**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Методика побудови безпечного мережевого доступу на базі платформи Cisco Identity Services Engine

|  |  |
| --- | --- |
| **Автор:** | К.О. Скорик |
| **Науковий керівник:** к.т.н., доц. | А.Б.Петренко |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Скрика Кирила Олександровича**

1. Тема: *Методика побудови безпечного мережевого доступу на базі платформи Cisco Identity Services Engine*  затверджена наказом ректора від «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ № \_\_\_\_\_/ст*.*
2. Термін виконання з \_\_.\_\_.20\_\_р. по \_\_.\_\_.20\_\_р*.*
3. Вихідні дані: проаналізувати вплив загроз мережевих атак на інформаційну систему і виявити вразливі місця; реалізувати план розгортання Cisco Identity Services Engine і за його допомогою реалізувати захищену мережу; на основі розрахунків проаналізувати та дослідити клас захищенності інформаційної системи.
4. Зміст пояснювальної записки: аналіз сучасних мережевих загроз;класифікація мережевих атак; дослідження архітектури CISCO ISE у якості механізму контролю доступу до мережі; побудова локальної мережі організації та дослідження ефективності роботи архітектури CISCO ISE; дослідження оцінки загрози на корпоративну мережу.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі |  | *Виконано* |
|  | Аналіз літературних джерел |  | *Виконано* |
|  | Обґрунтування вибору рішення |  | *Виконано* |
|  | Збір інформації |  | *Виконано* |
|  | аналіз сучасних мережевих загроз;класифікація мережевих атак |  | *Виконано* |
|  | дослідження архітектури CISCO ISE у якості механізму контролю доступу до мережі |  | *Виконано* |
|  | побудова локальної мережі організації та дослідження ефективності роботи архітектури CISCO ISE |  | *Виконано* |
|  | дослідження оцінки загрози на корпоративну мережу |  | *Виконано* |
|  | Перевірка на антиплагіат |  |  |
|  | Оформлення і друк пояснювальної записки |  | *Виконано* |
|  | Оформлення презентації |  |  |
|  | Отримання рецензій від рецензента |  |  |
|  | Захист в ЕК |  |  |

Магістрант К. Скорик

(підпис, дата)

Науковий керівник А. Ільєнко

(підпис, дата)

РЕФЕРАТ

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

Тема магістерської роботи 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 роботи 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.

Предметом дослідження є визначення платформи Cisco Identity Services Engine як ключеву систему захисту корпоративної мережі та вплив на інформацію яка оброблюється в мережі .

Наукова новизна роботи практичним та математичним шляхом вирахувати можливі загрози інформаційній системі та вдосконалення розгортання використанної технології шляхом змінення політик доступу, критеріїв аудиту.

Практична значущість вирішення проблем інформаційної безпеки в наші часи. Обравши потужний інструмент в цій сфері вирішено було дослідити роботу у сучасній мережі з тенденціями розвитку атак і загроз на інформаційну систему організації.

**ЗМІСТ**

[ПЕРЕЛІК СКОРОЧЕНЬ 7](#_Toc31042532)

[ВСТУП 9](#_Toc31042533)

[РОЗДІЛ 1. ОГЛЯД СУЧАСНИХ МЕРЕЖЕВИХ ЗАГРОЗ 11](#_Toc31042534)

[1.1 Загрози мережевої безпеки 11](#_Toc31042535)

[1.2 Вектор втрати даних 13](#_Toc31042536)

[1.3 Типи мережевих атак 17](#_Toc31042537)

[1.4 Фізична безпека 20](#_Toc31042538)

[1.5 Нормативно-правові засади у сфері захисту інформації 23](#_Toc31042539)

[1.6 Аудит інформаційної системи 25](#_Toc31042540)

[1.6.1 Активний аудит 25](#_Toc31042541)

[1.6.2 Експертний аудит 27](#_Toc31042542)

[1.7 Висновки з розділу 1 29](#_Toc31042543)

[РОЗДІЛ 2. ДОСЛІДЖЕННЯ АРХІТЕКТУРИ CISCO ISE У ЯКОСТІ МЕХАНІЗМУ КОНТРОЛЮ ДОСТУПУ ДО МЕРЕЖІ 31](#_Toc31042544)

[2.1 Сучасні засади загроз 31](#_Toc31042545)

[2.2 Аналіз механізму контролювання безпечного доступу 33](#_Toc31042546)

[2.3 Сегментація мережі 34](#_Toc31042547)

[2.4 Дослідження функцій Cisco ISE 36](#_Toc31042548)

[2.4.1 Аналіз послуг AAA RADIUS 39](#_Toc31042549)

[2.4.2 Аналіз послуг AAA TACACS+ 42](#_Toc31042550)

[2.4.3 Відповідність стану та інтеграція MDM 46](#_Toc31042551)

[2.4.4 Профілювання 47](#_Toc31042552)

[2.4.5 Управління гостьовим доступом 49](#_Toc31042553)

[2.4.6 Технологія BYOD 50](#_Toc31042554)

[2.4.7 Централізоване управління та моніторинг 51](#_Toc31042555)

[2.5 Розгортання Cisco ISE 52](#_Toc31042556)

[2.5.1 Вузли Cisco ISE 55](#_Toc31042557)

[2.5.2 Ліцензування Cisco ISE 58](#_Toc31042558)

[2.6 Дослідження служб сертифікації 59](#_Toc31042559)

[2.7 Політики Cisco ISE 61](#_Toc31042560)

[2.8 Переваги використання 61](#_Toc31042562)

[2.9 Висновки з розділу 2 62](#_Toc31042563)

[РОЗДІЛ 3. ОРГАНІЗАЦІЯ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОБОТИ АРХІТЕКТУРИ CISCO ISE 63](#_Toc31042564)

[3.1 Постановка задачі 63](#_Toc31042565)

[3.2 Налаштування базових політик доступу для дротового і бездротового доступу 64](#_Toc31042566)

[3.3 Створення політик авторизації 66](#_Toc31042567)

[3.4 Інтеграція Cisco ISE з Active Directory 67](#_Toc31042568)

[3.5 Налаштування гостьового доступу 72](#_Toc31042569)

[3.6 Дослідження ефективності архітектури 75](#_Toc31042570)

[3.7 Висновки з розділу 3 78](#_Toc31042571)

[РОЗДІЛ 4. ДОСЛІДЖЕННЯ ОЦІНКИ ЗАГРОЗИ НА КОРПОТАТИВНУ МЕРЕЖУ 79](#_Toc31042572)

[4.1 Метод дослідження 79](#_Toc31042573)

[4.2 Відповідність до стандартів 83](#_Toc31042574)

[4.3 Висновки з розділу 4 84](#_Toc31042575)

[ВИСНОВКИ 85](#_Toc31042576)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 86](#_Toc31042577)

# ПЕРЕЛІК СКОРОЧЕНЬ

|  |  |
| --- | --- |
| AAA | authentication, authorization, accounting — автентифікація, авторизація, облік |
| ACL  BYOD | Access Control List — список контролю доступу  Bring Your Own Device — ідеологія що дозволяє користуватися власними девайсами користувача на робочому місці |
| 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 — aтака 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 – Tпротокол 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

У сучасних умовах перед підприємствами та організаціями гостро постає завдання збереження як матеріальних цінностей, так і інформації, у тому числі відомостей, що становлять комерційну або державну таємницю. Ефективність роботи системи контролю доступу, як будь-якого високотехнологічного інструмента, залежить від того, наскільки правильно його використовують.

Підприємницька (комерційна) діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Однак захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні цінності підприємницької інформації необхідно керуватися такими критеріями (властивостями), як корисність, своєчасність і достовірність надійшли відомостей.

Розробку заходів щодо збереження комерційної таємниці підприємства слід здійснювати, дотримуючись принцип комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв. Загрози збереження комерційної таємниці можуть бути зовнішніми і внутрішніми.

Тим часом кіберзагрози постійно розвиваються, стають розумнішими та складнішими.

Яка відповідь? Традиційний підхід полягав у тому, щоб застосувати новітні засоби захисту від загрози, сподіваючись, що додавання до печворку рішень щодо безпеки може зробити свою справу. Настав час поставити кібербезпеку понад усе. Тому задля ефективності роботи викоистовується рішення безпечного мережевого доступу на базі платформи Cisco Identity Services Engine.

Завдяки Cisco ISE є можливість розмежувати доступ по безлічі критеріїв:

• Хто який має доступ;

• З яких пристроїв намагається підключитись клієнт;

• В який час відбувається підключення;

• Через які мережеві пристрої проходить ;

• Які налаштування мережевого екрану має клієнт;

# РОЗДІЛ 1. ОГЛЯД СУЧАСНИХ МЕРЕЖЕВИХ ЗАГРОЗ

## 1.1 Загрози мережевої безпеки

Інформаційна безпека в найширшому сенсі - це сукупність засобів захисту інформації від випадкового або навмисного впливу. Незалежно від того, що лежить в основі впливу: природні фактори або причини штучного характеру - власник інформації несе збитки.

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

Забезпечення і підтримка інформаційної безпеки включають комплекс різнопланових заходів, які запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи ІБ спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоб всі завдання вирішувалися одночасно, тільки тоді забезпечується повноцінна, надійний захист.

Загрозою інформації називають потенційно можливий вплив або вплив на автоматизовану систему з подальшим нанесенням збитку чиїмось потребам.

На сьогодні існує понад 100 позицій і різновидів загроз інформаційній системі. Важливо проаналізувати всі ризики за допомогою різних методик діагностики. На основі проаналізованих показників з їх деталізацією можна грамотно вибудувати систему захисту від загроз в інформаційному просторі.

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії.

Основні уразливості виникають унаслідок дії наступних факторів:

* недосконалість програмного забезпечення, апаратної платформи;
* різні характеристики будови автоматизованих систем в інформаційному потоці;
* частина процесів функціонування систем є неповноцінною;
* неточність протоколів обміну інформацією та інтерфейсу;
* складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливо і випадкове дію загроз через недостатній мірі захисту і масового дії загрозливого фактора.

Порушення режиму інформаційної безпеки може бути викликано як спланованими операціями зловмисників, так і недосвідченістю співробітників. Користувач повинен мати хоч якесь поняття про ІБ, шкідливий програмному забезпеченні, щоб своїми діями не завдати шкоди компанії і самому собі. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали. Основними джерелами загроз є окремі зловмисники ( «хакери»), кіберзлочинність групи і державні спецслужби (кіберпідрозділи), які застосовують весь арсенал доступних кіберсредств, перерахованих і описаних вище. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки в роботі програмного забезпечення і веб-додатків, вади в конфігураціях мережевих екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів.

Те, що буде проводитися атака, залежить від типу інформації, її розташування, способів доступу до неї і рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, то можливо, наприклад, використання спам-розсилок. Оцінювати загрози інформаційної безпеки необхідно комплексно, при цьому методи оцінки будуть відрізнятися в кожному конкретному випадку. Так, щоб виключити втрату даних через несправність обладнання, потрібно використовувати якісні комплектуючі, проводити регулярне технічне обслуговування, встановлювати стабілізатори напруги. Далі слід встановлювати і регулярно оновлювати програмне забезпечення (ПО). Окрему увагу потрібно приділити захисному ПО, бази якого повинні оновлюватися щодня.

## 1.2 Вектор втрати даних

* Виток інформації

Витоку інформації - неправомірна передача конфіденційних відомостей (матеріалів, важливих для різних компаній або держави, персональних даних громадян), яка може бути умисною або випадковою. Будь-які відомості, що знаходяться в комп'ютері, мають свою вартість. Тому викрадення особистих даних власника комп'ютера здатне завдати йому шкоди. Маючи доступ до логінів і паролів, а також до банківських картах і рахунках, зловмисники крадуть гроші громадян, промислові секрети і таємниці підприємств. Інформація витікає в результаті безконтрольного поширення секретів за межі кабінету, будівлі, підприємства. Втрата цінних відомостей може трапитися при неправильному використанні норм і правил політики безпеки. Недотримання правил захисту і зберігання даних тягнуть за собою їх витік і поширення в загальнодоступних місцях, таких як мережа «Інтернет». Також дії співробітників, що мають доступ до секретів легально, в силу своїх службових обов'язків. Всі варіанти інсайда умовно можна розділити на дві групи: в одному випадку співробітник, не маючи доступу до інформації, отримує її незаконно, а в іншому він має офіційний доступом до закритих даних і навмисне виносить їх за межі компанії. Крадіжка інформації (ззовні). Проникнення в комп'ютер за допомогою шкідливих програм і викрадення інформації з метою використання в корисливих інтересах. На хакерські атаки доводиться 15% від усього обсягу витоків інформації. Вторгнення в пристрій ззовні і непомітна установка шкідливих програм дозволяють хакерам повністю контролювати систему і отримувати доступ до закритих відомостями, аж до паролів до банківських рахунків і карт. Для цього можуть застосовуватися різні програми на кшталт «троянських коней». Головний атрибут даного виду витоку - активні дії зовнішніх осіб з метою доступу до інформації. Злом програмного забезпечення. Додатки, які використовуються в робочому процесі або на особистому комп'ютері співробітника, часто мають незакриті уразливості, які можна експлуатувати і отримувати тим самим різні небезпечні можливості на зразок виконання довільного коду або підвищення привілеїв. Шкідливі програми (бекдоров, трояни) націлені на заподіяння шкоди власнику пристрою, дозволяють непомітно проникати в систему і потім спотворювати або повністю видаляти інформацію, підміняти її іншими, схожими даними. Крадіжки носіїв. Дуже поширений варіант витоків, який трапляється в результаті навмисного розкрадання пристроїв з інформацією - ноутбуків, смартфонів, планшетів та інших знімних носіїв даних у вигляді флешок, жорстких дисків.

