ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Голенка Максима Юрійовича
представлену на здобуття освітнього ступеня бакалавр
зі спеціальності 123 «Комп'ютерна інженерія»

1. Робота виконана на тему „Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine".

2. Актуальність роботи зумовлена потребою впровадження підсистем аутентифікації на базі Cisco Identity Services Engine для контролю доступу до складної гетерогенної мережі реального підприємства.

3. Основний зміст пояснювальної записки роботи викладено на 95 сторінках тексту, записка містить 2 таблиці, 120 ілюстрацій, 8 додатків. Список використаних літературних джерел налічує 28 найменування. Невід'ємною складовою роботи є реалізований у середовищі моделювання GNS3 проект мережі на базі мережевого обладнання від Cisco, рішення Cisco Identity Services Engine і операційних систем Windows.

4. Пояснювальна записка складається з вступу, трьох розділів основного тексту, висновків, списку використаної літератури, додатків.

Розділ 1 присвячений аналізу протоколів та засобів забезпечення підсистеми аутентифікації, а саме у розділі розглянуто та проналізовано особливості організації та функцонування, переваги та недоліки протоколу AAA, стандарту 802.1X, протоколів RADIUS і TACACS+. У цьому ж розділі наведено призначення і сфери використання рішення ключового компоненту кваліфікаційної роботи Cisco Identity Services Engine.

Розділ 2 присвячений питанням проектування підсистеми аутентифікації, зокрема, здійснено аналіз та вибір програмного забезпечення для реалізації проекту, розроблено проект мережі та схему адресації її пристроїв, наведено сценарій встановлення Cisco Identity Services Engine та.

Розділ 3 присвячений опису процесу налагодження компонентів проекту підсистеми аутентифікації: мережевого обладнання, Windows Server, Cisco Identity Services Engine. Також у цьому розділі здійснено налагодження і продемонстровано перевірку працездатності підсистеми аутентифікації.

5. Висновки містять сумарні результати проведеної роботи.

6. Список використаних літературних джерел містить перелік підручників, фахових видань, стандартів, документації тощо, має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

7. Додатки містять лістинги конфігураційних файлів налагоджених пристроїв.

8. Таблиці та ілюстрації оформлені досить якісно, є інформативними та наведені у відповідних місцях роботи.

9. Якість оформлення роботи є високою.

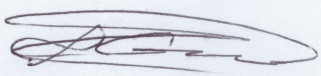
10. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту та доповіді враховані.

11. Ставлення студента до виконання випускної кваліфікаційної роботи – дуже відповідальне.

12. У цілому при написанні випускної кваліфікаційної роботи студент Голенко М.Ю. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Комп'ютерні мережі», «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж», «Операційні системи», «Теорія систем та системний аналіз», «Архітектура комп'ютера», «Хмарні технології». Також студент Голенко М.Ю. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити проект підсистеми аутентифікації, обрати відповідний інструментарій, створити закінчений цілісний продукт (у вигляді змодельованого проекту) і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Голенка М.Ю. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.
Пропонована оцінка – «відмінно».

Науковий керівник
к.т.н., завідувач кафедри КІ та КБ
1 червня 2020 року



А.А. Єфіменко

РЕЦЕНЗІЯ

на кваліфікаційну роботу
студента 4 курсу групи КІ-2 спеціальності «Комп'ютерна інженерія»
факультету інформаційно-комп'ютерних технологій
Державного університету «Житомирська політехніка»
Голенка Максима Юрійовича
на тему: „Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine"

Кваліфікаційна робота студента Голенка М.Ю. „Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine" присвячена актуальній тематиці – впровадженню контролю доступу у мережі для підвищення безпеки на основі рішення від виробника мережевого обладнання Cisco.

Робота містить реалізований проект мережі у середовищі графічного симулятора GNS3 на базі віртуального мережевого обладнання від Cisco, рішення Cisco Identity Services Engine, операційних систем Windows та пояснювальну записку наступного складу: вступ, три розділи основного тексту, висновки, список використаної літератури, вісім додатків.

У першому розділі пояснювальної записки проведено аналіз протоколів та засобів забезпечення підсистеми аутентифікації, розглянуто: протокол AAA, стандарт 802.1X, протоколи RADIUS і TACACS+ та проведено їх порівняння. У цьому ж розділі наведено призначення і сфери використання рішення ключового компоненту кваліфікаційної роботи Cisco Identity Services Engine.

У другому розділі пояснювальної записки здійснено проектування підсистеми аутентифікації, зокрема, здійснено аналіз та вибір програмного забезпечення для реалізації проекту, наведено сценарій встановлення рішення Cisco Identity Services Engine та розроблено схему адресації пристроїв мережі.

У третьому розділі пояснювальної записки наведено опис процесу налагодження всіх компонентів кваліфікаційної роботи, таких як: мережеве обладнання, Windows Server, Cisco Identity Services Engine. Також у цьому розділі здійснено і продемонстровано перевірку працездатності підсистеми аутентифікації під час виконання різних задач.

Зміст роботи відповідає поставленому завданню. У цілому кваліфікаційна робота виконана на високому рівні. Тема роботи розкрита повністю. Студентом продемонстровані ґрунтовні теоретичні знання та практичні фахові навички, що отримані як під час навчання, так і у процесі виконання роботи. Матеріал пояснювальної записки викладено логічно, науково і технічно грамотно. Ілюстративний матеріал (рисунки, таблиці), що наведений у роботі, оформлений якісно і наведений у відповідних місцях. Оформлення роботи у цілому відповідає вимогам стандартів. Проект мережі реалізовано у середовищі графічного симулятора GNS3. Його функціонал відповідає заявленому.

Позитивною стороною є те, що отримані результати мають практичну цінність – розроблений проект можливий до впровадження в діяльності реального підприємства. У цілому кваліфікаційна робота студента Голенка М.Ю. „Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine" відповідає вимогам рівня вищої освіти «бакалавр» спеціальності 123 «Комп'ютерна інженерія» і рекомендується до захисту в ЕК.

Пропонована оцінка роботи – «відмінно».

Рецензент,
декан факультету
інформаційно-комп'ютерних технологій,
канд. техн. наук, доцент Надія Лобанчикова
10 червня 2020 р.

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп’ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему:

«Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine»

Виконав студент 4-го курсу, групи КІ-2
спеціальності
123 «Комп’ютерна інженерія»
_____ Голенко М. Ю.
Керівник, завідувач кафедри КІ та КБ
_____ Єфіменко А. А.
Рецензент, декан ФІКТ, к.т.н., доцент
_____ Лобанчикова Н. М.

Житомир 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
Єфіменко А. А.
«06» квітня 2020 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу

Студента **Голенка Максима Юрійовича**
Тема роботи: **Проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine**
затверджена Наказом по університету від **«06» квітня 2020 р. № 98с**
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**
Вихідні дані для роботи:

1. Рішення Cisco Identity Services Engine
2. Операційні системи Windows Server 2016, Windows 10, Cisco IOS
3. Програмний продукт засобів віртуалізації VMWare Workstation
4. Графічний емулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А. А.	06.04.20	06.04.20
2	Єфіменко А. А.	23.04.20	23.04.20
3	Єфіменко А. А.	05.05.20	05.05.20

Керівник Єфіменко А. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2020 – 8 квітня 2020	Виконано
2	Пошук та аналіз джерел інформації з реалізації підсистем аутентифікації	9 квітня 2020 – 14 квітня 2020	Виконано
3	Аналіз інформації про протоколи та засоби забезпечення аутентифікації	15 квітня 2020 – 18 квітня 2020	Виконано
4	Огляд рішення контролю доступа Cisco Identity Services Engine	19 квітня 2020 – 22 квітня 2020	Виконано
5	Пошук та вибір програмного забезпечення для виконання проекту	23 квітня 2020 – 24 квітня 2020	Виконано
6	Встановлення рішення Cisco Identity Services Engine	25 квітня 2020 – 26 квітня 2020	Виконано
7	Розробка схеми адресації пристроїв мережі	27 квітня 2020 – 28 квітня 2020	Виконано
8	Налагодження мережевого обладнання та Windows server	29 квітня 2020 – 1 травня 2020	Виконано
9	Налагодження Windows Server	2 травня 2020 – 4 травня 2020	Виконано
10	Налагодження Cisco Identity Services Engine	5 травня 2020 – 20 травня 2020	Виконано
11	Перевірка працездатності мережі	21 травня 2020 – 23 травня 2020	Виконано
12	Аналіз результатів тестування	23 травня 2020 – 24 травня 2020	Виконано
13	Написання пояснювальної записки	25 травня 2020 – 29 травня 2020	Виконано
14	Підготовка презентації та виступу	30 травня 2020 – 31 травня 2020	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2020 – 10 червня 2020	Виконано
16	Захист	14 червня 2020	Виконано

Студент _____ Голенко М. Ю.

Керівник _____ Єфіменко А. А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми аутентифікації на базі рішення Cisco Identity Services Engine. Пояснювальна записка до роботи містить 96 сторінок, 120 ілюстрацій, 2 таблиці, список літературних джерел містить 28 найменувань, 8 сторінок додатків.

Метою роботи є розробка проекту підсистеми аутентифікації на базі рішення Cisco Identity Services Engine.

В роботі визначено основні завдання на розробку підсистеми аутентифікації, проаналізовано протоколи та засоби забезпечення підсистеми аутентифікації. Наведено вибір программного забезпечення, сценарій встановлення рішення Cisco Identity Services Engine та розробку схеми адресації пристроїв при проектування підсистеми. Також наводяться сценарії налагодження всіх пристроїв підсистеми та результати тестування системи.

КЛЮЧОВІ СЛОВА: ПІДСИСТЕМА АУТЕНТИФІКАЦІЇ, CISCO IDENTITY SERVICES ENGINE, МЕРЕЖА, ДОСТУП ДО МЕРЕЖІ, АДМІНІСТРУВАННЯ, ЗАХИСТ.

ABSTRACT

The qualification work consists of a project of the authentication subsystem based on the Cisco Identity Services Engine solution. The explanatory note to the work contains 96 pages, 120 illustrations, 2 tables, the list of references contains 28 titles, 8 pages of appendices.

The aim of the work is to develop a project of the authentication subsystem based on the Cisco Identity Services Engine solution.

The main tasks for the development of the authentication subsystem are defined in the work, the protocols and means of providing the authentication subsystem are analyzed. The choice of software, the scenario of installation of the Cisco Identity Services Engine solution and development of the scheme of addressing of devices at designing of a subsystem are resulted. Scenarios for debugging all subsystem devices and system test results are also provided.

KEY WORDS: AUTHENTICATION SUBSYSTEM, CISCO IDENTITY SERVICES ENGINE, NETWORK, NETWORK ACCESS, ADMINISTRATION, SECURITY.

ЗМІСТ

ПЕРЕЛІК УМНОВНИХ СКОРОЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1. ПРОТОКОЛИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ РОБОТИ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ 10
1.1. Протокол AAA 10
1.2. Протоколи RADIUS, TACACS+ 13
1.2.1. Протокол централізованої аутентифікації RADIUS 13
1.2.2. Протокол управління доступом TACACS+ 17
1.2.3. Порівняння протоколів RADIUS, TACACS+ 20
1.3. Стандарт котнролю доступу і аутентифікації 802.1X 22
1.4. Рішення Cisco Identity Services Engine 25
Висновки до першого розділу 29
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ 30
2.1. Вибір програмного забезпечення 30
2.1.1. Graphical Network Simulator 3 30
2.1.2. VMware Workstation 32
2.2. Встановлення рішення Cisco Identity Services Engine 35
2.3. Розробка схеми адресації пристроїв 38
Висновки до другого розділу 38
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ 39
3.1. Налагодження мережевого обладнання 39
3.2. Налагодження Windows Server 43
3.3. Налагодження Cisco Identity Services Engine 49
3.4. Перевірка працездатності підсистеми аутентифікації 71
Висновки до третього розділу 82
ВИСНОВКИ 83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 85
ДОДАТКИ 88

ПЕРЕЛІК УМНОВНИХ СКОРОЧЕНЬ

ПЗ – Програмне забезпечення

ІТ – Інформаційні технології

ІБ – Інформаційна безпека

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

RADIUS – Remote Authentication Dial-In User Service

TACACS – Terminal Access Controller Access Control System

PPP – Point-to-Point Protocol

AAA – Authentication, Authorization, Accounting

EAP – Extensible Authentication Protocol

EAPoL – Extensible Authentication Protocol over LAN

PEAP – Protected Extensible Authentication Protocol

EAP-TLS – Extensible Authentication Protocol Transport Layer Security

SNMP – Simple Network Management Protocol

DHCP – Dynamic Host Configuration Protocol

FTP – File Transfer Protocol

NAS – Network Access Server

GNS3 – Graphical Network Simulator 3

ISE – Identity Services Engine

BYOD – Bring Your Own Device

MS AD – Microsoft Active Directory

ЦОД – Центр обробки даних

ВСТУП

Комп'ютерні мережі виникли відносно недавно, трохи пізніше, ніж перші комп'ютери, але їх розвиток йде семимильними кроками і вже зараз є можливості передавати десятки гігабайт інформації в секунду. При наявності комп’ютерних мереж і з’являється гостра необхідність у спеціалістах за їх захистом.

Контроль доступу - ключовий захід інформаційної безпеки. Впровадження системи контролю доступу до мережі підприємства дозволяє не тільки значно знизити ризики реалізації загроз інформаційної безпеки, але і домогтися економічної вигоди від впровадження такого роду систем.

Актуальність обраної теми полягає в тому, що рішення Cisco Identity Services Engine контролює доступом у комп’ютерній мережі і підвищує її безпеку, рішення гнучко інтегрується з Windows Server і забезпечує аутентифікацію користувачів та полегшує адмініструання мережі.

Метою кваліфікаційної роботи є:

1. Дослідження протоколів AAA, RADIUS, TACACS+ та стандарту 802.1X;
2. Дослідження можливостей рішення Cisco Identity Services Engine;
3. Побудова проекту мережі у віртуальному програмному середовищі GNS3;
4. Налагодження рішення Cisco Identity Services Engine та його інтеграція з Windows Server;
5. Налагодження мережевого обладнання для роботи з AAA, RADIUS, TACACS+ та стандартом 802.1X.

Об’єктом дослідження є протоколи AAA, RADIUS, TACACS+, стандарт 802.1X особливості їх налаштування та застосування, можливості рішення Cisco Identity Services Engine.

Предметом дослідження є розробка проекту у віртуальном програмному середовищі GNS3 з використанням віртуальних образів Windows Server, Cisco Identity Services Engine, Windows 10, налагодженням мережевого обладнання та роботою з протоколоми AAA, RADIUS, TACACS+ та стандартом 802.1X.

РОЗДІЛ 1. ПРОТОКОЛИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ РОБОТИ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

1.1. Протокол AAA

При будівництві і експлуатації мережі важливо мати строгий контроль над тими, хто має доступ до її пристроїв. Якщо мережа невелика і число її користувачів невелике, то стежити за доступом і безпекою не складає труднощів, і часто за це відповідає один мережевий адміністратор. Але якщо організація має масштабну корпоративну мережу або це мережа оператора зв'язку з великим числом абонентів, то відслідковувати вручну, хто до чого має доступ, стає неможливо. У цьому випадку на допомогу приходить AAA.

AAA визначає архітектуру, яка аутентифікує та надає авторизацію користувачам та обліковує їх діяльність [28]. Якщо AAA не використовується, мережева архітектура «відкрита», де кожен може отримати доступ і зробити що завгодно, без будь-якого відстеження. Архітектура відкритої мережі зазвичай використовується в малому бізнесі, де доступ до офісу може бути фізично контрольований. Архітектура відкритої мережі погано підходить для провайдерів, де доступ потрібно суворо контролювати та враховувати [5].

