники надають фундаментальні будівельні блоки для політик Cisco ISE. Довідник являє собою набір окремих параметрів для використання в умовах конфігурації. Умови використовуються для створення політики автентифікації та авторизації. Умови задають

обмеження на атрибути сеансу, які використовуються для визначення, які політики застосовуються в режимі реального часу.

Джерела ідентифікації

- Використовуються для перевірки облікових даних для функцій аутентифікації користувачів.
- Використовуються для отримання відомостей про групу для використання в політиках авторизації.
- PSN запитує джерело посвідчення на атрибути політики.
- Можна групувати в послідовності джерела ідентифікаторів.
- Джерела внутрішньої ідентифікації Cisco ISE для користувачів і кінцевих точок.

Cisco ISE інтегрується з зовнішніми джерелами ідентифікації для перевірки облікових даних користувача під час аутентифікації. Джерела ідентифікації також використовуються для отримання відомостей про групи та інших атрибутів користувачів для авторизації. Cisco ISE підтримує кілька зазвичай реалізованих джерел ідентифікації, включаючи Active Directory і LDAP. Зовнішні джерела ідентифікації також включають відомості про сертифікат для сервера Cisco ISE і профілів аутентифікації сертифіката.

З Cisco ISE 1.3 існує опція локального сервера CA.

Джерела ідентифікації можуть бути перераховані в послідовності джерел ідентифікації. Коли це задано, Cisco ISE шукає ці джерела ідентичності в порядку, в якому вони визначені.

Cisco ISE підтримує внутрішні бази даних, які можуть використовуватися в якості джерел ідентичності під час процесу аутентифікації. Внутрішня база даних користувачів зазвичай використовується для підтримки гостьового входу. Внутрішня база даних користувачів перш за все заповнена за допомогою функції Cisco ISE profiler.

2.7 Авторизація та її компоненти

2.7.1 Авторизація Cisco ISE

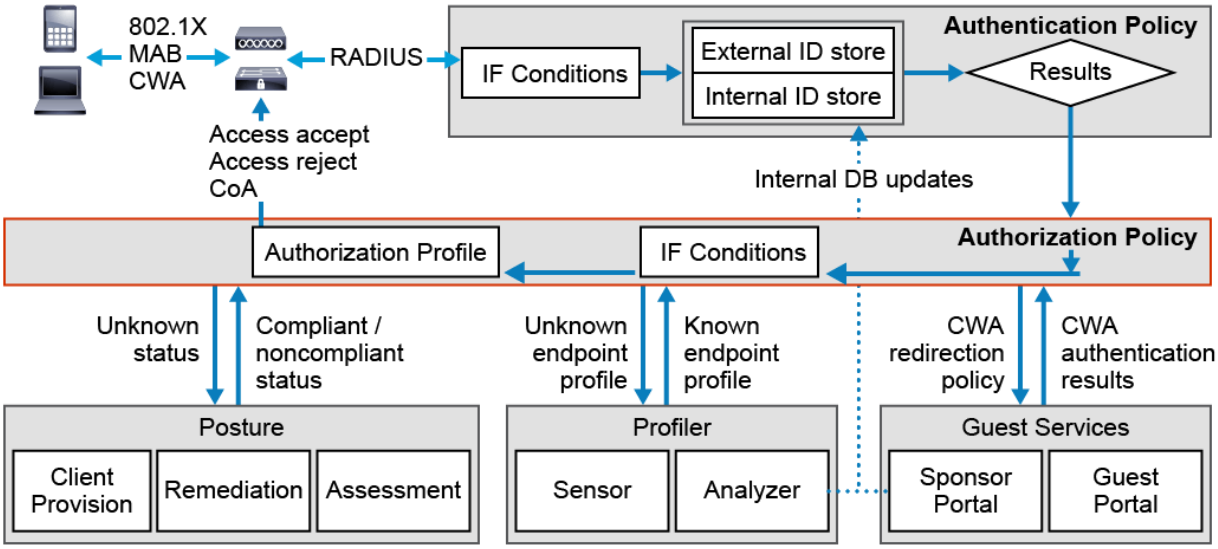


Рисунок 2.17 Схема компонентів політики авторизації Cisco ISE

Потік процесу на Cisco ISE розділяється після того, як аутентифікація завершена. Три окремих компонента можуть бути залучені в ці фази: сервіс положення, профілювальник і процес авторизації. Сервіси положення і профілювальника можуть використовуватися на додаток до служб аутентифікації та авторизації, якщо розгорнуто, вони можуть викликати додатковий обмін інформацією.

Після успішної аутентифікації авторизація управляє рівнями клієнтського доступу, і авторизація є фокусом цього обговорення.

Подібно до аутентифікації, Cisco ISE використовує модульну політику авторизації мережі.

Політика авторизації Cisco ISE заснована на наборі правил. Якщо ідентичність певного користувача і групи співпадає, поряд з набором умов, то відповідний профіль авторизації застосований. Цей профіль висунутий від вузла сервісу політики Cisco ISE до NAD для примусу відповідних

дозволів. Пам'ятайте, що Cisco ISE є заснованою на атрибуті системою політики, і ідентифікаційні групи - один з багатьох атрибутів.

Профілі авторизації складаються з атрибутів, обираних з набору ресурсів, який зберігається в довіднику [9]. Коли складене умова для певної політики авторизації збігається, відповідний профіль застосовується. Оскільки політики авторизації можуть включати складові умови, зіставляються з одним правилом мережевої служби, ці політики також можуть включати список перевірок авторизації.

Профілі авторизації визначають дозволи, надані сеансам клієнта, і можуть включати наступні елементи:

dACL: Cisco ISE може завантижити завантажувані списки управління доступом (DACL) до комутатора доступу, який застосований до певного сеансу користувача. Таким чином, коли співробітник початкового рівня підключається до будь-якого порту, у нього може бути дуже обмежений доступ. Але коли високопоставлений керівник підключається до того ж порту, він отримує підвищений доступ. Для портів, налаштованих в режимі Multi-Auth, він застосовується для кожного користувача. Список контролю доступу (ACL) завантажений один раз на NAD може бути застосований до багаторазових сеансів.

ACL Airespace: Cisco ISE може посилатися на іменовані ACL, налаштовані на контролері бездротової локальної мережі (WLC). Таким чином, різні користувачі можуть підключатися до одного ідентифікатора набору служб (SSID) і отримувати відповідні рівні доступу.

Веб-перенаправлення: перенаправлення до певного порталу для подальших дій, таких як завантаження клієнта положення. Цей процес використовує веб-автентифікації (CWA), реєстрація пристрою WebAuth (DRW), управління мобільними пристроями (MDM).

VLAN: порти проводового комутатора і бездротові SSID налаштовані з VLAN за замовчуванням. Коли ви підключаєтеся до потрібного порту або

SSID, призначається потрібна VLAN. Однак, коли певні користувачі аувтентифікуються, Cisco ISE може змінити цю VLAN за замовчуванням і призначити певним користувачам інший VLAN, можливо на основі членства в групі Active Directory або деяких інших критеріїв.

Автоматичний розумний порт: технологія Cisco Auto Smartports дозволяє відповідним параметрам якості обслуговування (QoS) бути застосованими до порту згідно шаблону.

Ідентифікатор фільтра: ім'я ACL, на яке посилається Cisco ISE. NAD застосовує локальний ACL з цим ім'ям до сеансу.

Повторна перевірка автентичності: потрібно повторна перевірка автентичності і задає таймер повторної перевірки автентичності.

Політика MACsec: безпека керування доступом до середовища (MACsec) - це стандарт IEEE 802.1 AE для автентифікації і шифрування пакетів між двома сусідніми пристроями.

WebAuth (локальний): включає веб-аутентифікацію, яка буде виконана на NAD.

ASA VPN: включає групову політику VPN пристрої адаптивного захисту (ASA), яка буде застосована до сеансу VPN клієнта.