* Несанкціонований доступ

Несанкціонований доступ слід розуміти як отримання можливості обробляти дані, що зберігаються на різних носіях і накопичувачах, за допомогою самовільної зміни або фальсифікації відповідних прав і повноважень. Подібне явище має місце, коли якісь відомості призначені тільки певному колу осіб, але існуюче обмеження порушується. НСД здійснюють за рахунок помилок, допущених контролюючої структурою або системою комп'ютерної безпеки, а також шляхом підміни засвідчують документів або протиправного заволодіння інформацією про інших осіб, яким надано такий доступ. Кіберзлочинець може заволодіти особистою інформацією, відомостями, що становлять комерційну таємницю, інтелектуальною, корпоративним листуванням. Особливий предмет замаху - державна таємниця. Періодично несанкціонований доступ призводить до того, що робота конкретної структури виявляється повністю або частково паралізованою. Основні способи отримання несанкціонованого доступу: Злом інформаційних ресурсів (корпоративних мереж, веб-сайтів, хмарних сервісів, окремих комп'ютерів і мобільних пристроїв). Перехоплення повідомлень. Мається на увазі усі його послання, включаючи електронну пошту, месенджери, SMS та інше. Збір даних. Може здійснюватися законними способами, але переслідувати протиправну мета. Шантаж, вимагання, давання хабара. Викрадення інформації. Слід врахувати, що нерідко перераховані варіанти поєднуються. Отримання несанкціонованого доступу загрожує не тільки витоком даних і (або) ризиком модифікації відомостей, а й імовірністю впровадження дистанційно керованого ПО, що ставить під загрозу систему комп'ютерної безпеки в цілому. З'являється ризик втрати управління. Також важливі дані редагуються, видаляються, зловмисник може заблокувати доступ до них, зняти копії з метою подальшого протиправного використання. НСД нерідко спрямований на перехоплення ключових повідомлень, що мають принципове значення для захисту ПК, локальної системи або ж конкретно взятих документів. В останньому випадку отримання несанкціонованого доступу стає частиною більш великої операції, нерідко має відношення до кіберрозвідку. Зловмисник здатний використовувати ПК як плацдарм для перехоплення даних від інших пристроїв всередині мережі, розсилки спаму, шкідливого коду. Нарешті, НСД дає можливість знищити зберігаються цінні дані і (або) повністю вивести з ладу комп'ютерну систему. Втрата контролю загрожує привести до збоїв в роботі провайдера, транспортної організації, онлайн-магазину і т.п. Окремі об'єкти мають стратегічне значення. Тому важливість розробки грамотно організованій захисту від подібних атак не викликає сумнівів.

* Втрата даних

Втрата даних - пошкодження або втрата інформації в результаті впливу різних чинників, випадкових або навмисних дій. Втратити дані можна під час роботи з ними, а також при зберіганні інформації на комп'ютері, сервері або на масивах RAID. Нерідко цілісність даних порушується в результаті саботажу. Ряд зловмисних дій призводить злочинця до поставленої мети. Це можуть бути шкідницька діяльність персоналу компанії, атаки кіберзлочинців, інші ситуації. До порушення цілісності може призвести збій програмного забезпечення. Збій може виникнути через вплив шкідливих програм, невірної настройки додатків, невдалого оновлення програмних продуктів, некоректного форматування при установці операційної системи або помилок при її оновленні. Несправність обладнання може привести до повної втрати даних користувача або будь-якої компанії. Вона виникає ненавмисно або ж в результаті певних дій зловмисника. Виділяють кілька причин несправності обладнання, наприклад стихійні лиха. Комп'ютерні пристрої можуть постраждати від повені, урагану, блискавки, пожежі і т.п. Устаткування прийде в неробочий стан і призведе до втрати даних в результаті катастрофи, будь вона техногенної або екологічної. Стрибок напруги, сильне підвищення температури навколишнього середовища веде до займання компонентів персональних комп'ютерів або серверів, пошкодження жорсткого диска. Устаткування може стати несправним з вини вандалів. Це можуть бути як звичайні правопорушники, так і спеціально найняті недоброзичливцями або конкурентами люди. Співробітники або зовнішні працівники, які обслуговують комп'ютерну техніку, можуть завдати шкоди з корисливих цілей (підкуп конкурентами), з помсти. Крім того, несправність обладнання може виникнути через проблеми в роботі окремих його вузлів або через збій операційної системи .

## 1.3 Типи мережевих атак

* DOS-атака

Атака типу «відмова в обслуговуванні» (DoS) - це спроба принести шкоду, зробивши недоступною цільову систему, наприклад веб-сайт або додаток, для звичайних кінцевих користувачів. Зазвичай зловмисники генерують велику кількість пакетів з запитами, які в кінцевому рахунку зупиняють нормальну роботу цільової системи. У разі атаки типу «розподілена відмова в обслуговуванні» (DDoS) зловмисник використовує для проведення атаки безліч зламаних або контрольованих джерел.

У загальному випадку DDoS-атаки можна розділити на декілька видів залежно від того, на якому рівні моделі OSI відбувається атака. Найбільш поширені атаки на мережевому рівні (рівень 3), транспортному рівні (рівень 4), рівні уявлення (рівень 6) і рівні додатків (рівень 7).

- ARP-spoofing

Атака ARP-spoofing заснована на тому, що протокол ARP не перевіряє справжність ARP-запитів і ARP-відповідей, таким чином мережеве обладнання буде обробляти ARP-відповідь навіть без запиту. При проведенні атаки ARP-spoofing зловмисникові необхідно знати IP-адресу жертви, на який він буде відсилати ARP-відповідь, для цього проводиться сканування мережі. Ідентифікувати жертву можна за різними ознаками, наприклад: використовувана операційна система, використовувані служби і т. Д. Після ідентифікації жертви і отримання її IP-адреси зловмисник посилає жертві і комутатора ARP-відповідь в якому вказані MAC-адресу зловмисника і IP-адреси жертви для комутатора і комутатора для жертви. В результаті комутатор і жертва записують в свою ARP - таблицю MAC - адреса зловмисника асоціюючи його з IP-адресою жертви і комутатора відповідно. Таким чином весь мережевий трафік починає проходити через зловмисника, так як жертва вважає його комутатором, а комутатор жертвою.

* Комп’ютерні віруси

Комп'ютерний вірус - це шкідлива програма, яка самовідтворюється, копіюючи себе в іншу програму. Іншими словами, комп'ютерний вірус поширюється сам по собі в інший виконуваний код або документи. Мета створення комп'ютерного вірусу - заразити вразливі системи, отримати контроль адміністратора та викрасти чутливі до користувача дані. Хакери проектують комп’ютерні віруси із шкідливим наміром і виловлюють користувачів Інтернету, обманюючи їх.

Один з ідеальних методів, за допомогою яких віруси поширюються, - це електронна пошта - відкриття вкладеного файлу в електронній пошті, відвідування зараженого веб-сайту, натискання на виконуваний файл або перегляд зараженої реклами може призвести до поширення вірусу у вашій системі. Крім того, інфекції поширюються і під час з'єднання з уже зараженими знімними пристроями, такими як USB-накопичувачі.

Досить легко і просто віруси прокрадаються до комп'ютера, ухиляючись від оборонних систем. Успішне порушення може спричинити серйозні проблеми для користувача, такі як зараження інших ресурсів або системного програмного забезпечення, зміна або видалення ключових функцій або програм та копіювання / видалення або шифрування даних.

* Парольні атаки

Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (bruteforce attack), троянський кінь, IP-спуфинг і сніф- фінг пакетів. Хоча логін і пароль часто можна отримати за допомогою IP- спуфинга і сніфінга пакетів, хакери часто намагаються підібрати пароль і логін, використовуючи для цього численні спроби доступу. Такий підхід носить назву простого перебору (bruteforce attack). Часто для такої атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті хакер отримує доступ до ресурсів, він отримує його на правах звичайного користувача, пароль якого був підібраний. Якщо цей користувач має значні привілеї доступу, хакер може створити для себе «прохід» для майбутнього доступу, який буде діяти навіть якщо користувач змінить свій пароль і логін.

- Мережева розвідка

Мережевий розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, луна-тестування (ping sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені. Відлуння-тестування (ping sweep) адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами. І, нарешті, хакер аналізує характеристики додатків, що працюють на хостах. В результаті видобувається інформація, яку можна використовувати для злому.

- Сніффери пакетів

Сніффер пакетів є прикладну програму, яка використовує мережеву карту, що працює в режимі promiscuous mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому сниффер перехоплює всі мережеві пакети, які передаються через певний домен. В даний час сніфери працюють в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей 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 сніффер можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі).

Перехоплення імен 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. Якщо додаток працює в режимі клієнт / сервер, а аутентифікаційні дані передаються по мережі в читається текстовому форматі, цю інформацію з великою ймовірністю можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів. Хакери занадто добре знають і використовують наші людські слабкості (методи атак часто базуються на методах соціальної інженерії). Вони прекрасно знають, що ми користуємося одним і тим же паролем для доступу до безлічі ресурсів, і тому їм часто вдається, дізнавшись наш пароль, отримати доступ до важливої ​​інформації. У найгіршому випадку хакер отримує доступ до призначеного для користувача ресурсу на системному рівні і з його допомогою створює нового користувача, якого можна в будь-який момент використовувати для доступу в мережу і до її ресурсів.

## 1.4 Фізична безпека

Фізична безпека - це захист персоналу, апаратних засобів, програмного забезпечення, мереж і даних від фізичних дій та подій, які можуть спричинити серйозні збитки або збитки для підприємства, установи чи установи. Сюди входить захист від пожежі, повені, стихійних лих, грабежів, крадіжок, вандалізму та тероризму. Фізичну безпеку часто не помічають - і її значення недооцінюють - на користь більшої кількості технічних загроз, таких як хакерство, зловмисне програмне забезпечення та кібереспіонаж. Однак порушення фізичної безпеки можуть бути здійснені з грубою силою і мало технічних знань з боку зловмисника.

Фізична безпека має три важливі компоненти: контроль доступу, спостереження та тестування. Перешкоди повинні ставитись на шляху потенційних зловмисників, а фізичні майданчики повинні бути загартовані проти аварій, атак чи екологічних катастроф. Такі заходи посилення включають огородження, замки, картки контролю доступу, біометричні системи контролю доступу та системи пожежогасіння. По-друге, фізичні місця слід контролювати за допомогою камер спостереження та систем оповіщення, таких як датчики виявлення вторгнень, теплові датчики та детектори диму. По-третє, політики та процедури відновлення стихійних лих повинні регулярно перевірятися, щоб забезпечити безпеку та скоротити час, необхідний для відновлення після руйнівних техногенних чи природних катастроф. Контроль фізичної безпеки, включаючи стримувальні, детективні та профілактичні заходи, - це засоби, які ми застосовуємо для пом’якшення питань фізичної безпеки. Стрижці мають на меті відмовити тих, хто може порушити нашу безпеку, детективні заходи попереджають нас або дозволяють нам виявити, коли у нас є потенційна вторгнення, а профілактичний контроль фактично запобігає вторгненням. Окремо жоден із цих елементів контролю не є повноцінним рішенням, але разом вони можуть поставити нас на набагато сильнішу основу для фізичної безпеки.

Захист людей - це головне питання при плануванні нашої фізичної безпеки. Хоча дані та обладнання, як правило, можна замінити, якщо вживати належних запобіжних заходів, люди можуть бути дуже важкими для заміни. Люди - це тендітні істоти, і один з найкращих кроків, який ми можемо зробити, зіткнувшись із ситуацією, коли їм може бути завдано шкоди, - це усунути їх з небезпечної ситуації. Крім того, ми можемо застосовувати різні адміністративні засоби контролю, щоб зберегти їх у безпеці в робочих умовах.

Захист даних, що поступається лише захисту наших людей, є надзвичайно важливою діяльністю у нашому світі технологічного бізнесу. Одне з наших головних питань щодо даних - це можливість забезпечити їх доступність тоді, коли це потрібно, а інша - забезпечити, що ми можемо повністю їх видалити, коли більше не хочемо їх зберігати. Одним з наших основних методів забезпечення доступності є виконання резервних копій, чи це через використання RAID для захисту від збоїв у носіях зберігання, чи резервне копіювання на знімних носіях, таких як DVD-диски або магнітна стрічка.

Захист нашого обладнання, хоча є найнижчою з трьох категорій нашого списку пріоритетів, все ще є життєво важливим завданням. Вибираючи сайт для нашого об'єкту, нам потрібно враховувати загрози, які можуть мати значення для місця розташування, і вжити заходів для їх зменшення. Нам також потрібно вжити необхідних заходів для забезпечення доступу назовні, до та в межах нашого закладу. Ми маємо захищати своє обладнання не тільки від того, яке б вторгнулося ззовні, але і від того, хто має законний доступ до об'єкта, але не до певних ділянок всередині нього. Нарешті, нам потрібно підтримувати відповідні екологічні умови для функціонування нашого обладнання, в основному потужності, температури та вологості.

## 1.5 Нормативно-правові засади у сфері захисту інформації

* Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

* Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

* Закон України «Про захист персональних даних»

Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

НД ТЗІ 1.1-005-07

Цей нормативний документ (НД) системи технічного захисту інформації (ТЗІ) визначає основи організації та етапи виконання робіт щодо створення комплексу на об’єкті інформаційної діяльності (ОІД) органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації (далі – установа), який має забезпечувати захист від витоку інформації з обмеженим доступом (ІзОД) можливими технічними каналами (далі – комплекс ТЗІ).

Вимоги цього НД можуть використовуватися під час обґрунтування, організації розроблення, впровадження заходів захисту ІзОД від загроз, що можуть бути здійснені каналами спеціального впливу на технічні засоби інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем (далі – ІТС) та на інші технічні засоби.

Захищеність об’єктів, комплексів та засобів спеціального зв'язку від витоку інформації технічними каналами визначається іншими НД.

НД ТЗІ 2.1-002-07

Цей нормативний документ (НД) системи технічного захисту інформації (ТЗІ) визначає загальні вимоги до організації проведення на об'єкті інформаційної діяльності (ОІД) органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації (далі – установа) випробувань щодо створення комплексу ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом (ІзОД) технічними каналами.

НД встановлює засади щодо проведення випробувань з метою перевірки (контролю) повноти та достатності реалізованих заходів із захисту інформації на ОІД, атестації комплексу ТЗІ, а також вимоги до розроблення висновків за результатами випробувань та їх програм і методик.

НД ТЗІ 3.1-001-07

Цей нормативний документ (НД) системи технічного захисту інформації (ТЗІ) визначає основні положення щодо проведення передпроектних робіт при створенні на об'єкті інформаційної діяльності (ОІД) органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації (далі – установа) комплексу ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом (ІзОД) технічними каналами.

Цим НД встановлюється порядок та зміст проведення передпроектних робіт на ОІД, які вже функціонують або будуються (модернізуються), вимоги до оформлення акта обстеження на ОІД, а також вимоги до порядку розроблення та оформлення технічного завдання на створення комплексу ТЗІ (далі – ТЗ).