У систему можна включити лише частину AAA. Наприклад, якщо компанія не переймається питанням оплати користувачів за користування мережею, вони можуть вирішити як аутентифікувати, так і авторизувати користувачів, але ігнорувати діяльність користувачів і не займатися бухгалтерським обліком. Так само система моніторингу шукатиме незвичну діяльність користувачів (облік), але може делегувати рішення про аутентифікацію та авторизацію в іншій частині мережі.

Без AAA мережевому адміністратору доведеться статично налаштувати мережу. AAA забезпечує гнучкість мережевої політики. AAA також дає мережевим адміністраторам можливість переміщати системи; без AAA їм доведеться чітко визначити параметри підключення.

Сьогодні розповсюдження мобільних пристроїв, різноманітних споживачів мережі та методів доступу до мережі поєднуються, щоб створити середовище, яке ставить більші вимоги до ААА. ААА має роль у майже всіх способах доступу до мережі: бездротові гарячі точки використовують ААА для безпеки; розділеним мережам потрібен ААА для забезпечення доступу; всі форми віддаленого доступу використовують ААА для авторизації віддалених користувачів.

Принцип роботи протоколу ААА можна описати, щоб зробити будь-яку дію в мережі ми повинні відслідковувати:

1. Хто ініціює цю дію (аутентифікація);

2. Чи має він право на виконання цієї дії (авторизація);

3. Що в журнал записані всі дії, які він скоїв (аудит/облік);

Існує два основних типи ААА для мереж:

1. Адміністрування мережевих пристроїв;

2. Доступ до мережі;

Адміністрування мережевих пристроїв зазвичай здійснює управління тими, у кого є доступ для входу в консоль мережевого пристрою, SSH-сесію, Telnet-сесію, або з використанням іншого методу. В той час як доступ до мережі ідентифікує користувача або пристрій ще до того, як йому буде надано доступ до мережі.

У сучасних комп’ютерних мережах використовують два основних рішення для ААА протоколи RADIUS і TACACS+.

Далі детально розглянемо основні компоненти протоколу ААА.

Аутентифікація - процес перевірки ідентичності користувача шляхом зіставлення даних, наданих користувачем (наприклад, імені, пароля) тим, які налаштовані на сервері ААА. Якщо облікові дані співпадають, користувач аутентифікується та отримує доступ до мережі. Якщо облікові дані не збігаються, аутентифікація не відбувається, а доступ до мережі забороняється. Аутентифікація також може не вдатися, якщо облікові дані користувачів введені неправильно. Наприклад, політика щодо веб-сайтів може дозволити

користувачеві доступ до мережі з місця розташування за допомогою пароля типу clear text. Однак якщо той самий пароль введений користувачем з віддаленого місця, доступ може бути заборонений. Інтернет-провайдери можуть забороняти доступ до мережі аутентифікованим користувачам, якщо обліковий запис користувачів було призупинено.

Авторизація – друга «А» в абревіатурі - процедура, значення якої часто недооцінюється або взагалі не сприймається як самостійна дія, так як у багатьох випадках авторизація виконується або одночасно з аутентифікацією, або з обліком [4]. Проте, авторизація має важливе значення в забезпеченні функцій ААА. Авторизація - наступний крок після успішної аутентифікації, визначення повноважень доступу до ресурсів. Аутентифікація дозволяє тільки переконатися, що особа або пристрій який претендує на доступ до ресурсів є саме тим, за кого себе видає. Після того як особистість достовірно встановлено, починається процес авторизації, тобто визначення, яка частина ресурсів може бути надана даному користувачу. Можливо, у людини є право проникнути в перше приміщення, але заборонено проходження далі. На мережевому диску права доступу найчастіше визначають перелік команд, які може виконати користувач, який пройшов аутентифікацію. Наприклад, мережевому інженеру з 1-м рівнем доступу дозволяється тільки перегляд конфігурації пристрою за допомогою команди show, а інженеру з 2-м рівнем доступу надається можливість вносити зміни. Фактично, авторизація має місце в будь-якій мережі.

Аудит/Облік - паралельний з аутентифікацією і авторизацією етап, який записує в журнал інформацію про виконання даних процесів, таких як:

1. Вдалось людині проникнути в приміщення чи ні;

2. Отримав користувач доступ до мережевих пристроїв і, якщо так, то які дії на ньому здійснював;

Цей процес важливий з точки зору безпеки та контролю доступу, так як дозволяє визначати потенційні загрози і шукати «вразливості» в системі.

1.2. Протоколи RADIUS, TACACS+

1.2.1. Протокол централізованої аутентифікації RADIUS

Під час створення протоколу RADIUS, системи доступу до мережі вже були розповсюджені по всій території та керували різними організаціями. Центральні адміністратори хотіли запобігти проблем із безпекою та масштабованістю, тому не хотіли поширювати імена та паролі користувачів. Натомість вони хотіли, щоб сервери віддаленого доступу звертались до центрального сервера, а він в свою чергу мав дозволити доступ до запитуваної системи чи послуги. У відповідь на контакт з сервером віддаленого доступу, центральний сервер мав повернути повідомлення з дозволом або відмовою, а вже віддалене мережеве обладнання буде виконувати обробку відповіді від сервера для кожного кінцевого користувача.

Таким чином, метою RADIUS було створити центральне місце для аутентифікації користувачів, в якому користувачі з багатьох місць можуть запитувати доступ до мережі.

Простота, ефективність та зручність використання системи RADIUS призвела до її широкого прийняття постачальниками мережевого обладнання настільки, що в даний час RADIUS вважається галузевим стандартом. RADIUS має широке поширення і підтримується більшістю виробників пристроїв і розробниками програмних продуктів [2].

Сучасна реалізація RADIUS використовує протокол UDP з відповідними портами. Порт 1812 для аутентифікації та 1813 порт для обліку (також можливе використання інших портів 1645 і 1646). Протокол UDP має високу швидкість, але також має ряд недоліків, які необхідно враховувати при його застосуванні, такі як безпека. Протокол RADIUS шифрує тільки поле з паролем і в цілому має середній ступінь безпеки.

RADIUS використовує модель клієнт/сервер. Запити на доступ надсилаються від клієнта на сервер RADIUS для підтвердження. Сервер отримує запити як пакет, що містить ім'я користувача, пароль, IP-адресу та порт клієнта,

а потім запитує базу даних про відповідність облікових даних. Залежно від інформації, отриманої від клієнта, сервер потім поверне дію/відповідь типу accept, reject або challange і надасть доступ до запитуваної послуги відповідно.

Клієнт RADIUS (або мережевий сервер доступу NAS) - це мережевий пристрій (наприклад, концентратор VPN, маршрутизатор, комутатор), який використовується для аутентифікації користувачів, а сервер RADIUS - це фоновий процес, який працює на сервері UNIX або Windows [3]. Це дозволяє підтримувати профілі користувачів у центральній базі даних. Отже, якщо у вас є сервер RADIUS, ви маєте контроль над тим, хто може з'єднатися з вашою мережею.

Зв'язок між NAS і сервером RADIUS заснований на протоколі UDP. В цілому вважається, що протокол RADIUS не має відношення до підключення. Всі питання, пов'язані з доступністю сервера, повторною передачею даних і відключеннями через певний період часу, контролюються мережевими пристроями, що працюють під управлінням протоколу RADIUS, але не самим протоколом передачі. Операції між клієнтом і сервером RADIUS аутентифіковані за допомогою загального ключа секрету, який ніколи не передається по мережевим каналам [25]. Крім того, обмін паролями користувачів між клієнтом і сервером RADIUS йде тільки в зашифрованому вигляді, що виключає підслуховування чужих паролів і подальше зловживання ними.

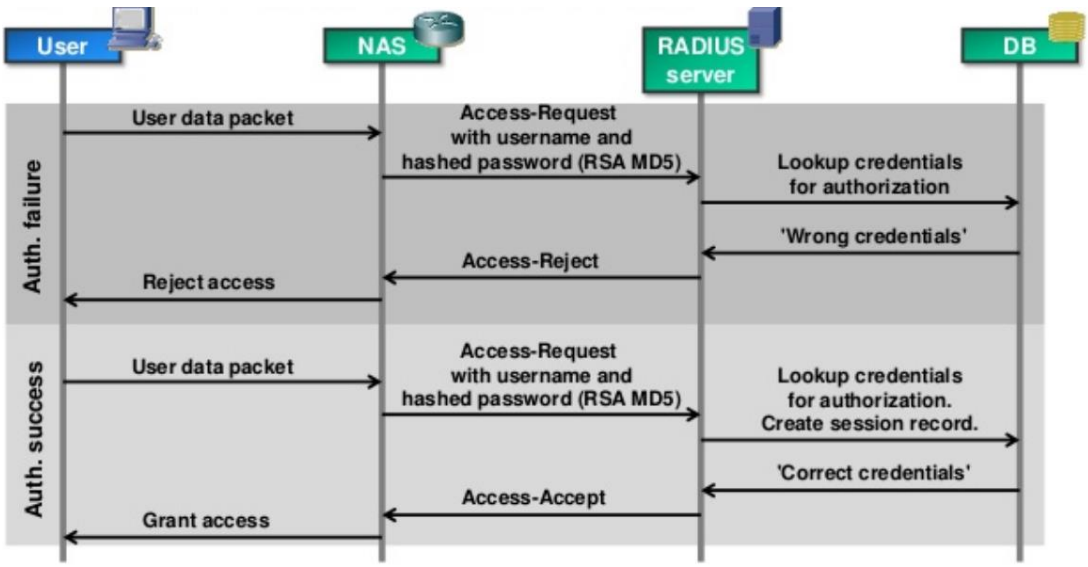


Рис. 1.1. Процес аутентифікації RADIUS

Сервер RADIUS підтримує різноманітні методи аутентифікації користувача. Аутентифікація та авторизація сервера RADIUS виконуються майже одночасно і зазвичай поєднуються, коли користувач намагається підключитися до клієнта RADIUS за допомогою імені користувача та пароля. Основний процес аутентифікації та авторизації RADIUS включає наступні етапи:

1. Клієнт RADIUS намагається пройти аутентифікацію на RADIUS сервері за допомогою облікових даних користувача (ім’я користувача та пароль).

2. Клієнт надсилає повідомлення із запитом доступу на сервер RADIUS. Повідомлення містить загальний ключ секрет. Паролі завжди шифруються у повідомленні Access-Request.

3. Сервер RADIUS зчитує загальний ключ секрет і гарантує, що повідомлення про запит доступу отримує від авторизованого клієнта. Якщо запит на доступ не від авторизованого клієнта, повідомлення відкидається.

4. Якщо клієнт має авторизацію, сервер RADIUS зчитує запитуваний спосіб аутентифікації.

5. Якщо метод аутентифікації дозволений, сервер RADIUS зчитує дані користувача з повідомлення. Він звіряє їх з обліковими даними користувачів в базі даних. Якщо є збіг, сервер RADIUS витягує додаткові дані користувача з бази даних.

6. Тепер сервер RADIUS перевіряє, чи існує політика доступу або профіль, який відповідає обліковим даним користувачів.

7. Якщо немає відповідної політики, сервер надсилає повідомлення про відхилення доступу. Транзакція RADIUS закінчується, і користувачеві забороняється доступ до системи.

8. Якщо існує відповідна політика, сервер RADIUS надсилає на пристрій повідомлення про дозвіл доступу.

9. Повідомлення Access-Accept складається з загального ключа секрету та атрибута Filter ID. Якщо загальний ключ секрет не співпадає, клієнт RADIUS відхиляє повідомлення.

10. Якщо загальний ключ секрет співпадає, клієнт зчитує значення атрибута Filter ID. Ідентифікатор фільтра - це рядок тексту. Клієнт RADIUS підключає користувача до певної групи RADIUS за допомогою цього ідентифікатора фільтра. Група RADIUS - це група користувачів, які мають однакове значення FilterID. Практично група RADIUS полегшує розподіл користувачів за функціональними групами (наприклад, відділ продажів, адміністратори, тощо).

11. Користувач остаточно проходить аутентифікацію та авторизацію і отримає доступ до клієнта RADIUS.

Сервери RADIUS також використовуються для обліку. Облік збирає дані для моніторингу мережі, на початку і в кінці кожної сесії [24]. Відправляються дані про кількість ресурсів, які використовуються в ході цієї сесії (пакети, байти, час і т.д.). Процес обліку зазвичай починається, коли користувачу надається доступ до сервера RADIUS. Однак облік RADIUS також може використовуватися незалежно від аутентифікації та авторизації.

Основний процес обліку RADIUS включає наступні етапи:

1. Процес починається, коли користувачеві надається доступ до сервера RADIUS.

2. Клієнт RADIUS надсилає на RADIUS-сервер пакет RADIUS Accounting-Request, відомий як «облік». Пакет запитів містить ідентифікатор користувача, мережеву адресу, ідентифікатор сеансу та точку доступу.

3. Під час сеансу клієнт може надсилати на сервер RADIUS додаткові пакети обліку-запиту, відомі як тимчасові оновлення. Ці пакети містять деталі, такі як поточна тривалість сеансу та використання даних. Цей пакет служить метою оновлення інформації про сеанс користувача на сервер RADIUS.

4. Після того, як доступ користувача до сервера RADIUS закінчується, Клієнт RADIUS надсилає на сервер RADIUS інший пакет обліку-запиту, відомий як Stop Accounting. Пакет включає інформацію, таку як загальний час, дані, пакети, та іншу інформацію, що стосується сеансу користувача.

1.2.2. Протокол управління доступом TACACS+

TACACS+ - протокол AAA, який розробляється Cisco. Через деякий час TACACS+ став стандартним протоколом, який підтримується всіма постачальниками. Основним обов'язком TACACS+ є забезпечення адміністрування пристроїв. Він також може використовуватися для доступу до мережі. За допомогою цього протоколу мережеві адміністратори аутентифікуються для входу в мережу таких пристроїв, як маршрутизатори, комутатори тощо. TACACS+ користується протоколом TCP. TACACS+ використовує порт 49 протоколу управління передачею (TCP) для зв'язку між клієнтом TACACS+ та сервером TACACS+ [23].

Протокол TACACS+ працює за технологією клієнт/сервер, де клієнтом TACACS+ є пристрій мережевого доступу (NAD) або сервер мережевого доступу (NAS), а сервером TACACS+, вважається процес «демон» запущений на машині UNIX. Прикладом є комутатор Cisco, що підтверджує та надає адміністративний доступ до IOS CLI комутатора. Комутатор - клієнт TACACS+, а Cisco Identity Services Engine - сервер.

Одним із ключових переваг протоколу TACACS+ є його здатність розділяти аутентифікацію, авторизацію та облік як окремі та незалежні функції [16]. Це надає можливість обмінюватись аутентифікаційними повідомленнями будь-якої довжини і змісту та використовувати для клієнтів TACACS+ будь-який аутентифікаційний механізм.

Адміністрування пристроїв може мати дуже інтерактивний характер, з необхідністю пройти аутентифікацію один раз, але виконовати авторизацію багато разів під час одного адміністративного сеансу в командному рядку пристрою. Маршрутизатору або комутатору може знадобитися авторизувати діяльність користувача на основі виконуваної команди. TACACS+ призначений для забезпечення цього типу авторизації.

Зазвичай аутентифікація передує авторизації, проте це не обов'язково. У запиті на авторизацію можна вказати, що аутентифікація користувача не проведена (особистість користувача не підтверджена). У цьому випадку особа,

яка відповідає за авторизацію, має самостійно вирішити, допускати такого користувача до запитуваної послуги чи ні. Протокол TACACS+ допускає тільки успішну або неуспішну авторизацію. Авторизація може проводитися на різних етапах, наприклад, коли користувач вперше входить в мережу і хоче відкрити графічний інтерфейс або коли користувач запускає PPP і намагається використовувати поверх PPP протокол IP з конкретною адресою IP. У цих випадках процес «демон» сервера TACACS+ може дозволити надання послуг, але накласти обмеження за часом або запросити список доступу IP для каналу PPP.

