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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо побудови системи контролю доступу до ресурсів в електронних освітніх платформах»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

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

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро СИРОТЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-43
СИРОТЕНКО Дмитро
(прізвище, ім'я)

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

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

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AES - Advanced Encryption Standard

RSA - Rivest-Shamir-Adleman (a public-key encryption technology)

DES - Data Encryption Standard

RBAC - Role-Based Access Control

IP - Internet Protocol

MFA - Multi-Factor Authentication

СУПД (DBMS in English) - Database Management System

LMS - Learning Management System

DAC - Discretionary Access Control

ABAC - Attribute-Based Access Control

MAC - Mandatory Access Control

IDS - Intrusion Detection System

SIEM - Security Information and Event Management

AI/ML - Artificial Intelligence / Machine Learning

SSL - Secure Sockets Layer

TLS - Transport Layer Security

Cisco ISE - Cisco Identity Services Engine

AD - Active Directory

PSN - Policy Service Node

MNT - Monitoring Node

LDAP - Lightweight Directory Access Protocol

RADIUS - Remote Authentication Dial-In User Service

TACACS - Terminal Access Controller Access-Control System

pxGrid - Platform Exchange Grid

WebAuth - Web Authentication

DNS - Domain Name System

ВСТУП

Актуальність дослідження. Контроль доступу до ресурсів в електронних освітніх платформах має вирішальне значення з кількох причин. По-перше, освітні платформи зберігають конфіденційні дані про студентів, викладачів та адміністративний персонал. Забезпечення безпеки цих даних є критично важливим для запобігання несанкціонованому доступу, витоку інформації та втраті даних. По-друге, електронні освітні платформи є точками входу для кібератак, а компрометація цих систем може мати серйозні наслідки для освітніх процесів та репутації навчального закладу. По-третє, ефективний контроль доступу є необхідним для підтримки безперебійного функціонування освітніх процесів. Невдалі спроби контролю доступу можуть призвести до перебоїв у навчанні та втрати продуктивності. По-четверте, із зростанням обсягу дистанційного навчання, питання контролю доступу до освітніх ресурсів набуває ще більшої ваги. Забезпечення безпеки доступу до цих платформ має вирішальне значення для створення безпечного навчального середовища для студентів і викладачів.

Системи контролю доступу відіграють важливу роль у забезпеченні безпеки електронних освітніх платформ. Вони призначені для регулювання доступу користувачів до різних ресурсів на основі встановлених політик безпеки. Системи контролю доступу можуть забезпечити гранулярний контроль, дозволяючи або забороняючи доступ до конкретних ресурсів залежно від ролей користувачів. Також вони надають можливість моніторингу та аудиту дій користувачів, що сприяє виявленню та розслідуванню інцидентів безпеки.

Системи контролю доступу аналізують запити на доступ до ресурсів, визначаючи, чи відповідають вони встановленим політикам безпеки. Відхилення від нормальних моделей доступу можна позначити як потенційну загрозу безпеці. У разі інциденту системи контролю доступу полегшують аналіз, надаючи детальну інформацію про дії, які призвели до інциденту. Якщо виявлено загрозу, системи контролю доступу можуть автоматично блокувати підозрілі запити на доступ, щоб запобігти компрометації ресурсів.

Рішення для контролю доступу дозволяють організаціям застосовувати політики безпеки на електронних освітніх платформах, забезпечуючи відповідність користувачів стандартам безпеки та конфігураціям. Поєднуючи заходи контролю доступу із сучасними системами безпеки, освітні заклади можуть створити надійний захист від широкого спектру загроз кібербезпеці та покращити загальну безпеку.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження шляхів та розробка рекомендацій щодо побудови системи контролю доступу до ресурсів в електронних освітніх платформах.

Об’єкт дослідження – контроль доступу до ресурсів в електронних освітніх платформах.

Предмет дослідження – методи та засоби побудови системи контролю доступу до ресурсів в електронних освітніх платформах.

Мета роботи – розробити варіант системи контролю доступу та рекомендації щодо застосування методів та засобів побудови системи контролю доступу до ресурсів в електронних освітніх платформах.

Наукові завдання:

- дослідити сутність проблеми контролю доступу до ресурсів в електронних освітніх платформах;

- проаналізувати основні підходи до контролю доступу до ресурсів в електронних освітніх платформах;

- проаналізувати існуючі рішення для контролю доступу до ресурсів в електронних освітніх платформах;

- проаналізувати методи та засоби побудови системи контролю доступу до ресурсів в електронних освітніх платформах;

- запропонувати варіант системи контролю доступу до ресурсів в електронних освітніх платформах;

- розробити рекомендації щодо застосування методів та засобів побудови

системи контролю доступу до ресурсів в електронних освітніх платформах на базі Cisco ISE.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ДО РЕСУРСІВ В ЕЛЕКТРОННИХ ОСВІТНІХ ПЛАТФОРМАХ

1.1 Аналіз проблеми системи контролю доступу в електронних освітніх платформах

Системи контролю доступу на платформах електронного навчання мають низку проблем, які можуть негативно вплинути на безпеку та ефективність навчання. По-перше, вимоги до паролів недостатньо суворі, а багатофакторна автентифікація недоступна, що може створити ризик несанкціонованого доступу до облікових записів. Хакери можуть використати цей доступ для витоку особистої інформації студентів та викладачів, зміни оцінок або впливу на навчальний процес.

Другою проблемою є відсутність гнучкості та контролю над управлінням правами доступу. Наприклад, деякі системи можуть мати обмежену здатність точно визначати, хто має доступ до яких матеріалів і функцій. Як наслідок, не всі студенти та викладачі можуть мати доступ до ресурсів, необхідних для навчання та викладання.

Крім того, погана ідентифікація та автентифікація може призвести до порушення цілісності даних. Слабкий контроль може призвести до підробки або втрати даних через несанкціонований доступ.

Нарешті, приватність і конфіденційність також важливо враховувати. Недостатні заходи безпеки можуть поставити під загрозу персональні дані учнів та вчителів і вплинути на довіру до платформи та її діяльності.

Важливо також звернути увагу на моніторинг та аналіз діяльності користувачів. Системи контролю доступу повинні мати можливість виявляти підозрілу або незвичну активність, наприклад, незвичні спроби входу, несподівані зміни прав доступу або використання облікового запису з несподіваних місць.

Аналізуючи такі дії, можна виявити потенційні загрози і вчасно відреагувати на них.

Ще однією проблемою є відсутність оновлень і патчів для систем контролю доступу. Оскільки вразливість програмного забезпечення може стати відправною точкою для кібератак, важливо, щоб системи регулярно оновлювалися, а заходи безпеки впроваджувалися вчасно.

Також важливо навчати користувачів правильному використанню систем контролю доступу та способам захисту своїх облікових записів. Це включає використання надійних паролів, запобігання доступу третіх осіб до облікових даних, не відкриття підозрілих електронних листів або посилань, своєчасну зміну паролів і перевірку оновлень системи безпеки.

Ще однією проблемою систем контролю доступу є те, що вони погано інтегровані з іншими системами безпеки та спостереження. Наприклад, якщо системи контролю доступу не інтегровані з системами виявлення вторгнень або системами аналізу журналів подій, може бути важко виявити і своєчасно відреагувати на потенційні загрози. Ефективна інтеграція цих систем призведе до вищого рівня безпеки та швидшого реагування на інциденти.

Важливо також враховувати адаптивність систем контролю доступу до мінливих вимог і загроз. Оскільки технологічне середовище постійно змінюється, системи контролю доступу повинні бути готові до впровадження нових методів і технологій безпеки та адаптації до нових типів загроз.

Також важливо мати механізм резервного копіювання та відновлення систем контролю доступу. Це гарантує швидке відновлення системи в разі збою або втрати даних.

Також слід враховувати законодавчі вимоги та стандарти безпеки, які застосовуються до освітніх установ і платформ. Дотримання відповідних стандартів безпеки допоможе уникнути юридичних проблем і забезпечить довіру користувачів до системи контролю доступу.

Ще однією проблемою, яка може виникнути в системах контролю доступу на платформах електронного навчання, є неадекватний контроль ідентифікації та автентифікації. Наприклад, якщо система не може ефективно ідентифікувати користувачів або не вимагає достатньо надійних методів автентифікації, вона може створювати ризик несанкціонованого доступу.

Іншою потенційною проблемою є неналежна обробка та захист даних під час передачі мережею. Якщо дані не зашифровані належним чином або не вжито заходів безпеки для запобігання підслуховуванню, це може призвести до витоку конфіденційної інформації.

Інша проблема полягає в тому, що програмне забезпечення для контролю доступу не оновлюється. Вразливості та помилки в програмному забезпеченні дозволяють зловмисникам атакувати системи та отримувати несанкціонований доступ.

Для вирішення цих проблем необхідно посилити заходи безпеки на різних рівнях системи контролю доступу. Це включає впровадження надійних методів ідентифікації та автентифікації, шифрування даних під час передачі, регулярне оновлення програмного забезпечення, а також використання моніторингу та аналітики для виявлення підозрілої активності.

Також важливо мати план реагування на інциденти безпеки для забезпечення надійного резервного копіювання даних, швидкого реагування на потенційні загрози та відновлення системи. Тільки комплексний підхід до безпеки систем контролю доступу може ефективно захистити інформацію на платформах електронного навчання та забезпечити безпеку користувачів.

Таким чином, аналіз проблем систем контролю доступу на платформах електронного навчання свідчить про необхідність комплексного підходу, що включає технічні, організаційні та правові аспекти безпеки. Тільки такий підхід може ефективно забезпечити безпеку даних в сучасному освітньому середовищі.

1.2 Аналіз підходів до захисту системи контролю доступу в електронних освітніх платформах

Надійні паролі та багатофакторна автентифікація є ключовими елементами захисту інформації та систем контролю доступу в електронному середовищі.

Надійні паролі містять довгі комбінації великих і малих літер, цифр і спеціальних символів. Такі паролі є більш безпечними, оскільки їх складно вгадати за допомогою грубої сили або словникових атак. Важливо також регулярно змінювати паролі та забезпечувати унікальність паролів для кожного облікового запису, щоб уникнути витоку великих обсягів даних у разі порушення безпеки.

Багатофакторна автентифікація додає додатковий рівень безпеки, вимагаючи додаткові ідентифікатори, такі як SMS-коди, електронні ключі або біометричні дані після введення основного пароля. Це ускладнює проникнення, оскільки зловмисникові потрібен доступ до другого ідентифікатора, навіть якщо він знає основний пароль.

Шифрування даних є важливим інструментом для захисту конфіденційної інформації та запобігання несанкціонованому доступу. Цей процес перетворює відкритий текст (дані) у криптографічно захищену форму, доступну лише тим, хто має відповідний ключ для розшифрування. Шифрування використовується в різних сферах, включаючи платформи електронного навчання, для забезпечення безпеки даних та уникнення загроз.

Ключові аспекти шифрування даних та захисту від несанкціонованого доступу включають наступне

Алгоритми шифрування: Існують різні алгоритми шифрування, такі як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) та DES (Data Encryption Standard). Кожен з цих алгоритмів має свої переваги та особливості, і вибір залежить від потреб і вимог безпеки конкретної системи.

Ключі шифрування: Ключі шифрування використовуються для захисту інформації та гарантують, що тільки авторизовані користувачі можуть розшифровувати дані. Важливо, щоб ключі зберігалися в безпечному місці для

забезпечення конфіденційності.

Шифрування в стані спокою: цей метод шифрування шифрує дані в пам'яті пристрою і запобігає перехопленню конфіденційних даних під час обробки.

Захист від атак типу "зловмисник посередині": шифрування даних запобігає атакам, коли зловмисник встановлює фальшиве з'єднання і перехоплює дані, що передаються між двома сторонами.

Регулярне оновлення шифрування: Оскільки методи шифрування можуть застарівати або бути вразливими до нових типів атак, важливо регулярно переглядати та оновлювати методи шифрування.

Шифрування в епоху відповідальності: це принцип, згідно з яким кожен користувач має власний ключ для шифрування та дешифрування даних і несе відповідальність за безпеку своїх даних.

Шифрування даних є важливим елементом захисту від несанкціонованого доступу, оскільки воно ускладнює доступ до конфіденційної інформації та допомагає захистити конфіденційність даних на платформах електронного навчання.

Управління правами доступу та контроль доступу до ресурсів платформи електронного навчання є надзвичайно важливими аспектами забезпечення безпеки даних та конфіденційності інформації. Ці процеси спрямовані на те, щоб кожен користувач мав доступ лише до тих ресурсів і функцій, які необхідні йому для виконання своїх завдань, і таким чином мінімізувати ризик витоку даних і несанкціонованого використання інформації.

Управління правами доступу (RBAC) дозволяє системі визначати дії, які кожен користувач може виконувати відповідно до своєї ролі. Наприклад, системний адміністратор має повний доступ до всіх функцій і ресурсів, тоді як студенти можуть мати доступ лише до навчальних матеріалів і завдань.

Контроль доступу до ресурсів вимагає встановлення правил і обмежень, які визначають, хто, коли і як може отримати доступ до певних даних і функцій. Наприклад, доступ до персональних даних учнів або важливих адміністративних ресурсів може бути обмежений для певних груп користувачів. Для забезпечення

безпеки даних також використовуються методи шифрування. Шифрування даних у стані спокою допомагає захистити інформацію, поки вона зберігається на сервері. Цей метод ускладнює доступ до даних, навіть якщо є фізичний доступ до сервера. Також важливо централізувати та автоматизувати процеси управління правами доступу та контролю доступу. Це дозволяє управляти доступом централізовано та ефективно, а також швидко реагувати на зміни в правах користувачів та вимогах безпеки. Такі заходи допомагають підвищити рівень безпеки та забезпечити довіру користувачів до платформи.

Моніторинг та аналіз дій користувачів є важливим аспектом кібербезпеки, особливо в контексті платформ електронного навчання. Ці процеси спрямовані на виявлення, моніторинг та аналіз дій користувачів у системі для виявлення підозрілих або несанкціонованих дій.

Моніторинг дій користувачів передбачає відстеження вхідних і вихідних дій кожного користувача, таких як вхід в систему, зміна прав доступу, перегляд і редагування даних, завантаження файлів. Цей процес дозволяє відстежувати зміни в поведінці користувачів і своєчасно реагувати на незвичну або підозрілу активність.

Аналіз поведінки користувачів передбачає використання спеціальних інструментів і алгоритмів для виявлення незвичної або потенційно небезпечної поведінки користувачів. Сюди входить виявлення надмірної кількості спроб входу з однієї IP-адреси, незвичних запитів до сервера та змін у моделях поведінки користувачів. Аналіз даних може допомогти виявити потенційні загрози безпеці та запобігти можливим кібератакам і витоку даних.

Моніторинг та аналіз дій користувачів на платформах електронного навчання має важливе значення для забезпечення безпеки та конфіденційності даних. Ці процеси допомагають своєчасно виявляти та реагувати на потенційні загрози, знижують ризик інцидентів та підвищують довіру користувачів до платформи.

1.3 Аналіз існуючих рішень із захисту системи контролю доступу в електронних освітніх платформах

Рис. 1 – Рішення із захисту системи контроля доступу

Аналіз існуючих технологій автентифікації в контексті платформ електронного навчання відображає важливість захисту доступу до систем і даних у навчальному середовищі. Технології автентифікації є важливим елементом безпеки, оскільки вони визначають, як користувачі підтверджують свою особу при вході в систему.

Однією з основних технологій автентифікації є багатофакторна автентифікація (MFA), яка використовує кілька різних методів для підтвердження особи, включаючи паролі та коди, що надсилаються на мобільні телефони. Ця технологія забезпечує додатковий рівень безпеки, оскільки зловмисник повинен зробити кілька кроків, щоб отримати доступ.

Біометрія - ще один поширений метод, який використовує унікальні фізичні характеристики користувача, такі як відбитки пальців, розпізнавання обличчя або голосу. Це знижує ризик перехоплення пароля і доступу через втрату або

компрометацію облікових даних.