## 1.6 Аудит інформаційної системи

Аудит інформаційної безпеки як послуга має на меті перевірку всіх активів, пов'язаних із захистом інформації, на відповідність обраним критеріям. Обсяг аудиту залежить від мети. Регулярний аудит оцінює різні процеси, послуги, продукти, процедури обробки інформації, практику роботи користувачів, безпеку конфігурації системи та оточення тощо. Основна мета - перевірити, чи відповідає система управління безпекою бізнес-цілям і як існуючий контроль дотримується оцінки ризику, стандарти найкращої практики та / або інші застосовні вимоги дотримання регуляторних норм.

Аудити безпеки, оцінки вразливості та тестування на проникнення є основними видами перевірок безпеки. Кожен з цих трьох типів відрізняється від інших за допомогою фокусування / мети та підходу. Аудит безпеки оцінює, наскільки добре інформаційна система відповідає набору встановлених критеріїв. Оцінка вразливості зосереджується на аналізі цілої інформаційної системи з метою виявлення потенційних недоліків та витоків безпеки. Тестування на проникнення фокусується на здатності тестованої системи протистояти хакерським атакам.

## 1.6.1 Активний аудит

Одним з найпоширеніших видів аудиту є активний аудит. Це дослідження стану захищеності інформаційної системи з точки зору хакера (або якогось зловмисника, який володіє високою кваліфікацією в області інформаційних технологій).

Найчастіше компанії-постачальники послуг активного аудиту називають його інструментальним аналізом захищеності, щоб відокремити даний вид аудиту від інших.

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (в тому числі систем аналізу захищеності) і спеціальних методів здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміються лише ті параметри і настройки, використання яких допомагає хакеру проникнути в мережі і завдати шкоди компанії.

При здійсненні даного виду аудиту на систему мережевого захисту моделюється як можна більшу кількість мережевих атак, які може виконати хакер. При цьому аудитор штучно ставиться саме в ті умови, в яких працює хакер, - йому надається мінімум інформації, тільки та, яку можна роздобути в відкритих джерелах.

Природно, атаки тільки моделюються і не надають будь-якого деструктивного впливу на інформаційну систему. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора.

Результатом активного аудиту є інформація про всі слабкі місця, ступеня їх критичності і методах усунення, відомості про широкодоступної інформації (інформація, доступна будь-якому потенційному порушнику) мережі замовника.

Після закінчення активного аудиту видаються рекомендації по модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості і тим самим підвищити рівень захищеності інформаційної системи від дій «зовнішнього» зловмисника при мінімальних витратах на інформаційну безпеку.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту інформаційної системи.

Активний аудит - послуга, яка може і повинна замовлятися періодично. Виконання активного аудиту, наприклад раз на рік, дозволяє упевнитися, що рівень системи мережевої безпеки залишається на колишньому рівні.

## 1.6.2 Експертний аудит

Експертна аудит можна умовно уявити як порівняння стану інформаційної безпеки з «ідеальним» описом, яке базується на наступному:

вимоги, які були пред'явлені керівництвом в процесі проведення аудиту;

опис «ідеальної» системи безпеки, засноване на акумульованому в компанії-аудитора світовому і приватному досвіді.

При виконанні експертного аудиту співробітники компанії-аудитора спільно з представниками замовника проводять такі види робіт:

збір вихідних даних про інформаційну систему, про її функціях і особливостях, використовувані технології автоматизованої обробки і передачі даних (з урахуванням найближчих перспектив розвитку);

збір інформації про наявні організаційно-розпорядчих документах щодо забезпечення інформаційної безпеки і їх аналіз;

визначення точок відповідальності систем, пристроїв і серверів ІС;

формування переліку підсистем кожного підрозділу компанії з категорірованія критичної інформації та схемами інформаційних потоків.

Один з найбільш об'ємних видів робіт, які проводяться при експертному аудиті, - збір даних про інформаційну систему шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців - збір інформації про функціонування мережі, а керівного складу компанії - з'ясування вимог, які пред'являються до системи інформаційної безпеки.

Необхідно відзначити, що при експертному аудиті безпеки інформаційної системи враховуються результати попередніх обстежень (в тому числі інших аудиторів), виконуються обробка і аналіз проектних рішень та інших робочих матеріалів, що стосуються питань створення інформаційної системи.

Ключовий етап експертного аудиту - аналіз проекту інформаційної системи, топології мережі та технології обробки інформації, в ході якого виявляються, наприклад, такі недоліки існуючої топології мережі, які знижують рівень захищеності інформаційної системи.

За результатами робіт даного етапу пропонуються зміни (якщо вони потрібні) в існуючій інформаційній системі і технології обробки інформації, спрямовані на усунення виявлених недоліків з метою досягнення необхідного рівня інформаційної безпеки.

Наступний етап - аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків ІС організації та складається їх діаграма, де для кожного інформаційного потоку вказуються його цінність (в тому числі цінність переданої інформації) і використовувані методи забезпечення безпеки, що відображають рівень захищеності інформаційного потоку.

На підставі результатів даного етапу робіт пропонується захист або підвищення рівня захищеності тих компонент інформаційної системи, які беруть участь в найбільш важливих процесах передачі, зберігання і обробки інформації. Для менш цінної інформації рівень захищеності залишається колишнім, що дозволяє зберегти для кінцевого користувача простоту роботи з інформаційною системою.

Застосування аналізу інформаційних потоків організації дає можливість спроектувати систему забезпечення інформаційної безпеки, відповідну принципом розумної достатності.

В рамках експертного аудиту проводиться аналіз організаційно-розпорядчих документів, таких як політика безпеки, план захисту та різного роду інструкції.

## 1.7 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: ARP-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.
5. Розглянуто закони України та нормативно-правові документи згідно яких регулюється нформаційна діяльність, обробка інформації, побудова системи захисту інформації, та безпосередньо відповідальність.

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

## 2.1 Сучасні засади загроз

У зв'язку зі збільшенням кількості користувачів, пристроїв і методів доступу корпоративні ІТ-інфраструктури сучасних підприємств стають більш динамічними. Поряд з розширенням можливих варіантів підключення і спектра призначених для користувача пристроїв з'являються нові ризики порушення безпеки і завдання по збереженню керованості. Для забезпечення інформаційної безпеки корпоративної ІТ-інфраструктури та ефективного управління такою інфраструктурою потрібні нові рішення, які забезпечать виконання політик доступу, аудит доступу до ІТ-інфраструктурі, моніторинг дотримання нормативних вимог, а також збір докладних відомостей про всіх мережевих взаємодіях. Cisco ISE дозволяє забезпечити високобезпечний доступ до мережі для користувачів та пристроїв. Це допомагає вам зрозуміти, що відбувається у вашій мережі, наприклад, хто підключений, які програми встановлені та запущені та багато іншого. Він також ділиться життєво важливими контекстними даними, такими як особистість користувачів та пристроїв, загрози та вразливості за допомогою інтегрованих рішень від партнерів технологій Cisco, щоб ви могли швидше визначати, містити та переадресовувати загрози. Cisco ISE пропонує цілісний підхід до захисту доступу до мережі. Ви отримуєте багато переваг при розгортанні ISE, включаючи:

Високобезпечний бізнес та доступ до контексту на основі політики вашої компанії. ISE працює з мережевими пристроями для створення всеохоплюючої контекстуальної ідентичності з такими атрибутами, як користувач, час, місцезнаходження, загроза, вразливість та тип доступу. Цей ідентифікатор може бути використаний для застосування високобезпечної політики доступу, яка відповідає ролі бізнесу. ІТ-адміністратори можуть застосовувати точний контроль над тим, хто, що, коли, де і як кінцеві точки дозволені в мережі.

Упорядкована видимість мережі через простий, гнучкий і дуже витратний інтерфейс. ISE зберігає детальну історію атрибутів усіх кінцевих точок, які підключаються до мережі, а також користувачів (включаючи такі типи, як гостьовий, працівник та підрядники) в мережі, аж до деталей програми про кінцеві точки та стану брандмауера.

Широке впровадження політики, яка визначає прості, гнучкі правила доступу, які відповідають вашим постійно змінюваним вимогам бізнесу. Усі контролюються з центрального місця, яке розподіляє правозастосування по всій мережі та інфраструктурі безпеки. ІТ-адміністратори можуть централізовано визначити політику, яка відрізняє гостей від зареєстрованих користувачів та пристроїв. Незалежно від їх місцезнаходження, доступ до користувачів та кінцевих точок дозволений на основі ролі та політики. Теги групи безпеки Cisco TrustSec (SGT) дозволяють організаціям базувати контроль доступу на бізнес-правилах, а не на IP-адресах або мережевій ієрархії. Ці SGT надають користувачам та кінцевим точкам доступ, принаймні, до політики привілеїв, яка постійно підтримується під час переміщення ресурсів по домену. Керування правилами комутатора, маршрутизатора та брандмауера стає простішим і показало, що це допомагає скоротити ІТ-операції на 80% та збільшити час на впровадження змін на 98%.

Надійний гостьовий досвід, який забезпечує безліч рівнів доступу до вашої мережі. Ви можете надати гостьовий доступ через доступ до точки доступу до кав’ярні, доступ до зареєстрованого самообслуговування або спонсорський доступ. ISE надає вам можливість високо налаштовувати різні гостьові портали через вікно-редактор порталів, що постачається у комплекті, або в хмарі, що забезпечує динамічні візуальні інструменти. Ви можете бачити попередній перегляд екрану порталу в реальному часі та досвід, який відвідувач матиме при підключенні до мережі.

Пристрій самообслуговування на борту для компанії "Налаштуйте свій власний пристрій" (BYOD) або гостьової політики. Користувачі можуть керувати пристроями відповідно до бізнес-політики, визначеної ІТ-адміністраторами. Співробітники інформаційних технологій матимуть автоматичне забезпечення пристрою, профілювання та розміщення пристрою, необхідне для дотримання політики безпеки. У той же час працівники можуть виводити свої пристрої в мережу, не вимагаючи ІТ-допомоги.

## 2.2 Аналіз механізму контролювання безпечного доступу

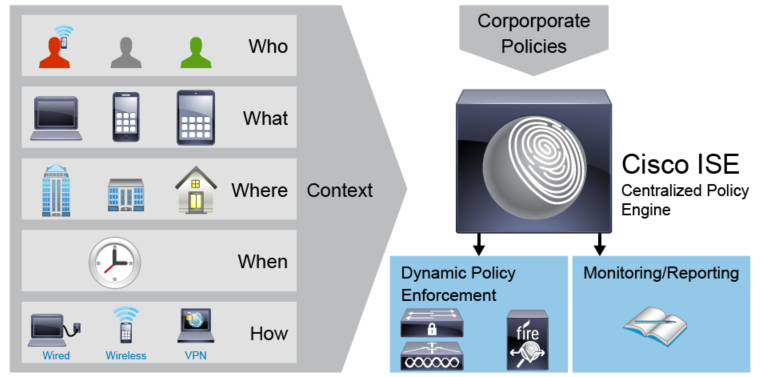
В платформі Cisco ISE всі запити на доступ до мережі відносяться до умов аутентифікації, авторизації, аудиту, тобто при будь-якій спробі отримати доступ до мережі система буде відстежувати "Хто, що, звідки, коли і як"

Рис 2.2.1

На малюнку можна побачити як платформа Cisco ISE збирає інформацію про користувачів, системи які поідключаються до мережі, звідки триває підключення, коли воно було встановлення та за якими протоколами безпосередньо намагається встановити з’єднання. Схематично показано на рисунку 2.2.1.

## 2.3 Сегментація мережі

Корпоративна мережа стала критично важливим інструментом бізнесу багатьох компаній, оскільки саме вона забезпечує роботу безлічі бізнес-процесів, пов'язаних з передачею інформації. У той же час загрози інформаційній безпеці безперервно еволюціонують, і потреба в ефективних засобах захисту зростає з кожним днем. Довгий час увагу фахівців з інформаційної безпеки було зосереджено в основному на захист периметра мережі. Але в сучасних мережах класичне поняття периметра поступово розмивається. Користувачі підключаються до мережі різними способами, включаючи доступ через дротові і бездротові сегменти, а також VPN-підключення. При цьому в рамках ІТ-інфраструктури організації, як правило, існує безліч типів користувачів і пристроїв, яким для виконання своєї роботи потрібен доступ до різних ресурсів мережі. Реалізація належного розмежування доступу в сучасних розподілених і динамічних ІТ-інфраструктурах є досить непростим завданням. З урахуванням великої кількості векторів атаки, що дозволяють зловмисникам і шкідливому програмному забезпеченню проникати в корпоративну ІТ-інфраструктуру, ймовірність порушення інформаційної безпеки можна вважати вкрай високою, як правило, це питання часу. Однією з популярних заходів, спрямованих на зниження шкоди від проникнення зловмисника в корпоративну ІТ-інфраструктуру, є сегментація мережі. Мається на увазі попереднім етапом сегментації є поділ користувачів і ресурсів мережі на ізольовані одна від одної групи (закриті групи користувачів і ресурсів). Обмін даними між цими групами контролюється або взагалі блокується в залежності від вимог політики безпеки організації. Принципи, які використовуються для поділу користувачів на групи, визначаються прийнятою в організації політикою безпеки. В якості одного з типових варіантів поділу користувачів і пристроїв за категоріями можна навести такий: співробітники, тимчасовий персонал, гості, користувачі з пристроями, що не відповідають корпоративній політиці (карантин), інженерні підсистеми будівель і так далі. Крім того, співробітники можуть бути розміщені не в одну групу, а розділені на кілька груп, наприклад рядові співробітники, керівництво, топ-менеджмент, бухгалтерія тощо. Поділ користувачів на групи і сегментація мережі не є самоціллю, але можуть бути дуже важливими для підвищення безпеки бізнес-процесів. У цьому сенсі такі бізнес-процеси спираються на сегментацію. Політика безпеки організації може вимагати, щоб співробітники різних категорій отримували доступ тільки до тих корпоративних ресурсів, до яких їм необхідно мати доступ для виконання своєї роботи. Наприклад, доступ до групи серверів системи ERP з конфіденційною бізнес-інформацією може надаватися тільки керівництву, а доступ до конфіденційних баз HR - тільки співробітникам HR-підрозділу і, можливо, керівництву. У той же час персонал нижчої ланки або тимчасові співробітники можуть отримувати доступ тільки до обмеженого набору корпоративних додатків, наприклад до кооперативної системи CRM і електронній пошті, і не мати права доступу до всіх інших ресурсів мережі. Вплив сегментації на бізнес-процеси в описуваних випадках полягає в тому, що сегментація важлива для забезпечення інформаційної безпеки, а оскільки інциденти в області ІБ можуть призводити до порушення доступності, то сегментація також сприяє підвищенню доступності бізнес-процесів. Крім того, існує ціла група бізнес-процесів, впровадження яких при відсутності сегментації є вкрай небажаним. Наприклад, до цієї групи належать процеси, пов'язані з доступом до корпоративної мережі користувачів, які не є співробітниками організації. Типовим прикладом є надання доступу в мережу (або в Інтернет) так званим гостьовим користувачам. В якості інших варіантів можна згадати доступ співробітників компанії-партнера, доступ аудиторів, підключення в мережу пристроїв, що належать іншим організаціям, наприклад банкоматів, цифрових вивісок, платіжних терміналів. Ще одним сценарієм, в якому рекомендується використання сегментації, є розмежування доступу між співробітниками афілійованих структур, що використовують одну і ту ж мережу.