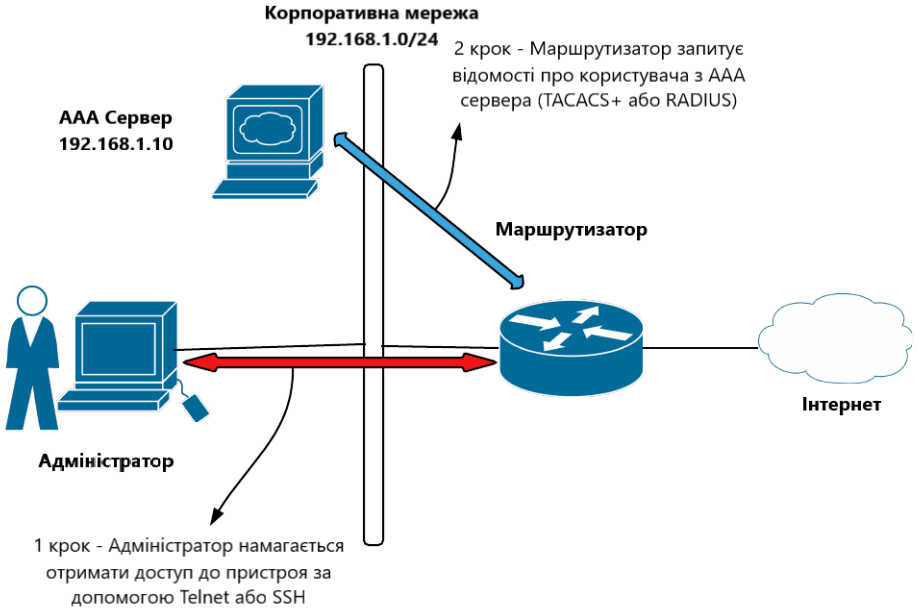


Рис. 1.2. Принцип роботи TACACS

Облік є записом дій користувача і зазвичай виконується після аутентіфікації і авторизації. В системі TACACS+ облік може виконувати два завдання:

1. Враховувати використані послуги;

2. Забезпечувати безпеку;

Для цього TACACS+ підтримує три типи облікових записів. Записи «старт» вказують, що послуга повинна бути запущена. Записи «стоп» говорять про те, що послуга тільки що закінчилася. Записи «оновлення» є проміжними і вказують на те, що послуга все ще надається. Облікові записи TACACS+ містять

всю інформацію, яка використовується в ході авторизації, а також інші дані, наприклад, дані про використання ресурсів, час початку і закінчення.

Транзакції між клієнтом і сервером TACACS+ ідентифікуються за допомогою загального ключа секрету, який ніколи не передається по каналах зв'язку. Зазвичай цей секретний ключ вручну встановлюється на сервері і на клієнті. Протоколи AAA можуть зашифрувати повний пакет або лише паролі. Тут TACACS + забезпечує повне шифрування пакетів.

Процес аутентифікації протоколу TACACS+ використовує пакети трьох видів: Reply, Start, Continue. Пакети Start і Continue завжди відправляються клієнтом, а пакет Reply - сервером.

Аутентифікація розпочинається тоді, коли клієнт відправляє серверу повідомлення Start, яке описує тип майбутньої аутентифікації і може містити аутентифікаційні дані (ім'я користувача та додаткові інші дані) [9]. Пакет Start відправляється тільки в якості першого повідомлення аутентифікаційної сесії TACACS+ або відразу ж після повторного запуску цієї сесії.

У відповідь на повідомлення почтаку сесії Start сервер відправляє повідомлення відповідь Reply. Повідомлення Reply вказує, чи аутентифікація була завершена або її необхідно продовжити. Якщо пакет Reply вимагає продовження аутентифікації, тоді він вказує, що йому необхідно отримати додаткову інформацію, щоб дозволити аутентифікацію. Клієнт збирає цю інформацію і відправляє її на сервер в повідомленні Continue.

Після успішної аутентифікації клієнт може почати процес авторизації. Сесія авторизації складається з двох повідомлень: повідомлення запиту Request і наступного за ним повідомлення відповіді Response. Повідомлення типу Request містить фіксоване число полів, які описують користувача, процес, і змінний набір аргументів, що описують послуги і опції, які вимагають авторизації.

1.2.3. Порівняння протоколів RADIUS, TACACS+

Таблиця 1.1

Параметри	RADIUS	TACACS+
Протоколи та порти	UDP: 1812, 1813 UDP: 1645, 1646	TCP: 49
Сервіси	Об’єднує аутентифікацію та авторизацію	Різні процеси для аутентифікації, авторизації та обліку
Шифрування	Шифрується тільки пароль в пакеті запиті доступа	Шифрується весь пакет протоколу TACACS+ крім заголовку
Підтримка AAA	Повна модель AAA	Тільки аутентифікація і авторизація
Виконання операцій	Дискретна AAA (можливість виконання тільки однієї функції)	Аутентифікація і авторизація при кожній операції
Підтримувані типи аутентифікації	Clear text (ASCII, PAP), CHAP	Clear text (ASCII, PAP), CHAP, ARAP
Можливість перенапревлення запиту	Наявна	Відсутня
Основне призначення	Доступ до мережі	Адміністрування пристроїв

Основні відмінності зводяться до того, що TACACS+ шифрує весь вміст пакету, залишаючи тільки простий заголовок [20]. Такий спосіб захищає від зловмисників, які прослуховують повідомлення, що передаються між пристроями. Також TACACS+ реалізує функції AAA окремо, що дозволяє винести кожну з них на окремий сервер або навіть використовувати інший протокол.

TACACS+ також пропонує тіснішу інтеграцію з пристроями Cisco і дозволяє здійснювати детальне управління маршрутизаторами (процес авторизації). З сервером TACACS+ можливо реалізувати управління командами із застосуванням рівнів доступу, які налаштовуються на самих пристроях. RADIUS дозволяє частково реалізувати цю можливість, але не так добре і гнучко, як TACACS+.

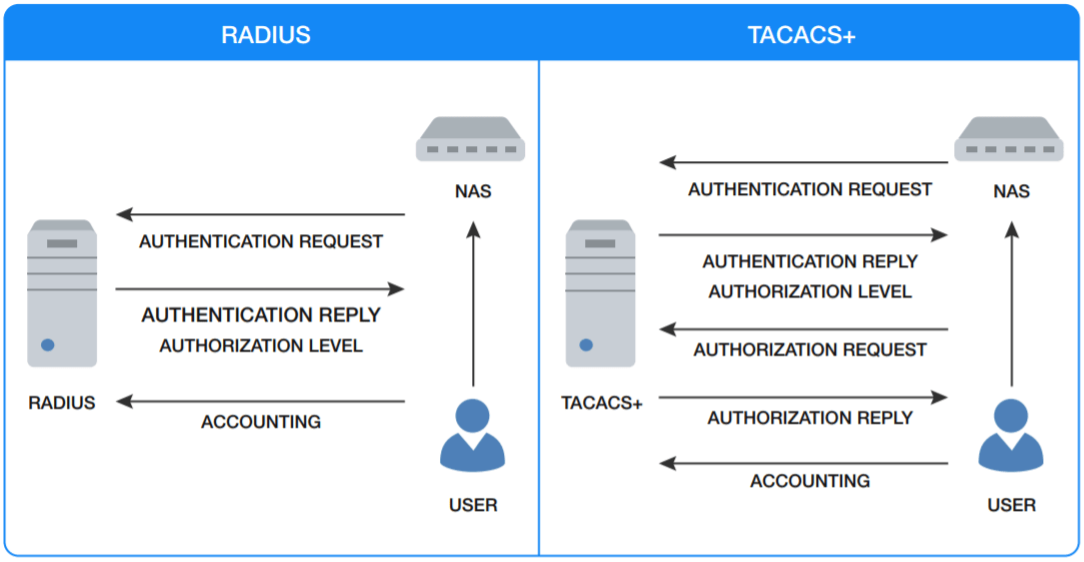


Рис. 1.3. Порівняння запитів під час роботи RADIUS та TACACS+

TACACS + також підтримує декілька інших техологій, таких як AppleTalk, NetBIOS, NetWare Asynchronous Service Interface (NASI) і X.25, але в сучасних мережах їх майже не використовують.

При використанні протоколу TACACS+ між клієнтом і сервером не може бути брендмауера, так як сервер повинен отримати запит від клієнта з його IP-адресою, а не з адресою брендмауера. У RADIUS IP-адреса клієнта міститься ще і в самому пакеті, що дозволяє AAA-серверу отримати її звідти.

А ось найбільший недолік TACACS+ полягає в тому, що Cisco розробила цей протокол для власних потреб і тому найширшу його підтримку отримали саме мережеві пристрої цієї компанії. Однак поступово ситуація змінюється, і інші виробники стали також підтримувати потокол TACACS+.

Який протокол для AAA-сервера використовувати, необхідно вибирати в залежності від завдання. Якщо це адміністрування пристроїв, то TACACS+ стане кращим варіантом, а якщо доступ до мережі, то більш універсальний і швидкий - RADIUS.

1.3. Стандарт котнролю доступу і аутентифікації 802.1X

Стандарт мережевої аутентифікації IEEE 802.1X знайшов широку підтримку у виробників мережевого обладнання та програмного забезпечення як для бездротових, так і для провідних мереж. Якщо говорити про технології мережевої аутентифікації користувачів, варто згадати протокол PPP. Протокол PPP спочатку використовувався для підключення віддалених користувачів, і тому він повинен був мати механізми аутентифікації користувачів. Спочатку підтримувалася тільки передача імені користувача або пароля в нешифрованому вигляді, що не відповідає сучасним вимогам мережевої безпеки [10].

Отже, протокол PPP спочатку використовувався для підключення віддалених користувачів, і тому він повинен був мати механізми аутентифікації користувачів. Спочатку підтримувалася тільки передача імені користувача або пароля в нешифрованому вигляді, що не відповідає сучасним вимогам мережевої безпеки.

Останнім часом були розроблені нові механізми аутентифікаціі під загальною назвою EAP. EAP - стандартний протокол аутентифікації, який використовується в зашифрованих мережах, є протоколом розширеної аутентифікації, який забезпечує захищений метод надсилання ідентифікаційної інформації для аутентифікації мережі [18]. Протокол був створений з метою скасування приватних механізмів аутентифікації і поширення стандартизованих підходів типу «запит-відповідь» challenge-response та інфраструктури, основаної

на публічних ключах і призначених для користувача сертифікатах. Стандартизація механізмів EAP дозволила зробити аутентифікацію прозорою для серверів доступу різних виробників. Наприклад, при підключенні користувача до сервера віддаленого доступу та використання механізму EAP протоколу PPP для аутентифікації, сам сервер доступу не повинен знати або підтримувати конкретні механізми або алгоритми аутентифікації. Його завдання в цьому випадку - лише передати пакети EAP-повідомлень RADIUS-сервера, на якому фактично проводиться аутентифікація [7]. У цьому випадку сервер доступу виконує роль посередника між клієнтом і RADIUS-сервером, в задачі якого входить передача EAP-повідомлень між ними.

Стандарт 802.1X описує процедуру передачі EAP-повідомлень сервером доступу (наприклад, комутатором або бездротовою точкою доступу) в провідних чи безпровідних Ethernet мережах. При цьому стандарт 802.1X безпосередньо упаковує EAP-повідомлення в Ethernet кадри, не застосовуючи для їх передачі протокол PPP. Це викликано тим, що використовувати протокол PPP в багатьох випадках не обов'язково, наприклад, при підключенні Ethernet робочої станції, що не підтримує протокол TCP/IP, або в тому випадку, коли використання протоколу PPP є надмірним.

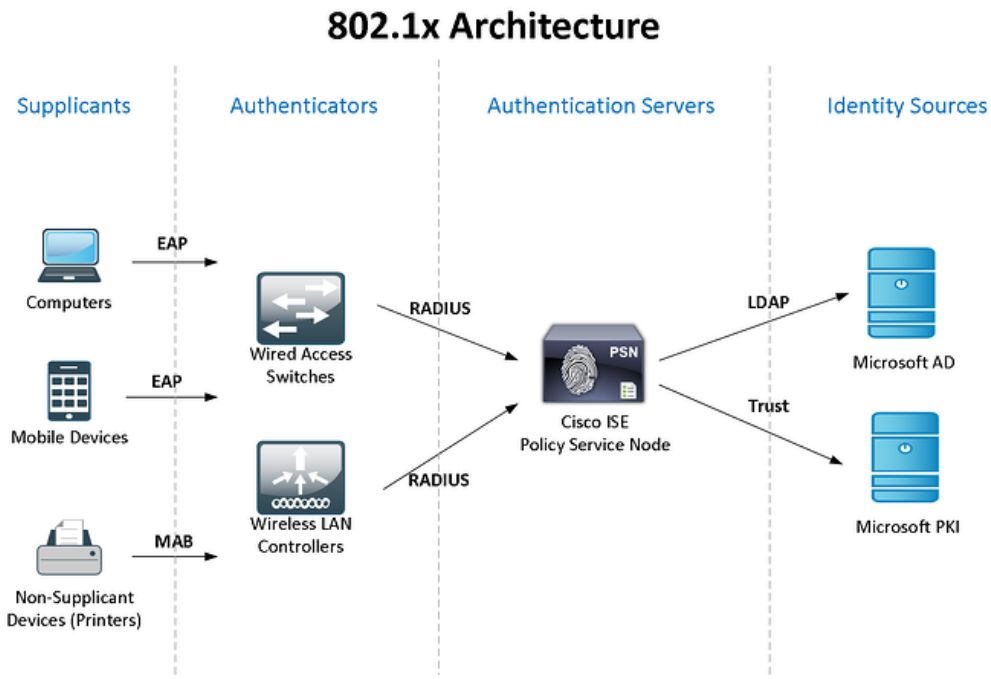


Рис. 1.3. Елементи стандарту 802.1X з рішенням Cisco ISE

У стандарті 802.1X визначається три основних елементи:

1. Суплікант - мережевий пристрій, який збирає облікові дані аутентифікації від кінцевого користувача та передає ці дані для процесу аутентифікації. Наприклад, програмне забезпечення, яке працює на робочій станції, приєднаному до мережевого порту.

2. Сервер аутентифікації - мережевий сервер, який перевіряє облікові дані, що надсилаються заявником на основі інформації, що зберігається в його базі даних, і визначає, чи дозволяти мережевий доступ чи забороняти доступ до мережі. Сервером аутентифікації може бути будь-який сервер RADIUS [27].

3. Аутентифікатор - мережевий пристрій, що знаходиться між суплікантом і сервером аутентифікації і надає доступ в мережу, наприклад, точка доступу або Ethernet комутатор.

Ключовим моментом є те, що мережеві пристрої (аутентифікатори) можуть бути досить простими, оскільки для реалізації функцій 802.1X в них потрібні мінімальні апаратні витрати, в той час як, вся обробка концентрується в RADIUS сервері.

Протокол передачі EAP-повідомлень в стандарті 802.1X називається EAPoL. EAPoL - це абревіатура протоколу розширюваної аутентифікації через локальну мережу. EAPoL - це мережевий протокол аутентифікації, який використовується в стандарті 802.1X. Іншими словами, це протокол інкапсуляції, який використовується між суплікантом і аутентифікатором. Схема роботи протоколу EAPoL досить проста. При цьому можна виділити наступні основні режими роботи:

1. Аутентифікатор надсилає запит на аутентифікацію EAP-Request/Identity супліканту, як тільки він визначить, що якийсь із його Ethemet портів перейшов в активний стан (підключений мережевий адаптер). Якщо відключити робочу станцію клієнта, яка вже пройшла аутентифікацію і знову підключити до порту, то буде потрібно пройти аутентифікацію повторно.

2. Супілікант надсилає повідомлення/відповідь EAP Response/Identity аутентифікатору, яке потім передається їм на сервер аутентифікації RADIUS[26].