Важливо інтегрувати ці технології з існуючими системами, щоб забезпечити високий рівень захисту конфіденційної інформації, такої як персональні дані студентів та викладачів, особливо на платформах електронного навчання. Враховуючи динамічний характер кіберзагроз, важливо постійно оновлювати технології автентифікації та впроваджувати нові методи і механізми захисту, щоб відповідати викликам сучасної кібербезпеки.

Аналіз існуючих систем управління правами доступу на платформах електронного навчання є важливим кроком на шляху до забезпечення безпеки та конфіденційності даних. Система управління правами доступу (СУПД) визначає, до яких дій та ресурсів кожен користувач може отримати доступ у системі залежно від своєї ролі та прав. Основна мета такої системи - гарантувати принцип найменших привілеїв, тобто надати користувачам лише ті права, які їм потрібні для виконання їхніх завдань.

LMS дозволяє адміністраторам налаштовувати, керувати та контролювати доступ до різних ресурсів, таких як навчальні матеріали, бази даних та персональні дані користувачів. Це реалізується за допомогою різних інструментів і механізмів, включаючи RBAC (контроль доступу на основі ролей), ABAC (контроль доступу на основі атрибутів) і DAC (дискреційний контроль доступу). Кожен з цих підходів має свої переваги та особливості, залежно від характеристик системи та потреб користувачів.

Наприклад, RBAC базується на призначенні ролей (наприклад, студент, викладач, адміністратор) з відповідними правами доступу. Такий підхід дозволяє ефективно управляти правами доступу та забезпечує легку масштабованість при зміні ролей користувачів. ABAC, з іншого боку, базується на атрибутах користувача, ресурсу та середовища і дозволяє більш гнучко конфігурувати правила доступу.

Важливим компонентом RMS є механізм аудиту та ведення журналів, який дозволяє відстежувати та аналізувати дії користувачів у системі. Це гарантує своєчасне виявлення потенційних загроз безпеці та реагування на них.

Інші методи управління правами доступу включають дискреційне управління доступом (DAC), обов'язкове управління доступом (MAC) та гібридні підходи, що поєднують різні елементи цих методів. DAC дозволяє власникам ресурсів визначати права доступу до своїх об'єктів і є корисним для створення індивідуальних правил доступу в навчальному середовищі. MAC базується на класифікації ресурсів та визначенні їхнього рівня конфіденційності та безпеки, що робить його ідеальним для середовищ з високим рівнем безпеки.

Системи моніторингу та аналізу активності користувачів на платформах електронного навчання важливі для забезпечення безпеки та виявлення потенційних загроз. Розглянемо кожну з них детальніше.

Внутрішні системи безпеки є ключовими для моніторингу та контролю дій користувачів у системі. Мережевий трафік, журнали подій та інші джерела інформації аналізуються для виявлення аномалій і підозрілих дій. Ці системи можуть виявляти незвичні обсяги даних, неочікувані з'єднання або інші ознаки можливих вторгнень.

Системи виявлення вторгнень (IDS) призначені для виявлення підозрілої або зловмисної активності в системі. Вони аналізують пакети даних, сигнали або журнали, щоб виявити зміни в мережевому трафіку, які можуть свідчити про потенційні загрози безпеці; IDS використовують різні методи для виявлення вторгнень, включаючи аналіз сигнатур, аналіз змін у поведінці та інші методи.

Системи виявлення вторгнень в режимі реального часу працюють в режимі суворого моніторингу мережі та користувачів. Вони миттєво реагують на події, аналізують потоки даних і швидко реагують на підозрілу або неочікувану активність.

Система аналізу безпеки використовує аналітичні методи для обробки великих обсягів даних і виявлення змін у моделях поведінки користувачів і сигналів, які вказують на потенційну загрозу безпеці. Виявляючи незвичні моделі активності та ризики, можна вчасно відреагувати на потенційні загрози.

Система управління інцидентами (SIEM) поєднує в собі моніторинг, аналіз та управління інцидентами для забезпечення безпеки та виявлення вразливостей.

Це дозволяє виявляти, класифікувати та реагувати на події, які можуть вплинути на безпеку системи.

Інструменти аналізу логів використовуються для аналізу та моніторингу журналів подій, що містять інформацію про активність користувачів, входи в систему, зміни прав доступу тощо. Це дає можливість виявляти неочікувані дії та аналізувати події для покращення безпеки та управління правами доступу.

AI/ML системи безпеки використовують алгоритми штучного інтелекту та машинного навчання для виявлення аномалій і прогнозування потенційних загроз безпеці. Вони навчаються на історичних даних і аналізують поведінку користувачів, щоб виявити аномалії, які вказують на потенційні загрози.

Кожна з цих систем має свої унікальні переваги та особливості, а разом вони забезпечують комплексний підхід до моніторингу та аналізу активності користувачів на платформах електронного навчання.

Шифрування даних є важливим аспектом безпеки на платформах електронного навчання. Цей процес використовується для захисту інформації від несанкціонованого доступу шляхом перетворення конфіденційних даних у формат, який можуть прочитати лише люди з відповідними правами доступу. Найпоширенішими алгоритмами шифрування є Advanced Encryption Standard (AES) та Rivest-Shamir-Adleman (RSA). Дані можуть бути зашифровані як у стані спокою (під час зберігання), так і в дорозі (під час передачі мережею), що гарантує захист інформації незалежно від її стану.

Протоколи транспортної безпеки, такі як Transport Layer Security (TLS) і Secure Sockets Layer (SSL), відіграють важливу роль у забезпеченні безпечної передачі даних між користувачами і серверами. TLS і SSL використовують технологію шифрування для передачі даних і зменшують ризик перехоплення конфіденційної інформації під час її передачі мережею.

Механізми контролю доступу включають автентифікацію та авторизацію, які перевіряють особу користувачів і надають їм відповідні права доступу до ресурсів. Аутентифікація використовує імена користувачів, паролі та біометричні дані для перевірки особи користувача, тоді як авторизація визначає, які дії користувач може

виконувати після аутентифікації.

Шифрування на рівні файлів і баз даних забезпечує додатковий рівень захисту конфіденційних даних. Це означає, що навіть якщо зловмисник отримає доступ до системи або файлів, дані будуть збережені в зашифрованому вигляді. Такий підхід забезпечує безпеку інформації навіть у разі втрати контролю над інфраструктурою.

Інші заходи безпеки включають використання технології багатофакторної автентифікації (MFA). Вона вимагає, щоб користувачі надавали кілька ідентифікаційних даних для доступу до системи. Це може включати те, що користувач знає (пароль), те, що він має (токен) і його власні характеристики (біометричні дані), що забезпечує вищий рівень безпеки.

Крім того, системи, які відстежують і аналізують поведінку користувачів, можуть виявляти підозрілу поведінку і незвичайні ситуації, що дозволяє швидко реагувати на потенційні загрози і захищати платформу в цілому.

Системи виявлення вторгнень (IDS) у сфері платформ електронного навчання призначені для виявлення, аналізу та реагування на зловмисні або незаконні дії, які можуть поставити під загрозу безпеку системи. Для досягнення цієї мети можуть використовуватися різні методи і підходи.

По-перше, системи аналізу сигнатур - один з найпоширеніших типів IDS. Вони використовують базу даних відомих сигнатур атак, які містять типові шаблони підозрілої активності та аномалії, що можуть бути пов'язані з вторгненням. Аналізуючи мережевий трафік або системну активність, система порівнює спостережувану активність з відомими сигнатурами і сповіщає або реагує, коли є збіг.

Крім того, системи аналізу поведінки є ще одним важливим типом IDS. Вони не обмежуються відомими сигнатурами атак, а розглядають звичайні моделі поведінки систем і користувачів. Якщо виявлено аномальну поведінку, яка не відповідає цим шаблонам, система може спровокувати її як підозрілу поведінку.

Крім того, системи виявлення аномалій спеціалізуються на пошуку відхилень від типових моделей поведінки та діяльності, які вказують на можливу загрозу.

Вони аналізують інформацію та події, щоб виявити незвичні або підозрілі зміни, які можуть бути пов'язані з вторгненнями або атаками.

Крім того, існують системи виявлення вторгнень у режимі реального часу, які працюють у режимі пильного спостереження. Ці системи миттєво відстежують дії та події і негайно реагують на підозрілі дії. Це дозволяє негайно виявляти потенційні загрози та реагувати на них, мінімізуючи час між виявленням та реагуванням.

Також можна розглянути системи виявлення вторгнень на рівні додатків. Ці системи спеціалізуються на виявленні аномальної поведінки програмного забезпечення та вразливостей, які можуть бути використані для атак або зловмисної діяльності. Вони аналізують взаємодію додатків і виявляють підозрілі зміни у функціональності додатків, які вказують на потенційне вторгнення або атаку.

Системи виявлення вторгнень на рівні хостів - ще один важливий аспект системної безпеки. Вони аналізують дії та події на конкретних комп'ютерах і серверах, щоб виявити незвичні дії або підозрілу активність, які вказують на можливе вторгнення на рівні хоста. Сюди входить моніторинг системних журналів, спостереження за активністю користувачів та інші показники, які можуть вказувати на шахрайство або підозрілу діяльність.

Нарешті, існують комплексні системи виявлення вторгнень, які поєднують різні підходи і технології для забезпечення максимального захисту. Ці системи використовують поєднання сигнатурного аналізу, поведінкового аналізу, аналізу аномалій, роботи в режимі реального часу та інших методів для виявлення та реагування на різні типи загроз і вторгнень.

Загалом, різні системи виявлення вторгнень мають свої переваги та особливості і можуть використовуватися разом для досягнення ефективного рівня захисту платформ електронного навчання. Це стає важливим аспектом забезпечення безпеки та надійності віртуальних навчальних середовищ, особливо в умовах зростання кількості атак і загроз у цій сфері.

Аналіз та оцінка ризиків в контексті платформ електронного навчання є

важливим кроком у забезпеченні безпеки та надійності системи. Для цього використовуються різні методи аналізу ризиків, а також стратегії мінімізації ризиків.

Важливим методом аналізу ризиків є виявлення потенційних загроз і вразливостей системи. Це включає визначення можливих атак, слабких місць у системі безпеки та потенційних проблем з доступом до даних і конфіденційністю. Після виявлення ризиків оцінюється їхній вплив та ймовірність виникнення, щоб визначити найбільш серйозні та небезпечні сценарії.

Потім розробляються стратегії зниження ризиків, щоб зменшити ймовірність настання небажаних подій і пом'якшити їхній вплив. Однією з таких стратегій є впровадження ефективних систем безпеки, таких як антивірусне програмне забезпечення, брандмауери та системи виявлення вторгнень. Ці системи можуть допомогти виявити і запобігти зловмисній або небезпечній діяльності в режимі реального часу.

Іншою важливою стратегією є регулярне оновлення та обслуговування програмного та апаратного забезпечення, що використовується на платформі. Це включає встановлення оновлень безпеки, виправлення вразливостей та належне налаштування систем для мінімізації ризиків.

Ще одним важливим аспектом є навчання та інформування користувачів про методи безпеки. Сюди входить навчання створенню надійних паролів, обізнаність про атаки соціальної інженерії та застосування принципів безпеки при використанні платформи.

Загалом, аналіз і оцінка ризиків та впровадження стратегій для їх мінімізації є важливими елементами для забезпечення безпеки та надійності платформи електронного навчання. Ефективна реалізація цих стратегій може запобігти потенційним загрозам і забезпечити безпечне та надійне середовище для користувачів платформи.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ДОСТУПУ ДО РЕСУРСІВ НА БАЗІ CISCO ISE

2.1 Архітектура та основні компоненти Cisco ISE

Cisco Identity Services Engine (ISE) - це інтегрована платформа управління доступом до мережі та безпеки, розроблена Cisco Systems. Система дозволяє організаціям централізовано контролювати, хто і як може підключатися до мережевих ресурсів, незалежно від того, чи використовується для цієї мети Дротове, бездротове або VPN-з'єднання. Основою роботи Cisco ISE є ідентифікація, аутентифікація і система користувачів і пристроїв, які надають доступ до мережевих ресурсів відповідно до певної політики безпеки, а система аналізує різні атрибути підключення, такі як ідентифікатор користувача, тип пристрою, місце розташування. та інші контекстні дані, щоб визначити, чи слід надавати чи відхиляти доступ. Крім того, Cisco ISE дозволяє створювати детальні політики доступу, які можна адаптувати в режимі реального часу на основі змін стану мережі та поведінки користувачів. Ключовою особливістю Cisco ISE є те, що вона включає інші системи безпеки та компоненти інфраструктури, такі як Active Directory, різні сервери LDAP, мережеві пристрої Cisco та інші виробники. Система також включає потужні інструменти для моніторингу та аналізу мережевої активності, щоб допомогти організаціям виявляти потенційні загрози в режимі реального часу. Використовуючи Cisco ISE, організації можуть значно підвищити рівень безпеки своєї мережевої інфраструктури, забезпечити надійний захист від несанкціонованого доступу та інших кіберзагроз, а також оптимізувати процеси контролю доступу для підвищення загальної ефективності мережі.

Використання Cisco Identity Services Engine (ISE) надає багато переваг організаціям, які прагнуть забезпечити високий рівень безпеки та ефективності своєї мережевої інфраструктури. Однією з ключових переваг є централізоване управління доступом до мережевих ресурсів, що дозволяє адміністраторам легко створювати, застосовувати та змінювати політику безпеки користувачів та пристроїв, що допомагає зменшити складність та покращити керованість мережею.

Cisco ISE забезпечує всебічну ідентифікацію та автентифікацію користувачів за допомогою різних методів, включаючи 802.1 x, обхід автентифікації Mac (MAB) та WebAuth. Це дозволяє організаціям ефективно контролювати доступ до мережі та зменшує ризики, пов'язані з несанкціонованим доступом. Крім того, система може підвищити гнучкість та безпеку мережі, адаптивно застосовуючи контекстну політику безпеки, таку як місцезнаходження Користувача, тип пристрою та час.

Інтегруючи Cisco ISE з іншими системами безпеки, такими як Active Directory, системи інформації про безпеку та управління інцидентами (SIEM) та інші інструменти управління, система також забезпечує детальний моніторинг та звітність про мережеву активність, допомагаючи виявляти аномальні дії та потенційні загрози в режимі реального часу. Це дозволяє адміністраторам швидко реагувати на інциденти безпеки та мінімізувати вплив на організацію.

Крім того, використання Cisco ISE полегшує дотримання нормативних вимог і стандартів безпеки, які мають вирішальне значення в багатьох галузях жовтня, особливо в умовах зростаючого числа регулюючих органів із захисту даних. Система підтримує автоматизацію процесу контролю доступу, знижує адміністративні витрати і підвищує продуктивність IT-персоналу.

Загалом, Cisco ISE надає організаціям потужні інструменти управління та безпеки мережі, які допомагають зменшити ризики, підвищити безпеку та оптимізувати операційні процеси.

Компонентна структура Cisco Identity Services Engine (ISE) включає в себе кілька ключових елементів, кожен з яких виконує певні функції, а комплексне управління доступом і мережева безпека ключовим компонентом є вузол управління (PAN), який забезпечує централізоване управління і настройку всієї системи ISE. Цей вузол дозволяє адміністраторам створювати та керувати політикою безпеки, аутентифікувати та авторизувати користувачів, а також інтегрувати системи з іншими компонентами інфраструктури.

Центр обслуговування політики (PSN) є ще одним важливим елементом структури Cisco ISE відповідає за обробку запитів на доступ, автентифікацію, авторизацію та виконання функцій пристрою та профілювання користувачів. PSN

оцінює відповідність підключених пристроїв політикам безпеки, дозволяючи або обмежуючи доступ залежно від зазначених умов. Цей вузол також оцінює стан пристроїв, підключених до мережі, щоб переконатися, що вони відповідають вимогам безпеки.