## 2.4 Дослідження функцій Cisco ISE

Платформа Cisco Identity Services Engine надає впровадження в корпоративну ІТ-інфраструктуру засобів аутентифікації і авторизації користувачів і кінцевих пристроїв, підключених до дротових мереж, бездротових мереж і мереж VPN, забезпечення дотримання узгодженої політики в масштабах всього підприємства.

● Запобігання несанкціонованого доступу до мережі для захисту корпоративних активів.

● Управління повним життєвим циклом гостьового доступу за рахунок надання запрошує особам

(Спонсорам) коштів для дозволу доступу їх гостей, що дозволяє знизити поточне навантаження на ІТспеціалістов.

● Підтримка настроюваних порталів і можливості публікації web-сторінок для спрощення роботи як нових,

так і досвідчених користувачів відповідно до прийнятих в організації процесами.

● Забезпечення повномасштабного моніторингу шляхом виявлення, класифікації та управління підключаються

до мережі кінцевими пристроями для надання відповідних сервісів і рівнів доступу.

● Усунення вразливостей на комп'ютерах користувачів шляхом регулярної перевірки та коригування їх стану,

що дозволяє нейтралізувати такі мережеві загрози, як віруси, черв'яки і шпигунські програми.

● Забезпечення дотримання політик безпеки за рахунок блокування та ізоляції невідповідних корпоративним

стандартам комп'ютерів в карантинній області, а також їх оновлення без залучення адміністратора.

● Підтримка вбудованої консолі моніторингу, звітності та усунення неполадок для спрощення роботи

фахівців служби підтримки та адміністраторів.

● Підвищення точності профілювання підключених до мережі пристроїв за рахунок методів активного сканування

пристрою. Цей механізм дозволяє підвищити точність профілювання пристроїв, для якого раніше

використовувалися тільки кошти аналізу мережевого трафіку, за рахунок сканування певних атрибутів

пристрою (відповідно до політики).

● Управління доступом кінцевих пристроїв до мережі за допомогою сервісу захисту кінцевих пристроїв (EPS). сервіс

EPS дозволяє адміністратору пов'язувати кінцеві пристрої і дії, які необхідно виконати при

підключенні пристрою (перенесення в нову VLAN, повернення в вихідну VLAN або повна ізоляція пристрою від мережі), за допомогою єдиного інтерфейсу.

Cisco ISE надає наступні можливості:

* Аутентифікація
* Авторизація
* Аудит
* Профілювання
* Централізація політик
* Моніторинг
* Деталізований аудит
* TACACS+
* Впровадження MDM
* Звіт в режимі реального часу
* Логування
* Відновлення
* Усунення проблем в роботі

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

З'єднання між серверами доступу до мереж (NAS) та серверами RADIUS засноване на протоколі UDP (User Datagram Protocol). У загальному вигляді протокол RADIUS представляє собою службу без встановлення з'єднань. Вопроси, пов'язані з доступною сервером, повторними передачами і часом очікування, решають пристрої з підтримкою RADIUS найкраще, чим протоколом передаються.

RADIUS - протокол типу «кліент-сервер». Клієнт RADIUS зазвичай представляє собою сервер NAS, а сервер RADIUS - процесор-демон на комп'ютерах з ОС Windows NT або UNIX. Клієнт передає інформацію про користувачів з вказаними серверами RADIUS і виконує різні дії в залежності від відхиленого рівня. Сервери RADIUS пропонують запросити підключення користувачів, виконуючи аутентифікацію користувачів та перевіряючи інформацію про конфігурації, необхідні для обслуговування користувачів клієнтами. Сервер RADIUS може створювати перехідний режим для інших серверів RADIUS або серверів аутентифікації інших типів. Сервер RADIUS може підтримувати багато методів аутентифікації користувача. Для перевірки подлинності імені користувача та пароля, представлення серверів, можна використовувати протоколи PPP, PAP, CHAP, вхід UNIX та інші механізми аутентифікації.

Забезпечується звичайний процес введення користувачем даних із передачею запиту (Access-Request) з сервером NAS на сервері RADIUS та з отриманням відповідного доступу до сервера (Access-Accept або Access-Reject). Пакет Access-Request містить вміст імені користувача, зашифрований пароль, IP-адресу сервера NAS і порт. Персонально сервери RADIUS розміщувались на UDP-порту 1645, що створювало конфлікт із службовими даними. По причині цього конфліктного документа RFC 2865 офіційно закрепився для протоколу RADIUS портрет 1812. Більшінші пристрої та запропоновані Cisco підтримують номер кімнати порталів. Формат запрошує також містити інформацію про типі сеансу, який збирає ініціювати користувача. Наприклад, якщо ви запросили представити у символічному режимі, то ви маєте надіслати інформацію як Service-Type = Exec-користувач, але будь-ласка, запропонуйте представити у пакеті режиму PPP, щоб ви побачили, як тип послуги = Framed User та Framed Type = PPP.

На півчасті від NAS запроса сервер Acceess-Request RADIUS виробляє пошук за вказаним ім’ям користувача в базі даних. Якщо ваш ідентифікатор користувача не знайдений у базі даних, то це значить, що завантажений профіль за умовчанням, або сервер RADIUS немедленно відправляє повідомлення Access-Reject. Дане повідомлення Access-Reject може підтримувати текстовими повідомленнями, в яких вказано вигляд із довідки.

В RADIUS аутентифікація та авторизація об'єднані. Якщо ваш ідентифікатор користувача знайдений і пароль логотип, то сервер RADIUS возвращает подтверждение доступа, включаючи список «значень атрибута», які описують параметри, необхідні для даного сеансу. У типових типових параметрах: тип служби (сеансовий інтерпретатор або кадрирування), тип протоколу, призначений користувальницький IP-адрес (статистичний або динамічний), призначається список доступних або статистичний маршрут для встановлення в таблицю маршрутизації NAS. Дані конфігурації серверів RADIUS визначають компоненти, які будуть встановлені на сервері NAS. Рисунок нижче показує аутентифікацію RADIUS та послідовність авторизації. Функції роботи протокола RADIUS можуть використовувати незалежну від функцій аутентифікацію або авторизацію RADIUS. Використовуючи функцію RADIUS, можливо, використовуйте дані в початкових і в інших сеансах, вказуючи ресурси (наприклад, час, пакети, банти та т. П.), Використовувані в часі сеансу. Для задоволення безпеки та безпечної безпеки для Інтернету (ISP) можна використовувати програмне забезпечення RADIUS для управління домом та навчанням. У великому пристрої Cisco в порталі якості RADIUS використовується порт 1646, але також може бути вибраний номер 1813 (за інформацією про номер порта, за закріпленим документом RFC 2139, від ostavljaciscoco.com). Підтримка транзакцій між клієнтами та серверами RADIUS підтверджується за допомогою загальнодоступного секретного ключа, нікого не пересілаемого по мережах. Крім того, обмінюючись паролями користувачів між клієнтами та серверами, RADIUS виконує в зашифрованому відеозаписі для перевірки вірогідності перехвата пароля користувача зловмисними користувачами через прослуховування незахищених мереж.

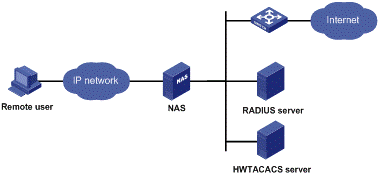


Рис 2.4.1

### 

### 2.4.2 Аналіз послуг AAA TACACS+

ACACS + (англ. Terminal Access Controller System Control Control plus) - сеансовий протокол, результатом якого є TASACS, виробник Cisco. TACACS + використовує поняття сеансів. У програмі TACACS + можливо встановлення трьох різних типових сеансів AAA (authentification, accounting, audit). Встановлення одного типу сеансу в загальному випадку не вимагає попереднього успішного встановлення какого-або іншого. Специфікація протокола не вимагає для відкриття сеансової авторизації відкрити початкові сеанси аутентифікації. Сервер TACACS + може вимагати аутентифікацію, але протокол цього не оговаривает. Аутентифікація. Указує, кому вирішено отримати доступ до мереж. Користувачі мають доказ, що вони дійсно такі, які вони говорять. Традиційні авторизовані користувачі були вивірені використовувати пароль для перевірки своєї особистості, однако це має багато обмежених безпеки. У той час як TACACS + може використовувати своїх користувачів і паролів, він також може використовувати інші механізми, такі як паролі «один раз». Якщо для аутентифікації використовуються стандартні паролі, то можна дозволити проникнення хакерів у систему. Наприклад: якщо пакет був перероблений і містив пароль користувача, перехвачений пакет був зроблений до того часу, як преступники смогуть декорувати шифрування, облегчаючи вхід у систему. Авторизація Відноситьсь до того, що користувач вирішив зробити, або ж, щоб мати якусь послугу у користувача, існує. Наприклад: якщо користувачі завантажують у мережі удалене та проходять аутентифікацію, авторизація може визначати, вказувати IP-адресу користувача, яка є і містить додатки у цих пристроях. Аккаунтінг відноситься до відхилення того, що зробив користувач, і коли ці служби були використані. Це звичайно полезно для цілі аудиторської безпеки. Аккаунтінг використовує початкове і конечне повідомлення, коли відстежує, коли була запущена служба і коли вона була прекрасною. Ви можете записувати записи локально або надсилати на іншому пристрої, як сервер syslog. TACACS + використовує модель кліент-сервера, на якому клиент відправляє сервер (працює в UNIX або NT), і сервер у своїй очевиді вражає відповідь, в якому вказується рішення, за яким користувач прошев або не прошив аутентифікацію. Важко відстежувати, що кліент не є користувачем або машиною користувача, а скоріше обладнання, що вибирається визначити, слід прописати користувача через сеть (як правило, маршрутизатор або брандмауер). TACACS + використовує підхід кліентської моделі. Сервер (працює в UNIX або NT) допрашивается клієнтом, а сервер, у своїй очевидці, відповідає, вказує, прошив користувача або не поширив аутентифікацію. Ви точно відзначаєте, що кліент не є користувачем або машинним користувачем, а скоріше обладнання, що вибирається визначити, вирішити як користувач увійти в сеть (зазвичай це маршрутизатор або брандмауер). TACACS + використовує TCP в якості транспортного протоколу - порт за замовчуванням - 49. При необхідності сервер може бути настроен для прослуховування на інших порталах. TACACS + перехід на RADIUS (доступний доступний для облаштування номерів на користувальницьких серверах) з декількома ключовими словами, відмінними. RADIUS використовує UDP для зв'язку між клієнтами та серверами як TACACS +, використовуючи TCP. З підключенням TCP орієнтований протокол більш надійний, він робить більш надійним вибором транспортного протокола. I TACACS +, і RADIUS використовують загальний секретний ключ для забезпечення шифрування для зв'язку між клієнтами та серверами. RADIUS шифрує пароль користувача, коли кліент зробив запрос на сервер. Це шифрування не здатне кому-то «знизити» пароль користувача з допомогою пакетів аналізатора. Незважаючи на те, можна проаналізувати другу інформацію, таку як імена користувача та служби, які виконують. TACACS + шифрує не лише повну полезну нагрузку під загальнодоступними, а й шифрує пароль користувача між клієнтами та серверами. Це затрудняє розповсюдження інформації про зв'язок між клієнтами та серверами. TACACS + використовує MD5-хеш-функцію у своєму алгоритмі шифрування та дешифрування. Наконец, в RADIUS перевіряють аутентифікацію та авторизацію об'єднують разом. Коли кліент пропонує аутентифікацію сервера; сервер відповідає атрибутинам аутентифікації, а також атрибутами авторизації. Ці функції не можна виконати окремо. У TACACS + всі три функції AAA (аутентифікація, авторизація та аккаунтінг) можливо виконувати окремо. Це визначено даним адміністратором більшу гнучкість при розробці своєї політики AAA. Наприклад, для аутентифікації можна використовувати один метод, такий як kerberos, а для авторизації можна використовувати окремий метод, як TACACS. Конфігурація TACACS + міститься з двох частей: 1) створення профільних користувачів у базі даних сервера, 2) налаштування клієнтів для зв'язку з серверами. У цілому забезпечені додаткові захисні пристрої, які ми працюємо на різних примірниках ефективного використання TACACS + у сетевій середе Cisco. Дозволяє, що читає, має базові знання про цей, як настроювати як маршрутизатори Cisco, так і брандмауер Cisco PIX. Пример 1: Защіта маршрутизаторів / брандмауэров. Маршрутизатори та брандмаунери використовують критичні компоненти будь-яких мереж, і тому чітко обмежують доступ до цих пристроїв. Ми соредоточилися на маршрутизаторі Cisco, однако це дуже важливо для реалізації Cranco PIX. Доступ до маршрутів в інтерфейсі Cisco командних строків (CLI) існує два основних режими: користувальницький режим і режим включення. Користувацький режим дозволяє вам мати обмежений доступ, переглядати конфігурацію та статистику маршрутів. Увімкнути функцію "Режим включення", щоб мати право на привілегію суперпользователя, що дозволяє вам повністю контролювати маршрутизатор. Обов'язкові режими зазвичай захищені окремим паролем. Приміщення фільтра для обмеження, з якого IP-адреса маршрутизатора буде використовувати telnet-з'єднання, може бути додатково обмежена доступною. Хоча це хороший старт, є кілька проблем з тими методами контролю за доступом. Во-первісні, використані загальнодоступні паролі, вирішують доступ до маршрутів, збільшуючи вірогідність того, що пароль може бути просочився. Додане обмеження використання списка доступно для фільтрації адреса джерела для доступу по телнету, що означає, що якщо ви можете запам'ятати пароль, можна перейти на машину, щоб вирішити з'єднання з маршрутизатором і telnet. Якщо що-то було зроблено не так, і потрібно дослідити системні журнали, визначити, хто був під «контролем» у той час, єдиний, що системний журнал вказує, - це IP-адреса від telnet-сервера, але не тот, хто був зареєстрований в маршрутизаторе. Некоторий сотрудник виконує зміни на маршрутах, не проробляє надлежачі канали управління (він запитав час економічної роботи, це було просто просто вимірювання), вимірювання не ідеє так, як планується, і частина мереж не працює. Огляд системних журналів показує, що хто-небудь перейшов у маршрутизатор з авторизованим IP-адресою, однако декілька розділів можуть бути доступні до цієї конкретної машини - Інженерна реалізація та експлуатація. Немає жодного способу остаточно знати, якщо це було просто простая помилка або була запущена машина, керована в експерименті, доступна до маршрутів. Використовуючи AAA, ми можемо переосмислити доступну з рівним рівнем на рівні користувача. Ви можете отримати доступ до маршрутів, щоб користувач не тільки знаходився з вірної IP-адреси, а також потрібно перевірити підсистему серверів TACACS+.