SGT: доступ групи безпеки (SGA) дозволяє ідентифікаційної інформації користувача бути перехопленим і промаркованим з кожним пакетом даних. Списки управління доступом групи безпеки (Sgacl) можуть бути реалізовані в точці виходу для деякого мережевого ресурсу (таких як файловий сервер). Керування доступом на основі SGA дозволяє зберегти існуючу логічну схему на рівні доступу. Гнучкі політики і служби дозволяють виконувати різні бізнес-вимоги без необхідності повторного розгортання елементів управління безпекою. Це рішення позначає кожен пакет на вхідному мережевому пристрої і дозволяє вихідним мережевим пристроям примусово керувати трафіком, найближчим до місця призначення.

2.8 Аналіз елементів політики авторизації

Рисунок 2.16, а саме знімок екрана ілюструє GUI, який використовується для налаштування елементів політики. Елементи політики визначаються як загальні завдання в профілях авторизації. Існує кілька стандартних категорій дозволів, а також додаткові параметри атрибутів. Додаткові параметри атрибутів дозволяють передавати додаткові атрибути довідника в NAD в якості параметрів авторизації.

Ім'я DACL: встановіть прапорець і виберіть існуючі завантажувані параметри ACL, які доступні. Cisco ISE надає два значення за замовчуванням у випадаючому списку: PERMIT_ALL_TRAFFIC або DENY_ALL_TRAFFIC. Список включатиме всі поточні списки DACL в локальній базі даних.

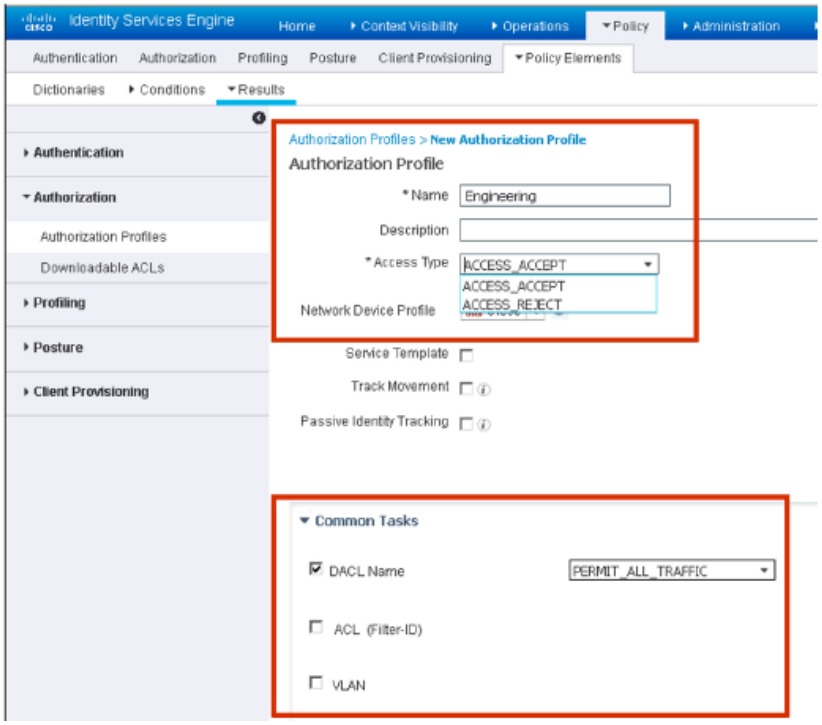


Рисунок 2.18 Графічний інтерфейс налаштування елементів політики авторизації

VLAN: встановіть прапорець і введіть значення атрибута, який визначає ідентифікатор VLAN, який необхідно пов'язати з новим профілем

авторизації, який створюється. Цілочисельні та рядкові значення підтримуються для ідентифікатора VLAN.

Веб-перенаправлення: встановіть прапорець, щоб включити процес перенаправлення. Виберіть тип процесу перенаправлення, CWA, DRW, MDM, NSP або CPP. Введіть назву ACL перенаправлення на пристрої, який потрібно пов'язати з цим профілем авторизації, і виберіть бажаний портал. Встановіть прапорець статичний IP / ім'я хоста, щоб вказати точну IP-адресу або ім'я хоста, на який необхідно перенаправити користувача. Якщо цей прапорець не встановлено, користувач буде перенаправлений на повне доменне ім'я вузла служби політики, який отримав цей запит.

ACL (Filter-ID): встановіть прапорець, щоб включити атрибут фільтра RADIUS, який передає назву ACL, яке визначене в текстовому полі. Це ім'я автоматично додається . На вибір відображається в області відомостей про атрибути.

Повторна перевірка: встановіть прапорець і введіть значення в секундах для підтримки зв'язку під час повторної перевірки автентичності. Можна також вибрати значення атрибутів зі спадного списку таймер.

Політика MACSec: встановіть прапорець для включення політики шифрування MACSec щоразу, коли клієнт з підтримкою MACSec з'єднується з Cisco ISE.

Web Authentication (Local WebAuth): встановіть прапорець, щоб включити локальну web-аутентифікацію для цього профілю авторизації. Це значення дозволяє комутатору розпізнавати авторизацію для веб-аутентифікації Cisco ISE, що відправляє VSA поряд з DACL. VSA є *cisco-av-pair=priv-lvl=15*, і цей атрибут буде відображений в області відомостей про атрибути.

Назві Airspace ACL: встановіть прапорець і введіть ім'я ACL в текстове поле. Це значення використовується в необхідному VSA Airespace для авторизації додавання локально певного ACL до з'єднання на

WLC. Наприклад, якщо ввести Engineering_WLC_ACL, це значення буде відображено в області відомостей про атрибути наступним чином: *Airespace-ACL-Name = Engineering_WLC_ACL*.

VPN ASA: встановіть прапорець, щоб увімкнути групову політику VPN ASA. У списку атрибутів виберіть значення для налаштування цього параметра.

2.9 Висновки з розділу 2

1. В розділі розглянуто про ієрархічну природу системи політики для управлінням мережевого доступу. Описано набори політик - верхню частину ієрархії - і як вони направляють користувачів на наступні ієрархічні рівні. Наступний рівень ієрархії включає політику автентифікації та політику авторизації.
2. Досліджено, як набори політик, політики автентифікації та політики авторизації сервера гарантують, що користувачі отримують відповідні рівні доступу, на основі вашої конкретної корпоративної політики.
3. Описано ключові компоненти сутності Cisco ISE і різні опції для їх розгортання. Також зможете описано, як компоненти архітектури Cisco ISE взаємодіють один з одним.

РОЗДІЛ 3. ОРГАНІЗАЦІЯ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОБОТИ АРХІТЕКТУРИ CISCO ISE

3.1 Постановка задачі

У віртулізованому середовищі VMware була побудована мережа топологія якої наведена на рисунку 3.1. Виписано задачі які були поставлені для впровадження архітектури Cisco ISE:

1. Налаштування базових політик доступу для дротового і бездротового доступу для співробітників і консультантів.
2. Інтеграція Cisco ISE з Microsoft Active Directory.
3. Налаштування гостьового доступу.
4. Аналіз інструментів мережевого злому.