Вузол моніторингу та усунення несправностей (MnT) виконує функції збору, зберігання та аналізу журналів та подій, що відбуваються в системі. Цей компонент дозволяє системі ISE відстежувати її продуктивність і працездатність, а також надає адміністраторам детальну інформацію про мережеву активність і потенційні загрози. Завдяки цьому вузлу організації можуть ефективно відстежувати аномалії та швидко реагувати на інциденти безпеки.

Іншим важливим елементом декомунізації є вузол pxGrid, який забезпечує обмін даними між ISE та іншими системами безпеки.1 Цей компонент дозволяє ISE інтегруватися з різними сторонніми рішеннями, включаючи системи виявлення загроз, SIEM та інші інструменти кібербезпеки. pxGrid забезпечує контекстну передачу даних, покращує координацію між декомунізованими системами безпеки і підвищує загальний рівень захисту мережі.

Компонентна структура Cisco ISE розроблена для забезпечення високої масштабованості і надійності системи. Кожен вузол може бути розгорнутий в різних режимах, включаючи розподілену архітектуру, яка дозволяє адаптувати систему до конкретних потреб організації. Ця архітектура забезпечує ефективне управління доступом і безпекою, що дозволяє організаціям забезпечувати високий рівень захисту своїх мережевих ресурсів.

Архітектура розгортання Cisco Identity Services Engine (ISE) може бути реалізована в 2 основних варіантах: незалежному і розподіленому.

В Автономній архітектурі всі функції Cisco ISE зосереджені на одному фізичному або віртуальному сервері. Це означає, що ролі вузла управління (PAN), вузла обслуговування політики (PSN) та вузла моніторингу та усунення несправностей (MnT) виконуються в одній установці Cisco ISE. Цей підхід полегшує розгортання та адміністрування системи, оскільки всі компоненти розміщені на одному вузлі, що забезпечує централізоване адміністрування та

просту конфігурацію. Автономна Архітектура підходить для малих і середніх організацій з відносно низьким мережевим трафіком і відносно невеликою кількістю користувачів. У той же час, оскільки вся система підключена до одного сервера, цей підхід може мати обмежену масштабованість та Надмірність.

І навпаки, розподілена Архітектура передбачає декомунізацію функціональності Cisco ISE між декількома вузлами, що значно підвищує продуктивність, масштабованість і надійність системи. У цьому випадку різні ролі, такі як PAN, PSN та MNT, виконуються окремими серверами або віртуальними машинами. Наприклад, 1 або більше серверів можуть функціонувати як вузли служби політики, які обробляють запити на автентифікацію та авторизацію, тоді як інші сервери можуть бути зарезервовані для адміністрування та моніторингу. Декомунізована архітектура забезпечує балансування навантаження між вузлами, забезпечує більший обсяг запитів і більш високу продуктивність навіть у великих мережах з великою кількістю користувачів і пристроїв. Крім того, розподілена Архітектура підвищує надійність і відмовостійкість системи, оскільки відмова 1 вузла не призводить до відключення всієї системи. Підвищує продуктивність системи.

Розподілені розгортання також дозволяють географічно розподіляти вузли для оптимізації продуктивності та забезпечення безперебійного доступу до мережі в різних регіонах. Цей підхід особливо корисний для великої кількості віддалених офісів та великих організацій з великими структурами, які повинні забезпечити ефективний доступ та управління безпекою для користувачів.

Загалом, вибір автономних та розподілених архітектур розгортання Cisco ISE залежить від розміру організації, вимог до продуктивності та надійності та підтримки системи, тоді як автономні архітектури простіші та економічніші в менших організаціях, а розподілені архітектури забезпечують високий рівень масштабованості, необхідний для великих мережевих середовищ. Забезпечує гнучкість і відмовостійкість.

Політики та профілі в Cisco ISE

- Типи політик (Authentication, Authorization, Profiling)
- Процес створення та застосування політик
- Профілі користувачів та пристроїв

Cisco ISE надає різні типи політик, які визначають правила та параметри безпеки для користувачів та пристроїв, підключених до мережі. 3 основні типи політик, що використовуються для забезпечення безпеки та контролю доступу до декомунізації, включають політику автентифікації, авторизації та профілювання.

Політика перевірки автентичності: ці політики визначають правила та методи, за допомогою яких користувачі та пристрої проходять автентифікацію в мережі. Сюди входять налаштування параметрів автентифікації, таких як методи (наприклад, 802.1 X, автентифікація Mac) та правила автентифікації ідентифікаційних даних, що використовуються для доступу до мережевих ресурсів.

Політика авторизації: ці політики визначають правила та умови, які вимагають від користувачів та пристроїв доступу до певних мережевих ресурсів після успішної автентифікації. Сюди входять обмеження прав доступу на основі ролей користувачів, визначень груп доступу та атрибутів контексту (таких як час, місцезнаходження та тип пристрою).

Політика профілювання: ці політики визначають правила та процеси ідентифікації та класифікації пристроїв, підключених до мережі, на основі їх ефективності та характеристик. Обмеження доступу можна задати в залежності від типу пристрою, власника, типу пристрою та інших заходів безпеки parameters.It це допомагає керувати мережевою безпекою та захищати від несанкціонованого доступу.

Ці 3 типи політик взаємодіють в Cisco ISE для ефективного управління доступом і забезпечення надійного захисту інформації та мережевих ресурсів.

Процес створення і застосування політик в системі Cisco ISE являє собою складний процес, що включає кілька етапів, спрямованих на визначення правил і умов контролю доступу і мережевої безпеки. Початок цього процесу, як правило, визначається потребами організації у захисті мережі та встановленні стандартів безпеки.

Першим кроком є визначення вимог політики безпеки. Це включає в себе аналіз потреб мережі, виявлення потенційних загроз і ризиків, а також визначення прав доступу для різних користувачів і пристроїв. На цьому етапі важливо враховувати внутрішню політику безпеки Організації, добре відомі стандарти організації безпеки та вимоги Законів Про захист даних.

2 крок полягає в тому, щоб встановити певну політику безпеки в Cisco ISE. Це включає налаштування параметрів автентифікації, визначення прав доступу, ролей користувачів, груп доступу та інших умов, що використовуються для прийняття рішень щодо доступу до мережевих ресурсів. Це враховує контекстні атрибути, такі як час підключення, тип пристрою та місце підключення.

Третій крок-перевірити та перевірити правильність вашої політики безпеки. Це включає моделювання різних сценаріїв, аудит політики, перевірку взаємодії з іншими системами безпеки та мережевими пристроями та аналіз журналів подій.

Останній етап-впровадження та застосування політик, створених у вашому робочому середовищі. Це включає Налаштування Cisco ISE для використання створених політик, публікацію та включення їх для контролю доступу та безпеки в режимі реального часу.

Загалом, процес розробки та впровадження політики в Cisco ISE є послідовним та впорядкованим підходом до визначення, розробки, тестування та впровадження правил безпеки для забезпечення надійного захисту мережі та даних вашої організації.

Профілі користувачів та пристроїв Cisco ISE використовуються для налаштування мережі на основі контекстної інформації про користувачів та пристрої, зібраної та проаналізованої системою.

Профілювання користувачів включає ідентифікацію та аналіз властивостей користувачів, таких як рівні доступу, ролі, членство в певних групах та інші атрибути, які впливають на можливість доступу до мережевих ресурсів. Цю інформацію можна використовувати для налаштування правил доступу та політики безпеки, що відповідають контекстним властивостям користувача.

Що стосується профілювання пристроїв, Cisco ISE ідентифікує та класифікує пристрої на основі характеристик пристроїв, включаючи тип, модель, операційну систему, обладнання, сертифікати та програмне забезпечення пристроїв, підключених до мережі, та надає відповідну інформацію про доступ та безпеку для кожного типу пристроїв. Перевірте правила

Профілі користувачів і профілі пристроїв в Cisco ISE використовуються для створення контекстної безпеки, а правила і політики доступу визначаються не тільки ідентифікацією, а й аналізом контекстної інформації. Це забезпечує більш гнучкий та ефективний захист мережі для конкретних умов та потреб вашої організації.

Інтеграція з іншими технологіями

- Інтеграція з Active Directory та іншими LDAP серверами
- Взаємодія з мережевими пристроями (Cisco та інших виробників)
- Використання API та pxGrid для розширення функціоналу

Інтеграція Cisco ISE з Active Directory та іншими серверами LDAP є ключовим елементом ефективного контролю доступу та безпеки в мережевому середовищі. 1. Active Directory є одним з найпоширеніших каталогів ідентифікації користувачів та адміністрування в корпоративному середовищі, і сервери LDAP (простий протокол доступу до каталогів) часто відіграють важливу роль у цьому процесі.

Під час інтеграції Cisco ISE взаємодіє з Active Directory або іншими серверами LDAP для визначення політики безпеки та отримання інформації про користувачів,

групи, дозволи та інші атрибути, необхідні для управління доступом до мережевих ресурсів. Це означає, що інформація, що зберігається в Active Directory або на інших серверах LDAP, використовується для автентифікації користувачів, визначення їх прав доступу та включення їх до певних груп користувачів.

Однією з ключових переваг інтеграції з Active Directory є зручність та централізація управління користувачами та їх правами. Cisco ISE може підвищити ефективність і безпеку процесу управління користувачами, автоматично оновлюючи інформацію про користувачів з Active Directory. Крім того, інтеграція з іншими серверами ldap покращує здатність Cisco ISE використовувати різні ресурси для забезпечення безпеки та управління доступом

Цей процес інтеграції забезпечує надійну та узгоджену інтеграцію між Cisco ISE та існуючими системами ідентифікації та управління, що дозволяє системі задовольняти потреби конкретної організації.

Взаємодія з мережевими пристроями є важливим аспектом системи Cisco ISE (інфраструктура служб ідентифікації) і забезпечує ефективний контроль доступу і політики безпеки в мережевому середовищі. Оскільки Cisco ISE взаємодіє як з власними мережевими пристроями Cisco, так і з пристроями інших виробників, вона забезпечує гнучкість і масштабованість в управлінні мережевою безпекою.

Перш за все, Cisco ISE інтегрується з мережевими пристроями Cisco, такими як Маршрутизатори та комутатори, щоб забезпечити розширений контроль доступу та захист через мережу. Це пов'язано з тим, що Cisco ISE використовує інформацію, отриману з цих пристроїв, для визначення прав доступу, забезпечення дотримання політик безпеки та обмеження мережевого шахрайства.

Крім того, оскільки Cisco ISE підтримує стандарти протоколів, такі як RADIUS (служба віддаленого доступу користувачів з віддаленою аутентифікацією) і TACACS + (система контролю доступу з контролером доступу до терміналу плюс), пристрої інших виробників, що підтримують ці протоколи, можуть бути розгорнуті в різних мережевих середовищах незалежно від виробника обладнання. Він стає інструментом контролю доступу.

В цілому, взаємодія з мережевими пристроями в Cisco ISE може підвищити

рівень безпеки і ефективність контролю доступу до мережевих ресурсів, включаючи інтеграцію і сумісність з різними типами пристроїв власного виробництва та інших виробників Cisco, а також стандартизовані процеси для забезпечення розширених можливостей управління мережею. Це досягається за рахунок використання протоколу.

Використання інтерфейсу прикладного програмування (API) і сітки обміну платформами (Pxgrid) є важливим фактором для розширення можливостей Cisco ISE (інфраструктура служб ідентифікації) і підвищення її ефективності в управлінні мережевою безпекою. API забезпечує інтерфейс для програмної взаємодії з Cisco ISE і дозволяє створювати, розгортати та автоматизувати різні завдання безпеки. PxGrid - це механізм обміну даними та співпраці між декомунізацією Cisco ISE та іншими продуктами безпеки.

За допомогою цього API Cisco ISE може інтегруватися з іншими системами безпеки та мережевими пристроями для розширення можливостей контролю доступу та політики безпеки. Завдяки API можна автоматизувати процеси, створювати власні програми та інтеграції, сприяючи більш гнучкому та ефективному управлінню безпекою в мережі. Буде.

pxGrid забезпечує обмін контекстною інформацією в реальному часі між Cisco ise деки та іншими продуктами безпеки. Оскільки pxGrid використовується для передачі даних користувачів, пристроїв, загроз та інших засобів захисту для прийняття рішень та реагування на загрози через мережу, Cisco ISE стає центральним елементом екосистеми мережевої безпеки шляхом координації та синхронізації заходів безпеки між декомунізованими продуктами та системами.

Таким чином, за допомогою API і pxGrid ви можете розширити можливості Cisco ISE, щоб забезпечити більш гнучкий і автоматизований процес управління мережевою безпекою і підвищити безпеку мережі.

2.2 Призначення та основні функції компонентів Cisco ISE

Cisco ISE (identity Services Engine) - це інтегрована система безпеки, яка використовується для централізованого управління доступом до мережевих ресурсів. Основною метою Cisco ISE є підвищення безпеки мережі шляхом перевірки, надання та контролю доступу до користувачів та пристроїв, підключених до мережі.

Ця система дозволяє адміністраторам створювати та застосовувати політику безпеки на рівні користувачів, пристроїв та мережевих ресурсів. Ви можете використовувати контекстні дані, такі як ідентифікатор користувача, тип пристрою, час підключення та інші атрибути, щоб надати інформацію про дозвіл або обмеження доступу до мережевих ресурсів.

Крім того, Cisco ISE може впроваджувати різні методи аутентифікації, включаючи аутентифікацію 802.1 X і MAC, яка забезпечує гнучкість управління доступом і захист мережі від несанкціонованого доступу та інших загроз безпеці.

Основні компоненти Cisco ISE

- Policy Service Node (PSN)
    - Функції та роль PSN
    - Обробка запитів на аутентифікацію та авторизацію
- Monitoring and Troubleshooting Node (MnT)
    - Збір та аналіз логів
    - Моніторинг продуктивності та вирішення проблем
- Administration Node (PAN)
    - Централізоване управління та налаштування
    - Створення та управління політиками безпеки
- pxGrid Node
    - Інтеграція та обмін інформацією з іншими системами безпеки
    - Роль в контекстуальному обміні даними

У системах Cisco Identity Services Engine (ISE) вузол служби політики (PSN) отримує доступ до мережевих ресурсів, застосовуючи можливості автентифікації,

авторизації та профілювання для користувачів та пристроїв. PSN-це вузол, який безпосередньо обробляє запити на доступ до мережі за допомогою політик безпеки, визначених адміністраторами через вузол адміністрування (PAN). Цей компонент аналізує контекстні запити, такі як ідентифікатор користувача, тип пристрою, місцезнаходження та інші атрибути, а потім оновлює додаток відповідно до встановлених політик.

Функція PSN включає кілька важливих аспектів. По-перше, він автентифікує користувачів та пристрої, перевіряючи їх облікові дані та визначаючи, чи відповідають вони вимогам безпеки. Це може включати такі методи автентифікації, як 802.1 x, обхідний шлях автентифікації Mac (MAB) та WebAuth. Потім PSN здійснює авторизацію, застосовуючи політику доступу, яка визначає, які ресурси та послуги будуть доступні певному користувачеві чи пристрою після успішної автентифікації. Політики можуть бути створені з урахуванням різних контекстуальних факторів, які забезпечують гнучкість і динамічність контролю доступу.

Крім того, PSN відповідає за профілювання пристрою, визначення типу підключеного пристрою та дотримання відповідних політик безпеки. Це корпоративні пристрої, гостьові пристрої, пристрої Інтернет речей і т.д. Це дозволяє розрізняти Дека і диякон. і забезпечте правильний рівень доступу та безпеки. PSN також оцінює стан пристрою та перевіряє його відповідність політиці безпеки, перш ніж дозволити доступ до мережі. Цей процес, який називається оцінкою простою, допомагає виявляти та ізолювати пристрої, які не відповідають вимогам безпеки, тим самим зменшуючи мережевий ризик.

Ізоляція функціональності PSN на декількох вузлах в розподіленій архітектурі Cisco ISE забезпечує високу масштабованість і надійність системи. Це дозволяє балансуванню навантаження між вузлами обробляти велику кількість запитів на доступ одночасно і забезпечує високий рівень продуктивності. Декомунізація дозволяє виконувати балансування навантаження між вузлами для одночасної обробки великої кількості запитів на доступ і забезпечує високий рівень продуктивності. Взаємодія Psn з PAN та іншими компонентами ISE, такими як

вузол моніторингу та усунення несправностей (MnT), забезпечує координацію та узгодженість політики безпеки в мережі.