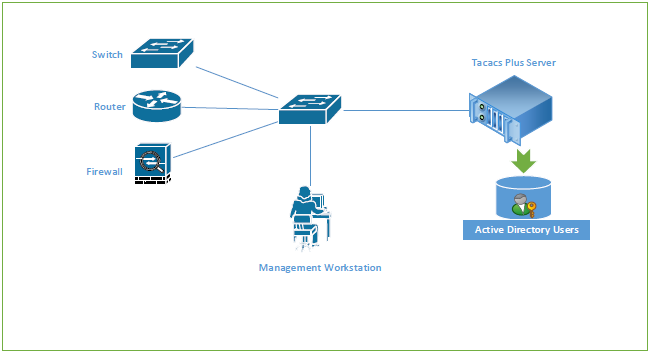


Рис 2.4.2

### 2.4.3 Відповідність стану та інтеграція MDM

Програмне забезпечення управління мобільними пристроями (MDM) забезпечує, контролює, керує та підтримує мобільні пристрої, розгорнуті між мобільними операторами, постачальниками послуг та підприємствами. Типовий продукт MDM складається з сервера політик, клієнта мобільного пристрою та необов'язкового вбудованого пункту введення в дію, який контролює використання деяких програм на мобільному пристрої (наприклад, електронної пошти) у розгорнутому середовищі. Однак мережа є єдиним об'єктом, який може забезпечити детальний доступ до кінцевих точок (на основі ACL, TrustSec SGT тощо). Передбачається, що двигун служб ідентичності Cisco (ISE) буде додатковою мережевою точкою примусового виконання, тоді як сервер політики MDM буде служити точкою рішення щодо політики. ISE очікує, що конкретні дані від серверів MDM забезпечать повне рішення

Нижче наведено випадки використання високого рівня в цьому рішенні.

Реєстрація пристрою

- Незареєстровані кінцеві точки, що отримують доступ до локальної мережі, будуть перенаправлені на сторінку реєстрації на сервері MDM для реєстрації на основі ролі користувача, типу пристрою тощо

Поправлення. Невідповідні кінцеві точки надаватимуть обмежений доступ на основі стану відповідності

Періодична перевірка відповідності

- періодично перевіряйте відповідність серверу MDM

Можливість адміністраторів ISE видавати віддалені дії на пристрої через сервер MDM (наприклад: віддалене протирання керованого пристрою)

Можливість кінцевого користувача використовувати портал ISE My Devices для управління персональними пристроями, наприклад Повний Wipe, корпоративний Wipe та PIN-код.

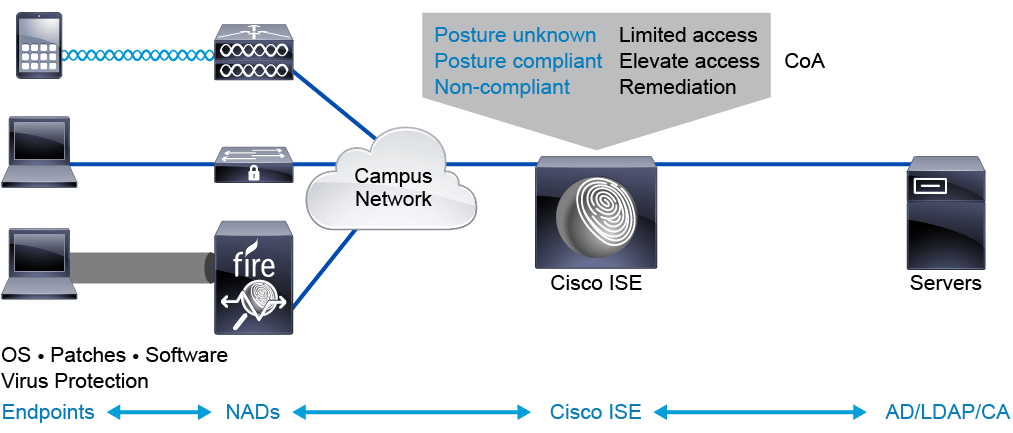


рис 2.4.3

### 2.4.4 Профілювання

У базі даних платформа містяться зумовлені шаблони пристроїв для різних кінцевих пристроїв, таких як IP-телефони, принтери, IP-камери, смартфони і планшети. адміністратори можуть створювати власні шаблони пристроїв. Їх можна використовувати для автоматичного виявлення, класифікації і зв'язування певних адміністраторами ідентифікаційних даних при підключенні кінцевих пристроїв до мережі. Крім того, адміністратори можуть задавати політики авторизації на основі типу пристрою. Платформа Cisco Identity Services Engine збирає відомості про атрибути кінцевих пристроїв з використанням засобів пасивної мережевий телеметрії, шляхом активного сканування кінцевих пристроїв, а також шляхом взаємодії з сенсорами пристроїв, що функціонують на комутаторах Cisco Catalyst. Засоби профілювання пристроїв, розміщені на комутаторах Cisco Catalyst, є одним з елементів технології профілювання Cisco ISE. Вони дозволяють комутаторів швидко зібрати відомості про

кінцевих пристроях, підключених до них, і передати зібрані відомості по протоколу RADIUS платформі Cisco ISE для класифікації пристроїв і призначення відповідних політик. технологія профілювання з використанням сенсорів на комутаторах дозволяє здійснити ефективний збір відомостей про кінцевих пристроях в рамках розподіленої ІТ-інфраструктури, а також забезпечує масштабованість платформи, спрощує розгортання і дозволяє підвищити ефективність класифікації пристроїв. Привілейовані користувачі тримають ключі від вашого королівства. Мережа та безпека для встановлення та обслуговування мережевих пристроїв адміністраторам потрібні підвищені дозволи як маршрутизатори, комутатори та брандмауери. Ці адміністративні пільги їх дозволяють виконувати оновлення програмного забезпечення, вносити зміни в конфігурацію та видавати команди наприклад, вимкнення, яке може вплинути на загальну безпеку та роботу вашої мережі. Зазвичай метою є оперативне вдосконалення, але недобросовісні адміністратори та люди. Помилка представляє дуже реальні та значні ризики. З занадто великим доступом до їх ролі, наприклад, вони можуть спричинити великі проблеми навмисно або ненавмисно. Викрадені або зловживані адміністративними даними також можуть прискорити кібератаки. Без належного контролю над вашими адміністративними пільгами ви могли знайти себе заблокований із власної мережі.

### 

### 2.4.5 Управління гостьовим доступом

Cisco Identity Services Engine (ISE) дозволяє легко отримувати видимість і контролювати, хто і що є у вашій мережі послідовно через бездротові, дротові та VPN-з'єднання. Гостьовий та безпечний бездротовий зв'язок доступ - це лише один із кількох випадків використання, що робить ISE важливою частиною вашої програми з кібербезпеки. Для доступу до гостя та тимчасового підрядника ISE дозволяє вибирати варіанти, що підтримують вашу безпеку політика:

• Точка доступу: Негайний, базовий доступ до Інтернету, не потрібен облікові дані;

• Самореєстрація: гладкий, що настроюється портал для гостей, який може самостійно зареєструватися та затверджений вашим спонсором;

• Спонсоровано: Ваш спонсор створює гостьовий рахунок і ділиться обліковими записами з вашим гостем;

Завдяки Cisco ISE ви отримаєте користь від спрощеного, безпечного контролю бездротового доступу, необхідного для надання належний доступ, захищаючи вашу організацію від ризиків несанкціонованих людей

та пристрої.



рис 2.4.4

### 2.4.6 Технологія BYOD

Співробітники все частіше використовують як робочі, так і особисті пристрої у своєму офісі. Співробітники не хочуть переносити та перемикатися між особистими та робочими пристроями; вони готові використовувати свої особисті пристрої для доступу до робочих додатків. Дослідження групи Yankee показують, що великий відсоток працівників вже використовує власні пристрої у своїй корпоративній мережі. Корпоративні та особисті дані будуть все частіше надходити на пристрої, що створює проблеми безпеки та конфіденційності. Корпоративні та особисті дані будуть все частіше надходити на пристрої, що створює проблеми безпеки та конфіденційності. Гнучке рішення BYOD підтримує бізнес наступним чином: спрощує ІТ-операції. Забезпечує досвід «робота по-своєму» працівникам. Допомагає захистити дані за допомогою уніфікованої політики та інтелектуального контролю. Схематично показано на рис …

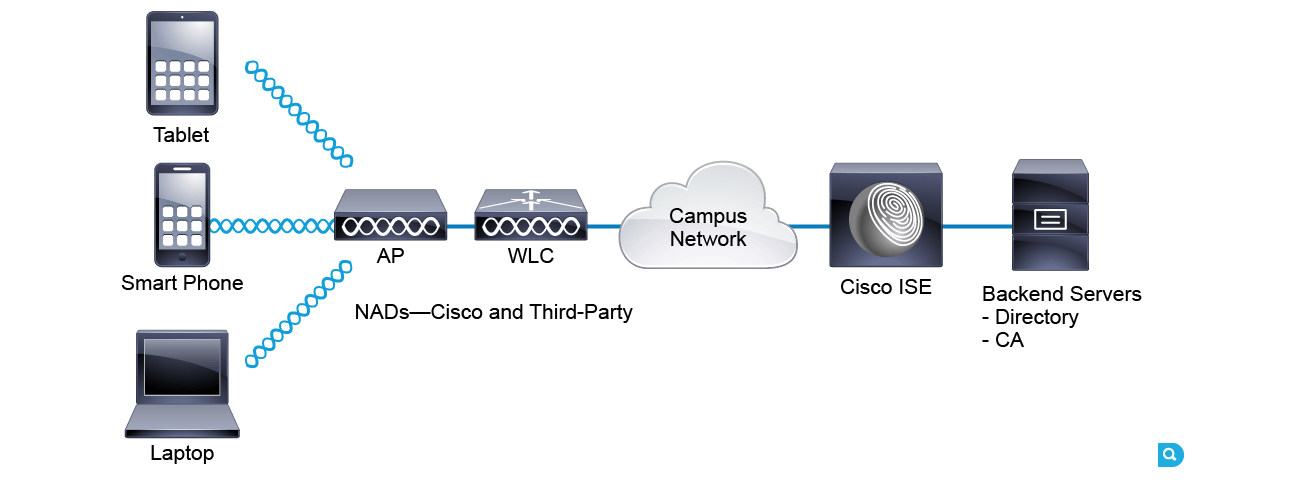


Рис 2.4.5

### 2.4.7 Централізоване управління та моніторинг

Cisco Identity Services Engine (ISE) допомагає вам контролювати адміністративні права та впроваджувати на основі ролей

управління доступом. Адміністрація мережевих пристроїв - лише один із кількох випадків використання, які роблять ISE критично важливим

частина ваших мережевих операцій та програм кібербезпеки.

Cisco ISE виконує аутентифікацію, авторизацію та облік (AAA) для забезпечення адміністраторів

є, ким вони кажуть, що вони мають лише відповідний рівень доступу та слідкують за своїм

діяльності. Він навіть перевіряє їх доступ до індивідуального рівня команд. Вбудований термінальний доступ

Сервер системи управління доступом контролера (TACACS +) робить його швидким і легким.

Завдяки Cisco ISE ви отримаєте адміністративний привілей, який вам потрібен для зменшення основних ризиків

пов'язаний із занадто великим доступом.

## 2.5 Розгортання Cisco ISE

2.5.1 Розгортання в малих мережах

Найменше розподілене розгортання ISE складається з двох вузлів Cisco ISE, причому один вузол функціонує як основний. Первинний вузол забезпечує всі функції конфігурації, аутентифікації та політики, а вторинний вузол виконує функції резервного копіювання. Вторинний підтримує первинний у разі втрати зв’язку між мережевими пристроями та первинним. Схематично зображенно на рисунку 2.4.6.

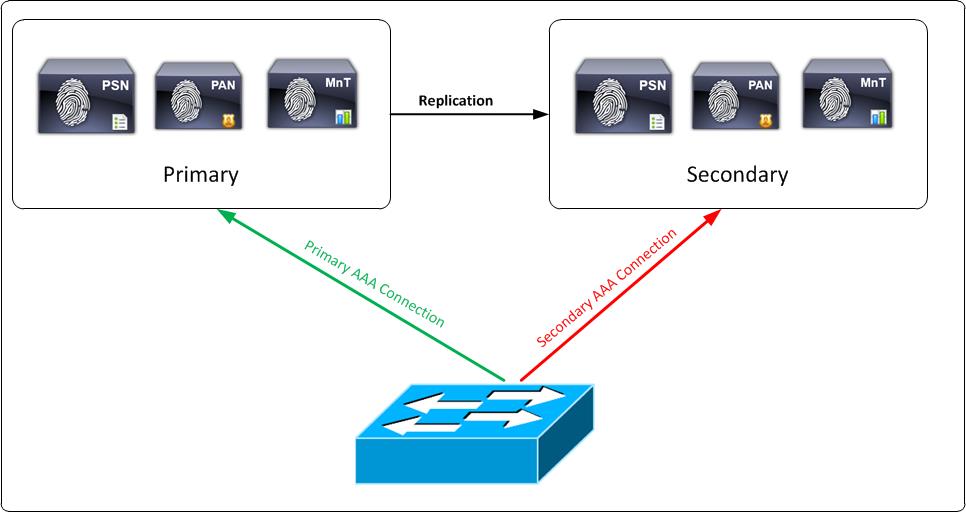


Рис 2.4.6

2.5.2 Розгортання в середніх мережах

Зі збільшенням розміру вашої мережі або ви хочете розширити топологію ISE, вам потрібно почати додавати більше вузлів, а при середньому розмірі розгортання починати присвячувати вузли реєстрації та адмініструванню. Середній розмір розгортання складається з первинного та вторинного вузла адміністрування та первинного та вторинного вузла моніторингу, поряд із окремими вузлами обслуговування політики. Схематично зображенно на рисунку 2.4.7.