3. Сервер аутентифікації у відповідь посилає пакет-запит challenge аутентіфікатору, який потім переупаковує його з IP-транспорту в EAPOL та передає суппліканту. У різних схемах аутентифікації число таких повідомлень може змінюватися. У EAP підтримується як аутентифікація клієнтської сторони, так і взаємна «сильна» аутентифікація клієнта і сервера.

4. Супплікант відповідає на запит у відповідність з обраним алгоритмом і передає його аутентифікатору, який пересилає його на сервер аутентифікації.

5. Якщо супплікант надає правильну відповідь на запит, сервер посилає повідомлення про успішну аутентифікації суппліканту. У цій ситуації аутентифікатор відкриває клієнту доступ до локальної обчислювальної мережі, який може залежати від додаткових параметрів, переданих йому RADIUS сервером.

Стандарт включає декілька видів протоколу EAP:

1. EAP-MD5 - з хешем імені користувача і пароля за алгоритмом MD5.
2. EAP-OTP - з підтримкою доступу за одноразовими паролями.
3. EAP-TLS - аутентифікація з встановленням захищеного каналу SSL.

1.4. Рішення Cisco Identity Services Engine

Контроль доступу - ключовий захід інформаційної безпеки. Впровадження системи контролю доступу до мережі підприємства дозволяє не тільки значно знизити ризики реалізації загроз інформаційної безпеки, але і домогтися економічної вигоди від впровадження такого роду систем.

Cisco Identity Services Engine - багатофункціональне рішення, що закриває повний спектр питань контролю доступу до корпоративної мережі. Централізація політик доступу до мережі та автоматизація багатьох великих завдань - основні переваги рішення Cisco ISE.

Cisco Identity Services Engine - рішення для централізованого управління політиками в рамках рішення Cisco TrustSec. Воно дозволяє ефективно визначати політики інформаційної безпеки та керувати ними в масштабі всієї організації.

Можливості рішення Cisco ISE:

1. Вирішує проблему підтримки «будь-якого пристрою» за допомогою політики контролю доступу з урахуванням контексту;

2. Розрізняє корпоративні і особисті призначені для користувача пристрої;

3. Автоматизує функції забезпечення інформаційної безпеки по всій організації за допомогою засобів контролю доступу та шифрування, реалізованих на рівні мережі;

4. Спрощує повсякденну роботу IT-підрозділу, дозволяючи розробляти політики, що відображають правила ведення бізнесу з урахуванням користувачів, пристроїв, додатків та місця розташування;

Утримувати окрему базу користувачів для кожного рішення контролю доступу незручно. Виникає питання синхронізації з іншими подібними базами. В більшості організацій є корпоративний каталог - єдине місце зберігання даних про користувачів. Найчастіше це Microsoft Active Directory, але може бути і LDAP сервер. Зручно заводити користувачів в одному місці і управляти більшістю налаштувань їх робочого оточення. Безліч систем можуть отримувати дані з активного каталогу: поштовий сервер, CRM та ін. Проблема в тому, що «мережа» не вміє проводити аутентифікацію в каталозі. Має бути проміжний пристрій, що розуміє, наприклад MS AD і мережу.

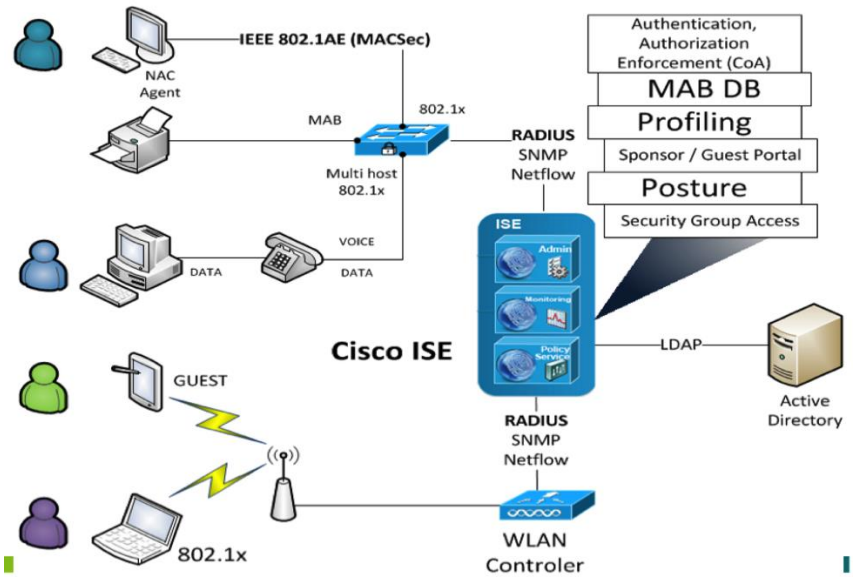


Рис. 1.5. Приклад архітектури рішення КД на базі Cisco ISE

В сучасних дизайнах мереж Cisco роль такого RADIUS сервера виконує Cisco ISE. Крім цього, Cisco ISE дозволяє автоматизувати безліч завдань, які неминуче виникають спільно з проектами впровадження RADIUS сервера для контролю доступу до мережі.

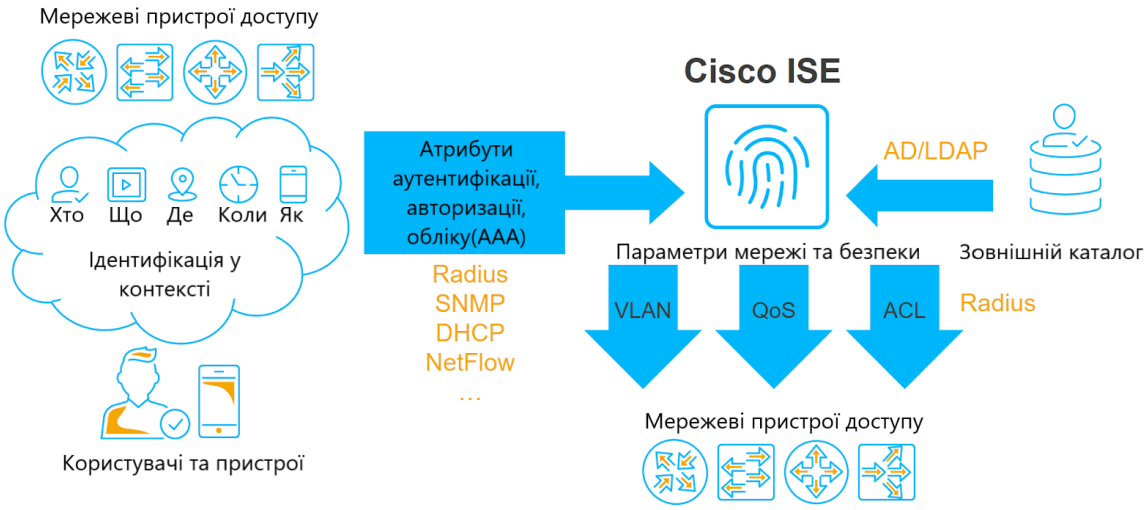


Рис. 1.6. Структура мережевої взаємодії рішення Cisco ISE

Cisco ISE дозволяє вирішити цілий комплекс завдань, пов'язаних з КД. Для підвищення спостережливості і швидкості вирішення проблем доцільно впровадити єдине рішення, глибоко інтегроване в існуючу інфраструктуру і яке буде зв'язувати воєдино всі політики доступу на мережевому обладнанні. Таке завдання для IT-підрозділів вирішує Cisco ISE.

Cisco ISE дозволяє домогтися спрощення і централізації політики мережевого доступу.

Корпоративна інформація має свою цінність. Контроль доступу до мережі - один із засобів захисту інформації. При такому різноманітті варіантів підключень ручне управління політиками стає досить важким і це вносить значні затримки на швидкість реакції мережі на зміни. Деякі завдання, такі як моніторинг стану підключень до мережі в реальному часі, неможливо здійснити вручну і однозначно вимагають розробки будь-яких скриптів і зведення воєдино всіх їх функцій в одну систему управління. Щоб мати

впевненість у тому, що в мережі підприємства тільки довірені пристрої, необхідна централізація управління політиками мережі і глибока інтеграція з іншими мережевими сервісами [13].

Значно скоротивши операційні витрати, можна підвищити ефективність роботи IT і підприємства в цілому. Впровадження засобів автоматизації мережевих політик доступу дозволить розділити завдання і зони відповідальності IT та ІБ. Витрати часу на внутрішні і зовнішні обіки також можуть бути зведені до мінімуму. Вся облікова інформація зберігається в одному місці. Завжди є можливість оцінити поточний стан.

Впровадження рішення автоматизації контролю доступу Cisco ISE дозволить знизити операційні витрати на супровід всіх мережевих сервісів [12].

Cisco ISE допоможе прискорити прийняття нових технологій підтримки бізнесу. Такі тренди як Mobility, BYOD можуть бути легко прийняті на озброєння IT-підрозділами.

Варто зазначити, що використання Cisco ISE дозволить значно знизити витрати в ЦОД за рахунок застосування нових архітектур і технологій. Важливо мати єдине рішення, що зв'язують політики доступу на різних пристроях: комутатори доступу, інфраструктура ЦОД.

Завдяки Cisco ISE є можливість розмежувати доступ по багатьом критеріям:

1. Хто повинен мати доступ;
2. З яких пристроїв;
3. В який час доби;
4. Через які мережеві пристрої;
5. Який рівень доступу необхідний;

Підрозділи інформаційної безпеки - основний внутрішній замовник рішень контролю мережевого доступу.

Контроль доступу - первинна міра безпеки. Cisco ISE надає можливість підвищити простоту контролю над доступом і надати можливість динамічного моніторингу підключення користувачів до мережі. Спрощення і централізація

політики мережевого доступу роблять можливим перегляд інформації, яка раніше була не доступна. Знайти найбільш проблемні моменти, прийняти оперативні заходи для зниження ризиків інформаційної безпеки.

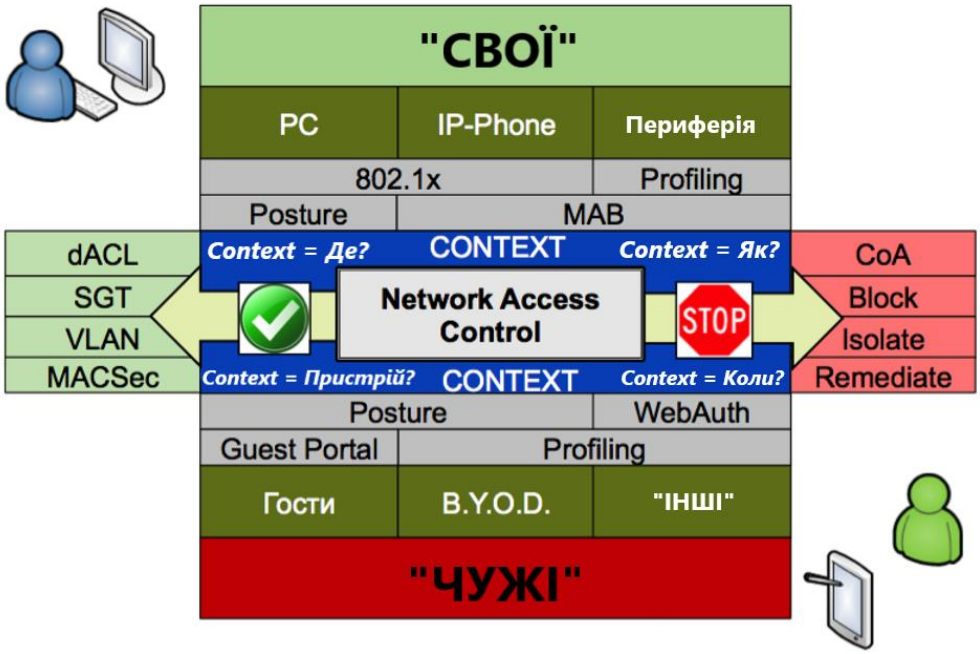


Рис. 1.7. Структура мережевої взаємодії рішення Cisco ISE

Отримуючи в своє розпорядження ефективний інструмент, який дозволяє персоніфікувати доступ в мережу, підрозділи ІБ значно підвищують ефективність своєї повсякденної роботи.

Висновки до першого розділу

В данному розділі було розглянуто протоколи, які необхідні для реалізації підсистеми аутентифікації, сфери у яких вони використовується, розглянуто основне призначення та особоливості протоколів AAA, RADIUS, TACACS+. Проведено порівняльний аналіз протоколів TACACS+ та RADIUS, розглянуто переваги та недоліки кожного. Проаналізовано принцип роботи стандарту 802.1X. В останньому пункті розглянуто рішення Cisco Identity Services Engine, як засіб реалізації проекту, принцип його роботи, для яких цілей використовується та переваги його використання у великих інфраструктурах.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

2.1. Вибір програмного забезпечення

2.1.1. Graphical Network Simulator 3

Graphical Network Simulator 3 (GNS3) - програмне забезпечення, яке забезпечує інтерфейс до засобів для емуляції, таких як Dynamips, VMware, QEMU і дозволяє емулювати та конфігурувати мережеві системи з різними пристроями (Cisco, Juniper, HP, Arista, Citrix, Brocade маршрутизатори та комутаційні пристрої) та різними операційними системами [8]. У додатку є два основні компоненти - це сервер GNS, який управляє всіма технологіями емуляції, та графічний інтерфейс GNS3, що надає простий інтерфейс для взаємодії із сервером [22].

Нижче наведено основні технології і що вони дозволяють:

1. Dynamips - апаратна емуляція Cisco, яка дозволяє працювати із зображеннями IOS, такими як платформа c7200.

2. QEMU - віртуалізація обладнання, що використовується для запуску зображень x86, таких як Cisco ASA, NXos, JunOS, Vyos тощо.

3. KVM - модуль ядра Linux, який дозволяє QEMU підтримувати апаратну віртуалізацію.

4. IOU / IOL - внутрішній процес Cisco Unix / Linux, який імітує IOS без будь-якої віртуалізації.

5. Docker - платформа контейнерів для запуску легких емульованих пристроїв / служб під контейнерами LXC.

6. uBridge - мостовий інструмент для встановлення даних користувачів, який допомагає з'єднувати емульовані пристрої разом.

7. VPCS - легкий симулятор ПК, який забезпечує лише клієнт DHCP та команду ping.

8. VMware Workstation / Fusion VMware - забезпечує прискорену емуляцію x86 на Linux / Windows / macOS, як правило, виключно для запуску попередньо

упакованого віртуального образу сервера GNS3, який містить IOU, KVM, Dynamips тощо. Також можна використовувати для запуску віртуальних машин в топологіях GNS3.

9. VirtualBox - альтернатива VMware з відкритим кодом, однак набагато менш ефективна для запуску віртуальної машини GNS3. Можна також використовувати для запуску віртуальних машин у топологіях GNS3.

Якщо ми порівнюємо GNS3 з іншим популярним програмним забезпеченням, яке використовується в освіті. Cisco Packet Tracer - це дуже широко використовуване програмне забезпечення для моделювання, особливо в програмі Cisco Network Academy. Найбільша відмінність програмного забезпечення GNS3 від програмного забезпечення Cisco Packet Tracer полягає в тому, що GNS3 є емулятором, а Cisco Packet Tracer - симулятором. Отже, поки GNS3 запускає операційну систему, що використовується на реальному маршрутизаторі, Packet Tracer використовує програмно визначену віртуальну операційну систему. Хоча це заважає нам використовувати всі команди конфігурації в програмному забезпеченні Packet Tracer, можна використовувати всі команди, дійсні для IOS, що використовуються в GNS3. Ще одна важлива відмінність полягає в тому, що комутаційні пристрої (комутатори) не емулюються в GNS3, в той час як це можливо в трекері пакетів. У програмному забезпеченні GNS3 комутаційні пристрої можуть використовуватися лише як керовані комутатори. Хоча комутаційні пристрої, доступні за замовчуванням у програмному забезпеченні GNS3, не керуються, це можна подолати, використовуючи маршрутизатори як комутаційний пристрій або з використанням образів типу VIRL які мають комутатори 2-3 рівня з підтримкою керованості.