В цілому вузли служби політик допомагають організаціям ефективно управляти доступом до мережевих ресурсів, підвищувати безпеку і знижувати ризики, пов'язані з несанкціонованим доступом.

Вузол моніторингу та усунення несправностей (MnT) у системах Cisco Identity Services Engine (ISE) є критичним компонентом, призначеним для забезпечення збору, зберігання та аналізу журналів та подій, що відбуваються у вашій мережі. Його функції включають моніторинг стану системи та її елементів, а також виявлення аномалій, виявлення потенційних загроз та надання адміністраторам інструментів для вирішення проблем.

MnT дозволяє накопичувати Історичні дані про мережеву активність і взаємодії користувачів і пристроїв з системою Cisco ISE. Сюди входять журнали автентифікації, авторизації, профілювання, а також інформація про зміни політики безпеки та події безпеки. Зберігаючи ці дані, ви можете аналізувати тенденції, виявляти аномалії та створювати звіти для перевірок безпеки та звітів.

Основною функцією mnt є виявлення проблем та аномалій у мережі та системі безпеки. Проаналізуйте активність та поведінку користувача та пристрою, щоб знайти ознаки порушень безпеки, збоїв або збоїв конфігурації. Наприклад, Mnt може виявити надмірну кількість невдалих спроб автентифікації, що може свідчити про спробу несанкціонованого доступу. Виявляючи такі ситуації, адміністратори можуть своєчасно реагувати і вживати заходів для захисту мережі.

Крім того, MnT надає аналіз поведінки системи та її компонентів, допомагаючи визначити продуктивність, виявити проблеми та визначити можливі точки вразливості в системі. Це важливо для запобігання проблемам та забезпечення стабільності та ефективності Cisco ISE.

Нарешті, MnT надає інструменти для вирішення проблем та інцидентів безпеки. Це включає швидке виявлення та усунення проблем, відновлення систем після збоїв та допомогу адміністраторам у прийнятті правильних рішень для забезпечення безпеки мережі.

Таким чином, вузол моніторингу та усунення несправностей (MnT) відіграє ключову роль у забезпеченні ефективного моніторингу, аналізу та усунення несправностей системних проблем Cisco ISE та забезпечує високий рівень мережевої безпеки.

Вузол управління (PAN) в системі Cisco Identity Services Engine (ISE) є центральним вузлом, відповідальним за централізоване адміністрування та адміністрування всієї інфраструктури мережевої безпеки. Основна функція Pan-надати адміністраторам доступ до загальних політик конфігурації та безпеки, а також керувати конфігурацією всіх компонентів системи ISE.

PAN відповідає за створення, редагування та виконання політик безпеки, які визначають правила доступу до мережевих ресурсів для користувачів та пристроїв. Ці політики можуть бути в контексті, який враховує основи прийняття рішень щодо доступу, загальні налаштування правил доступу або різні атрибути користувачів та пристроїв. PAN також керує розгортанням цих політик на інших вузлах системи, таких як вузли служби політики (PSN), щоб забезпечити реалізацію та синхронізацію через мережу.

Крім того, адміністративний вузол відповідає за управління користувачами, ролями та правами доступу до системи Cisco ISE. Це дає адміністраторам та користувачам відповідні дозволи на створення та керування обліковими записами відповідно до їхніх обов'язків та обов'язків, а також на доступ до функцій системи.

Однією з ключових особливостей Pan є надійна інтеграція Cisco ISE з іншими системами безпеки та мережевими пристроями за допомогою різних протоколів та інтерфейсів. Це дозволяє створювати складні та інтегровані рішення для управління безпекою та захисту мережі.

Таким чином, вузол управління відіграє важливу роль у централізованому адмініструванні та управлінні системою мережевої безпеки Cisco ISE. Його функції включають в себе створення політик безпеки, управління користувачами та інтеграцію з іншими системами. Це допомагає забезпечити високий рівень безпеки та ефективне управління мережею.

Вузол pxGrid в Cisco Identity Services Engine (ISE) є ключовим компонентом,

призначеним для забезпечення інтеграції та обміну даними між Cisco ISE та іншими системами безпеки та мережевими інструментами декомунізації. Це функція, яка дозволяє ділитися інформацією про свій бізнес.

Цей вузол дозволяє cisco ISE обмінюватися контекстною інформацією про користувачів, пристрої, події безпеки та стан мережі, спілкуючись через pxGrid, який інтегрується з іншими системами та службами безпеки, такими як системи запобігання виявленню загроз (IDS / IPS), системи SIEM та системи управління інцидентами. Це допомагає швидше виявляти загрози та забезпечує більш ефективний захист мережі.

Одним з найважливіших аспектів вузлів pxGrid є їх здатність виконувати взаємодії в режимі реального часу, які можуть бути використані Cisco ISE systems та іншими системами безпеки для автоматизації реагування на інциденти, прийняття рішень на основі аналізу безпеки та підвищення ефективності загального захисту мережі.

Крім жовтня дека, вузли pxGrid сприяють створенню інтегрованої екосистеми безпеки, в якій дані та інформація про мережеві умови та загрози можуть бути передані між різними системами та інструментами. Це дозволяє підвищити рівень захисту мережі, поліпшити видимість і контроль безпеки, а також реагувати на загрози в режимі реального часу.

Таким чином, вузол pxGrid є ключовим компонентом Cisco ISE і забезпечує інтеграцію та обмін даними між системою безпеки та іншими інструментами безпеки, забезпечуючи ефективний захист мережі та швидке реагування на загрози безпеці.

2.3 Використання функціоналу рішення задля забезпечення контролю доступу до ресурсів

Рис. 2 – забезпечення контролю доступу до ресурсів за допомогою Cisco ISE

Аутентифікація користувачів: Cisco ISE дозволяє налаштовувати різні методи аутентифікації, такі як 802.1X, MAC-аутентифікація, а також інші протоколи для перевірки ідентифікаційних даних користувачів перед наданням доступу до мережевих ресурсів.

Авторизація та ролі користувачів: За допомогою Cisco ISE можна визначити рівні доступу для різних ролей користувачів та груп доступу, що дозволяє обмежувати доступ до конкретних ресурсів залежно від їхніх прав та повноважень.

Профілювання пристроїв: Cisco ISE визначає та класифікує пристрої, які підключаються до мережі на основі їхніх технічних параметрів, що дозволяє застосовувати відповідні політики безпеки та контролю доступу до мережевих ресурсів.

Контроль доступу на основі контексту: Cisco ISE використовує контекстуальну інформацію, таку як час підключення, місцезнаходження, тип пристрою тощо, для прийняття рішень щодо надання або обмеження доступу до ресурсів.

Інтеграція з іншими системами безпеки: Cisco ISE підтримує інтеграцію з

іншими системами безпеки, що дозволяє координувати заходи безпеки та обмінюватися контекстуальною інформацією для ефективного контролю доступу та виявлення загроз.

Аналіз та моніторинг: Cisco ISE забезпечує можливості аналізу та моніторингу активності користувачів і пристроїв у реальному часі, що дозволяє виявляти аномалії та вчасно реагувати на потенційні загрози безпеці мережі.

Централізоване керування: Cisco ISE надає централізоване керування всіма аспектами контролю доступу та безпеки, що спрощує управління та підвищує ефективність заходів безпеки в мережі.

Інтеграція з іншими рішеннями Cisco: Cisco ISE легко інтегрується з іншими рішеннями Cisco, такими як системи моніторингу, аналізу безпеки та інші, що забезпечує уніфіковану платформу для всіх аспектів безпеки мережі.

Такий функціонал Cisco ISE дозволяє організаціям ефективно керувати контролем доступу та забезпечувати надійний рівень захисту мережі та ресурсів в ній.

Дозволи та ролі користувачів у системі Cisco ISE є важливим механізмом для визначення доступу та дозволів у мережевому середовищі. Цей процес базується на визначенні ролей, встановлених для кожного користувача, залежно від місцезнаходження Користувача, його функціональних обов'язків та вимог до доступу до мережевих ресурсів.

Кожна роль користувача в Cisco ISE має свої атрибути та дозволи, які визначають ресурси та процеси, які можуть виконуватися в мережі. Наприклад, адміністратор мережі може мати повний доступ до всіх налаштувань та елементів керування на мережевому пристрої, тоді як звичайний користувач може отримати доступ до певної служби або мережевого пристрою.

Під час процесу авторизації Cisco ISE враховує інформацію Користувача та контекстну інформацію про з'єднання, отриману в процесі аутентифікації, що забезпечує безпеку та контроль доступу до різних ресурсів, які Користувачеві дозволено виконувати, запобігає шахрайству та забезпечує дотримання політики безпеки організації.

Аутентифікація користувача в системі Cisco ISE є важливим кроком у забезпеченні мережевої безпеки і контролю доступу до ресурсів. Цей процес включає перевірку ідентифікаційних даних Користувача для перевірки особи користувача та законності доступу до мережевих служб та даних.

Cisco ISE використовує різні методи автентифікації, включаючи автентифікацію 802.1x, автентифікацію Mac, LDAP, RADIUS, TACACS + та автентифікацію в діалоговому вікні., щоб підтвердити ідентифікаційні дані Користувача. Ці методи декомунізують введення імен користувачів і паролів, використання сертифікатів, біометричних даних та інших механізмів аутентифікації, які гарантують впевненість у законності доступу.

Після отримання ідентифікаційних даних від користувача Cisco ISE перевіряє сумісність з даними, що зберігаються в базі даних або на віддаленому ресурсі, такому як Active Directory або LDAP-сервер. Цей процес дозволяє визначити, чи дозволено користувачам доступ до мережевих ресурсів та які обмеження застосовуються до вашого облікового запису.

Таким чином, аутентифікація в Cisco ISE аутентифікує користувача і забезпечує безпеку мережі, надаючи тільки законний доступ до ресурсів, тим самим зберігаючи цілісність мережевого середовища і уникаючи несанкціонованого доступу до конфіденційної інформації.

Профілювання пристроїв у системі Cisco ISE є важливим механізмом, який може автоматично ідентифікувати та класифікувати підключені до мережі пристрої відповідно до специфікацій та специфікацій. Цей процес дозволяє системі Cisco ISE отримувати контекстну інформацію про кожен пристрій, дозволяючи їй надавати доступ і застосовувати відповідні політики безпеки.

Під час процесу профілювання Cisco ISE використовує різні методи та механізми для збору та аналізу інформації про пристрій. Це може включати сканування властивостей мережі, визначення типу операційної системи, аналіз мережевого трафіку, виконання інтерактивних запитів до пристроїв та інші методи для створення ідентифікації.

Однією з ключових переваг профілювання є те, що ви можете застосовувати

відповідні політики безпеки та доступу до ресурсів залежно від типу та характеристик пристрою. Наприклад, до мобільних пристроїв можуть застосовуватися спеціальні політики безпеки, а до пристроїв Інтернету речей можуть застосовуватися відповідні обмеження доступу.

Крім того, профілювання пристроїв можна використовувати для виявлення ненормальних або небезпечних дій в мережі, таких як підключення невідомих пристроїв або виявлення ненормального трафіку, що підвищує безпеку мережі і знижує ризик інцидентів безпеки.

Таким чином, у Cisco ISE профілювання пристроїв є ключовим компонентом для забезпечення безпеки та контролю доступу до мережевих ресурсів шляхом автоматичної ідентифікації та класифікації пристроїв відповідно до специфікацій та специфікацій.

Контекстне управління доступом в системах Cisco ISE є важливим підходом для забезпечення безпеки мережі та ефективного управління доступом до ресурсів, включаючи час, місце розташування, тип пристрою, стан мережі та інші параметри, а також самі ідентифікаційні дані Користувача. Контекстна інформація

Cisco ISE використовує контекстну інформацію для прийняття рішень у режимі реального часу щодо дозволу або обмеження доступу до мережевих ресурсів. Наприклад, якщо користувач зазвичай працює з внутрішньої мережі офісу, але раптом намагається отримати доступ до нього із зовнішнього місця, Cisco ISE намагається змінити цей контекст.

Основними перевагами управління доступом на основі контексту є зменшення ризиків безпеки шляхом прийняття рішень, заснованих на реальному контексті використання мережі, та покращення зручності користувачів шляхом автоматичного налаштування прав доступу відповідно до їх поточного стану.

Крім того, Контекстний контроль доступу дозволяє політикам безпеки автоматично реагувати на зміни жовтня і застосовувати необхідні заходи безпеки, дозволяючи їм ефективно виявляти і запобігати несанкціоновані дії в мережі, такі як злом і несанкціонований доступ.

Загалом, ситуаційний контроль доступу в Cisco ISE розроблений, щоб

допомогти вам приймати рішення на основі фактичного використання мережі та швидко реагувати на зміни у вашому мережевому середовищі.、

Інтеграція з іншими системами безпеки є важливим аспектом функції Cisco ISE, яка допомагає координувати та підвищувати ефективність заходів безпеки в мережі. Cisco ISE підтримує різні системи безпеки, включаючи платформи моніторингу, системи аналізу безпеки, портали безпеки інтрамережі та інші рішення. Підтримує інтеграцію з системою.

Ця інтеграція дозволяє обмінюватися контекстною інформацією в режимі реального часу між декомунізацією Cisco та іншими системами безпеки. Наприклад, інформація про статус аутентифікації та авторизації Користувача може бути відправлена в систему моніторингу подій для аналізу та ідентифікації потенційних загроз. Крім того, інтеграція дозволяє автоматично реагувати на виявлені загрози та аномалії, активуючи відповідні заходи безпеки в режимі реального часу.

Однією з переваг інтеграції Cisco ISE з іншими системами безпеки є ефективність виявлення загроз шляхом спільного використання та аналізу більш широкого контекстного діапазону information.In крім того, інтеграція сприяє централізації управління і координації заходів безпеки, спрощує управління і знижує ризик людського фактора в процесі захисту мережі.

Загалом, інтегруючи Cisco ISE з іншими системами безпеки, організації можуть підвищити безпеку, координуючи та співпрацюючи з різними рішеннями безпеки в режимі реального часу. Ця інтеграція стає ключовим компонентом стратегій захисту мережі, особливо в умовах зростаючого обсягу та складності загроз кібербезпеці.

В системі Cisco ISE аналіз і моніторинг є критично важливим компонентом для забезпечення ефективної роботи і безпеки вашого мережевого середовища. Ці процеси включають збір, обробку та аналіз різної інформації, яка визначає потенційні загрози, аномалії та полегшує прийняття обґрунтованих рішень щодо безпеки.

У Cisco ISE моніторинг використовує спеціалізовані механізми для

регулярного або реального моніторингу стану мережевих пристроїв, користувачів і потоків даних, включаючи моніторинг активності користувачів, перегляд журналів подій, аналіз мережевого трафіку і виявлення аномальних шаблонів, що вказують на потенційні загрози безпеці.

Аналіз даних Cisco ISE проводиться для виявлення потенційних загроз та аномалій у вашому мережевому середовищі. Це включає аналіз журналів подій, виявлення незвичних змін у поведінці користувачів та використання інтелектуальних алгоритмів для виявлення нових та нових загроз кібербезпеці.

За допомогою аналізу і моніторингу в Cisco ISE ви можете швидко реагувати на загрози і аномалії в своїй мережі, запобігати виникненню інцидентів безпеки і підтримувати безперервну роботу мережевого середовища. Крім того, ці процеси можуть допомогти виявити та вирішити проблеми з ефективністю мережі, такі як перевантаження каналу зв'язку та помилки конфігурації пристрою.

У Cisco ISE узагальнення, аналіз та моніторинг є ключовими елементами для забезпечення безпеки та ефективності мережі, і вони можуть виявляти, аналізувати та реагувати на різні події та умови у вашому мережевому середовищі, щоб запобігти потенційним загрозам та забезпечити надійність та безпеку даних.