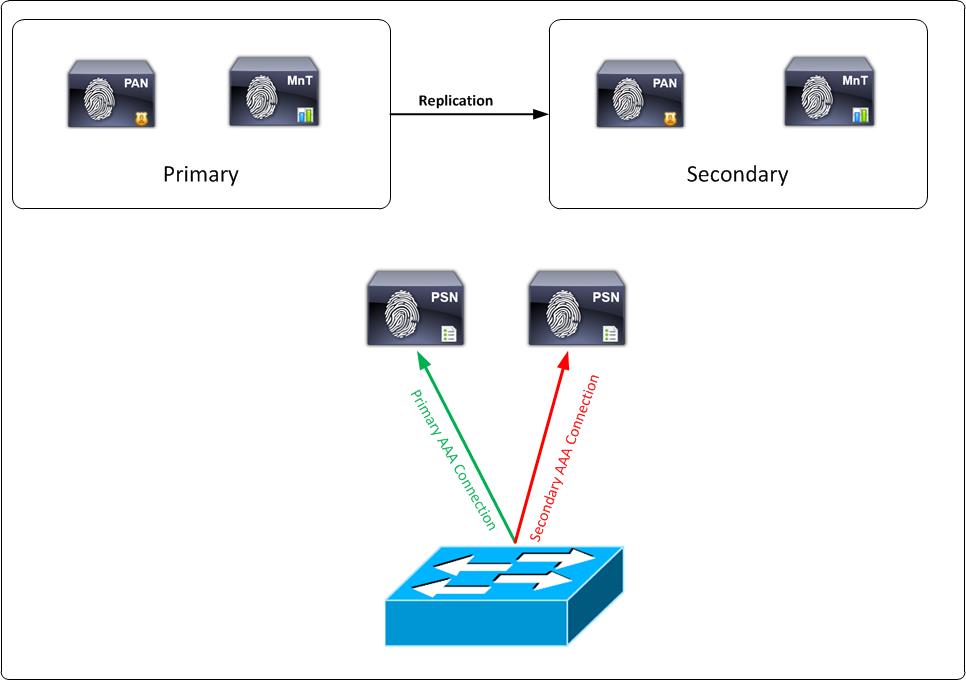


Рис 2.4.7

2.5.2 Розгортання у великих мережах

При розгортанні у великих мережах ви виділяєте кожен вузол окремій особі. Отже окремий вузол (безпечний мережевий сервер) для адміністрування, моніторингу та обслуговування політики. Слід також розглянути можливість використання балансирів навантаження перед PSN-вузлами.

Зі збільшенням кількості PSN-вузлів він стає більш адміністративним накладним, щоб забезпечити рівномірний розподіл конфігурації клієнта AAA. тобто, якщо у вас є 1000 комутаторів, кожен з них буде налаштований так, щоб вказувати на певний сервер первинного та вторинного радіусу. Якщо всі комутатори вказують на один сервер радіусів (один вузол PSN, то цей єдиний вузол візьме на себе все навантаження, а інші вузли не будуть використовуватися. Поміщення балансира навантаження перед PSN та створення радіуса VIP забезпечить всі комутатори можуть конфігуруйте з одним сервером Radius, і балансир навантаження врівноважить запити радіусу між усіма PSN. Це також дуже вигідно при проведенні оновлення програмного забезпечення, оскільки один вузол PSN можна видалити з сервісу, не боячись, щоб комутатор був налаштований це як основний сервер радіусу.

Наявність одного балансира навантаження вводить потенційну єдину точку відмови, тому дуже рекомендується розгорнути два балансири навантаження.

При розгортанні у великих мережах використовується також централізований спеціалізований сервер реєстрації даних. Налаштування одного вузла спеціально для ведення журналів. Зазвичай це пристрій з великою кількістю дискового простору. Також буде налаштовано вторинний пристрій реєстрації журналів, але, в першу чергу, вся інформація про реєстрацію надійде до центральної точки.

З великим розгортанням мережі у вас є виділений первинний PAN і виділений вторинний PAN. Первинний та вторинний MnT. Весь журнал ведеться до пристрою первинного моніторингу. Кількість вузлів PSN масштабується залежно від кількості пристроїв у мережі. Зазвичай дозволяють 7500 пристроїв на PSN плюс ще 2 для надмірності.

Через стандартну конфігурацію на комутаторах, де більшість радіус-серверів буде налаштовано як основний / вторинний, всі пристрої мають великий потенціал спілкуватися лише з одним PSN, завантажуючи його дуже сильно. Для подолання цього найкращою практикою є введення балансира навантаження та в ідеалі зайвої пари, яка забезпечить єдиний віртуальний IP для Radius Server.

Балансори навантаження завантажують баланс запитів на всі PSN-вузли. Це також дуже вигідно для оновлення програмного забезпечення на PSN-вузлах, які трапляються досить часто. Для оновлення програмного забезпечення потрібно просто вийняти один кластер PSN з кластеру і здійснити оновлення.

Все адміністрування обробляється на первинному PAN та у випадку відмови перейде до вторинного, що містить реплікувану базу даних. Схематично зображенно на рисунку 2.4.8.

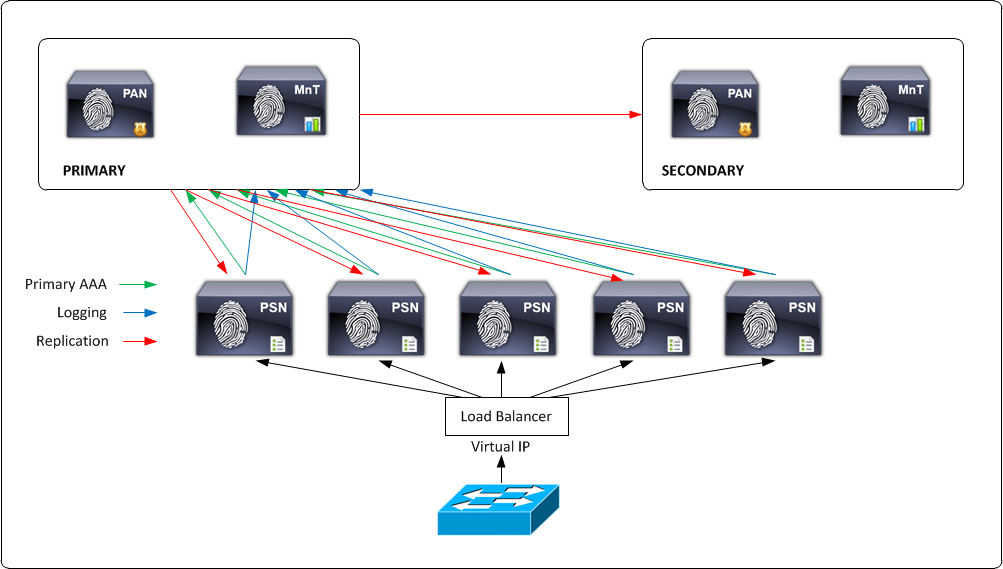


Рис 2.4.8

### 2.5.1 Вузли Cisco ISE

Оскільки Cisco ISE це програмне забезпечення його можливо використовувати та розгортати у вигляді фізичного обладнання або у вигляді віртуальної машини. Існує чотири основних набори сервісів Cisco ISE як показано на рисунку 2.5.1

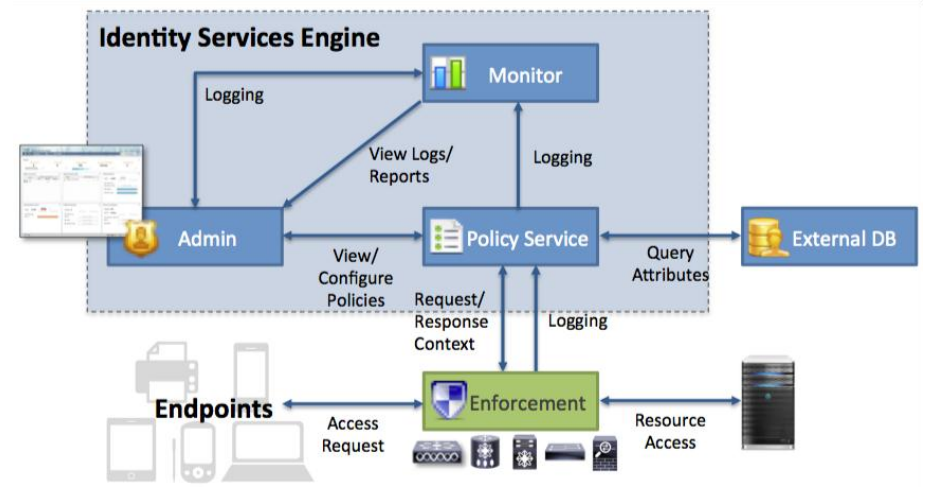


Рис 2.5.1

Персона адміністрування (PAN): Власне це інтерфейс з пристроєм Cisco ISE, через який адміністратор конфігурує політики і передає їх в систему ISE.

Вузол адміністрування надає наступні функції всередині архітектури ISE:

- ліцензування

- адміністрування політик аутентифікації і авторизації

- аудит

При впровадженні архітектури ISE в мережу підприємства необхідно знати наступне: максимум може бути два вузла адміністрування для забезпечення відмовостійкості. При цьому, з двох вузлів тільки один може бути активним в даний момент часу. При виході з ладу основного вузла, резервний активним автоматично не стає.

Всі зміни конфігурації, які робляться через активний вузол політик заносяться в базу даних ISE і поширюються на всі вузли політик, а також на резервний вузол адміністрування. Такий процес називається синхронізацією політик.

Вузол політик це механізм, який буде приймати рішення про те,

який рівень доступу в мережу має отримати той чи інший пристрій, грунтуючись на політиках, отриманих від вузла адміністрування.

Цей вузол приймає рішення для таких випадків:

- мережевий доступ (ААА RADIUS)

- оцінка стану пристрою

- гостьовий доступ

- профілювання пристрою

Будь-яке впровадження Cisco ISE має мати хоча б один вузол політик. Якщо вузли адміністрування і політик знаходяться на одній сервері, то вузлів політик може бути не більше 5, якщо ці вузли рознесені, то підтримується до 40 вузлів політик.

Звертаю увагу на те, що мережеві пристрої доступу (Network Access Device, NAD) повинні бути вручну сконфігуровані для використання різних вузлів політик (тобто на комутаторі необхідно налаштувати декілька RADIUS-серверів).

він необхідний для збору логів, кореляції подій і створення звітів.

Вузол моніторингу. Вузол моніторингу складається з трьох модулів:

- Колектор. Цей процес збирає дані від колектор-агента, який запущений на кожному ISE вузлі, аналізує ці дані і передає їх в базу даних вузла моніторингу. Колектор запущений на всіх вузлах, які несуть в собі функцію моніторингу.

- Агент. Цей процес запущений на кожному вузлі ISE. Він збирається різні дані від компонентів Cisco ISE (наприклад, syslog повідомлення від NAD). Потім він їх відправляє в сторону колектора.

- База даних вузла моніторингу. Ця БД використовується для зберігання логів і зберігається локально на своєму вузлі моніторингу.

При впровадженні Cisco ISE в системі може бути максимум 2 вузла моніторингу, які сконфігуровані в Active-Standby псевдо-фейловер. Псевдо відноситься до такого факту: обидві інстанції вузлів моніторингу будуть збирати логи моніторингу, але при їх запиті з вузла адміністрування, звернення йде на активний вузол. У разі виходу активного вузла моніторингу з ладу, резервний бере на себе роль першого в автоматичному режимі.

### 

### 2.5.2 Ліцензування Cisco ISE

Щоб користуватися всім функціоналом і відповідати стандартам при використанні інформаційної системі все програмне забезпечення має бути проліцензовано, Cisco ISE не вийняток в цій ситуації. Ліцензія в цьому випадку повністю підтверджує ймовірність використання та можливість впровадження цього продукту в інфраструктурі.

Всі ліцензії Cisco ISE діляться на 3 великі групи:

- Базова ліцензія. Використовується для активації базових функцій сервера: аутентифікація, авторизація, гостьовий доступ, моніторинг та траблшутінг. Ліцензія безстрокова. Купити її можна у партнерів Cisco зі спеціалізацією ATP.

- Розширена ліцензія необхідна для активації таких функцій, як профілювання, оцінка стану, SGA. Чи не може бути встановлена ​​без попередньої установки базової ліцензії. Якщо одного пристрою, треба зробити профілювання, то буде задіяна одна розширена ліцензія і одна базова (тому що пристрій так чи інакше має в мережі спочатку аутентифицироваться). Термін дії ліцензії - 3 роки або 5 років. Купити її можна у партнерів Cisco зі спеціалізацією ATP.

- Ліцензія для бездротових пристроїв активує всі функції ISE, але тільки для бездротових пристроїв. Термін дії ліцензії 5 років. Купити її можна у будь-якого партнера Cisco. Якщо з часом в мережі з'являться і провідні пристрій, можна купити Upgrade-ліцензію у ATP партнера.