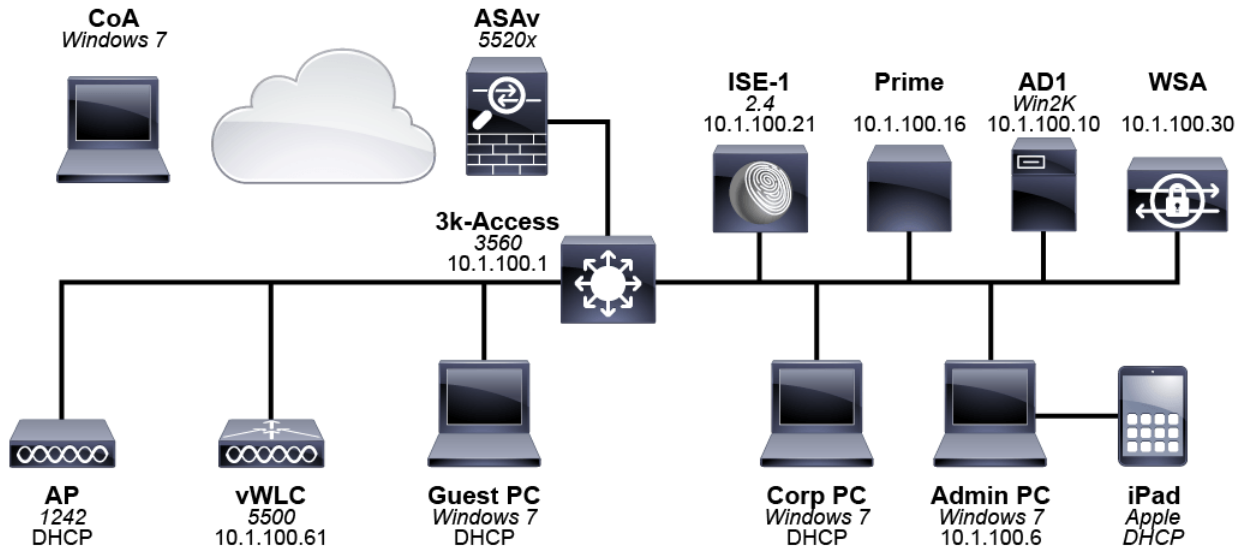


Рисунок 3.1 Топологія локальної мережі організації

Вузол Cisco ISE був розгорнутий у якості віртуальної машини на платформі VMware з версією 2.4. Інсталяція та налаштування було проведено раніше та в магістерській роботі не описано. Доступ до вузла виконується через web браузер за посиланням https://ise-1.demo.local.

3.2 Налаштування базових політик доступу для дротового і бездротового доступу

Для створення блоку диференціювання пристроїв мережевого доступу переходимо до панелі: *Administration* > *Network Resources* > *Network Device Groups*. Використовуємо таблицю 4.1 для створення груп мережевих пристроїв.

Табл. 3.1 – Parent Group

Назва	*Опис*	*Батьківська група*
Wired	Wired Access Switches	All Device Types
Wireless	WLCs	All Device Types
VPN	VPN Access Devices	All Device Types
HQ	Headquarters	All Locations
Branch1	Branch1	All Locations
RnD Lab	Research_Development Lab	All Locations

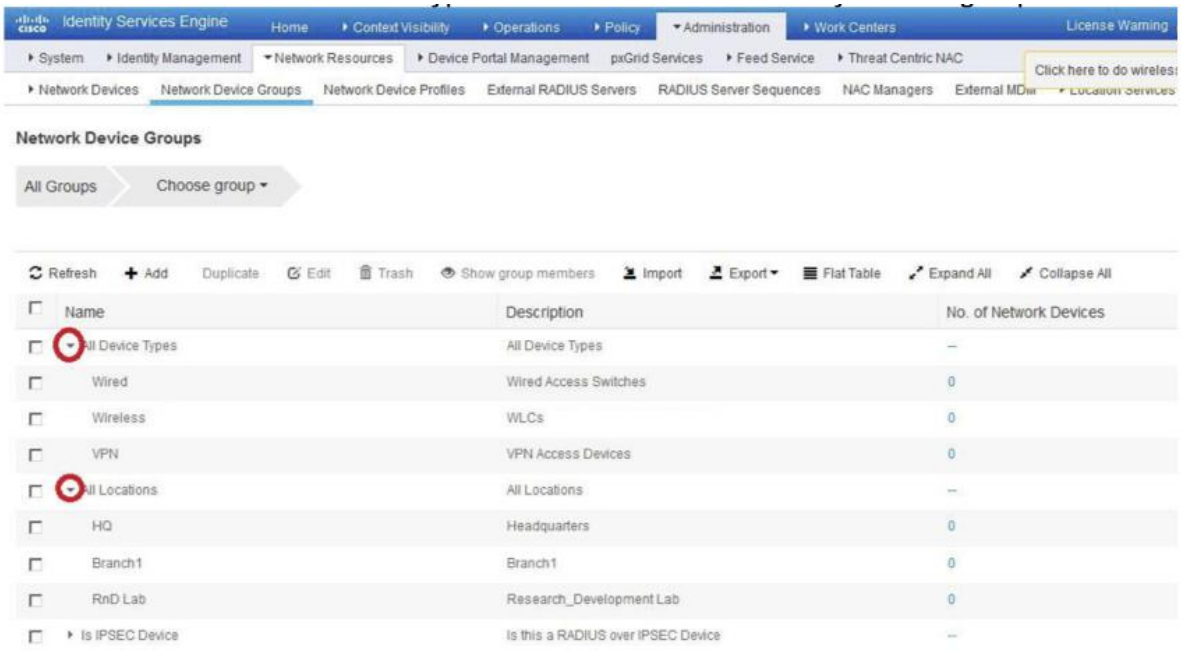


Рисунок 3.2 Результат створення груп

Визначаємо фактичні проводові та бездротові мережеві пристрої які будуть членами щойно створених груп згідно таблиці 4.2, для цього переходимо до вкладки *Administration* > *Network Resources* > *Network Devices*. У правій області натисніть кнопку *+Add* на панелі інструментів. Для прикладу опишемо атрибути проводового пристрою: комутатор Catalyst 3560.

Табл. 3.2 – NAD – 3k-acess

Атрибут	*Значення*
Name	3k-access
Description	3560 access switch
IP Address	10.1.100.1/32
Model Name	<blank>
Software Version	<blank>
Network Device Group	
Location	HQ
IPSEC	No
Device Type	Wired
RADIUS Authentication Settings	Checked
Shared Secret	ISEisC00L
TACACS Authentication Settings	Unchecked
SNMP Settings	Unchecked
Advanced TrustSec Settings	Unchecked

Вже створені групи пристроїв, визначені пристрої і призначені ці пристрої відповідним групам. Тепер можна створювати окремі набори політик для дротового і бездротового доступу.

Переходимо на вкладку *Policy* у верхній частині екрана і обираємо *Policy Sets*.

Переходимо до значка *Gear* в наборі політик за замовчуванням і обираємо *Insert a new row above*. Буде створено новий набір політик. Перейменуємо політику в *Wired Access Policy*. У спадному меню обираємо доступ до мережі за замовчуванням.

Умова набору політик має виглядати наступним чином, як на рисунку 3.3.

Рисунок 3.3 Політика для проводового доступу

Аналогічно для безпровідного доступу – рисунок 3.4.

Рисунок 3.4 Політика для безпровідного доступу

3.3 Створення політик авторизації

Переходимо на вкладку елементи політики та обираємо результати. Далі, *Authorization > Downloadable ACLs*. Натискаємо кнопку додати на панелі інструментів правій панелі. Створюємо список DACL для співробітників за допомогою наступних атрибутів:

Табл. 3.3 Downloadable ACL: acl_employee

Атрибут	*Значення*
Name	acl_employee
Description	Employee access ACL restricting access to the Quarantine Network.
DACL Content	*deny ip any 10.1.30.0 0.0.0.255* *permit ip any any*

Створюємо інший dACL згідно таблиці 3.4.

Табл. 3.4 Downloadable ACL: acl_contractor

Атрибут	*Значення*
Name	acl_contractor
Description	Contractor access ACL restricting access to the Quarantine and AP Network.
DACL Content	*deny ip any 10.1.30.0 0.0.0.255* *deny ip any 10.1.90.0 0.0.0.255* *permit ip any any*

Створюємо профілі авторизації для співробітників – в лівій панелі.

3.4 Інтеграція Cisco ISE з Active Directory

У порталі адміністрування Cisco ISE переходимо до *Work Centers* > *Network Access* > *Overview*

Обираємо посилання *Introduction* на лівій панелі. На панелі *Prepare* робочого центру обираємо посилання зовнішні сховища посвідчень. Звідти

в розділі зовнішні джерела посвідчення на лівій панелі виберіть Active Directory.

У правій області натисніть кнопку *Add* на панелі інструментів.