2.1.2. VMware Workstation

VMware Workstation — гіпервізор компанії VMware для платформ x86 і x86-64, що дозволяє запустити на комп'ютері декілька операційних систем одночасно. Кожна віртуальна машина може виконувати свою власну операційну систему, включаючи Microsoft Windows, Linux, BSD і MS-DOS. VMware Workstation розроблений компанією VMware Inc., підрозділом корпорації EMC.

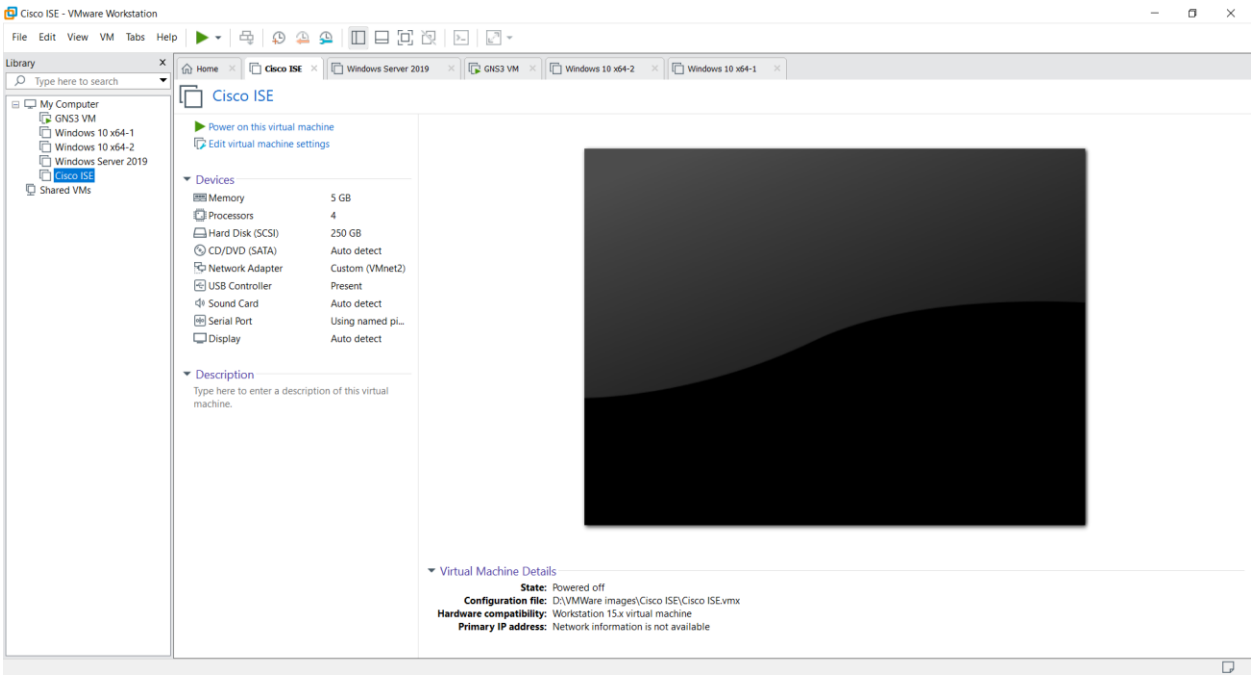


Рис. 2.1. Інтерфейс VMware Workstation

VMware Workstation підтримує з'єднання дійсних мережевих хостів та обміну фізичних дисків і USB пристроїв з віртуальною машиною. Крім того, за допомогою VMware Workstation можна імітувати образи дисків. Можна змонтувати файл ISO у віртуальний привід оптичних дисків, так що віртуальна машина побачить його як реальний диск.

У VMware Workstation є можливість призначати кільком віртуальним машинам команди, які потім можуть бути запущені, закриті, перервані або відновлені як єдиний об'єкт, що робить її особливо корисною для тестування клієнт-серверних середовищ.

Основне завдання настільних засобів віртуалізації - це тестування, дослідження та навчальна діяльність. А це вимагає можливості швидко

обмінюватися між хостом і віртуальними машинами різною інформацією, тому настільні засоби надають загальний буфер обміну, перетягування файлів, загальні папки і т.д. Що в засобах серверної віртуалізації не потрібно і навіть шкідливо, в основному з точки зору безпеки.

Ще одне завдання - взаємодія віртуальних машин з різними типами периферійних пристроїв, в тому числі специфічними, що дуже часто потрібно при розробці та налагодженні, але практично ніколи не потрібно в серверному застосуванні.

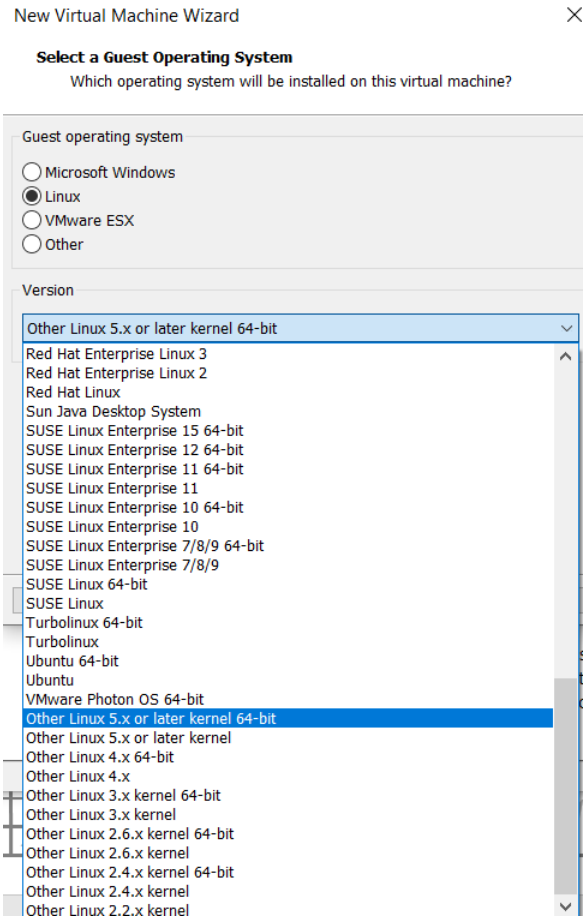


Рис. 2.2. Вибір підтримуваних гостьових систем

Однією з безаперечних переваг VMWare Workstation є найширший вибір підтримуваних гостьових систем. Набагато важче знайти щось непідтримуване. Це вигідно відрізняє даний продукт від Hyper-V, де нормально підтримуються тільки рідні ОС і Linux з ядрами 3.4 і вище, і від VirtualBox, де є проблеми з підтримкою старих ОС.

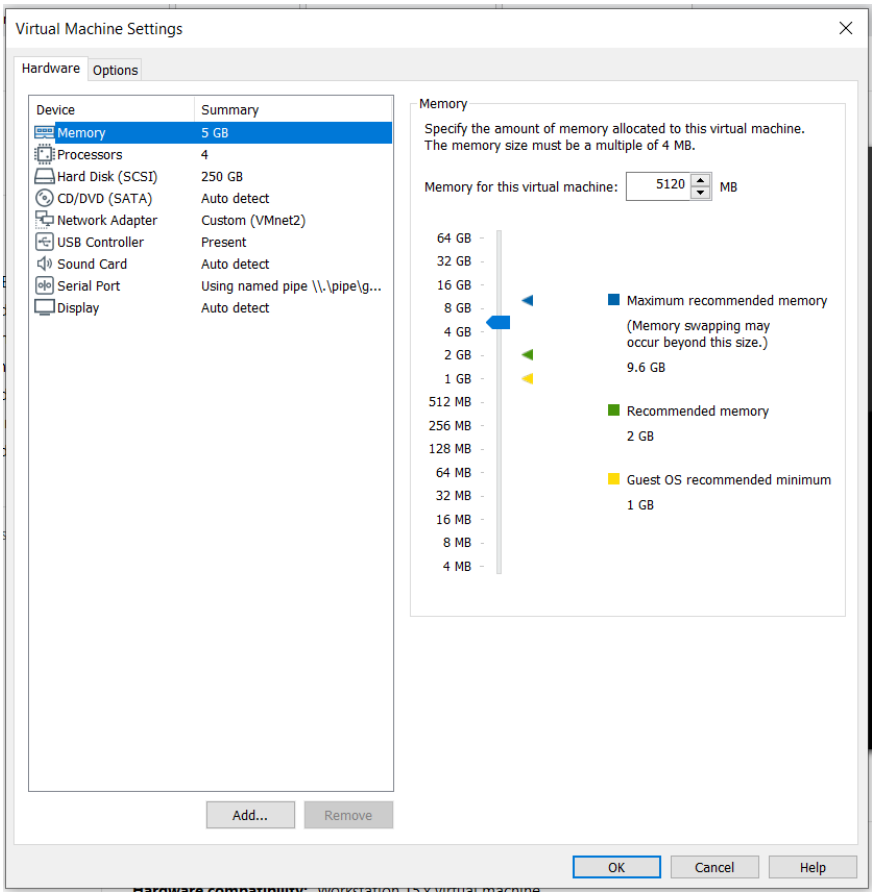


Рис. 2.3. Детальне налаштування обладнання

Переваги VMware:

1. Автоматична встановлення систем за шаблоном;
2. Детальне налаштування обладнання, включаючи налагодження ID процесора, довільної кількості відеопам'яті і інших параметрів;
3. Просте налагодження віртуальної мережі між машинами, піднімається автоматично на відміну від VirtualBox;
4. Покращена підтримка графіки і DirectX 10;
5. Більш повна реалізація BIOS і підтримки EFI;

З мінусів можна назвати відсутність запису відео, відсутність підтримки снапшотів в безкоштовній версії. Хоча машини можна клонувати, таким чином, роблячи знімки, але нативна функціональність знімків набагато зручніше. Якщо брати професійну версію, то там присутні і знімки, і інтеграція з хмарою [21].

2.2. Встановлення рішення Cisco Identity Services Engine

Cisco ISE базується на UNIX системі, тому має схожий принцип встановлення з іншими операційними системами на цій базі, але має деякі відмінності.

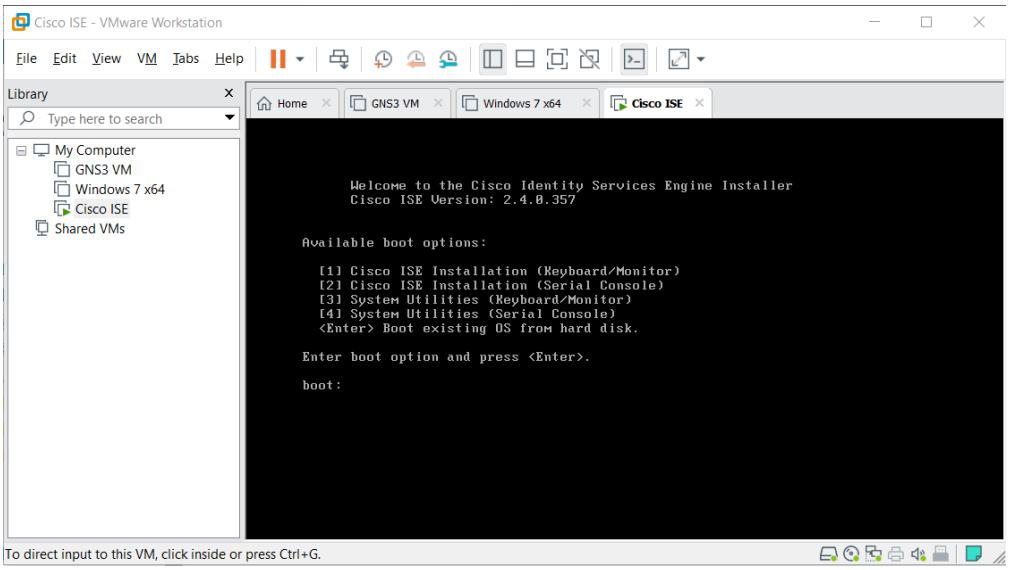


Рис. 2.4. Початок встановлення зображення Cisco ISE

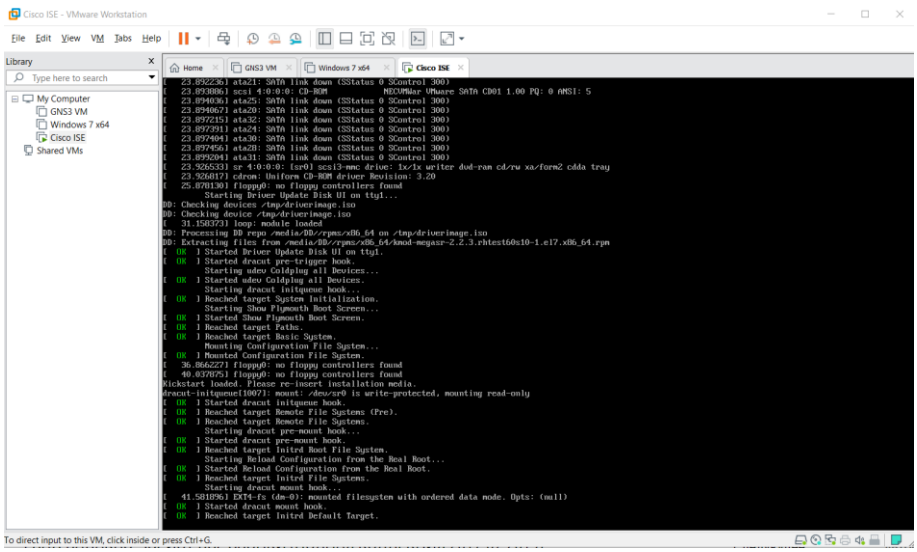


Рис. 2.5. Процесс встановлення зображення

Після розгортання зображення віртуальної машини ми маємо деяку початкову конфігурацію, яку потрібно виконати у майстрі налаштування. Це налагодження проводиться в консолі VMware.

Перший раз, коли ISE включаються після встановлення, він запропонує запустити «налаштування». Де необхідно вказати базові параметри для роботи у мережі.

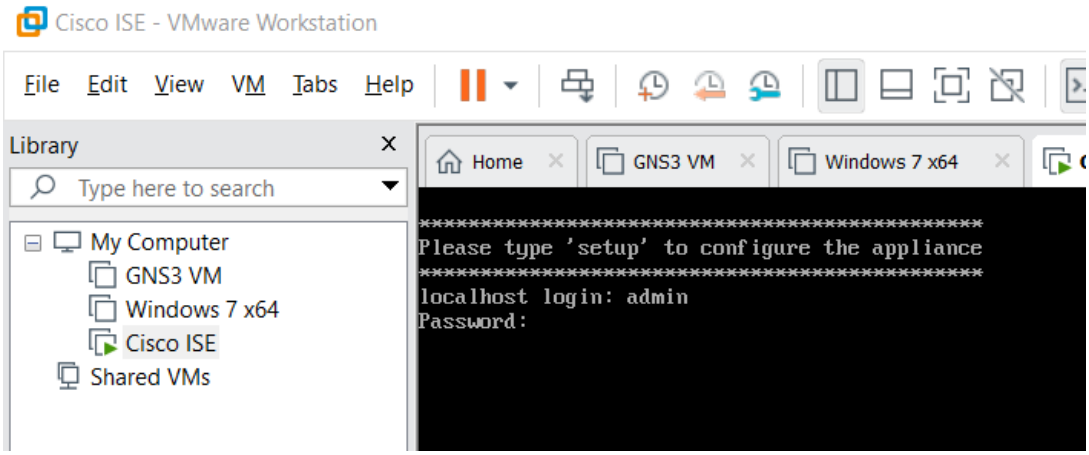


Рис. 2.6. Екран входу

На цьому етапі налаштовуємо параметри IP-вузла ISE та послуги периферійних мереж, назву домену та NTP, вмикаємо можливість віддаленого підключення за допомогою SSH.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ISE
Enter IP address[]: 10.10.10.254
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.10.10.1
Enter default DNS domain[]: ca-center.local
Enter primary nameserver[]: 10.10.10.250
Add secondary nameserver? Y/N [N]: n
Enter NTP server[time.nist.gov]:
Add another NTP server? Y/N [N]: n
Enter system timezone[UTC]: Europe/Kiev
Enable SSH service? Y/N [N]: Y
Enter username[admin]:
Enter password:
Enter password again:
Error: Password must not contain control characters
Enter password:
Enter password again:
Error: Password must not contain control characters
Enter password:
Enter password again:
Error: Password must not contain control characters
Enter password:
Enter password again:
Error: Password must not contain control characters
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
Pinging the gateway...
Gateway ping failed. Retry? Y/N [Y]: N
Testing VM disk I/O performance...
Average I/O bandwidth writing to disk device: 268 MB/second
Average I/O bandwidth reading from disk device: 742 MB/second
I/O bandwidth performance within supported guidelines
Sync with NTP server failed. Incorrect time could render the system unusable until it is re-installed. Retry? Y/N [Y]: N

Do not use 'Ctrl-C' from this point on...
```

Рис. 2.7. Налагодження параметрів ISE

ISE виконує встановлення вузла відповідно наданій інформації при налагодженні, це займає близько 15 хвилин. Після її завершення встановлення знову з’явиться екран входу і у фоновому режимі відбувається ініціалізація всіх компонентів ISE. Знадобиться додатковий час для ініціалізації компонентів ISE. Потрібно виконати команду «show application status ise», щоб побачити, що «Application Server» працює. Запуск серверу залежить від виділених ресурсів і займає приблизно 10 хвилин.