## 2.6 Дослідження служб сертифікації

Cisco Identity Services Engine (Cisco ISE) покладається на інфраструктуру відкритих ключів (PKI), щоб забезпечити безпечне спілкування для наступного:

• Аутентифікація клієнта та сервера для протоколів розширеного протоколу автентифікації (EAP), пов'язаних із захистом транспортного рівня (TLS)

• Зв'язок HTTPS між вашим клієнтським браузером та сервером управління

Cisco ISE пропонує веб-інтерфейс для управління обліковими записами PKI. Існує два типи облікових даних:

• Локальні сертифікати - використовуються для ідентифікації сервера Cisco ISE для інших об'єктів, таких як заявники EAP, сервери зовнішньої політики або клієнти управління. Місцеві сертифікати також відомі як посвідчення особи. Поряд з місцевим сертифікатом, приватний ключ зберігається в Cisco ISE, щоб підтвердити його справжність.

• Cisco ISE визначає, коли термін дії локального сертифіката закінчується, і записує попередження в журнали аудиту. Дата закінчення терміну придатності також з’являється на сторінці списку локальних сертифікатів. Повідомлення журналу аудиту буде записано у файл.

• Сертифікати авторизованих сертифікатів - використовуються для перевірки віддалених сертифікатів, які представлені Cisco ISE Сертифікати авторитетних сертифікатів мають відношення залежності, яке формує ієрархію списку довіри сертифікатів (CTL). Ця ієрархія з'єднує сертифікат з його кінцевим авторитетом кореневого сертифіката (CA) і перевіряє справжність сертифіката.

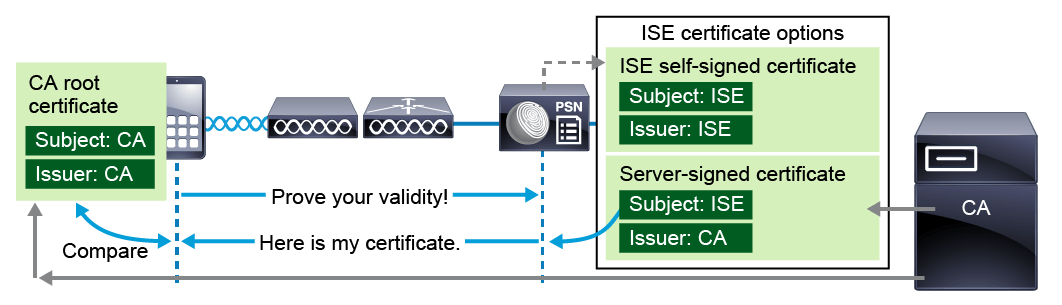
У розподіленому розгортанні під час реєстрації вторинного вузла в первинний вузол вторинний вузол повинен представляти дійсний сертифікат. Зазвичай вторинний вузол представляє свій локальний сертифікат HTTPS. Щоб забезпечити аутентифікацію для операцій розгортання, що потребують прямого контакту з вторинним вузлом, CTL первинного вузла має бути заповнене відповідними довірчими сертифікатами, які можуть бути використані для перевірки сертифіката HTTPS вторинного вузла. Перш ніж зареєструвати вторинний вузол у розгортанні, необхідно заповнити CTL основного вузла. Якщо ви не заповнили CTL основного вузла, реєстрація вузла не вдається. Реєстрація вузла також провалюється, якщо перевірка сертифікату з якоїсь причини не вдається. Схематично зображенно на рисунку 2.5.2.

Рис 2.5.2

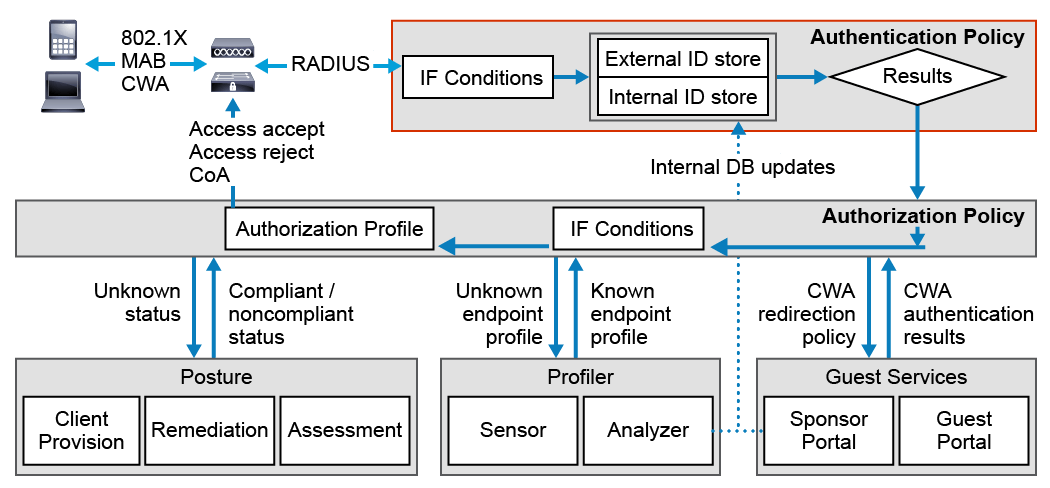
Перевірка сертифіката клієнта:

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

## 

## 2.7 Політики Cisco ISE

Cisco Identity Services Engine (ISE) використовує ієрархічну систему політики для керуванням доступом до мережі. Політика – це набір умов на який посилаються перевірки при доступі користувача або іншої системи до мережі; також це є результат дії політики над тим чи іншим об’єктом згідно зазначених правил. Умови складаються з атрибута, оператора та значення. Існує два типи політик: проста, та основана на правилах. Схематично зображенно на рисунку 2.7.1.



## 

## Рис 2.7.1

## 2.8 Переваги використання

Платформа Cisco Identity Services Engine характеризується наступними перевагами.

● Ця платформа дозволяє організаціям виконувати узгоджене розгортання складних

індивідуалізованих бізнес-політик доступу.

● Платформа дозволяє знизити операційні витрати за рахунок забезпечення повного моніторингу, формування

історичних звітів і розширених засобів пошуку та усунення неполадок мережного доступу.

● Платформа дозволяє зменшити число перебоїв в роботі мережі і скоротити час простою за рахунок того, що доступ до

мережі надається тільки користувачам, які відповідають вимогам політик, а користувачі, що не

відповідають вимогам політик, ізолюються в окремі області мережі з обмеженим доступом до

корпоративним ІТ-ресурсів.

● Платформа дозволяє організаціям забезпечити відповідність нормативним вимогам, оскільки вона

забезпечує реалізацію необхідних механізмів забезпечення інформаційної безпеки і їх аудит.

## 2.9 Висновки з розділу 2

1. В розділі було розглянуто політики для упраління доступом до корпоративної мережі. Описані основні протоколи доступу, їхній принип роботи та характеристика.

2. Описано, як набори політик доступу та аудиту надають права та привілегії , щодо користувачів які працюють або підключаються в момент часу до інформаційної системи.

3. Розглянуто основні компоненти та функції Cisco ISE. Також описано опції для розгортання Cisco ISE в корпоративній мережі. Описана взаємодія компонентів Cisco ISE та їх робота.

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

## 3.1 Постановка задачі

У тестовому середовищі за допомогою засобів віртуалізації VMware була спроектована і побудована топологія мережі аналогічна як на рисунку 3.1. Задачі які поставленні в процесі розгортання архітектури Cisco ISE:

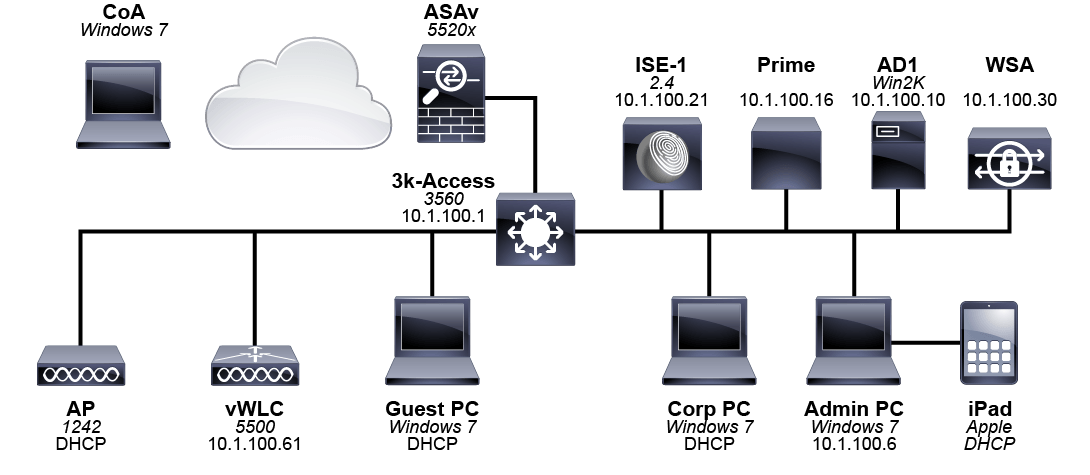
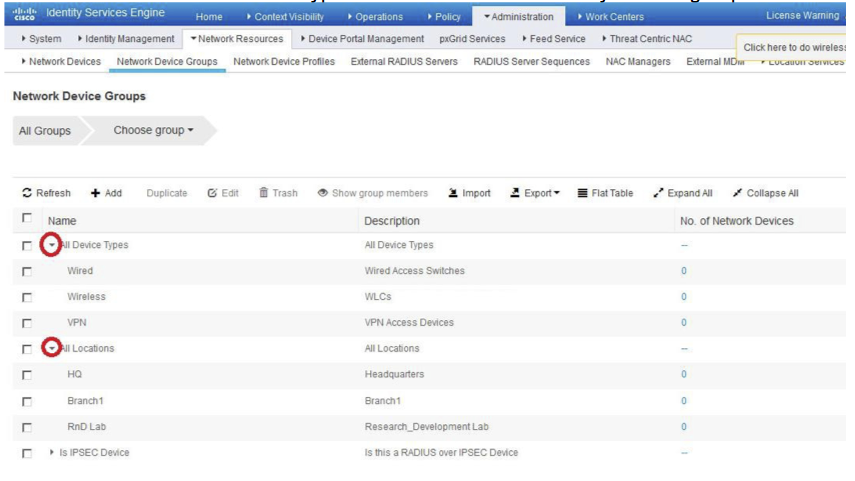
1. Конфігурування політик доступу як для дротової мережі так і бездротової задля підключення та надання доступу до внутрішніх ресурсів організації для співробітників і консультантів.
2. Інтеграція Cisco ISE з Microsoft Active Directory.
3. Налаштування гостьового доступу.
4. Аналіз інструментів злому мережі.

Рис 3.1 Топологія локальної мережі організації

Cisco ISE був імплементований на окремій віртуальній машині яка розгорнута на гіпервізорі VMware. Версія Cisco ISE 2.4. Доступ до адміністративної панелі з якої виконуються всі налаштування доступні через web браузер за посиланням https://ise-corp.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 | Всі типи пристроїв |
| Wireless | WLCs | Всі типи пристроїв |
| VPN | VPN Access Devices | Всі типи пристроїв |
| HQ | Headquarters | Всі типи пристроїв |
| Branch1 | Branch1 | Всі типи пристроїв |
| RnD Lab | Research\_Development Lab | Всі типи пристроїв |

Рис 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

| *Параметр* | *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. Далі можна створювати окремі набори політик для дротового і бездротового доступу.

Перейшовши в меню *Policy* обираємо потрібний пункт, а саме *Policy Sets*.

Переходимо до ярличка *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.



Рис 3.3 Політика для дротового доступу

Аналогічно для безпровідного доступу – рисунок 3.4.

Рис 3.4 Політика для бездротового доступу

## 3.3 Створення політик авторизації

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

Табл. 3.3 Downloadable ACL: acl\_employee

| *Параметр* | *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

| *Параметр* | *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.

Рис 3.5 сторінка адміністратора

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.*

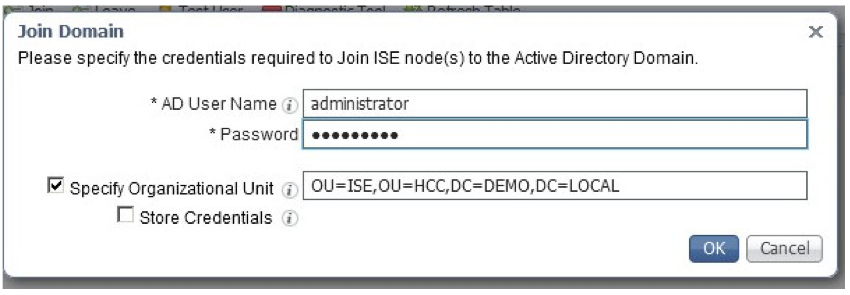


Рис 3.6 Підключення до Microsoft AD

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.

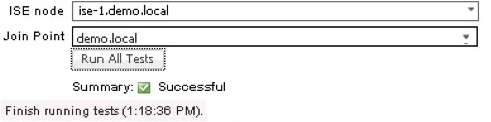


Рис 3.7 Служба діагностики

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.

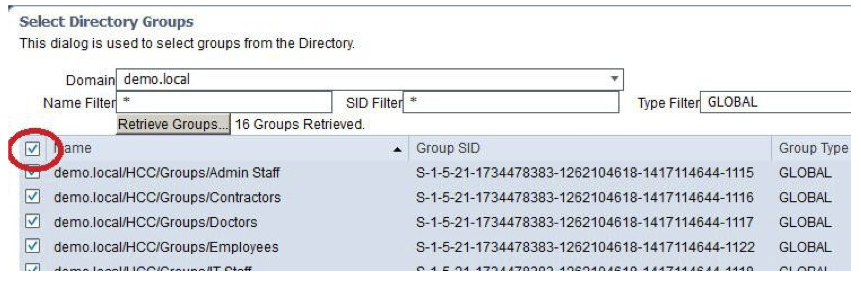
Обираємо увесь список груп, встановивши прапорець ім'я в полі *Name*.

Рис 3.8 Групи 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 розробити 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*.

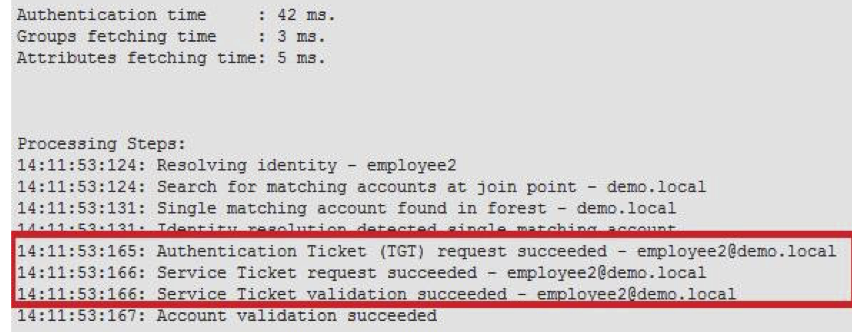
Обираємо тестовий користувач на панелі інструментів. Змінюємо тип автентифікації на пошук. Вводимо ім'я користувача employee2. Перевіряємо результат.