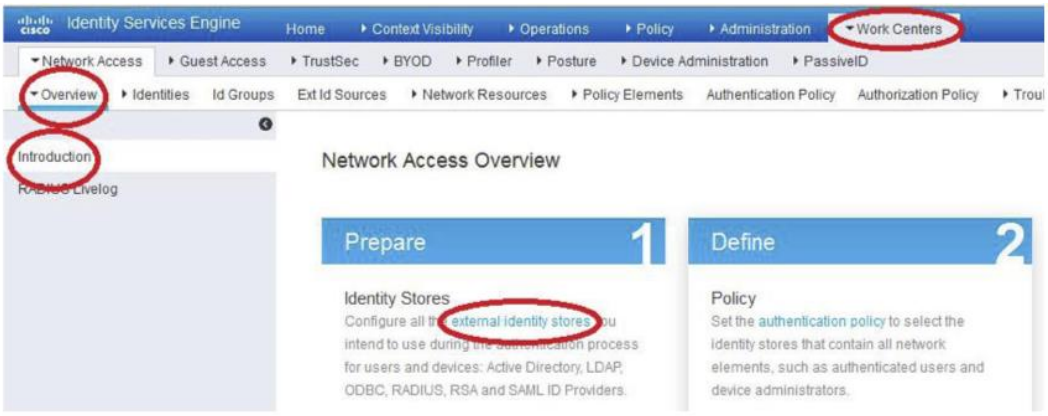


Рисунок 3.5 Портал адміністрування

Вводимо *demo.local* в полях Join Point Name і домен Active Directory.

Підтверджуємо налаштування кнопкою *Submit* у спливаючому вікно, що запитує нас чи хочете ми приєднатися до всіх вузлів ISE до цього домену Active Directory. У полі приєднати домен використовуємо облікові дані ім'я користувача: *administrator* і пароль: *ISEisC00L*. Встановлюємо прапорець вказати підрозділ. Змінюємо значення DN відповідно до наступних: *OU=ISE,OU=HCC,DC=DEMO,DC=LOCAL*.

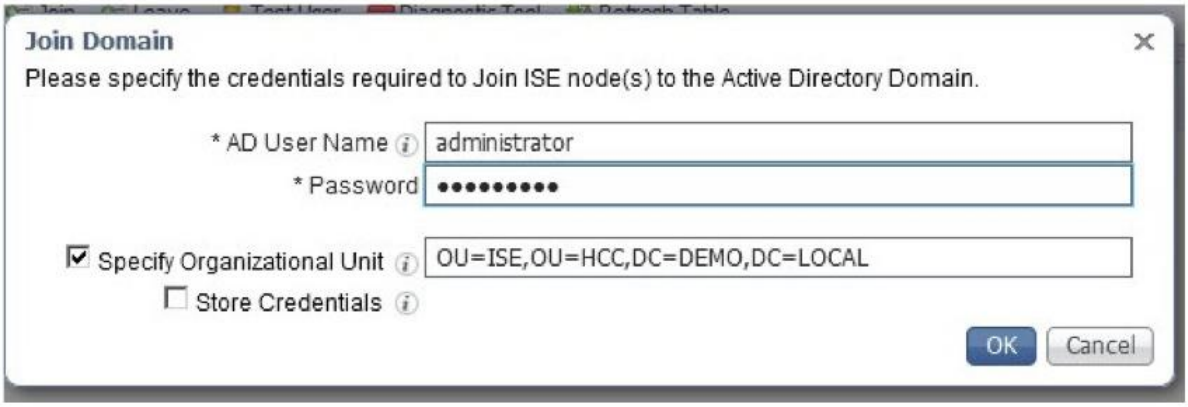


Рисунок 3.6 Панель зв'язку з доменом

З Cisco ISE v1.3 можна додатково визначити місце, де обліковий запис Cisco ISE буде створено замість використання контейнера комп'ютерів за замовчуванням. Для цього організаційний підрозділ має бути попередньо створений. Cisco ISE не створить структуру організаційної одиниці в Active Directory для відповідності.

Після завершення процесу закриваємо вікно та запускаємо служби діагностики. Обираємо вузол ise-1 зі списку. На панелі інструментів вибираємо засіб діагностики. Натискаємо кнопку запустити тести. Тест може зайняти кілька хвилин. Всі тести повинні виконуватися зі статусом успішно, як показано на рисунку 3.7.

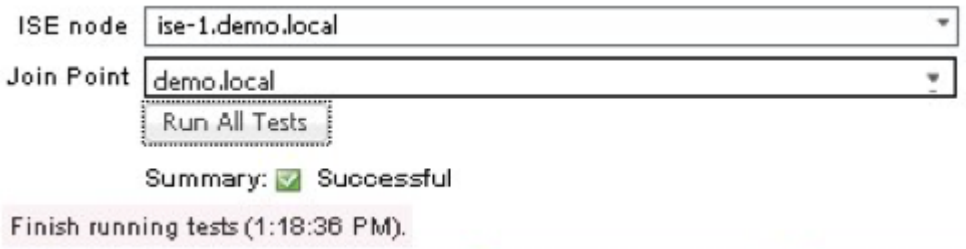


Рисунок 3.7 Запуск служби діагностики

Додаємо атрибути Active Directory до словника Cisco ISE.

У лівій області вибираєм *demo.local* запис в Active Directory. У правій області переходимо до вкладки *Group*. Натискаємо кнопку *+Add* на панелі інструментів і обираєм групи з довідника.

Cisco ISE розширила можливості фільтра у виборі груп від Active Directory. Залишаємо тип фільтру як все і натискаємо кнопку *Retrieve Groups…*

Спостерігаємо за списком і звернімо увагу, що існує багато груп, які, ймовірно, не були б придатними для використання в Cisco ISE для відповідності політики.

Тепер змінюємо тип фільтра на глобальний і натискаємо кнопку *Retrieve Groups…*

Отриманий список тепер, ймовірно, більш підходить для використання політики.

Обираємо увесь список груп, встановивши прапорець ім'я в полі *Name*.

Рисунок 3.8 Список груп авторизації

У цьому списку скасуємо вибір наступних груп:

- Demo.local/Users/DnsUpdateProxy
- Demo.local/Users/Domain Controllers
- Demo.local/Users/Domain Guests
- Demo.local/Users/Group Policy Creator Owners
- Demo.local/Users/Read-only Domain Controllers

У правій області переходимо до вкладки атрибутів.

Натискаємо кнопку *+Add* на панелі інструментів і обираємо атрибути з каталогу.

Вводимо *employee2* в текстове поле для прикладу облікового запису користувача або комп'ютера і натискаємо кнопку *Retrieve Groups...*

Далі, обираємо *badPwdCount* і *userPrincipalName* зі списку і натискаємо OK.

Будуть показані тільки встановлені атрибути. Якщо один обліковий запис не має набору атрибутів, а інший, наприклад має посаду або відділ, то при витяганні атрибутів з облікового запису з набором атрибутів будуть показані ці атрибути. Атрибут може бути встановлений після того, як цей

список витягнув, і якщо цей користувач знову запитується додатковий атрибут буде відображатися в списку.

В Cisco ISE є функція виконати різні методи перевірки автентичності користувача тестування до Active Directory. Ця функція буде розглянута нижче.

У лівій області обираємо *demo.local* запис в Active Directory. У правій області вибираємо *ise-1.demo.local*.

Обираємо тестовий користувач на панелі інструментів. Змінюємо тип автентифікації на пошук. Вводимо ім'я користувача employee2. Перевіряємо результат.

Зверніть увагу на кроки обробки в нижній частині вкладки результат перевірки автентичності. Приклад знімка екрана показаний нижче на рисунку 3.9. Тепер натискаємо на групи, а потім вкладки атрибути і спостерігаємо деталі.

```
Processing Steps:
14:13:39:406: Resolving identity - employee2
14:13:39:406: Search for matching accounts at join point - demo.local
14:13:39:491: Single matching account found in forest - demo.local
14:13:39:491: Identity resolution detected single matching account
```

Рисунок 3.9 Перевірка пошуку користувача в базі

Змінюємо тип автентифікації за протоколом Kerberos. У полі пароль вказуємо *ISEisC00L*. Перевіряємо результат. Звернемо увагу на кроки обробки в нижній частині вкладки результат перевірки автентичності (рисунок 3.10).

Також звернімо увагу, що запити квитка автентифікації (TGT) успішні і наступні два елементи рядка вказують на успіх відпрацювання протоколу Kerberos.