```
ISE/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
------------------------------------------------------------------
Database Listener                      running          2923
Database Server                        running          69 PROCESSES
Application Server                     running          11933
Profiler Database                      running          5091
ISE Indexing Engine                    running          14348
AD Connector                           running          15789
M&T Session Database                   running          4901
M&T Log Collector                      running          12205
M&T Log Processor                      running          12116
Certificate Authority Service          running          15559
EST Service                            running          15880
SXP Engine Service                     disabled
Docker Daemon                          running          5874
TC-NAC Service                         disabled

Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE RabbitMQ Container                 running          6753

ISE/admin# _
```

Рис. 2.8. Всі процеси Cisco ISE запущені та працюють коректно

На цьому етапі початкове базове налагодження для зображення ISE завершено і його можна під’єднувати в інфраструктуру мережі.

2.3. Розробка схеми адресації пристроїв

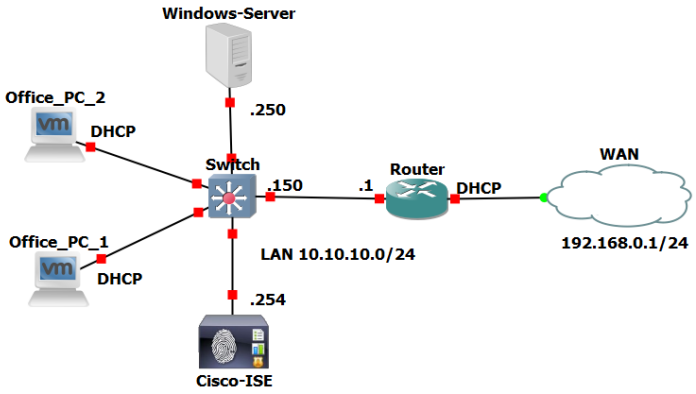


Рис. 2.9. Проект мережі у ПЗ GNS3

Таблиця 2.1

Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/ Мережевий адаптер	IP-адреса	Маска	Префікс
Підмережа A	-	192.168.0.0	255.255.255.0	/24
Підмережа B	-	10.10.10.0	255.255.255.0	/24
Маршрутизатор Router	Gi0/0	DHCP		
	Gi0/1	10.10.10.1	255.255.255.0	/24
Комутатор Switch	Vlan 1	10.10.10.150	255.255.255.0	/24
Windows Server	Eth0	10.10.10.250	255.255.255.0	/24
Cisco ISE	Eth0	10.10.10.254	255.255.255.0	/24
Робоча станція Office_PC_1	Eth0	DHCP		
Робоча станція Office_PC_2	Eth0			

Висновки до другого розділу

В данному розділі було проведено аналіз програмного забезпечення за допомогою якого можливе виконання проекту, такого як GNS3 та VMware Workstation. Наведено сценарій встановлення зображення віртуальної машини на базі рішення Cisco Identity Services Engine. Розроблено адресацію майбутньої мережі, з врахуванням кількості всіх пристроїв.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

3.1. Налагодження мережевого обладнання

В данному пункті буде проведено базове налагодження маршрутизатора для доступу до мережі інтернет та SNMP, комутатора 2 рівня для роботи з TACACS+, RADIUS, SNMP та 802.1X.

Спочатку ми додаємо додатковий інтерфейс типу bridged (міст) для того щоб мати змогу підключитись до фізичної мережі.

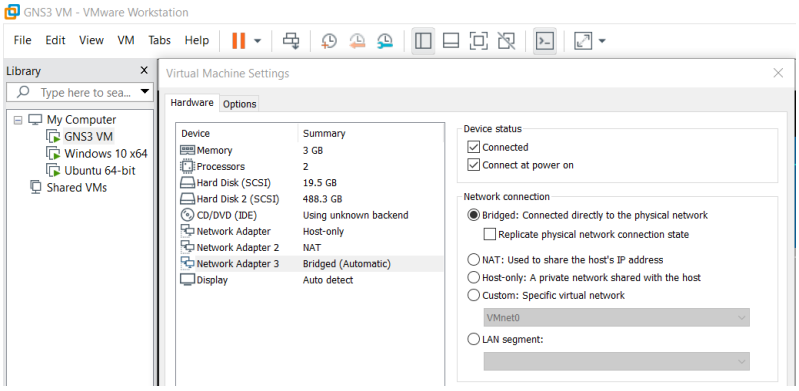


Рис. 3.1. Додавання нового адаптера типу bridged у образі GNS3

Додаємо в проект пристрій Cloud і обов'язково вказуємо сервер GNS3 VM. Для того щоб пристрій підтримував віртуалізацію і міг з'єднатись з фізичною мережею через інтерфейс bridged віртуального образу GNS3 VM.

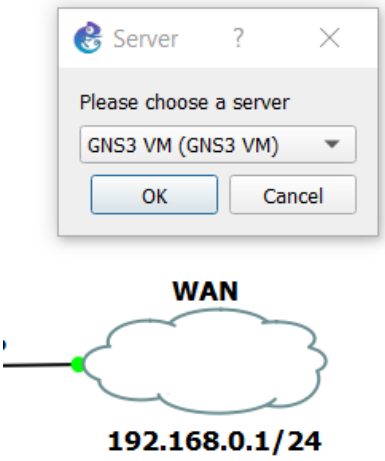


Рис. 3.2. Додавання пристроя Cloud у проекті

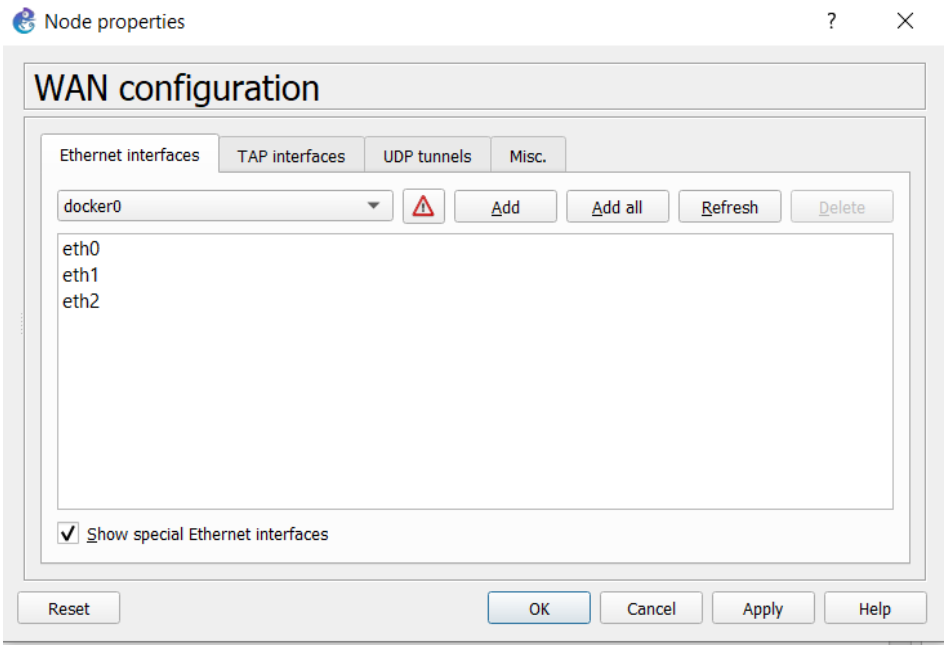


Рис. 3.3. Вибір інтерфейсу GNS3 VM у пристрої Cloud

Робимо базові налагодження на маршрутизаторі. На інтерфейсі який підключений до пристроя Cloud визначаємо ip-адресу динамічно, щоб маршрутизатор із фізичної мережі мав змогу видати адресу нашому віртуальному пристрою. Далі налагоджуємо NAT на інтерфейсах та список доступу.

```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gi0/0
Router(config-if)#ip add dhcp
Router(config-if)#ip nat outside
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#int gi0/1
Router(config-if)#ip add 10.10.10.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#ip domain-lookup
Router(config)#ip name-server 192.168.0.1
Router(config)#access-list 1 permit 10.10.10.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface gi0/0 overload
Router(config)#do copy run st
```

Рис. 3.4. Налагодження маршрутизатора

Після налагоджень маємо побачити повідомлення, що інтерфейсу динамічно призначено IP-адресу з пулу адрес фізичного маршрутизатора.

```
%GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
%DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0 assigned DHCP address 192.168.0.104, mask 255.255.255.0, hostname
```

Рис. 3.5. Динамічно видана ip-адреса на маршрутизаторі

Перевіряємо зв’язок з інтернетом. Фізичний маршрутизатор надає можливість віртуальному маршрутизатору встановити зв’язок з глобальною мережею.

```
Router#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/23 ms
Router#ping google.com
Translating "google.com"...domain server (192.168.0.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.16.14, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/22 ms
Router#
```

Рис. 3.6. Перевірка зв’язку



Рис. 3.7. Фізичний маршрутизатор видав адреси для віртуальних пристроїв

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
Switch(config)#cdp run
Switch(config)#lldp run
Switch(config)#no ip domain-lookup
Switch(config)#ip http server
Switch(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Failed to generate persistent self-signed certificate.
    Secure server will use temporary self-signed certificate.

Switch(config)#ip domain-name ca-center.local
Switch(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Switch.ca-center.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Switch(config)#service password-encryption
Switch(config)#ip ssh version 2
Switch(config)#ip device tracking
Switch(config)#
Switch(config)#username cisco privilege 15 password cisco
Switch(config)#enable secret cisco
Switch(config)#
Switch(config)#int vlan 1
Switch(config-if)#ip add 10.10.10.150 255.255.255.0
Switch(config-if)#ip helper-address 10.10.10.254
Switch(config-if)#no ip redirects
Switch(config-if)#no
*May 30 16:01:18.552: %SSH-5-ENABLED: SSH 1.99 has been enabledip proxy-arp
Switch(config-if)#no sh
Switch(config-if)#exit
```

Рис. 3.8. Базове налагодження комутатора

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#snmp-server community public RO
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server host 10.10.10.254 version 2c public
Switch(config)#
```

Рис. 3.9. Налагодження SNMP на комутаторі

Налагодження SNMP необхідно зробити на всіх мережевих пристроях в інфраструктурі. Це необхідно для в подальшому для того, щоб пристрій ISE мав змогу автоматично визначити інформацію про відповідні пристрої в мережі при вказуванні даних SNMP.

```
Switch(config)#aaa new-model
Switch(config)#
Switch(config)#tacacs server TACACS-ISE
Switch(config-server-tacacs)#address ipv4 10.10.10.254
Switch(config-server-tacacs)#key TACACSSecret654321
Switch(config-server-tacacs)#exit
Switch(config)#
Switch(config)#aaa group server tacacs+ default
Switch(config-sg-tacacs+)#server name TACACS-ISE
Switch(config-sg-tacacs+)#ip tacacs source-interface vlan 1
Switch(config-sg-tacacs+)#exit
Switch(config)#
Switch(config)#aaa authentication login default local group tacacs+
Switch(config)#aaa authentica
*May 30 16:01:20.561: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to up
*May 30 16:01:22.299: %LINK-3-UPDOWN: Interface Vlan1, changed state to uption e
nable default group tacacs+ enable
Switch(config)#aaa authorization config-commands
Switch(config)#$zation exec default group tacacs+ local if-authenticated
Switch(config)#$mands 0 default group tacacs+ local if-authenticated
Switch(config)#$mands 1 default group tacacs+ local if-authenticated
Switch(config)#$mands 7 default group tacacs+ local if-authenticated
Switch(config)#$mands 15 default group tacacs+ local if-authenticated
Switch(config)#aaa accounting exec default start-stop group tacacs+
Switch(config)#aaa accounting commands 0 default start-stop group tacacs+
Switch(config)#aaa accounting commands 1 default start-stop group tacacs+
Switch(config)#aaa accounting commands 7 default start-stop group tacacs+
Switch(config)#aaa accounting commands 15 default start-stop group tacacs+
```

Рис. 3.10. Базове налагодження протоколу TACACS+

```
Switch(config)#radius server radius-ise
Switch(config-radius-server)#$4 10.10.10.254 auth-port 1812 acct-port 1813
Switch(config-radius-server)#key RADIUSSecret123456
Switch(config-radius-server)#timeout 5
Switch(config-radius-server)#retransmit 3
Switch(config-radius-server)#exit
Switch(config)#
Switch(config)#aaa group server radius radius-group
Switch(config-sg-radius)#server name radius-ise
Switch(config-sg-radius)#ip radius source-interface vlan 1
Switch(config-sg-radius)#exit
Switch(config)#
Switch(config)#aaa authentication dot1x default group radius-group
Switch(config)#aaa authorization network default group radius-group
Switch(config)#aaa accounting dot1x default start-stop group radius-group
Switch(config)#aaa accounting system default start-stop group radius-group
Switch(config)#aaa accounting update newinfo periodic 5
Switch(config)#
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#$0.10.254 server-key RADIUSSecret123456
Switch(config-locsvr-da-radius)#exit
Switch(config)#
Switch(config)#radius-server vsa send accounting
Switch(config)#radius-server vsa send authentication
Switch(config)#radius-server attribute 6 on-for-login-auth
Switch(config)#radius-server attribute 6 support-multiple
Switch(config)#radius-server attribute 8 include-in-access-req
Switch(config)#radius-server attribute 25 access-request include
Switch(config)#radius-server attribute 31 mac format ietf upper-case
Switch(config)#radius-server attribute 31 send nas-port-detail
Switch(config)#radius-server dead-criteria time 30 tries 3
```

Рис. 3.11. Базове налагодження протоколу RADIUS

```
Switch(config)#dot1x system-auth-control
Switch(config)#
Switch(config)#int gi0/3
Switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#authentication priority dot1x mab
Switch(config-if)#authentication order dot1x mab
Switch(config-if)#authentication event fail action next-method
Switch(config-if)#authentication violation restrict
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#mab
Switch(config-if)#dot1x timeout tx-period 10
Switch(config-if)#authentication port-control auto
Switch(config-if)#spanning-tree portfast edge
Switch(config-if)#authentication host-mode single-host
Switch(config-if)#exit
Switch(config)#
Switch(config)#int gi1/0
Switch(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled

Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#authentication priority dot1x mab
Switch(config-if)#authentication order dot1x mab
Switch(config-if)#authentication event fail action next-method
Switch(config-if)#authentication violation restrict
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#mab
Switch(config-if)#dot1x timeout tx-period 10
Switch(config-if)#authentication port-control auto
Switch(config-if)#spanning-tree portfast edge
Switch(config-if)#authentication host-mode single-host
Switch(config-if)#exit
```

Рис. 3.12. Базове налагодження інтерфейсів для роботи з стандартом 802.1X

3.2. Налагодження Windows Server

В данному пункті буде проведено встановлення необхідних компонентів для Windows Server. Active Directory для зберігання облікових записів працівників, створення підрозділів, користувачів та груп, центр сертифікації для отримання довіренних сертифікатів для пристроя ISE, налагоджено шаблони видачі сертифікатів для робочих станцій та користувачів, розгортання DHCP-серверу, FTP-серверу, автоматичних політик для 802.1X.

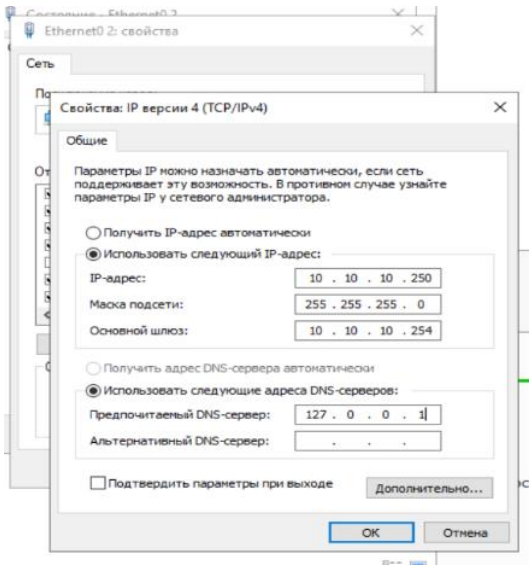


Рис. 3.13. Налагодження ip-адресації Windows Server.

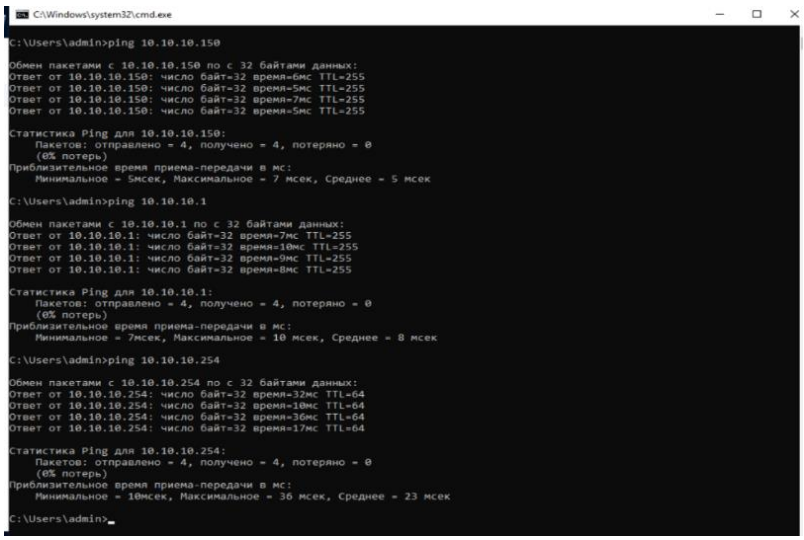


Рис. 3.14. Перевірка зв’язку з іншими вузлами мережі

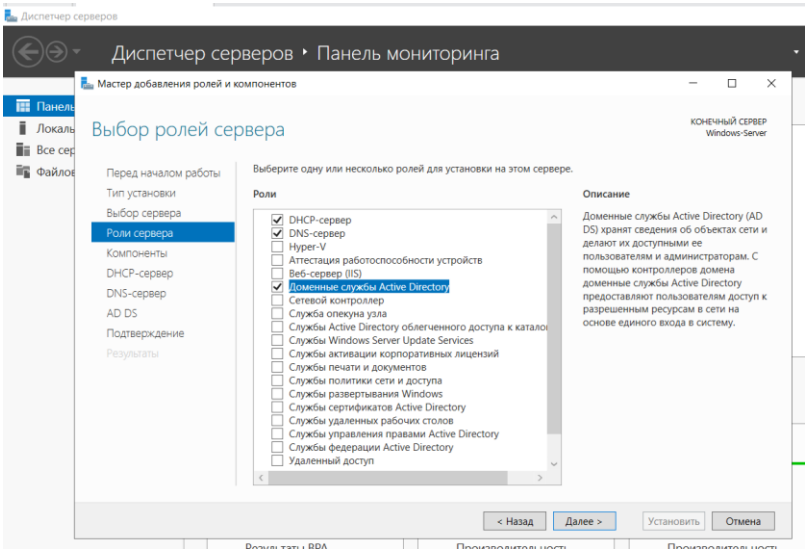


Рис. 3.15. Встановлення компоненту Active Directory

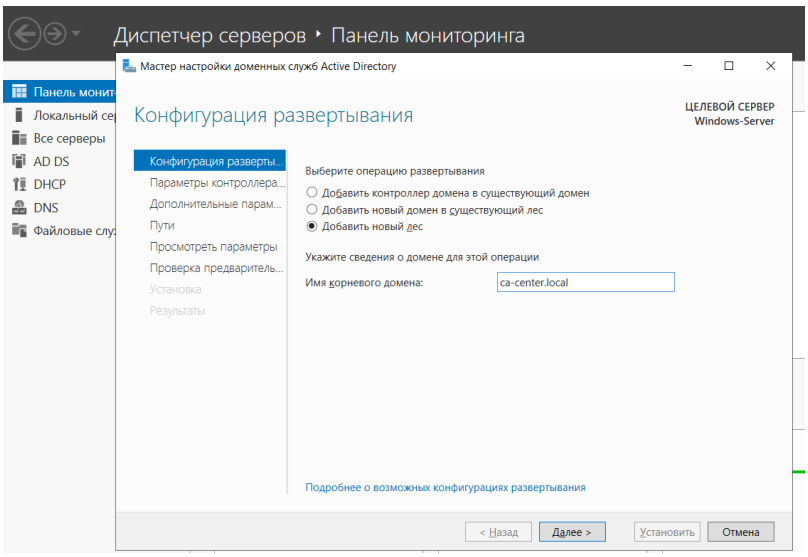


Рис. 3.16. Налагодження конфігурації розгортання домену

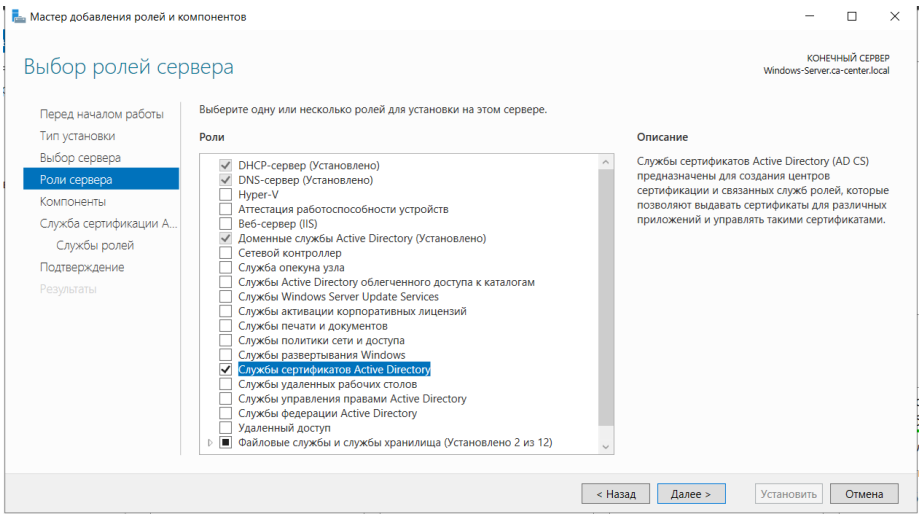


Рис. 3.17. Встановлення компонента служби сертифікатів

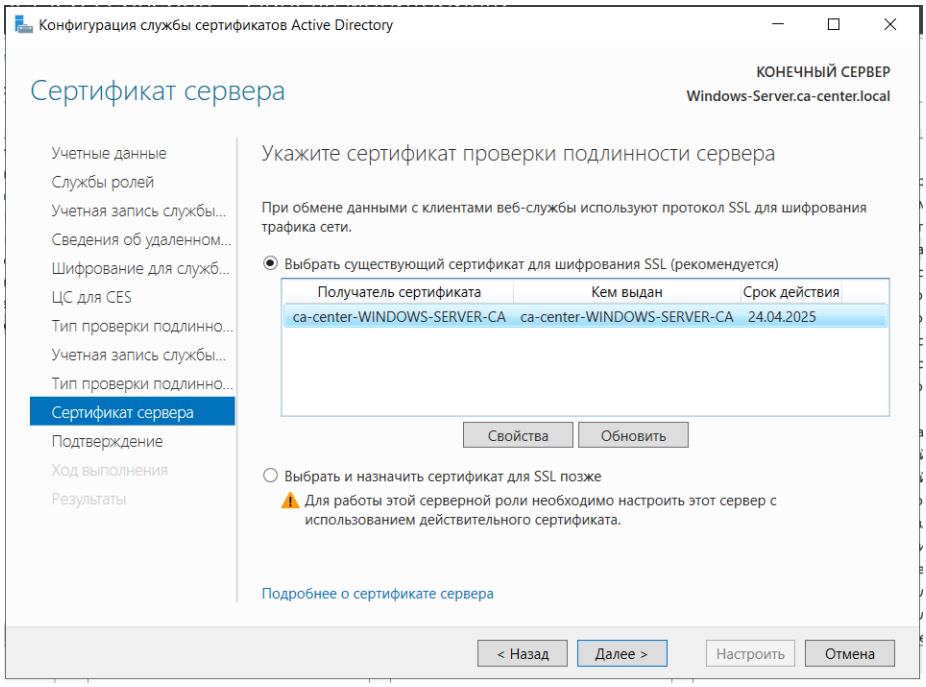


Рис. 3.18. Налагодження та створення кореневого сертифікату сервера

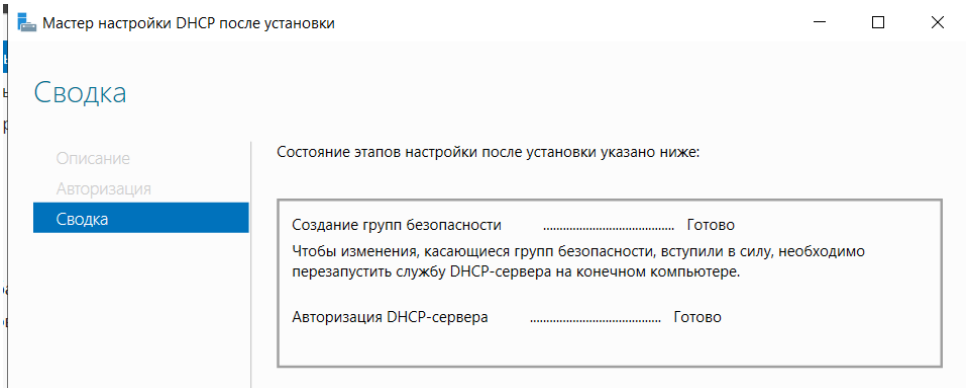


Рис. 3.19. Налагодження DHCP

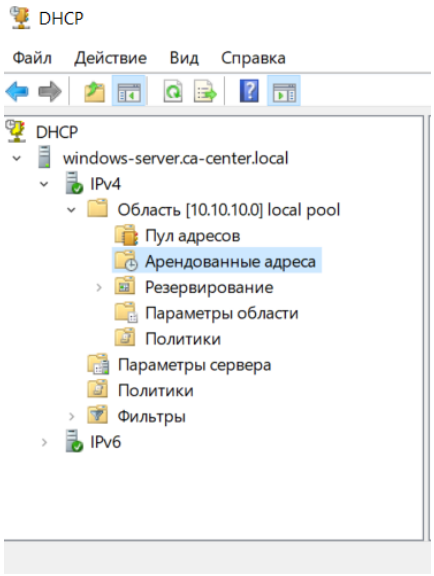


Рис. 3.20. Створена нова область адрес DHCP

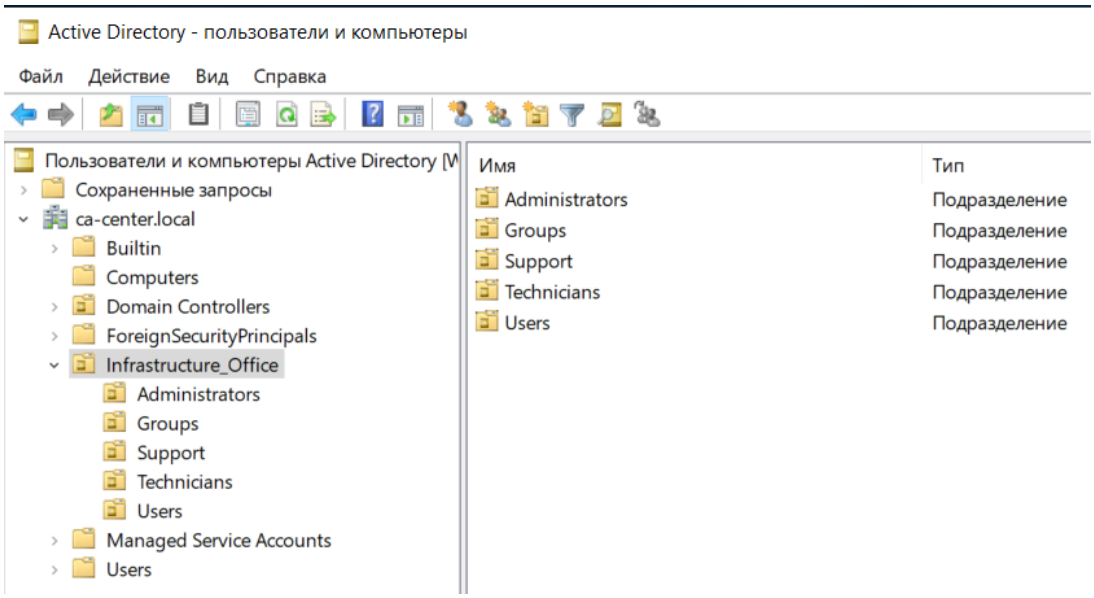


Рис. 3.21. Створені підрозділи для користувачів та груп