Централізоване управління системою Cisco ISE дозволяє ефективно управляти всіма аспектами безпеки і доступу до мережевого середовища з єдиної центральної контрольної точки (тобто Вся конфігурація, політики безпеки, правила аутентифікації і авторизації, моніторинг і аналіз подій виконуються з єдиного центрального інтерфейсу Cisco ISE).

Централізоване адміністрування дозволяє уникнути розподіленого та фрагментованого адміністрування, спрощує адміністрування та забезпечує однакові стандарти та політику безпеки у всій мережі. Адміністратори можуть централізовано налаштовувати параметри безпеки, встановлювати правила доступу, відстежувати інциденти і забезпечувати захист від загроз з усіх пристроїв і локальних мереж.

Крім того, централізоване управління забезпечує рівномірність управління та захисту даних незалежно від розміру мережі або кількості підключених пристроїв.

жовтень. Він також може автоматизувати процес управління подіями та реагування на них, підвищити ефективність та допомогти зменшити витрати на управління та обслуговування мережі.

Основними принципами централізованого управління в Cisco ISE є:

Уніфіковане управління: Cisco ISE надає єдиний централізований інтерфейс для налаштування і управління всіма аспектами безпеки і доступу до мережі. Це дозволяє адміністраторам керувати різними аспектами мережі, включаючи автентифікацію, авторизацію, профілювання пристроїв, моніторинг та аналіз, з єдиного інтерфейсу.

Центральна база даних Cisco ISE використовує центральну базу даних для зберігання інформації про користувачів, пристрої, політику безпеки, події та журнали. Це дозволяє менеджерам швидко отримувати доступ до необхідних даних та приймати обґрунтовані рішення.

Політики безпеки-адміністратори можуть створювати та керувати політикою безпеки за допомогою централізованого інтерфейсу Cisco ISE. Ці політики визначають правила доступу до мережевих ресурсів, правила автентифікації та авторизації, вимоги до профілю пристрою та інші параметри безпеки.

Моніторинг та аналіз: Cisco ISE забезпечує моніторинг та аналіз даних безпеки в режимі реального часу. Це включає виявлення аномалій, аналіз змін у мережі та стані Користувача, а також моніторинг подій, які можуть вказувати на потенційні загрози безпеці.

Автоматизація і реагування: Cisco ISE дозволяє автоматично реагувати на виявлені загрози, налаштовувати права доступу, змінювати політики в залежності від контексту, а також підвищувати ефективність і швидкість реагування на інциденти.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДОСТУПУ ДО ЕЛЕКТРОННО ОСВІТНІХ ПЛАТФОРМ

3.1 Розгортання системи контролю доступу до електронно освітніх платформ на базі Cisco ISE

Завдання

1. Сертефікати

2.Active Directory

3. Aunthenticator

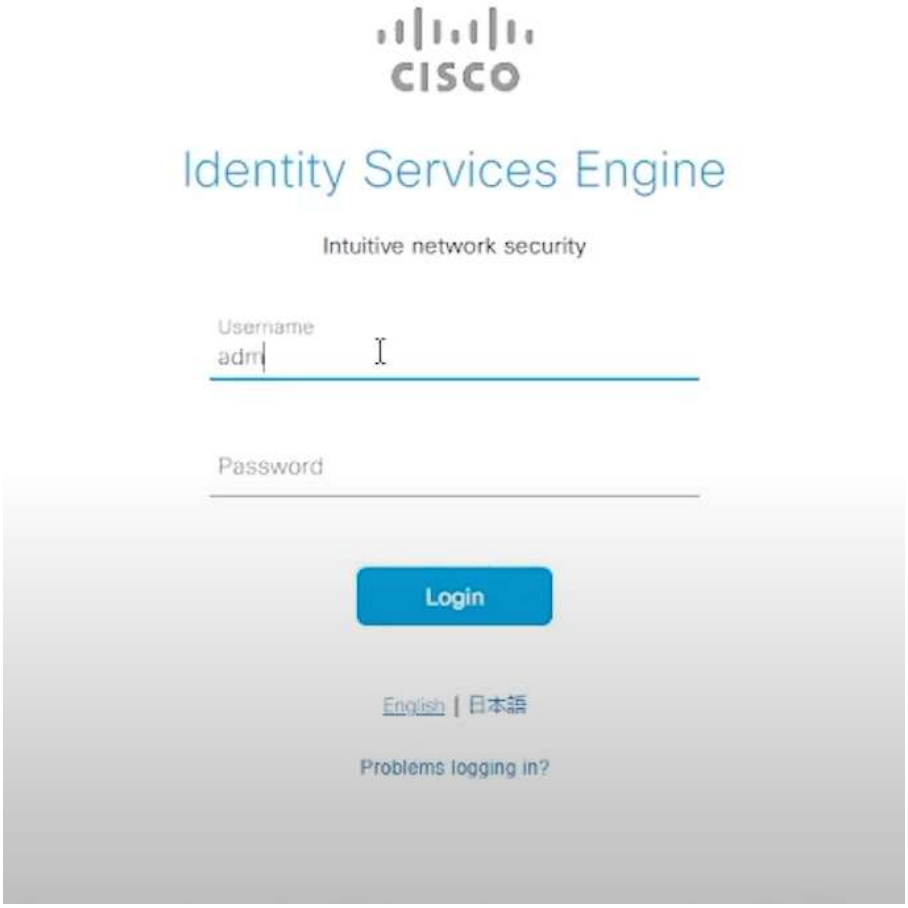

Рис. 3 – заходимо в Cisco ISE

Нам потрібно приєднати ISE до інфраструктури відкритого ключа

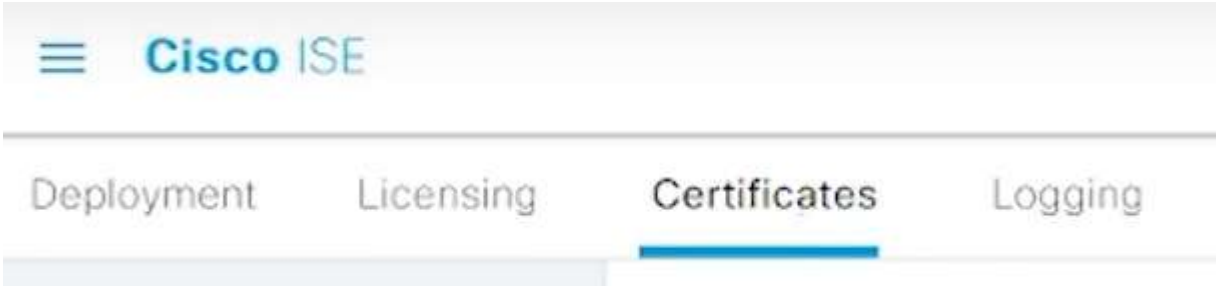

Рис. 4 – заходимо на вкладку “Сертефікати”

Нам треба зробити запит на сертифікат та відправити його на центр сертифікації, Отримати сертифікат та добавити його в ISE.

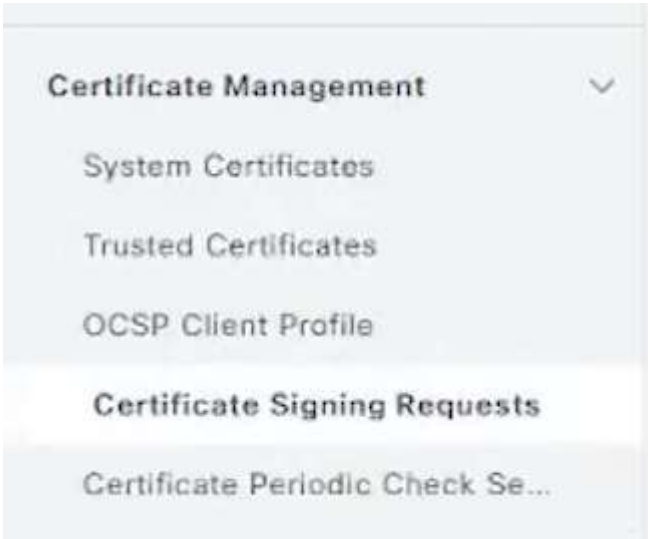

Рис. 5 – заходимо на вкладку “Certificate Signing Requests”

Рис. 6 – натискаємо на кнопку “CSR”

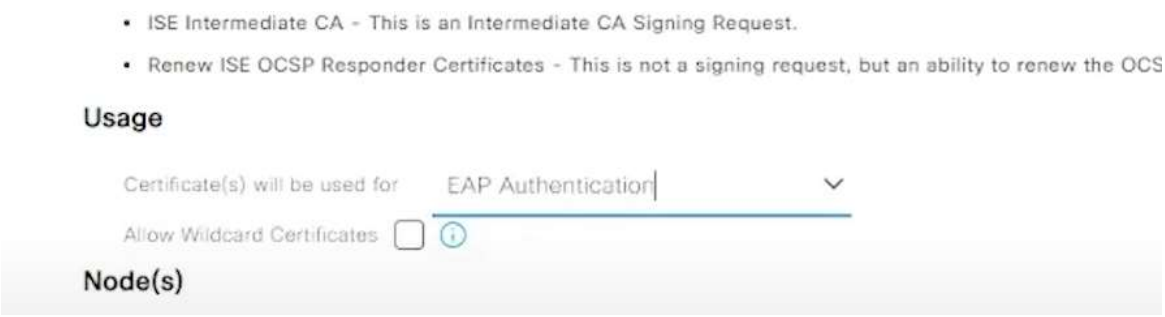

Рис. 6 – у вкладці Usage вибираємо EAP Authentication

Рис. 7 – виписуємо DNS Name та IP адресу

Після цього натискаємо кнопку “Згенерувати”

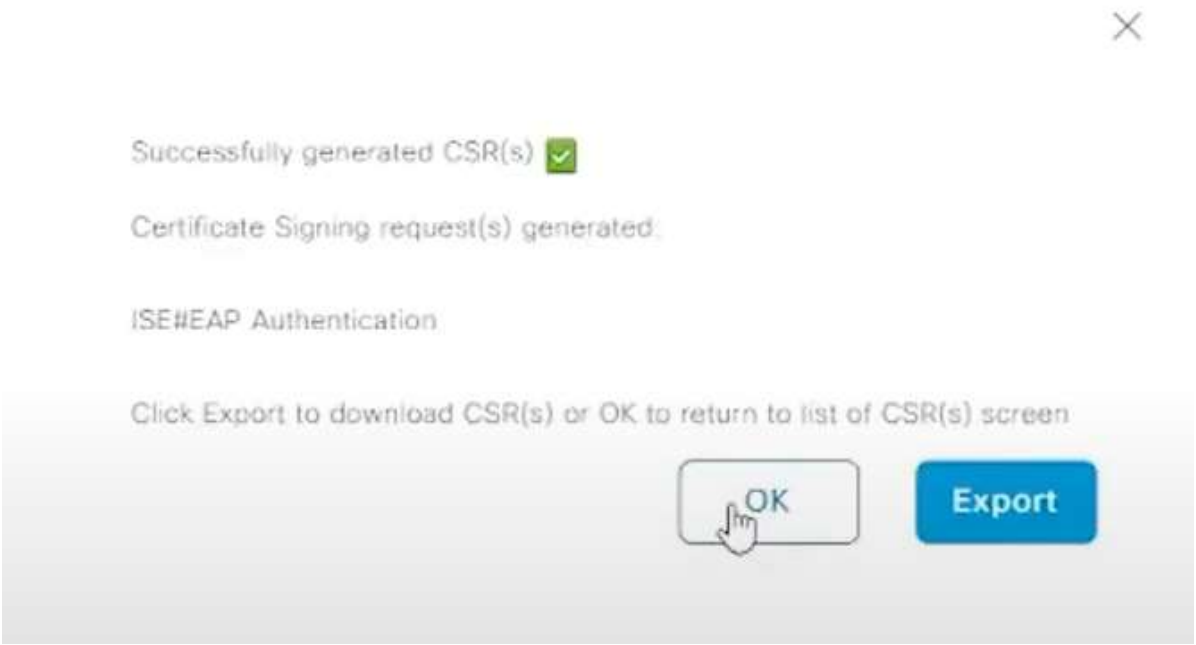

Рис. 8 – отримуємо успішне згенерування запиту на сертифікацію

Після цього натискаємо на кнопку “Export” і наш забит буде успішно завантажений як файл.

Далі переходимо в графічний центр сертифікації.

Рис. 9 – вигляд графічного центру сертифікації.

Натискаємо на кнопку “Request a certificate”

Рис. 10 – натискаємо на advanced certificate request

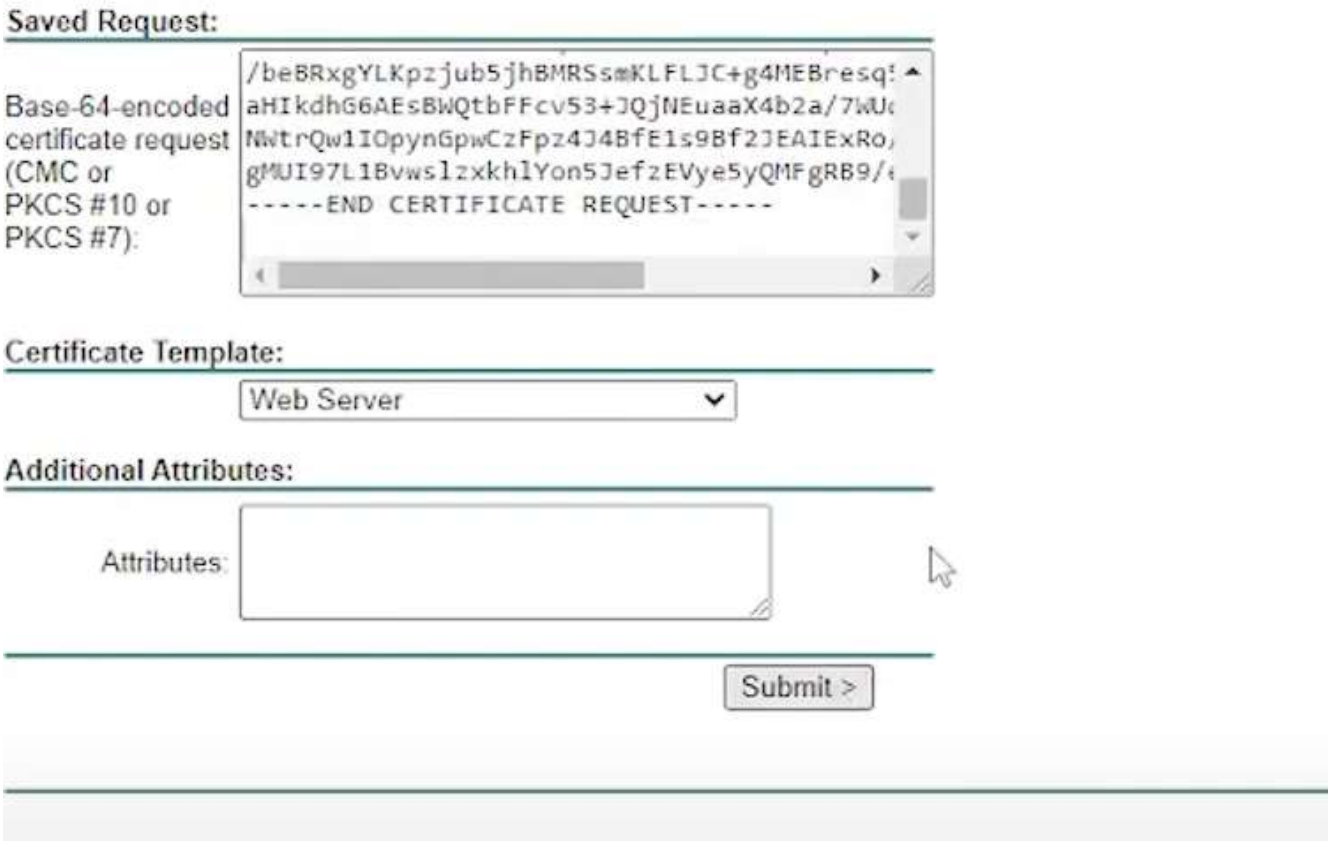

Рис. 11 - поле advanced certificate request

Вибираємо шаблон Web Server та вставляємо наш запит який було відкито та

скопійовано в блокноті. Натискаємо кнопку Submit.