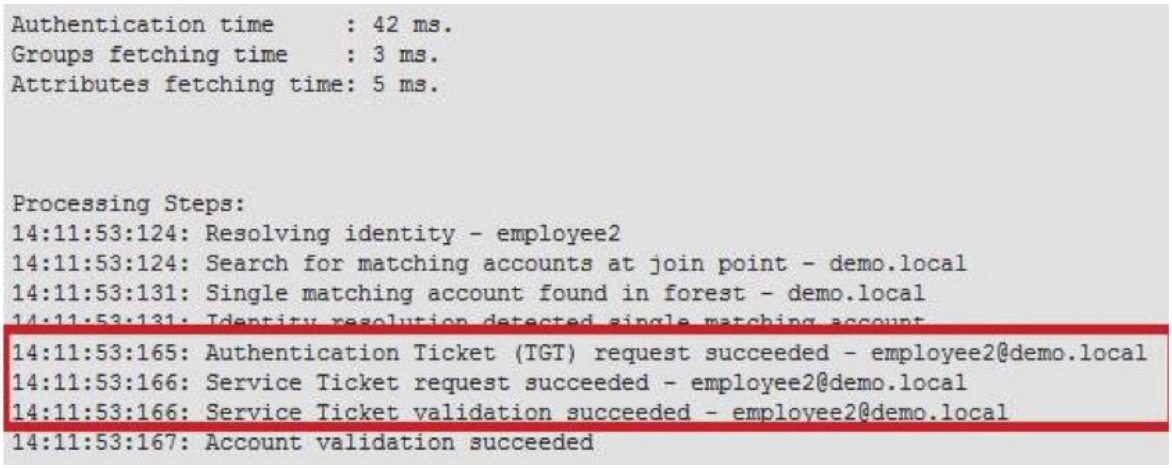


Рисунок 3.10 Відпрацювання протоколу Kerbreros

Ми налаштували наш POD Active Directory в якості зовнішнього джерела посвідчень. Ця конфігурація буде використовуватися для аутентифікації.

3.3 Налаштування гостьового доступу

Гостьовий доступ буде налаштований у вигляді порталу Cisco ISE, де не корпоративні користувачі зможуть мати обмежений доступ до мережі. Цей портал призначений для тих людей, яким потрібен найпростіший метод гостьового доступу, і які менше піклуються про суворий контроль або відстеження користувачів організації. Портал включає екран для входу, екран з допустимою політикою використання, екран для зміни паролю та екран само реєстрації.

Деякі організації вимагають трохи більше контролю і обізнаності для гостей. Для реалізації цих сценаріїв необхідно налаштувати гостьовий доступ для самостійної реєстрації.

На PC адміністратора в порталі адміністрування Cisco ISE переходимо до *Work Centers* > *Guest Access* > *Overview*.

У розділі визначення переходимо до посилання гостьові портали та обираємо вкладку портали і компоненти на вкладці гостьовий доступ.

У верхній частині цієї сторінки натискаємо кнопку *Create*.

У спливаючому вікні вибираємо *Hotspot Guest Portal* і переходимо далі кнопкою *Continue*…

У вікні параметри порталів і налаштування налаштуємо наступні параметри за таблицею 3.5:

Табл. 3.5 – Налаштування гостьового порталу

Атрибут	*Значення*
Portal Name	Demo – Hotspot
Description	The demo.local Hotspot
Portal Behavior and Flow Settings	
Portal Settings	
HTTPS Port	8443
Allowed interfaces	Gigabit Ethernet 0
Certificate group tag	ISE Lab CGT
Endpoint identity group	GuestEndpoints
Display language	Use browser locale
Acceptable Use Policy (AUP) Page Settings	
Include in AUP page	[X]
Require an access code	[X] 130876
Require scrolling to the end of AUP	[ ]
Post – Access Banner Page Settings	
Included Post–Access Banner page	[ ] Leave unchecked
VLAN DHCP Release Page Settings	
Enable VLAN DHCP release	[ ] Leave unchecked
Authentication Success Settings	

Атрибут	*Значення*
Once authenticated, take guest to	Authentication Success page
Support Information Is Settings	
Included Support Information page	[X]
Fields to include	[X] MAC address [X] IP address [X] Browser user agent [ ] Policy server [X] Failure could
Empty fields	Hide field

Створюємо наступні дозволи профілю для гостей:

Табл. 3.6 - Профіль гостьового доступу

Атрибут	*Значення*
Name	Guest Access
Загальний дозвіл	
Airespace ACL Name	GUEST_ACL

Переходимо до *Policy > Policy Sets* і відкриваємо *Wireless_Access* політику. Додаємо наступне правило політики авторизації безпосередньо під правилом бездротового чорного списку.

- Назва правила: Hotspot
  - Результати профілю: Hotspot Access
  - Умова: Airspace:Airspace-Wlan-id Equals 2.
- Назва правила: Гостьовий доступ
  - Результати профілю: Гостьовий Доступ
  - Умова: IdentityGroup-Name Equals Endpoint Identity Groups: GuestEndpoints.

На рисунку 3.11 результат налаштувань.

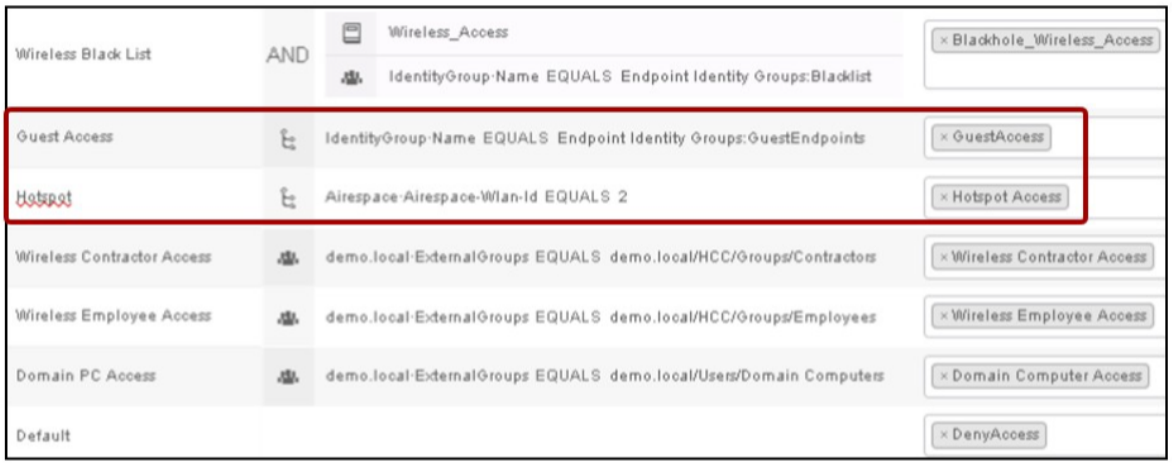


Рисунок 3.11 Налаштування політик гостьового доступу

У браузері відкриваємо посилання http://ise-1.demo.local. На рисунку 3.12 бачимо результат підключення.

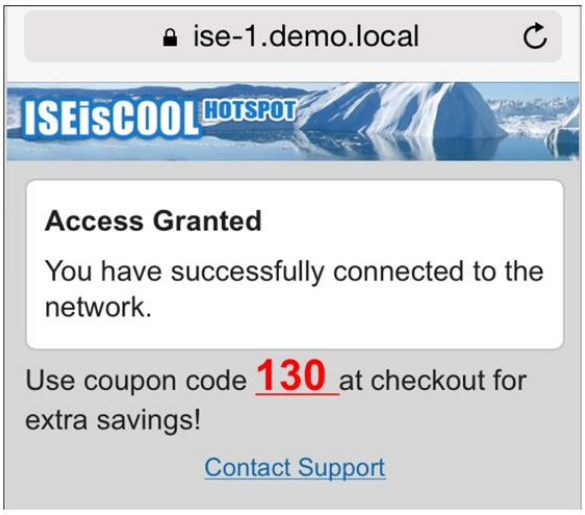


Рисунок 3.12 Гостьовий доступ

3.4 Дослідження ефективності архітектури

У якості тестування на проникнення використовуються інструменти, щоб спробувати проникнути на захист безпеки організації.