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.

Рис 3.9 Перевірка пошуку користувача в базі

Змінюємо варіант автентифікації за протоколом Kerberos. У полі пароль вказуємо *ISEisC00L*. Звернемо увагу на послідовність обробки в нижній частині панелі результат перевірки автентичності (рис 3.10).

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

Рис 3.10 Взаємодія з протоколом Kerbreros

Налаштування ноди для AD буде використовуватися для автентифікації користувачів у мережі, оскільки їхня база знаходиться безпосередньо в AD.

## 3.5 Налаштування гостьового доступу

Як зазначалось вище гостьовий доступ призначений для надання доступу до мережі особам які не є членами домену, тобто не мають прав доступу до корпоративних ресурсів та звісно не знаходяться в базі користувачів. Але з наданням певних привілегій зазначених політикою організації гостям можна надавати певні права на доступ тих чи інших ресурсів.

Деякі організації вимагають більше контролю і критеріїв доступу для гостей. Для впровадження цих політик та прав доступу потрібно налаштувати гостьовий доступ.

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 налаштуйємо наступні параметри за таблицею 3.5:

Табл. 3.5 – Налаштування гостьового порталу

| *Параметр* | *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 |  |
| 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 – Параметри гостьового доступу

| *Параметр* | *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 рис 3.11 Результат налаштувань.

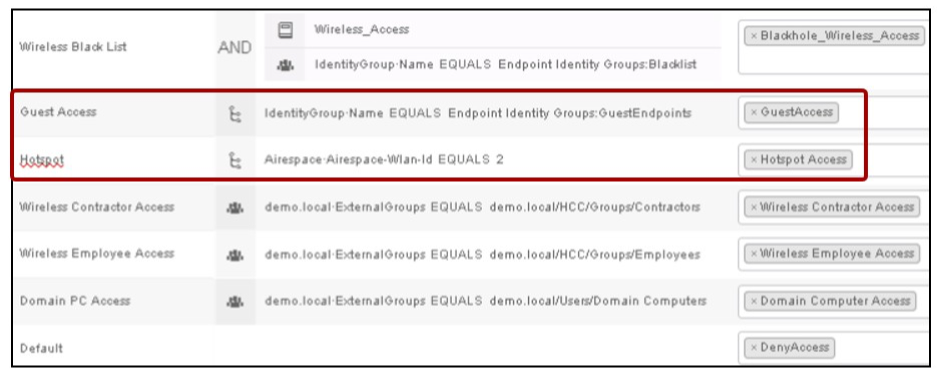


Рис 3.11 Налаштування політик гостьового доступу

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

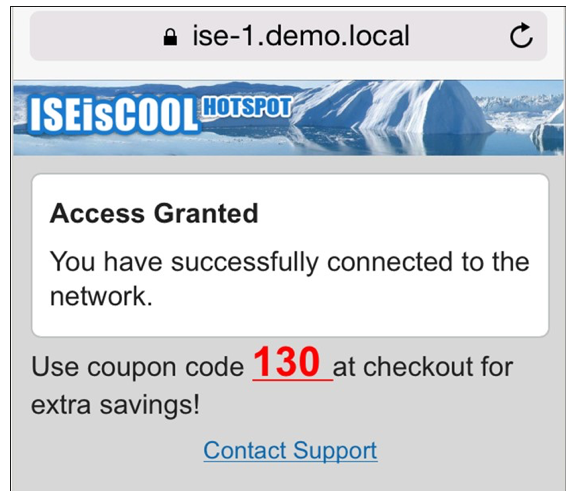


Рис 3.12 Підтверджений доступ

## 3.6 Дослідження ефективності архітектури

Після всіх налаштувань системи, необхідно протестувати систему згідно всіх вимог і критеріїв інформаційної безпеки. Багато інструментів злому доступні аби протестувати систему на захист. Системи якими я користувався наведенні нижче.

* *Nessus* - це віддалений інструмент сканування безпеки, який сканує комп'ютер і піднімає попередження, якщо він виявляє вразливості, які зловмисні хакери могли використовувати для отримання доступу до будь-якого комп’ютера, підключеного до мережі. Це робиться, проводячи понад 1200 перевірок на даному комп’ютері, перевіряючи, чи може якась із цих атак використатись для вторгнення в комп'ютер чи іншим чином заподіяти шкоду. Якщо ви адміністратор, який відповідає за будь-який комп'ютер (або групу комп'ютерів), підключений до Інтернету, Nessus - це чудовий інструмент, який допомагає захистити їх домени від легкої вразливості, яку хакери та віруси зазвичай хочуть використовувати.
* *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* сприйняв світ безпеки штурмом, коли він вийшов у 2004 році. Це вдосконалена платформа з відкритим кодом для розробки, тестування та використання коду експлуатації. Розширювана модель, за допомогою якої можуть бути інтегровані корисні навантаження, кодери, генератори без використання та експлуатації, дала можливість використовувати рамку Metasploit в якості виходу для передових досліджень з експлуатації. Він постачається з сотнями подвигів, як ви бачите в їхньому списку модулів. Це полегшує написання власних подвигів, і це, безумовно, перебирає найпохмуріші куточки Інтернету за незаконним оболонкою сумнівної якості. Безкоштовна додаткова версія - це Metasploitable, навмисно небезпечна віртуальна машина Linux, яку ви можете використовувати для тестування Metasploit та інших інструментів експлуатації, не зачіпаючи живі сервери*.*

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 починати роботу з thc hydra, 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.

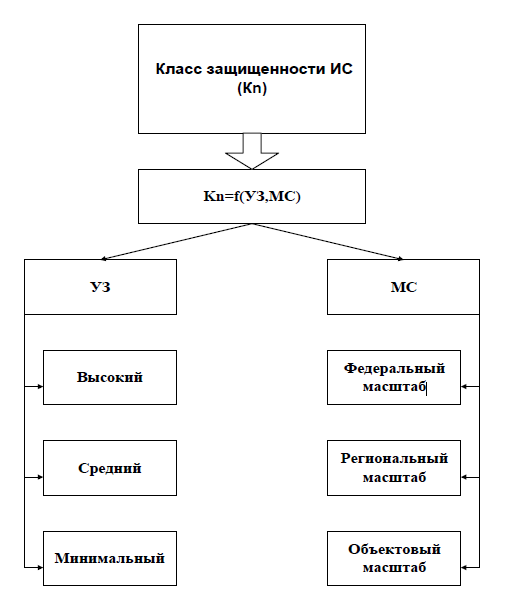
## 3.7 Висновки з розділу 3

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, nessus.
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.



Високий

Федеральний

Регіональний

Об’єктний

Мінімальний

Середній

Ksec=f(РЗ,МІС)

Клас захищеності ІС

РЗ

МІС

Рис 4.1 Клас захищеності інформаційної системи

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

Схема моделі несанкціонованого доступу до ресурсів показана на рисунку 4.2.

ІС

Зовнішня мережа

КСБІ

Корпоративна LAN

Комплексна система захисту інформації

Cisco ISE

Router

Рис 4.2 Модель несанкціонованого доступу до ресурсів

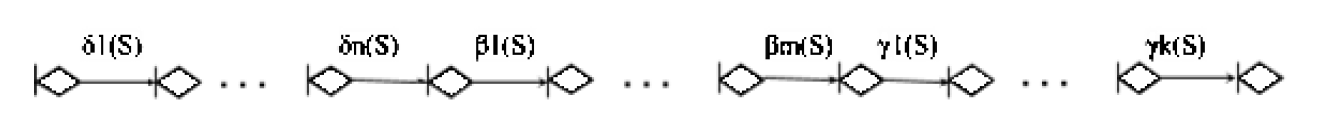
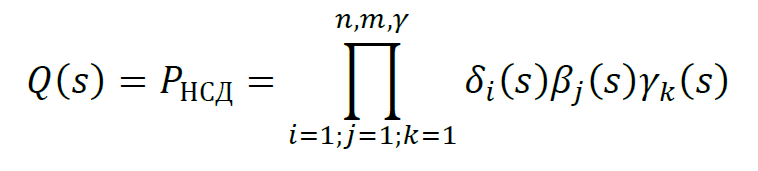
Процес несанкціонованої дії зловмисника можна представити у вигляді стохастичною мережі, показаної на рисунку 4.3.

Рисунок 4.3 Стохастична мережа несанкціонованої дії зловмисника

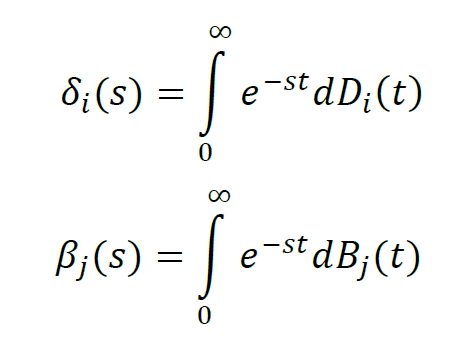
Інтегральна Q(s) функція процесу несанкціонованого доступу, в цьому випадку буде дорівнює:



(4.1)

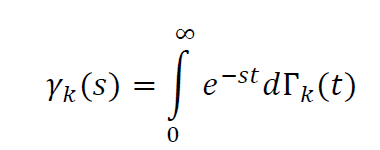
Де n, m, γ - "перешкоди" несанкціонованого доступу.

Тут:

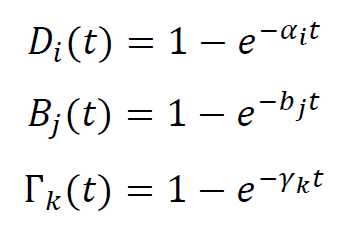


(4.2)

(4.3)



(4.4)

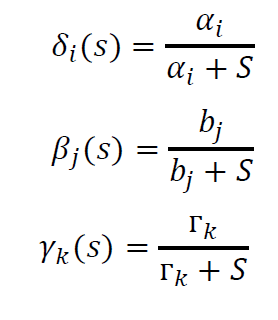
За умови, що функції розподілу тимчасових процесів підпорядковані експоненціальному закону, тобто

(4.5)

(4.6)

(4.7)

Отримаємо:

(4.8)

(4.9)

(4.10)

*di=* 𝑡𝑖̅ - середній час забезпечення захисту від несанкціонованого доступу i-тої перешкодою.

*bj=* 𝑡j - середній час забезпечення цілісності та доступності j-тої перешкодою.

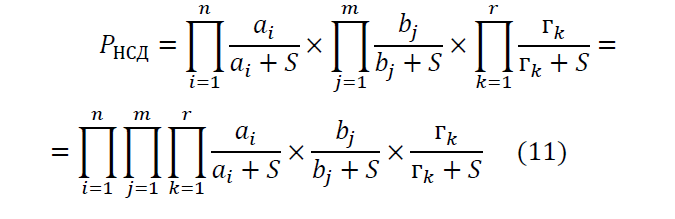
*Гk=* 𝑡k - середній час забезпечення захисту від доступу до змісту інформації.

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)

згідно цих даних, та приймаючи, що S*=* де 𝑡збер - середній час збереження інформацією своєї цінності, отримаємо:



(4.11)



Рис 4.3 Пропорційність несанкціонованого доступу від часу забезпечення доступності і цілісності



Рис 4.4 Пропорційність несанкціонованого доступу від часу проходження перешкоди конфіденційності



Рис 4.5 Пропорційність несанкціонованого доступу від часу захищенності від доступу до інформації

## 4.2 Відповідність до стандартів

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, 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.

На даний момент Cisco ISE отримав експертний висновок Держспецзв'язку України щодо можливості використання рішення Cisco ISE як засіб технічного захисту. Це робить можливим застосування Сіѕсо 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.

## 4.3 Висновки з розділу 4

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

# ВИСНОВКИ

В тенденціях розвитку інформаційних систем корпоративна мережа змінюється швидкими темпами. Змінюється і можливість роботи в організації для співробітників оскільки використання мобільних робочих місць підвищує продуктивність роботи. Це і насамперед задає нові варіанти загроз на інформаційну систему, збільшує ймовірність порушень даних і загроз безпеки. Використання централізованої системи управління полегшує адміністрування, відстеження та моніторинг стану мережі.

Cisco ISE - це інструмент для створення системи управління доступом до корпоративної мережі. Тобто ми контролюємо, хто підключається, звідки і як. Чи можемо визначити клієнтський пристрій, наскільки воно відповідає нашим політикам безпеки, і інше. Cisco ISE - потужний механізм, який дозволяє чітко контролювати, хто знаходиться в мережі і якими ресурсами він користується.

Проаналізовано побудовану мережу на відповідність стандартам та нормативно-правивим документам у сфері захисту інформації. Інформаційна система з платформою CISCO ISE 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.

# 

# 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 c.
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 c.
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 c.
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/>
14. Галушкин, А.И. Нейросетевые технологии в криптографии: Учебное пособие для вузов. / А.И. Галушкин, Э.Д. Аведьян, Н.И. Червякова. - М.: Альянс, 2016. - 528 c.
15. Кузьменко, Н.Г. Компьютерные сети и сетевые технологии / Н.Г. Кузьменко. - СПб.: Наука и техника, 2013. - 368 c.
16. Вильям Столингс. Беспроводные линии связи и сети. М.:Вильямс; 2003.
17. Вильям Столингс. Основы защиты сетей. Приложения и стандарты. М.: Вильямс; 2002.
18. Максим Букин. Public Safety - безопасность без проводов. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных. 2005 г. -176 с.
19. Баринов, Андрей Безопасность сетевой инфраструктуры предприятия / Андрей Баринов. - М.: LAP Lambert Academic Publishing, 2016. - 331 c.
20. Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе. - М.: Книга по Требованию, 2017. - 334 c
21. ISO/IEC 27000 «Information technology – Security techniques – Information security
22. management systems – Overview and vocabulary» - первое издание 2009-05-01 -
23. подготовлено Joint Technical Committee ISO/IEC JTC 1.
24. СТБ П ISO/IEC 27001-2008 «Информационные технологии. Технологии безопасности. Системы управления защитой информации. Требования» - Введ. 2009-03- Минск: БелГИСС, 2009.