Рис. 12 – вибираємо кодування Base 64 та натискаємо Download certificate

Далі в Cisco ISE переходимо на вкладку Trusted Certificates

Рис. 13 – вкладка Trusted Certificates

Переходимо на вкладку Import

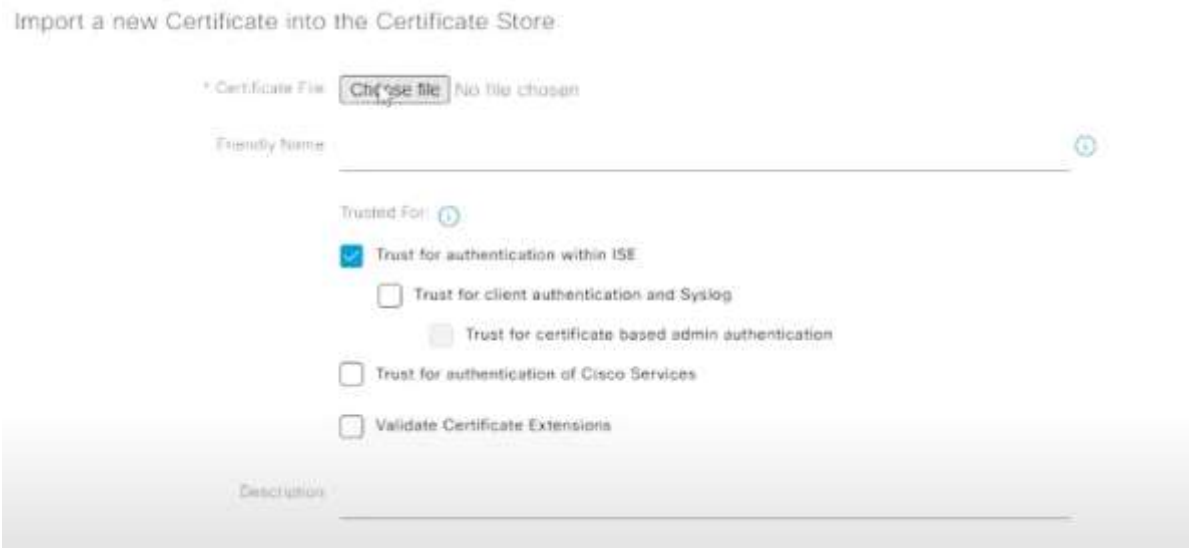

Рис. 14 – меню вкладки Import

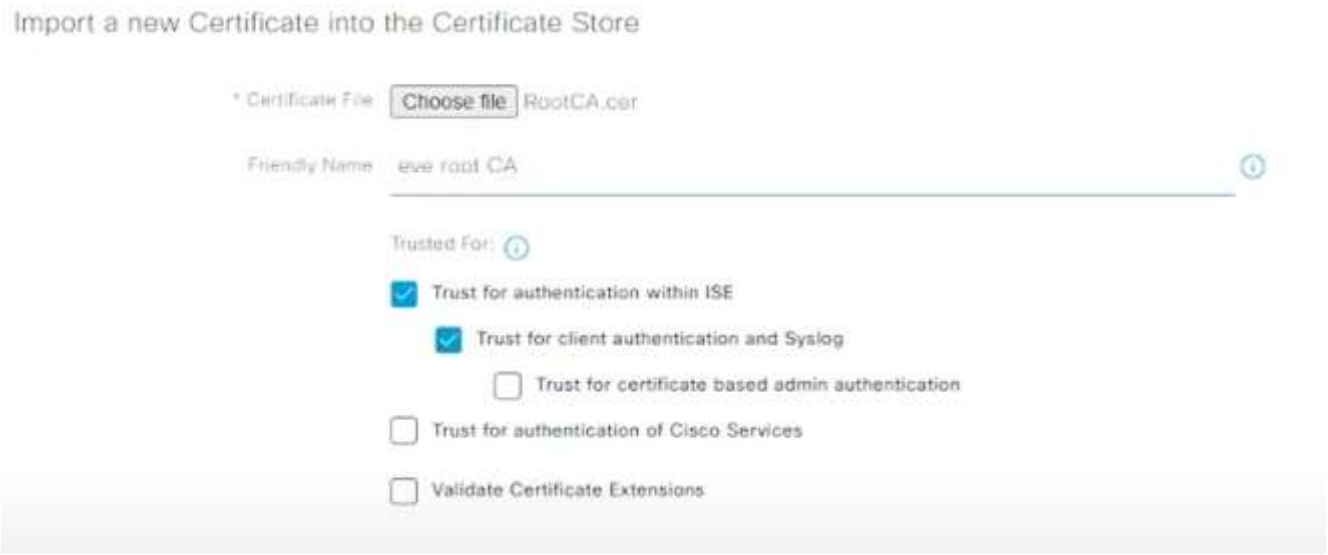

Рис. 15 – завантажуємо сертифікат та натискаємо на клавішу Trust for client authentication and Syslog

Далі нам треба завантажити сертифікат для ISE

Переходимо на вкладку Certificate Signing Requests

Рис. 16 – вкладка Certificate Signing Requests

Рис. 17 – вибираємо активний запит

Натискаємо на кнопку Bind Certificate

Рис. 18 – вибираємо сертифікат який нам підтвердив центр сертифікації, і завантажуємо його

Далі нам треба інтегрувати Active Directory

Заходимо в розділ Адміністрації

Там вибираємо External Identity Sourses

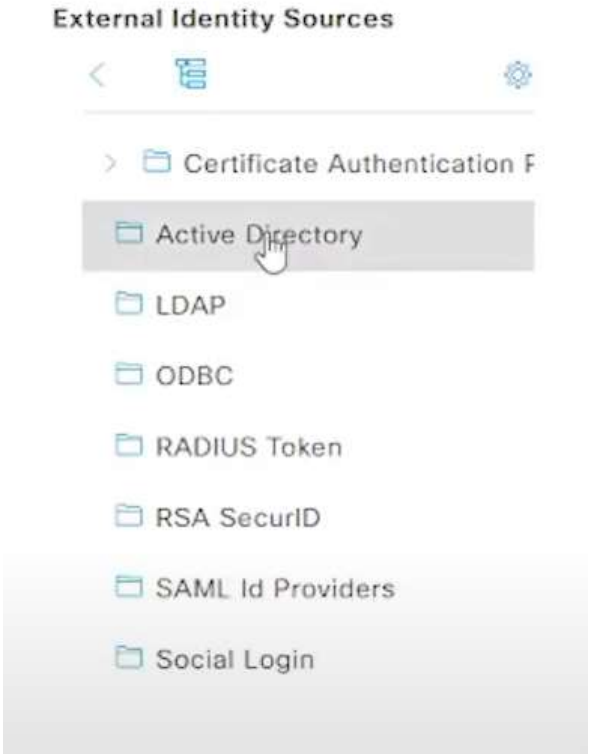

Рис. 19 – у цьому полі вибираємо Active Directory

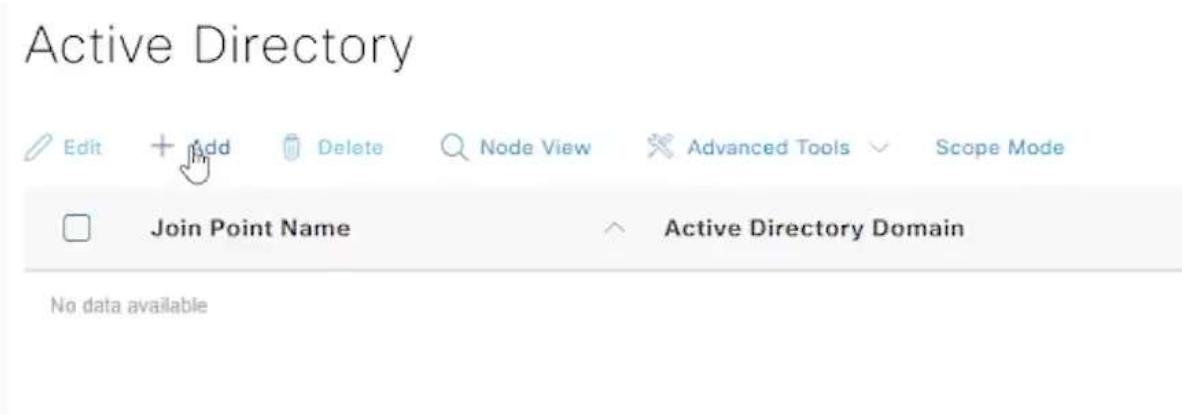

Рис. 20 – у полі Active Directory натискаємо на клавішу Add

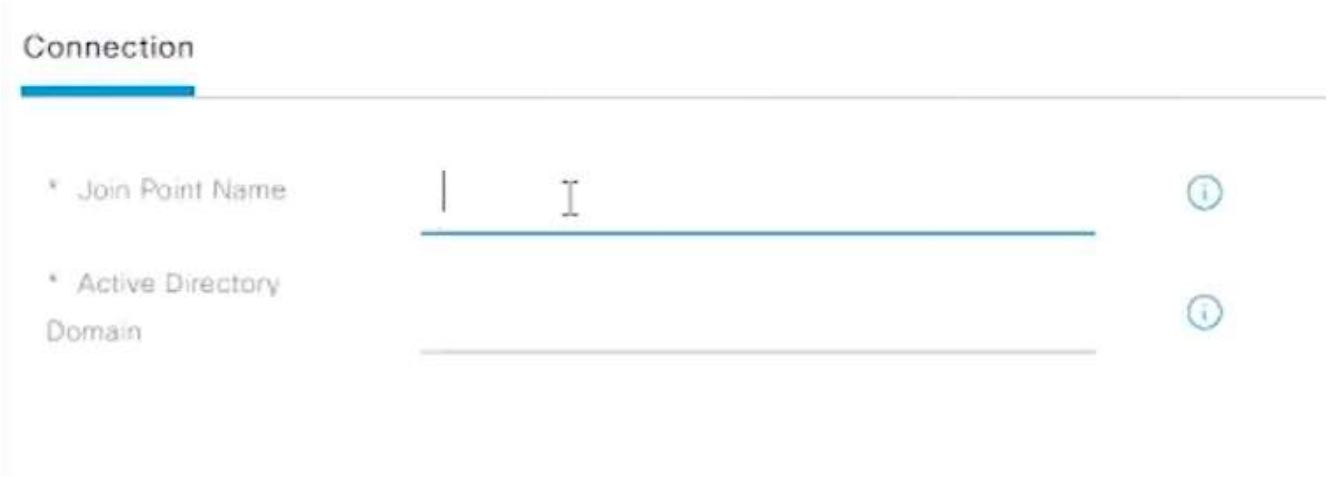

Рис. 21 – вводимо ім’я та домен

Прокручуємо вниз та натискаємо кнопку Submit

Далі відкриється меню де треба ввести логін та пароль від адмінського профілю Active Directory

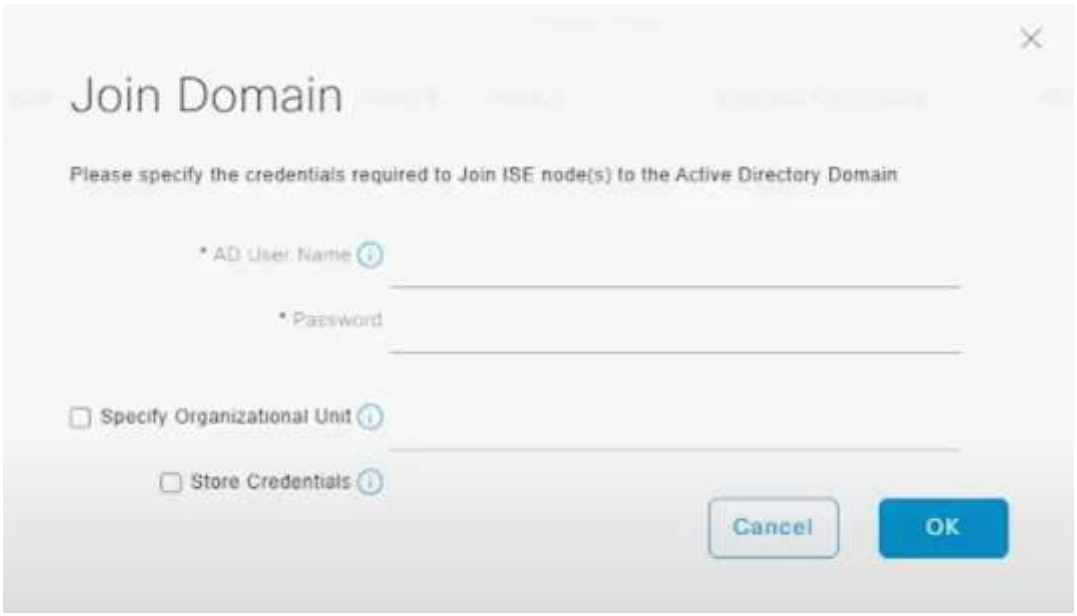

Рис. 22 – меню вводу даних від профілю Active Directory

Якщо все було введено правильно, то з’явиться така меню.