Незліченну кількість інструментів злому (або безпеки) можна знайти в Інтернеті. Більш важливим, ніж деталі будь-якого окремого прикладу, є

розуміння того, наскільки легко отримати і використовувати дуже потужні інструменти атаки. Наразі відомо про такі інструменти злому:

– *sectools.org*: це веб-сайт, який управляється проектом Nmap, який регулярно опитує співтовариство мережевої безпеки щодо своїх улюблених інструментів безпеки[9]. У ньому перераховані кращі інструменти безпеки в порядку популярності. Для кожного інструменту наводиться короткий опис, а також відгуки користувачів і посилання на веб-сайт видавця. Серед багатьох категорій є аудитори паролів, сніфферів, сканерів вразливостей, крафтерів пакетів і інструментів експлуатації.

– *Kali Linux*: The Knoppix Security Tools Distribution був опублікований в 2004 році. Це був живий дистрибутив Linux, який працював з компакт-диска і включав в себе більше ста інструментів безпеки. Тому, коли засоби безпеки були рідкістю в Windows, користувачі Windows могли завантажувати свої ПК з компакт-диска Knoppix STD і мати доступ до цього набору інструментів. Протягом багатьох років Knoppix STD розвивався через WHoppix, Whax і повернувся до свого поточного дистрибутиву як Kali Linux. Деталі еволюції не так важливі, як той факт, що живий дистрибутив Linux, який можна легко завантажити зі знімних носіїв або встановити на віртуальній машині, добре підтримується вже більш десяти років. Технологія продовжує оновлюватися, щоб залишатися актуальною[9]. Kali Linux вміщає більше трьохсот інструментів безпеки в дистрибутив Linux на основі Debian.

– *Metasploit*: коли Metasploit був вперше представлений, він зробив великий вплив на галузь мережевої безпеки. Це було дуже потужне доповнення до інструментарію тестера на проникнення. Незважаючи на те, що він надав платформу для розробки та тестування коду експлойтів передовими інженерами з безпеки, він

також знизив поріг досвіду, необхідного починаючому зловмиснику для виконання складних атак. Платформа відокремлює експлойт (код, що використовує уразливість системи) від корисних даних (код, який вводиться в скомпрометованої системі). Платформа поширюється з сотнями модулів експлойтів і десятками модулів корисного навантаження. Щоб почати атаку за допомогою Metasploit, необхідно спочатку вибрати і налаштувати експлойт. Кожен експлойт націлений на вразливість незакріпленої операційної системи або сервера додатків. За допомогою сканера вразливостей можна визначити найбільш підходящі експлойти. Експлойт повинен бути налаштований з відповідною інформацією, такою як цільова IP-адреса. Далі необхідно вибрати корисне навантаження. Корисним навантаженням може бути віддалений доступ до оболонки, доступ VNC або віддалене завантаження файлів. Експлойти можна додавати поступово. Експлойти Metasploit часто публікуються з або незабаром після публічного розкриття вразливостей[9].

Звернем увагу, що використання засобів безпеки в мережах часто є порушенням політики безпеки цих мереж. Ніколи не слід експериментувати з засобами безпеки в мережі, де у вас немає явного дозволу на це.

У якості спроби злому мережі, та доступу до ресурсів організації було проаналізовано дистрибутив Kali Linux у якості віртуальної машини, та обрано інструмент злому автентифікації та авторизації, а саме - THC Hydra.

Перед тим почати користуватися thc hydra, нам необхідно розібратися які параметри команді передавати і як це робити.

Загальний синтаксис: *$ hydra опції логіни-паролі -s порт адреса_цілі модуль параметри_модуля*

THC hydra перебирає паролі з переданого їй файлу, звідти ж беруться і логіни.

Спробуємо дістатися до мережі використовуючи словник логінів і паролів найдений в Інтернеті:

$ hydra -l admin -P john.txt ftp://10.1.100.231

Нажаль через деякий проміжок часу було від'єднано нас від мережі, бо Cisco ISE помітила активне посилання пакетів автентифікації клієнта до серверу через мережевий пристрій (10 пакетів на 1 секунду). Що було записано до журналу моніторингу персони MnT. Спробуємо під єднатись до мережі через гостьовий профіль.

$ hydra -l admin -P ~/john.txt -o ./result.log -V -s 80 ise-1.demo.local http-get /login/

І знову роз'єднання, Cisco ISE помітила аномалію на нашому пристрої Guest PC. Повторюючи спроби отримання доступу до корпоративної мережі отримуємо відмову, так як на сервері автентифікації та авторизації не існує такої пари - логін/пароль наведений в нашому словарі, якщо ми використаємо налаштовані на сервері пару – логін/пароль також отримаємо заборону на вхід, бо нашого пристрою не наведено у політики авторизації.

3.5 Висновки з розділу 3

1. В розділі було проведено налаштування базових політик доступу для дротового і бездротового доступу для співробітників і консультантів, інтеграція Cisco ISE з Microsoft Active Directory та налаштування гостьового доступу в архітектурі Cisco ISE.

2. Були проаналізовані сучасні на сьогоднішній час відомі інструменти на проникнення в мережу організації. Серед них – набір інструментів Kali Linux, Metasploit та сайт sectools.org
3. Досліджено програмне забезпечення THC Hydra для злому автентифікації за допомогою словників до мережі при налаштованій архітектурі Cisco ISE.

РОЗДІЛ 4. ДОСЛІДЖЕННЯ ОЦІНКИ ЗАГРОЗИ НА КОРПОТАТИВНУ МЕРЕЖУ

4.1 Метод дослідження

Клас захищеності інформаційної системи (Ksec) прямо пропорційний функції f (РЗ, МІС). З цього можна зробити висновок, що клас захищеності безпосередньо залежить від рівня значущості інформації та розмаху інформаційної системи. Відокремлюють три рівні значущості: високий, середній, мінімальний. Масштаб інформаційної системи буває: федеральним, регіональним, об’єктним. Схематично це видно на рисунку 4.1.

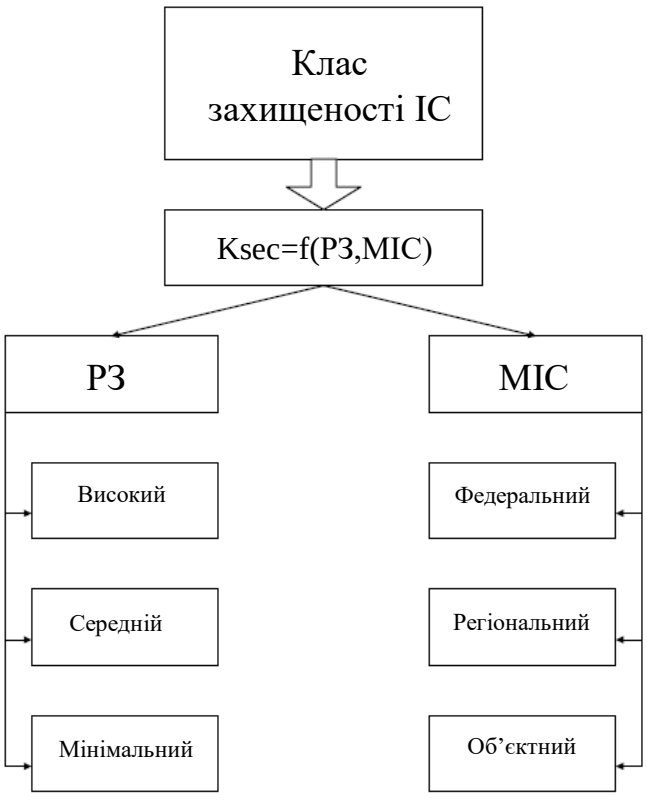


Рисунок 4.1 Клас захищеності інформаційної системи

Для кількісної оцінки найбільш актуальної загрози безпеки персональних даних, необхідно розробити модель несанкціонованого доступу до ресурсів інформаційної системи.

Структурна схема моделі несанкціонованого доступу до ресурсів показана на рисунку 4.2.

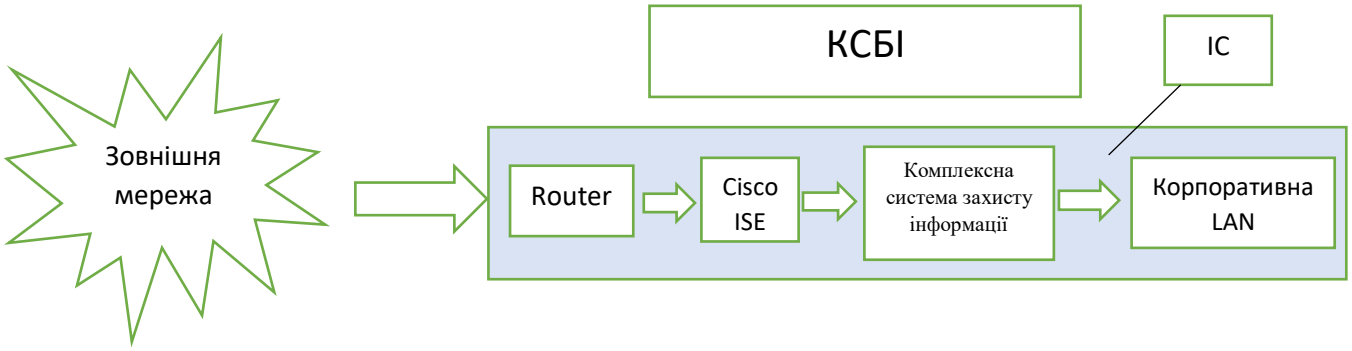


Рисунок 4.2 Модель несанкціонованого доступу до ресурсів

Процес несанкціонованої дії зловмисника можна представити у вигляді стохастичною мережі, показаної на рисунку 4.3.

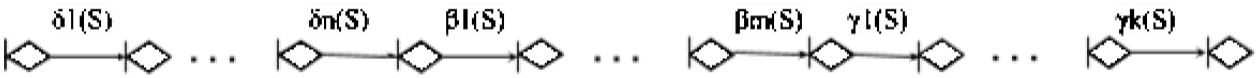


Рисунок 4.3 Стохастична мережа несанкціонованої дії зловмисника

Інтегральна Q(s) функція процесу несанкціонованого доступу, в цьому випадку буде дорівнює:

$$Q(s) = P_{\text{НСД}} = \prod_{i=1;j=1;k=1}^{n,m,\gamma} \delta_i(s)\beta_j(s)\gamma_k(s) \qquad (4.1)$$

Де n, m, γ - "перешкоди" несанкціонованого доступу.

Тут:

$$\delta_i(s) = \int_0^{\infty} e^{-st} dD_i(t) \qquad (4.2)$$

$$\beta_j(s) = \int_0^{\infty} e^{-st} dB_j(t) \qquad (4.3)$$

$$\gamma_k(s) = \int_0^{\infty} e^{-st} d\Gamma_k(t) \qquad (4.4)$$

За умови, що функції розподілу тимчасових процесів підпорядковані експоненціальному закону, тобто

$$D_i(t) = 1 - e^{-\alpha_i t} \qquad (4.5)$$

$$B_j(t) = 1 - e^{-b_j t} \qquad (4.6)$$

$$\Gamma_k(t) = 1 - e^{-\gamma_k t} \qquad (4.7)$$

Отримаємо:

$$\delta_i(s) = \frac{\alpha_i}{\alpha_i + S} \qquad (4.8)$$

$$\beta_j(s) = \frac{b_j}{b_j + S} \qquad (4.9)$$

$$\gamma_k(s) = \frac{\Gamma_k}{\Gamma_k + S} \qquad (4.10)$$

$d_i=\frac{1}{t\bar{i}}$, $t_{\bar{i}}$ - середній час забезпечення захисту від несанкціонованого доступу і-тої перешкодою.

$b_j=\frac{1}{tj}$, t_j - середній час забезпечення цілісності та доступності j-тої перешкодою.

$\Gamma_k=\frac{1}{tk}$, t_k - середній час забезпечення захисту від доступу до змісту інформації.

n - число перешкод забезпечення захищеності від несанкціонованого доступу (як правило n = 3).

m - число перешкод забезпечення захищеності від порушення цілісності та доступності (як правило m = 2)

r - число перешкод захищеності захищеності від доступу до змісту оброблюваної інформації (як правило r=1)

З урахуванням цього, та приймаючи, що S=$\frac{1}{\text{tзбер}}$, де $t_{\text{збер}}$ - середній час збереження інформацією своєї цінності, отримаємо:

$$P_{\text{НСД}} = \prod_{i=1}^{n} \frac{a_i}{a_i + S} \times \prod_{j=1}^{m} \frac{b_j}{b_j + S} \times \prod_{k=1}^{r} \frac{\text{г}_k}{\text{г}_k + S} = \tag{4.11}$$

$$= \prod_{i=1}^{n} \prod_{j=1}^{m} \prod_{k=1}^{r} \frac{a_i}{a_i + S} \times \frac{b_j}{b_j + S} \times \frac{\text{г}_k}{\text{г}_k + S}$$

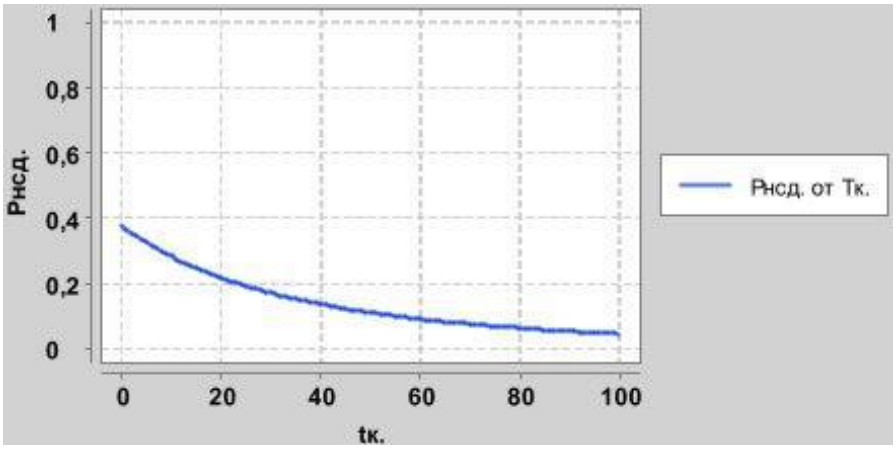


Рисунок 4.3 Залежність вірогідності несанкціонованого доступу від часу проходження перешкоди конфіденційності

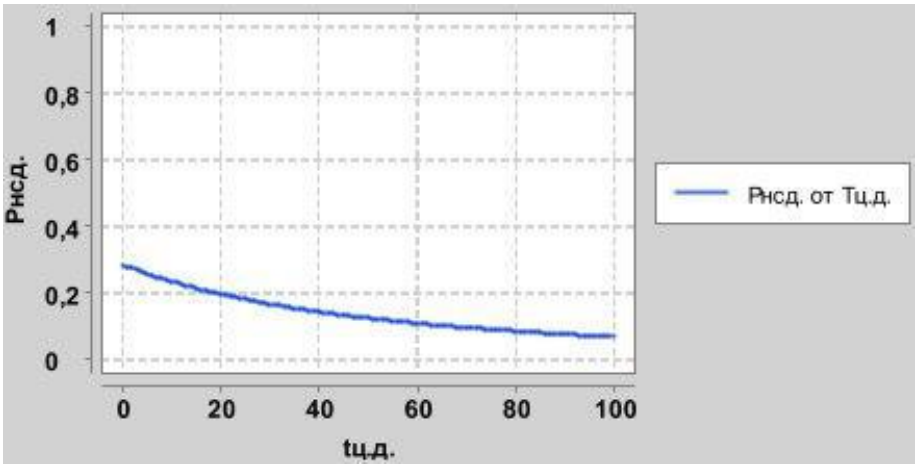


Рисунок 4.4 Залежність вірогідності несанкціонованого доступу від часу забезпечення цілісності та доступності