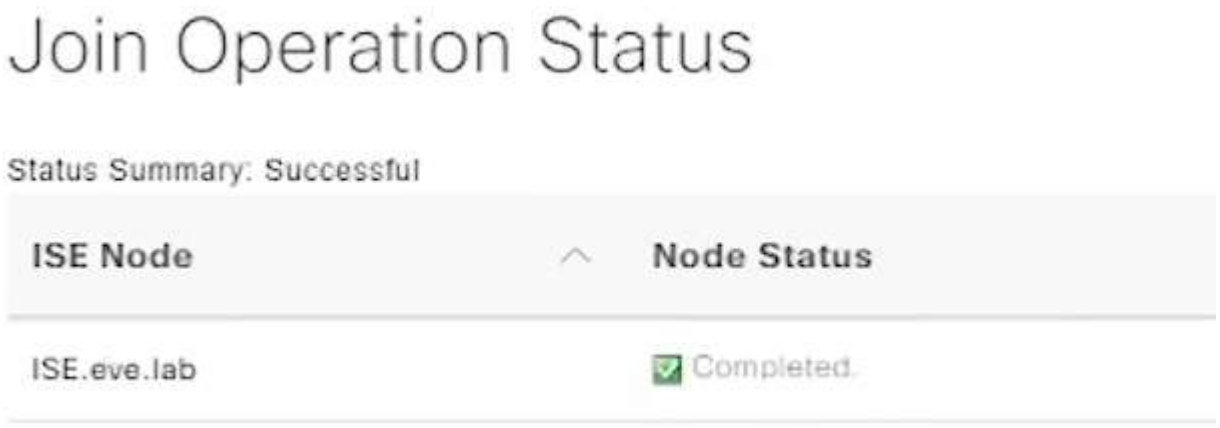

Рис. 23 – підтвердження правильного введення даних Active Directory

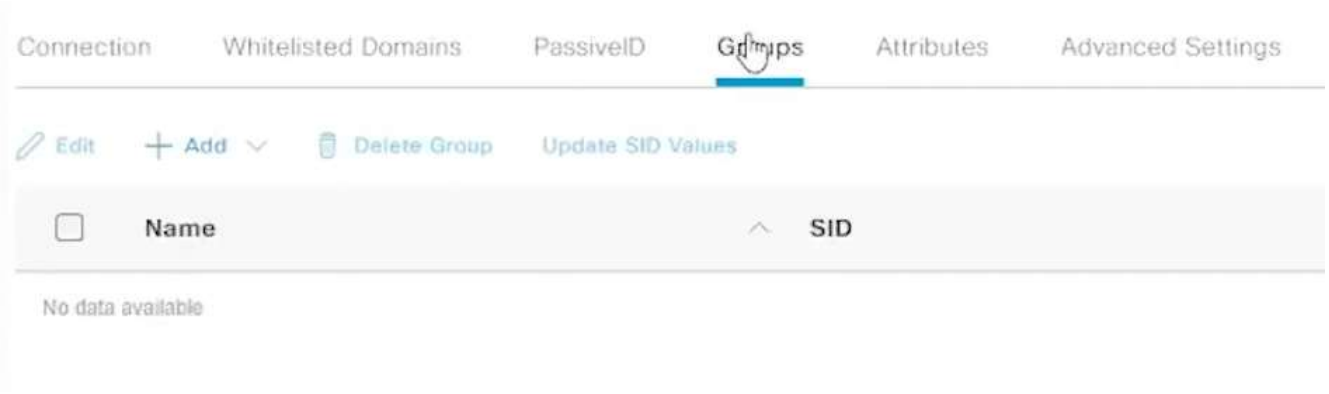

Рис. 24 – заходимо на вкладку Groups

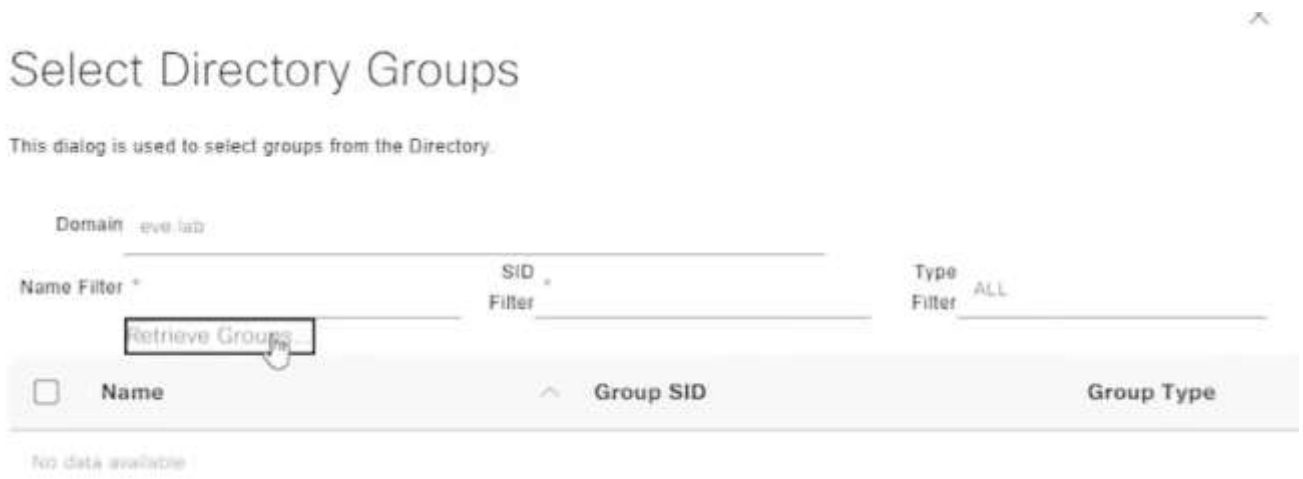

Рис. 25 – на цій вкладці вибираємо Retrieve Groups

Вибираємо потрібні нам групи, після чого натискаємо кнопку Збарагти

Далі створимо профіль серифікації

Заходимо в профіль, натискаємо Add

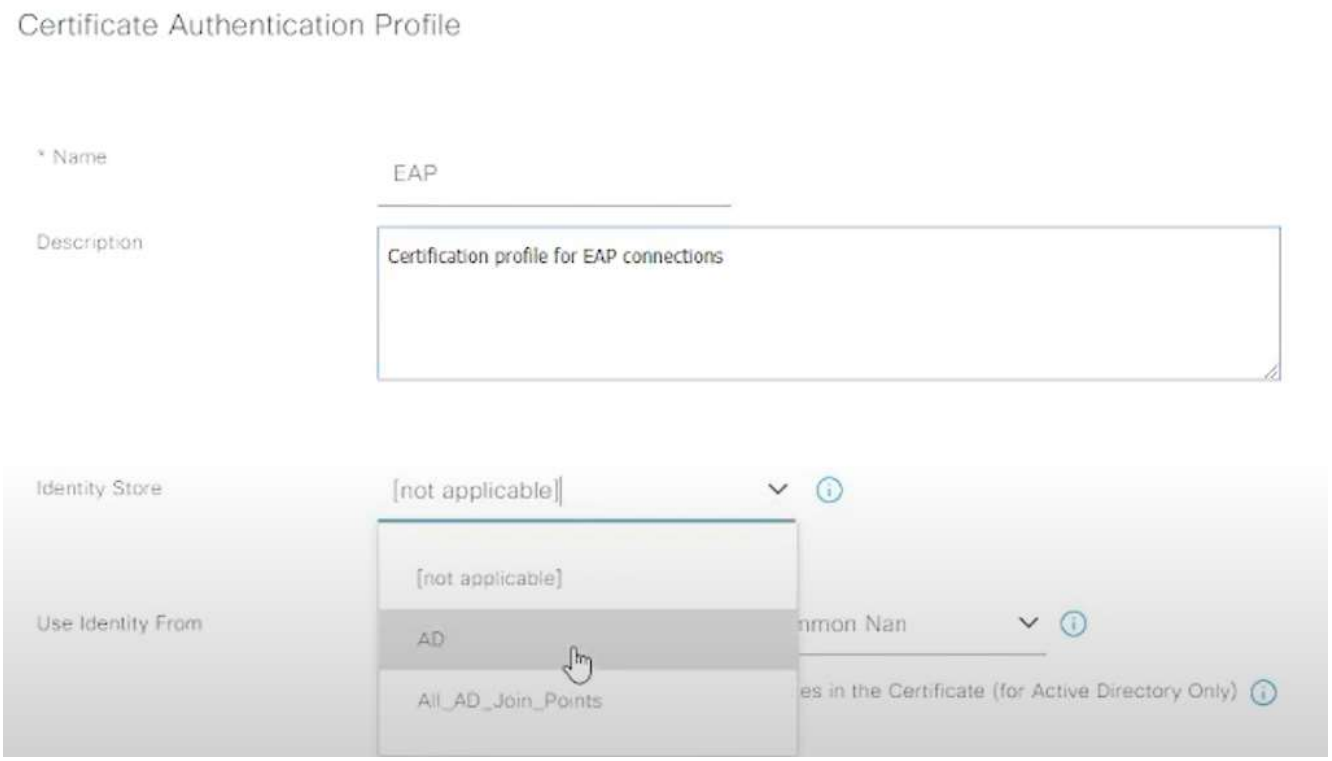

Рис. 26 – меню профілю

У відкритому меню заповнюємо інформацію, вибираємо AD як базу даних юзерів,

Вибираємо пункт Any Subject name.

Тепер в нас є сертифікаційний профіль який ми будемо використовувати далі.

Далі додамо секвенцію

Переходимо на Identity Source Sequence

Рис. 27 – меню секвенції

Натискаємо кнопку Add

Рис. 28 – вибираємо профіль для сертефікатів

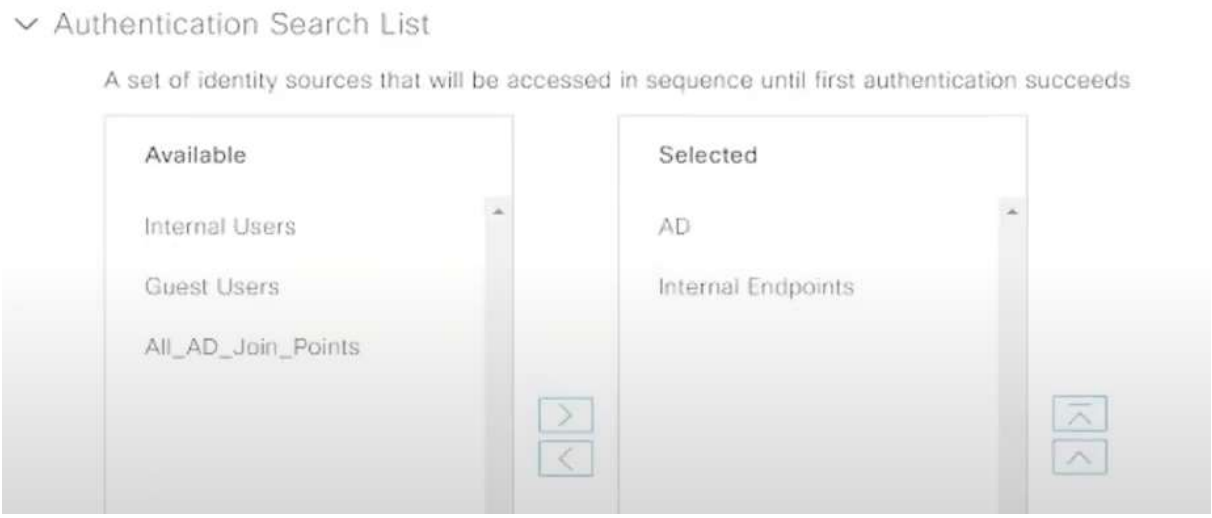

Рис. 29 – спочатку вибираємо Active Directory потів внутрішню базу пристроїв

Натискаємо зберегти.

Тепер треба додати пристрої

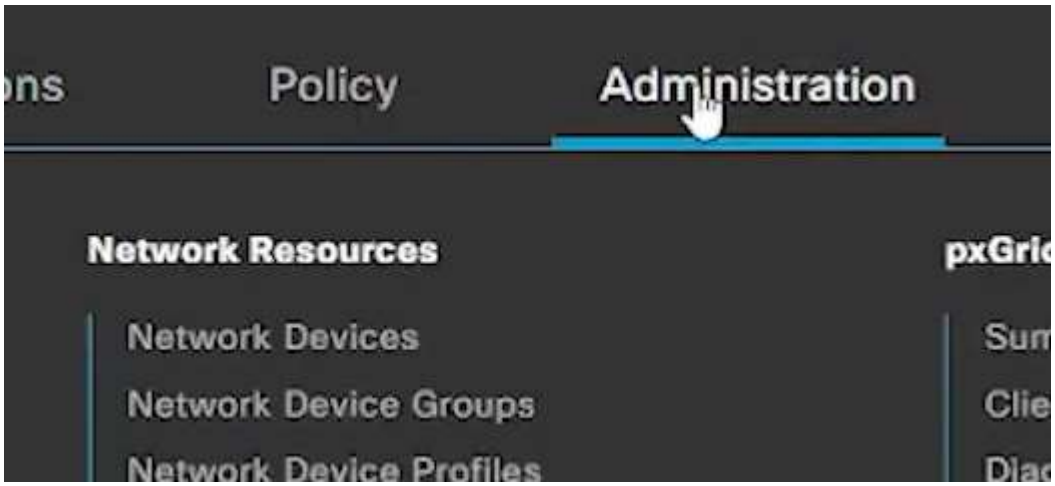

Рис. 30 – в розділі Administration Network Devices

Натискаємо кнопку Add та додаємо пристрій

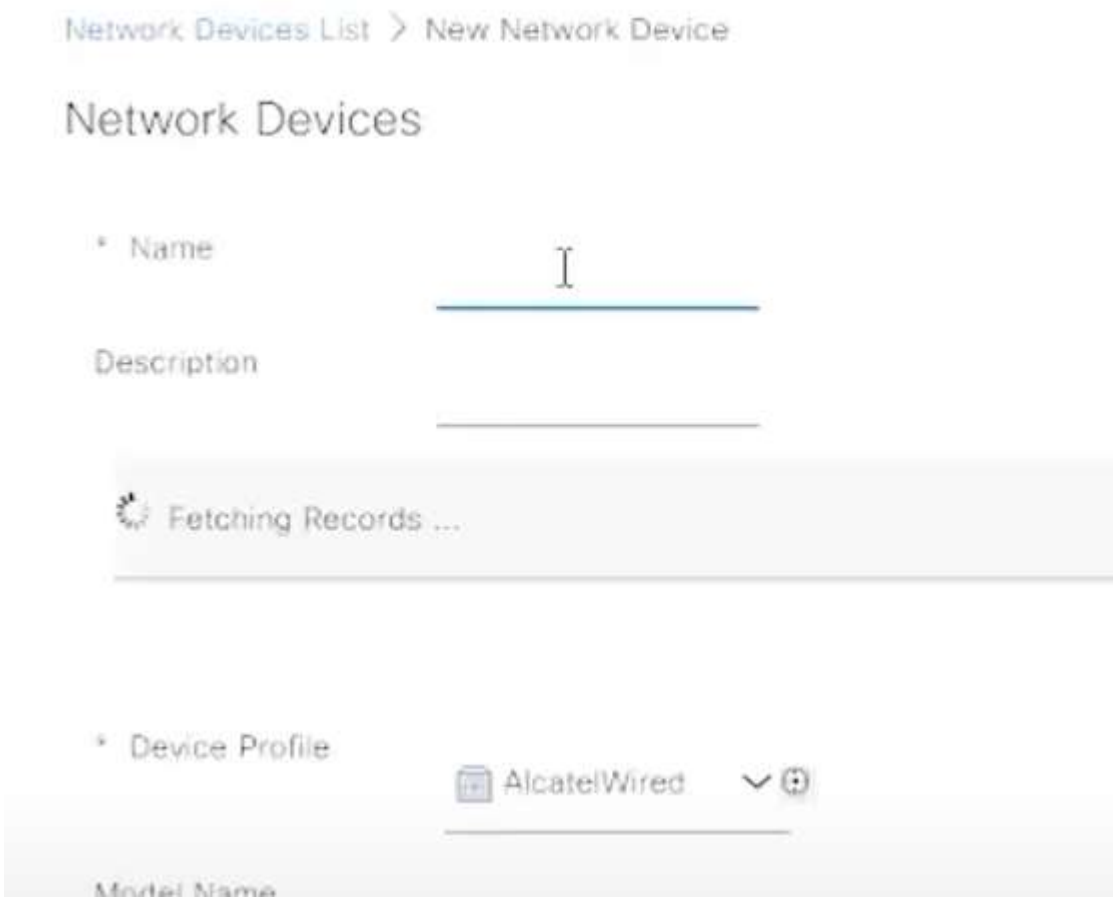

Рис. 31 – заповнюємо інформацію про пристрій

Рис. 32 – вводимо налаштування RADIUS

3.2 Побудова зв'язків з наявними системами безпеки та оцінка ймовірності ризику недостовірних спрацювань

В системі Cisco ISE у вкладці Dashboard наявні декілька “плиток” зі всією інформацією стосовно системи.