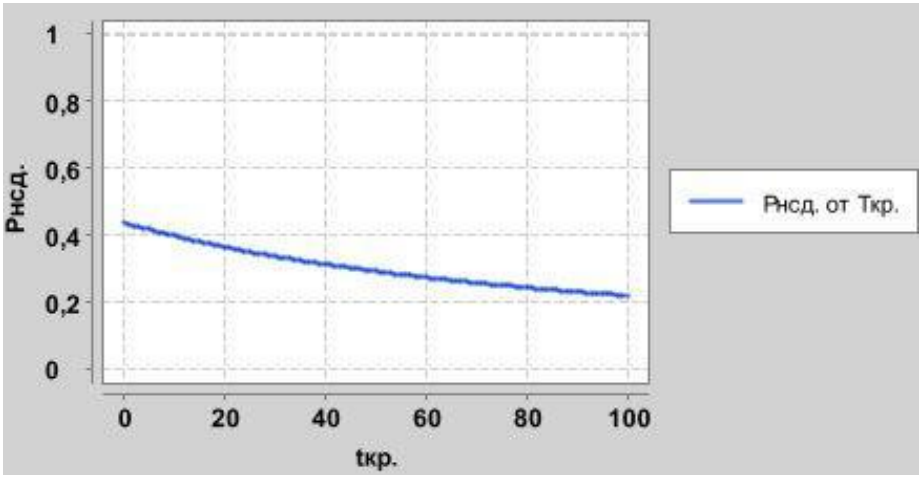


Рисунок 4.5 Залежність вірогідності несанкціонованого доступу від часу захищеності від доступу до змісту інформації

В організації існує інформаційна система, де зберігається уся її інформація, а саме: інформація яка приносить прибуток, персональні, конфіденційні дані працівників, персональні дані клієнтів і інше. На цю інформаційну систему можуть нападати з різними цілями, наприклад з метою дізнатися, знищити або змінити інформацію, що зберігається в ній.

Проведемо оцінку стану безпеки корпоративної інформаційної системи.

Проаналізувавши стан системи з точки зору безпеки інформації, можна зробити висновок, що інформаційна система може бути в одному з 4 станів:

а) Висока безпека інформації – інформація в безпеці;

б) Середня безпека інформації – інформація у відносній безпеці, що може принести за собою середню ступінь можливого збитку;

в) Низька безпека інформації – інформація поза безпеки, що може принести за собою високу ступінь можливого збитку;

г) Дуже низька безпека інформації – інформація не захищена, що може принести за собою дуже високу ступінь можливого збитку.

З точки зору стану безпеки корпоративної інформації на базі архітектури Cisco ISE має інформаційна система за даною платформою має найвищий стан захищеності так як це ефективний інструмент побудови політик, приведений у відповідність стандартам (як загальним, так і галузевим) і підтверджений відповідності для зовнішніх і внутрішніх аудиторів:

- загальноприйнятий ISO 27001 (розділи 8, 10, 11, 13, 15);
- галузевий стандарт PCI DSS (розділи 5, 6, 7, 8, 10, 12) і заснований на ISO 27001 СОУ Н НБУ 65;
- законів України щодо захисту інформації (Закон «Про захист інформації в ІТС», «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою КМУ № 373 від 29.03.2006).

На даний момент Cisco ISE отримав експертний висновок Держспецзв'язку України щодо можливості використання рішення Cisco ISE як засіб технічного захисту інформації (експертний висновок № 454, дійсний з 13.08.2013 по 13.08.2016). Це робить можливим застосування Cisco ISE для захисту державної інформації та захисту персональних даних.

Варто пам'ятати, що стандарти формуються на кращих практиках, і навіть якщо немає необхідності відповідати їм повною мірою, завжди буде корисно врахувати передові напрацювання і вимоги.

4.2 Висновки з розділу 4

1. В результаті роботи розробленої методики були отримані графіки залежності вірогідності несанкціонованого доступу

($P_{НСД}$) від часу проходження кожної з перешкод (рисунки 4.3, 4.4).

2. Головними перевагами методики є простота у використанні і, як наслідок, спроможність реалізації оцінки загрози на корпоративну мережу без залучення сторонніх організацій; автоматизація процесу підрахунку ймовірності несанкціонованого доступу та побудови графіків.
3. Було досліджено архітектуру Cisco ISE на відповідність стандартам як засіб технічного захисту інформації організації (ISO 27001, PCI DSS).

ВИСНОВКИ

Сьогоднішня корпоративна мережа швидко змінюється, особливо коли справа стосується мобільності співробітників. Співробітники більше не прив'язані до настільним робочим станціям, а замість цього звертаються до корпоративних ресурсів за допомогою різних пристроїв: планшетів, смартфонів та персональних ноутбуків. Можливість доступу до ресурсів з будь-якого місця значно підвищує продуктивність, але також збільшує ймовірність порушень даних і загроз безпеки, оскільки ви не можете контролювати стан безпеки пристроїв, що звертаються до мережі. Відстеження всіх пристроїв, які отримують доступ до мережі, являє собою величезну задачу саме по собі, і в міру того, як виникає потреба в більшому доступі, тим більш нестійкому управління.

Cisco Identity Services (ISE) - це система контролю доступу до мережі та управління політиками на основі ідентифікації. ISE дозволяє адміністратора централізовано керувати політиками доступу для дротових і бездротових кінцевих пристроїв на основі інформації, зібраної через повідомлення RADIUS півночі передача даних між пристроєм та вузлом ISE, також відомими як визначення профілю або профілювання (вибір групи клієнтів або потенційних клієнтів і аналіз того, які характеристики є для них загальними; інформація про профіль використовується для збільшення обсягу продажів і вдосконалення маркетингових програм). База даних профілювання регулярно оновлюється, щоб йти в ногу з останніми і найкращими пристроями, тому в видимості пристрою немає прогалин.

По суті, ISE прикріплює ідентифікатор до пристрою, заснованого на призначених для користувача, функціональних або інших атрибутах, для забезпечення дотримання політики і забезпечення безпеки, перш ніж пристрій отримає дозвіл на доступ до мережі. Ґрунтуючись на результатах

різних змінних, кінцева точка може бути дозволена в мережі з певним набором правил доступу, що застосовуються до інтерфейсу, до якого він підключений, інакше він може бути повністю позбавлений або надано гостьовий доступ на основі конкретних рекомендацій компанії.

Було проаналізована математична модель, за якою були отримані графіки залежності вірогідності несанкціонованого доступу від часу проходження кожної з перешкод (див. рис. 4.3, рис. 4.4, рис. 4.5).

Головним плюсом методики є:

- Простота у використанні і, як наслідок, можливість реалізації оцінки безпеки без залучення сторонніх організацій.
- Автоматизація процесу підрахунку ймовірності несанкціонованого доступу і побудови графіків.

Проаналізована архітектура Cisco ISE (див. рис. 2.2).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технологии защиты информации в компьютерных сетях. –М. : НОУ «Интуит», 2016. – 368 с.
2. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учеб. пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. – Екатеринбург: Изд-во Урал. ун-та, 2016. – 180с.
3. Организация защиты сетей Cisco. –М. : Издательский дома «Вильямс», 2015. – 1053с.
4. Полный справочник по Cisco. –К. : Издательский дома «Вильямс», 2014. – 768с.
5. Годовой отчет по информационной безопасности Cisco, Сан-Хосе, 2018. – 110 с.
6. Решения компании Cisco Systems по обеспечению безопасности корпоративных сетей, составитель М. Кадер, Cisco Press, 2015. – 102 с.
7. Cisco Networks: Engineers’ Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Chris Carthern, William Wilson, Richard Bedwell, Noel Rivera. –New York, 2015. – 856 с.
8. W. Odom. CCNA ICND2 Official Exam Certification Guide, 3nd Edirion. Cisco Press. Aug 30, 2016.
9. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. –М.: Интуит, Бином. Лаборатория, 2007. — 608 с.
10. Запись вебинара "Cisco ISE в управлении доступом к сети" [Електронний ресурс] – Режим доступу: https://www.youtube.com/watch?v=kIRlMxnVKdo.

11. Атаки на сетевое оборудование с Kali Linux [Електронний ресурс] – Режим доступу: https://habrahabr.ru/company/pentestit/blog/326968/
12. Cisco ISE. Краткое руководство. Часть 2 [Електронний ресурс] – Режим доступу: http://nosovdn-cisco.blogspot.com/2012/09/cisco-ise-2.html
13. Cisco Identity Services Engine – Part 1 – Overview [Електронний ресурс] – Режим доступу: http://thenetworksurgeon.com/cisco-identity-services-engine-part-1-overview/