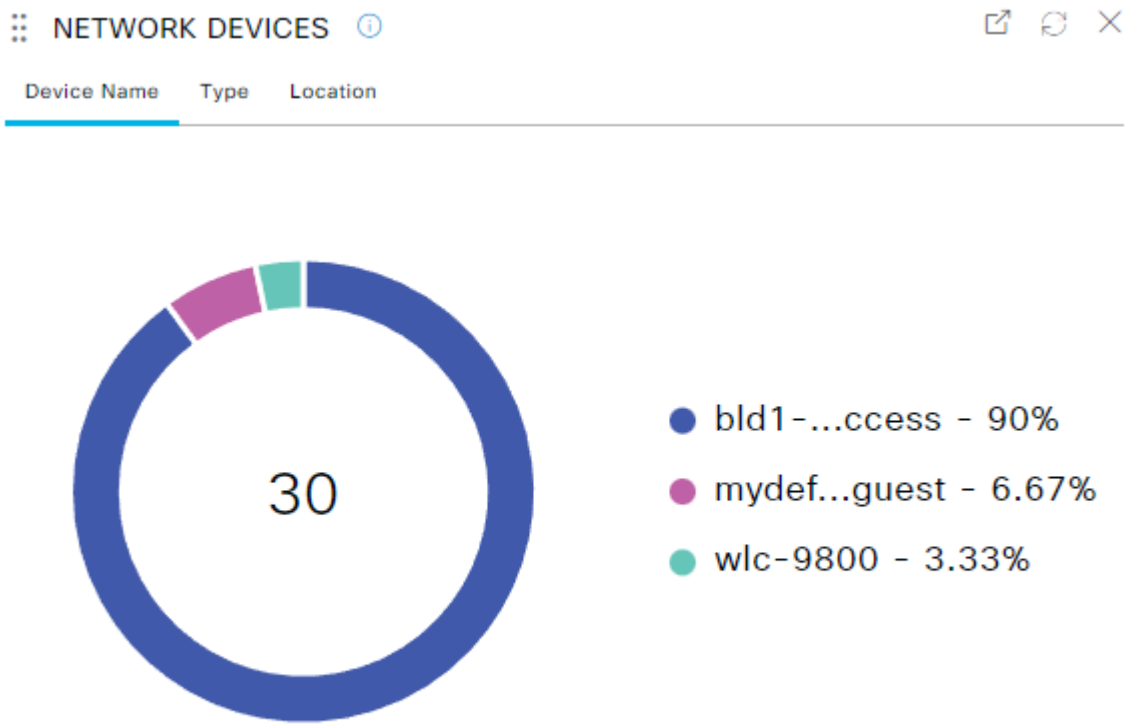

Рис. 33 – зовнішній вигляд Network Devices

У цьому полі ми маємо інформацію про втентифікацію кінцевих точок за мережевим пристроєм, яка фільтрується за назвою пристрою, типом пристрою, розташуванням.

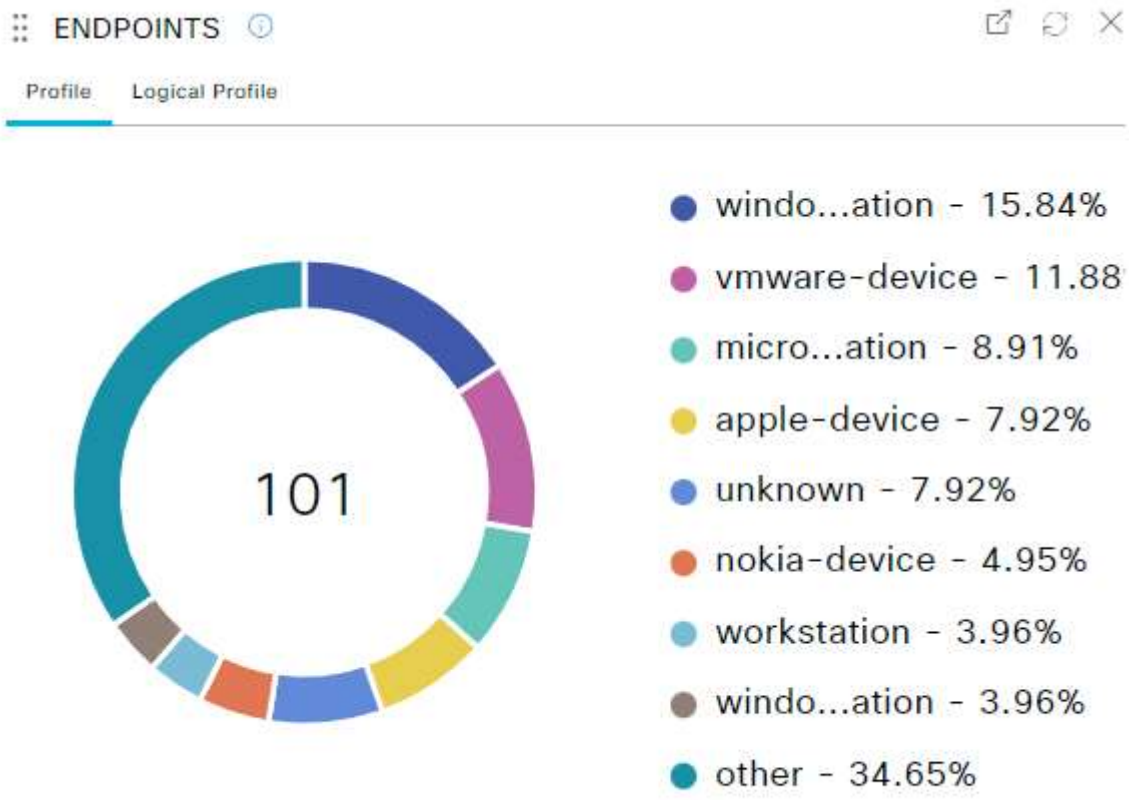

Рис. 34 – зовнішній вигляд Endpoints

У цьому полі ми бачимо інформацію про кінцеві точки, профільовані за функцією мережі та відфільтровані за типом кінцевої точки за профілем кінцевої точки.

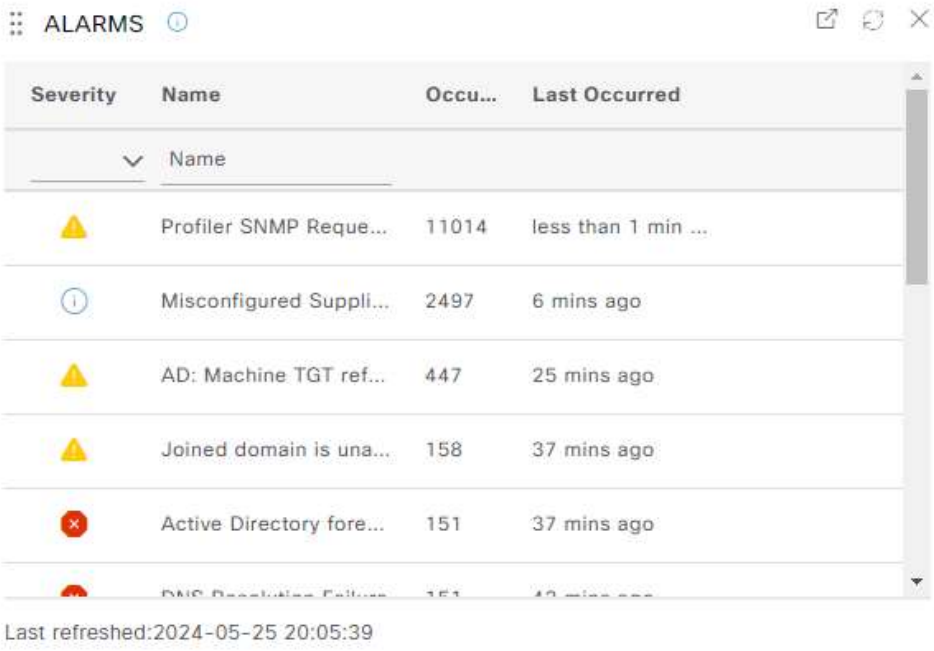

Рис. 35 – зовнішній вигляд Alarms

Цю плитку можна вважати найголовнішою тому що, тут відображаються всі недостовірні спрацювання, ситуації які могли статися через проблеми з профілями, та невдалі спроби взлому. Якщо вчасно реагувати на ці пункти то система буде захищеною.

Також ми маємо окремий розділ для Endpoints

Рис. 36 –окремий розділ для Endpoints

В цьому розділі більш детально описані підключення до мережі, статус кінцевих точок на основі сесії інформації та профільовані кінцеві точки відфільтровані за ідентифікатором. Групи, служба політики, вузли та типи ОС

Ось інструкції для подальших дій при недостовірних спрацюваннях:

Невідомий мережевий пристрій:

Симптоми: Cisco ISE не може ідентифікувати вказаний пристрій мережевого доступу (NAD).

Вирішення: перевірте тип і конфігурацію NAD і знову додайте NAD до Cisco ISE.

CoA не ініціюється на клієнтській машині:

Симптоми: Користувачі в мережі Cisco ISE не проходять необхідну зміну авторизації (CoA).

Вирішення: Переконайтеся, що така команда існує у файлі конфігурації комутатора (це потрібно в комутаторі для активації та налаштування coa):

aaa server radius dynamic-author

client <*Monitoring_node_IP_address*> server-key <*radius_key*>

Під час сеансів доступу до мережі користувачам призначається неправильна VLAN:
Симптоми: Клієнтська машина стикається з різними проблемами доступу, пов'язаними з призначенням VLAN.
Вирішення: Перевірте конфігурацію (конфігурації) VLAN на точках доступу/застосування мережі (комутаторах) у вашому розгортанні.

Функція перенаправлення URL-адрес клієнтського комп’ютера не працює:
Симптоми: Користувачі не перенаправляються належним чином на правильну URL-адресу для автентифікації.
Вирішення: Перевірте та (за потреби) налаштуйте конфігурацію комутатора.

Пакети (атрибути) обліку RADIUS не надходять від комутатора:
Вирішення: Переконайтеся, що конфігурація комутатора RADIUS для цього пристрою правильна та містить відповідні команди.

3.2 Рекомендації з удосконалення захисту інформаційно-комунікаційних систем від протікання даних, базуючись на функціоналі Cisco ISE

Динамічний контроль доступу є важливим аспектом захисту інформаційно-комунікаційних систем, який забезпечує адаптивний контроль доступу до мережевих ресурсів на основі контекстної інформації шляхом реалізації динамічного контролю доступу з використанням механізму служб ідентифікації Cisco (ISE), організації можуть ефективно реагувати на різні ситуації і потенційні загрози. Основний принцип динамічного контролю доступу полягає в тому, що права доступу користувачів і пристроїв можуть змінюватися в режимі реального часу в залежності від різних факторів, таких як тип пристрою, місце розташування користувача, час, рівень відповідності політиці безпеки та інші атрибути. Cisco ISE збирає та аналізує ці дані, застосовуючи політику, що визначає рівні доступу, які можуть бути автоматично змінені відповідно до виявлених умов.

Цей підхід забезпечує більш гнучкий і детальний контроль доступу в порівнянні з традиційними статичними методами, коли права доступу визначені один раз і не змінюються незалежно від контексту. Наприклад, користувач, який намагається отримати доступ до мережі з корпоративного пристрою в офісі, може мати набір дозволів, тоді як той самий користувач, який намагається підключитися з персонального пристрою з невідомої мережі, може отримати обмежений або повністю заблокований доступ. Ви також можете використовувати наступні методи: Cisco ISE рекомендує ознайомитися з функціями безпеки, переглянувши необхідні оновлення, антивірусне програмне забезпечення та інші функції безпеки, перш ніж надавати доступ до мережі.

Крім того, динамічний контроль доступу дозволяє реалізувати концепцію мінімальних привілеїв, коли користувачі і пристрої отримують тільки ті привілеї, які необхідні для виконання поточного завдання. Це значно знижує ризик несанкціонованого доступу до конфіденційної інформації. Це особливо важливо в ситуації, коли зростає кількість мобільних пристроїв та віддалених користувачів, які підключаються до корпоративної мережі з різних місць та пристроїв.

Інтегруючись з іншими системами безпеки, такими як системи виявлення та запобігання вторгненням, рішення для захисту кінцевих точок, а також системи інформаційної безпеки та управління інцидентами, Cisco ISE може забезпечити комплексний підхід до захисту, автоматично реагуючи на виявлені загрози. Наприклад, якщо пристрій або мережа виявляють підозрілу активність, ISE може автоматично змінити рівень доступу або ізолювати пристрій, поки ситуація не проясниться.

Багатофакторна аутентифікація (MFA) є дуже важливою технологією в сучасних системах інформаційної безпеки і значно підвищує рівень захисту інформаційно-комунікаційних систем. Реалізація МЗС, що використовує Cisco Identity Services Engine, забезпечує багаторівневий підхід до автентифікації користувачів, що зменшує ймовірність несанкціонованого доступу до корпоративних ресурсів, навіть якщо один із факторів автентифікації був скомпрометований.

Суть MFA полягає в тому, що для успішної аутентифікації користувача, інформації (пароль або PIN-код), володіння (фізичні об'єкти, такі як смарт-карти та мобільні пристрої), пов'язаних з цим функцій (відбитки пальців) Cisco ISE надає одноразовий пароль (OTP). , додатки для аутентифікації на мобільних пристроях, біометричні системи, і так далі. забезпечити використання цих елементів.

Впровадження MFA за допомогою Cisco ISE має кілька ключових переваг. По-перше, це сильно ускладнює завдання зловмисника, оскільки для отримання несанкціонованого доступу необхідно зламати або обійти відразу кілька механізмів безпеки. Останнє пов'язане з крадіжкою або втратою облікових даних MFA, оскільки навіть з паролями система недоступна без додаткових факторів аутентифікації. По-друге, використання MFA підвищує впевненість як внутрішніх, так і зовнішніх користувачів у безпеці системи. Це особливо важливо для організацій, які працюють з конфіденційними або критично важливими даними.
Cisco ISE надає можливість налаштовувати і управляти MFA, надаючи гнучкість у виборі методу аутентифікації, що відповідає конкретним потребам вашої організації. Як частина програми MFA, ми можемо використовувати Cisco ISE,

RADIUS, SAML і т.д. він підтримує різні протоколи і стандарти, в тому числі, тому існуючі інфраструктурні рішення і сервіси можуть бути інтегровані в CISCO ise незалежно від того, чи маєте Ви доступ до критично важливих ресурсів. з нових або менш надійних пристроїв або з географічно віддалених місць. Ви можете створити та застосувати політику безпеки, яка автоматично визначає необхідність додаткових елементів автентифікації в різних сценаріях, наприклад, коли користувач отримує доступ до елемента автентифікації.

Важливим аспектом впровадження МЗС є забезпечення зручності та простоти використання кінцевих користувачів, оскільки складні та незручні процеси аутентифікації можуть призвести до зниження продуктивності та невдоволення користувачів. Cisco ISE надає інтуїтивно зрозумілий інтерфейс і підтримує різні методи аутентифікації, які дозволяють організаціям вибирати найкраще рішення відповідно до вимог зручності користувача і безпеки.

Таким чином, багатофакторна аутентифікація з використанням Cisco ISE є ефективним інструментом захисту інформаційних і комунікаційних систем, використання декількох незалежних елементів аутентифікації і зниження високого рівня ризику несанкціонованого доступу, підвищення надійності користувачів системи і забезпечення відповідності останнім вимогам інформаційної безпеки.

Оновлення та обслуговування інформаційних та комунікаційних систем, особливо засобів забезпечення безпеки, є важливим аспектом забезпечення надійності, актуальності та стійкості до нових загроз. Механізм служб ідентифікації Cisco (ISE) потребує регулярних оновлень і відповідної підтримки для забезпечення його ефективної функціональності і відповідності останнім вимогам інформаційної безпеки. Процес оновлення включає як впровадження нової версії програмного забезпечення, так і установку виправлень, що усувають виявлені уразливості.

Періодичні оновлення Cisco ISE необхідні для інтеграції нових функцій, що підвищують безпеку та ефективність контролю доступу. Нові оновлення часто включають виправлення помилок, підвищення продуктивності та додаткові функції, які забезпечують більш гнучке та надійне управління політикою безпеки.

Ці оновлення гарантують, що пристрої залишаються сумісними з іншими системами та протоколами, що використовуються в мережі, забезпечуючи цілісність та безперервність всієї інформаційної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Troubleshooting Cisco ISE: URL: https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_troubleshooting.html#wp1035869

2. Платформа Cisco Identity Services Engine: URL: https://www.telesphera.net/blog/cisco-identity-services-engine.html

1. Cisco Identity Services Engine (ISE): URL: https://www.cisco.com/site/us/en/products/security/identity-services-engine/index.html

2. Cisco ISE Solution Overview: URL: https://www.cisco.com/c/en/us/products/security/identity-services-engine/ise-flexibility-choice-psr-zta-so.html

3. Проблеми дистанційного навчання учнів: шляхи їх вирішення: URL: https://naurok.com.ua/problemi-distanciynogo-navchannya-uchniv-shlyahi-h-virishennya-318487.html

4. Access Control in Security: Methods and Best Practices: URL: https://frontegg.com/guides/access-control-in-security

5. Access Control: Models and Methods: URL: https://delinea.com/blog/access-control-models-methods

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)