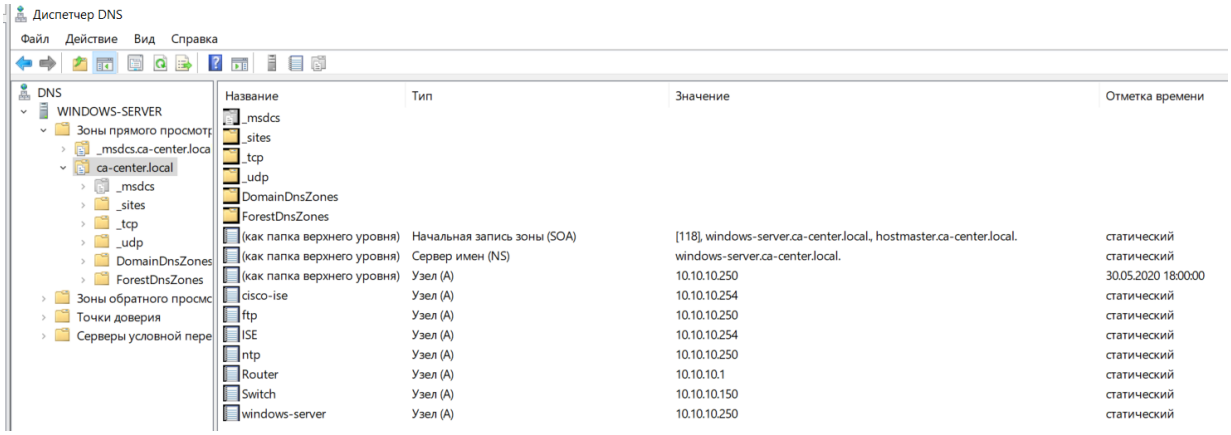


Рис. 3.22. Створення нових вузлів домену

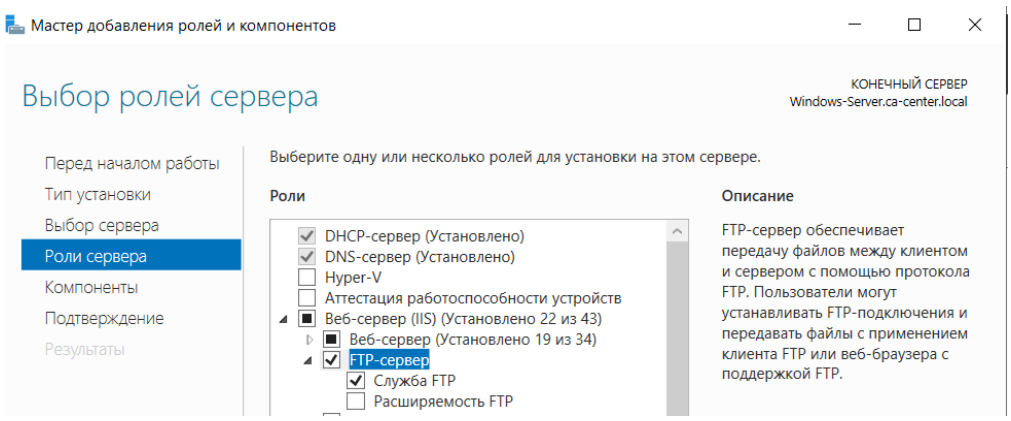


Рис. 3.23. Встановлення компоненту FTP-серверу

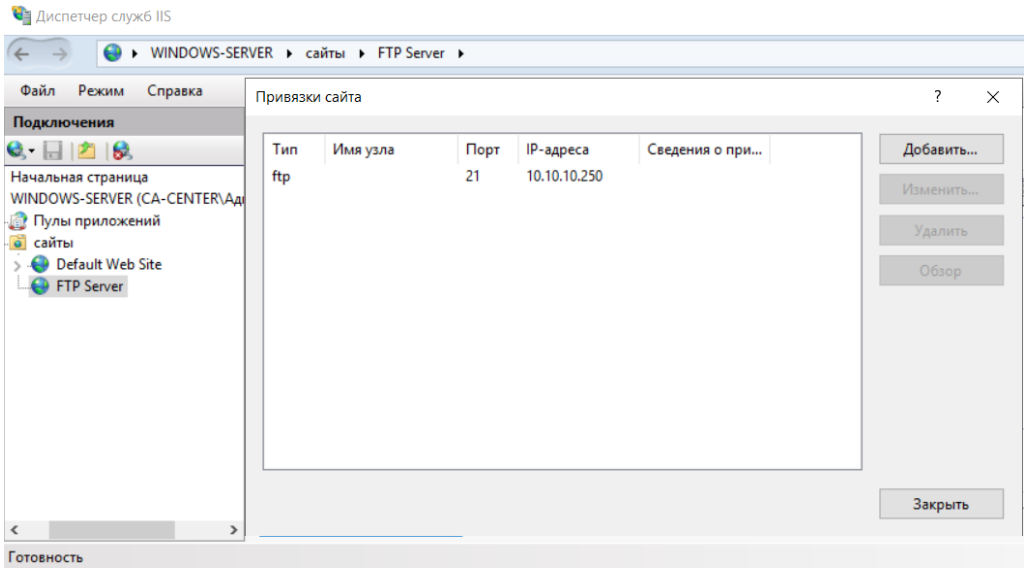


Рис. 3.24. Налагоджений FTP-сервер

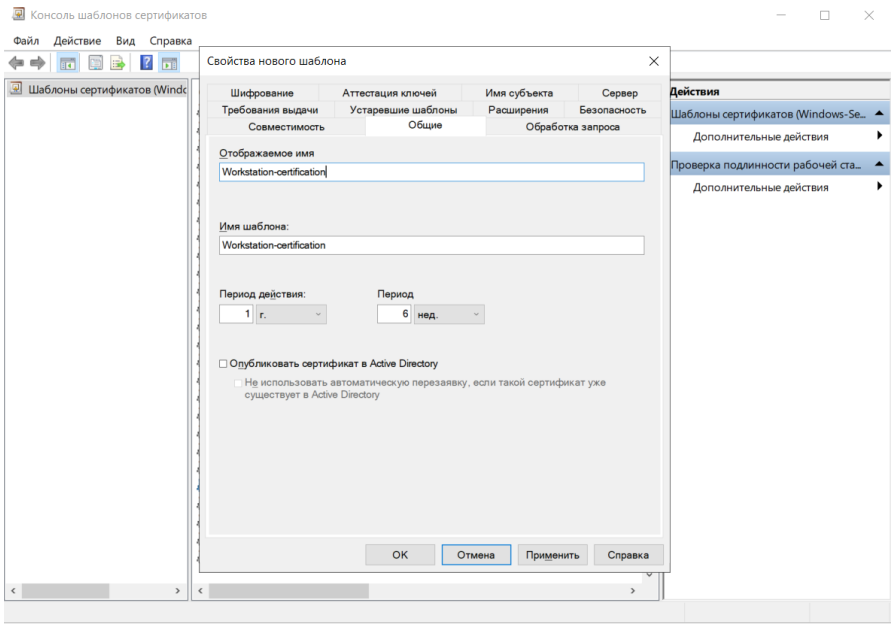


Рис. 3.25. Налагодження шаблону сертифікату для робочих станцій

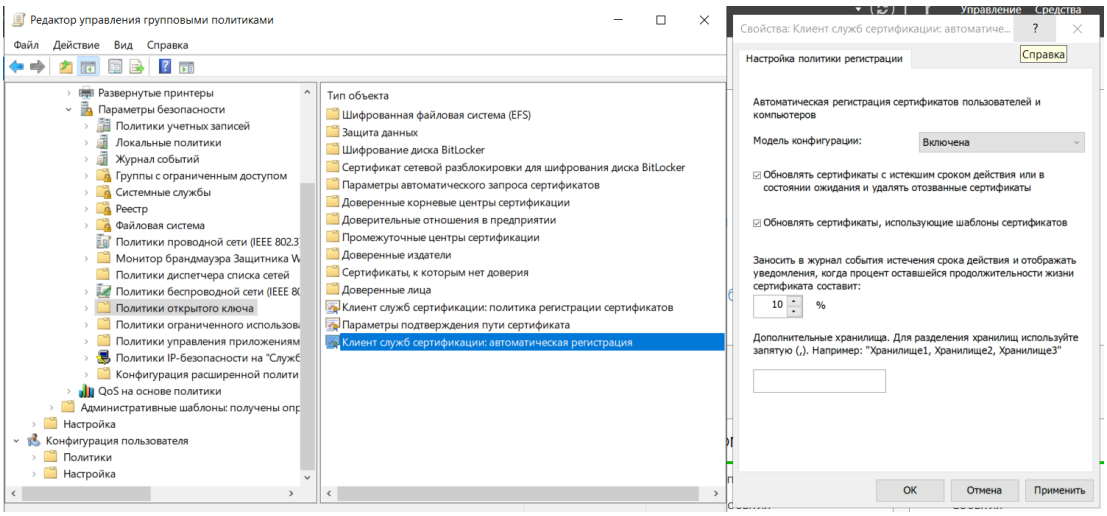


Рис. 3.26. Налагодження автоматичного встановлення сертифікатів

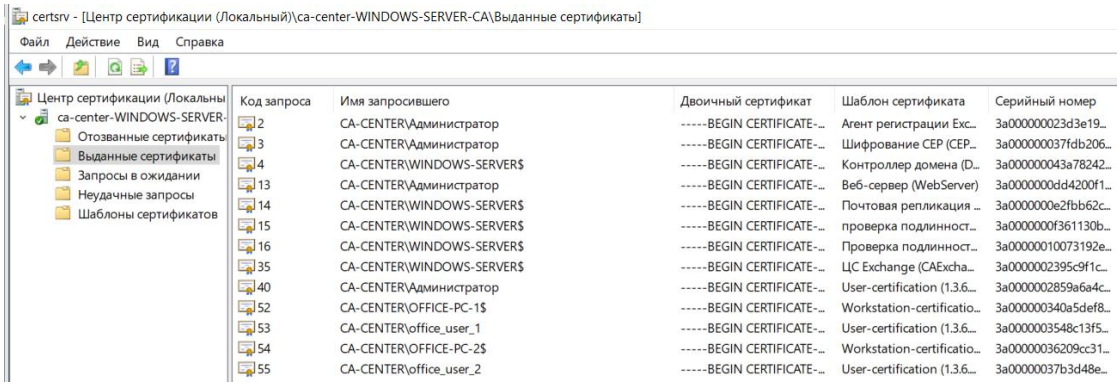


Рис. 3.27. Видані сертифікати користувачам та робочим станціям

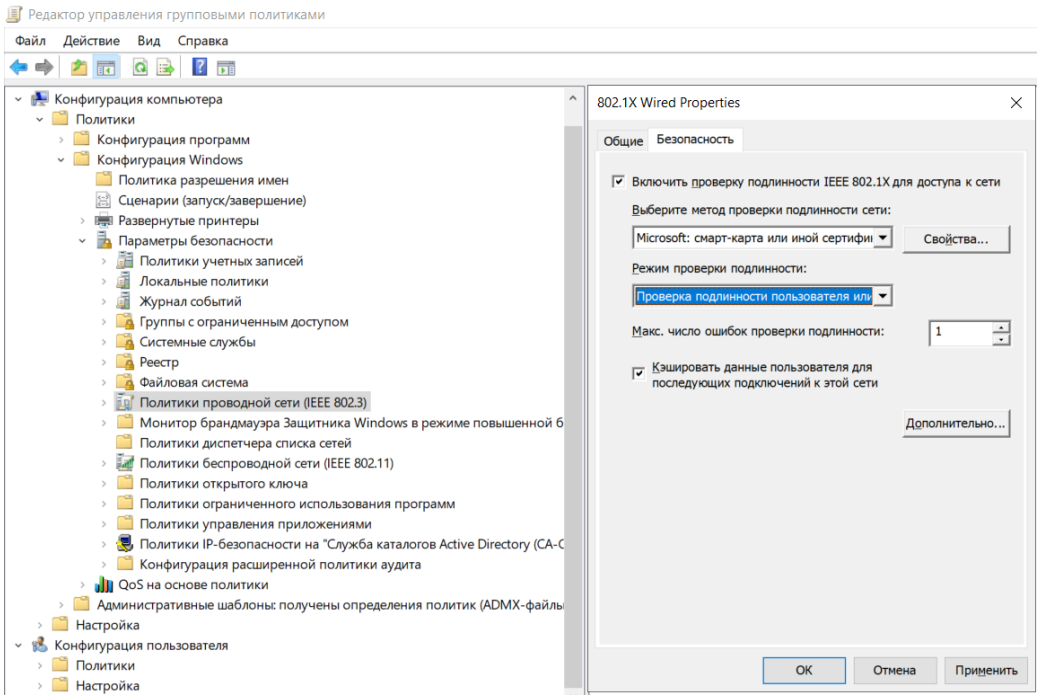


Рис. 3.28. Ввімкненя політики для використання 802.1X на робочих станціях

3.3. Налагодження Cisco Identity Services Engine

В данному пункті відбуваються основні налагодження пристрою Cisco Identity Services Engine. Інтеграція з Windows сервером і підключення до служби каталогу Active Directory, встановлення сертифікатів, налагодження TACACS+, RADIUS та набору політик доступу для протоколів на основі груп користувачів. Налагодження двох методів аутентифікації EAP-TLS/PEAP та налагодження репозиторію для створення резервних копій на віддаленому FTP-сервері.

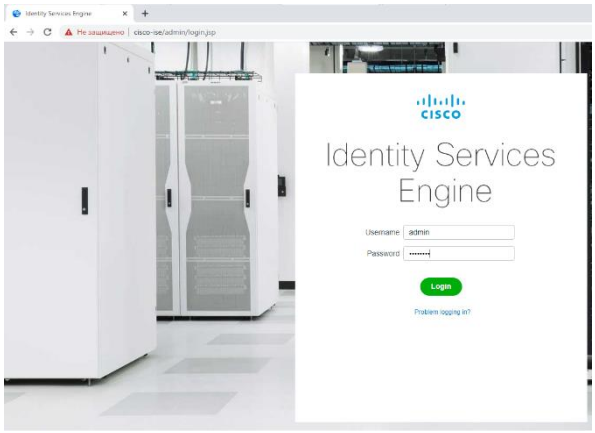


Рис. 3.29. Вхід у систему.

При початковому вході у систему використовується логін та пароль, які вказувались при початковому налагоджені ISE, надалі при підключенні до каталогу Active Directory це можна буде змінити, щоб доступ мали адміністратору домену.

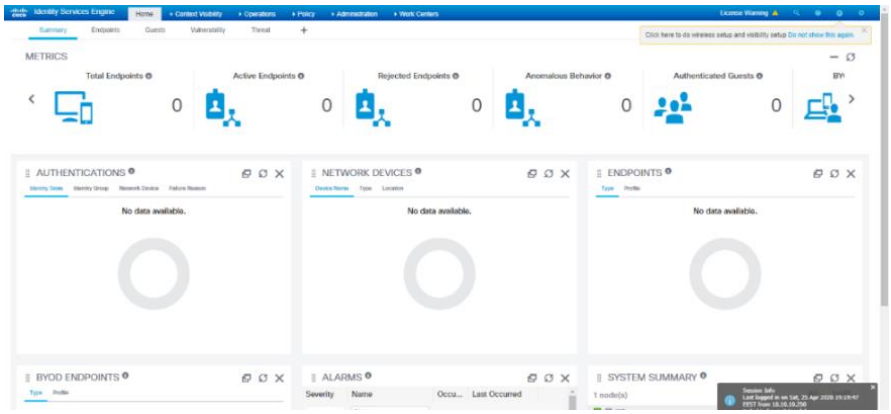


Рис. 3.30. Головна інофрмаційна сторінка системи

На головній сторінці відображається вся інформація про пристрої мережі: загальна кількість, активні пристрої, аутентифіковані пристрої і т.д.

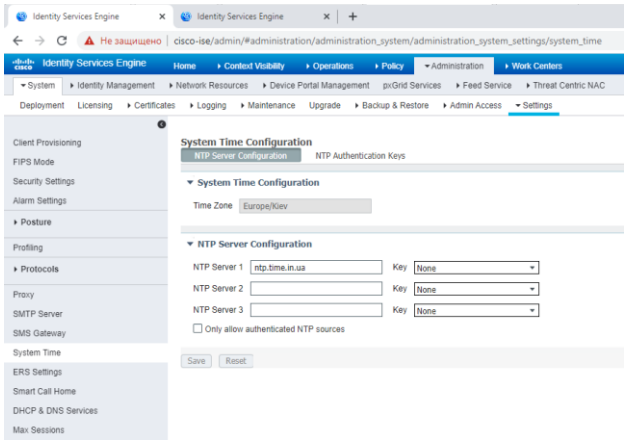


Рис. 3.31. Налагодження NTP серверу.

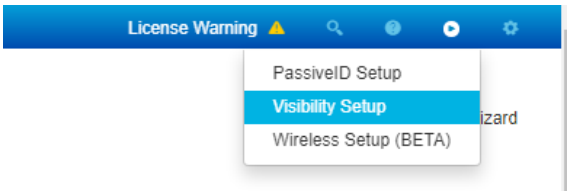


Рис. 3.32. Перехід у вкладку налагодження відображення пристроїв

Для того щоб пристрій ISE бачив пристрої у мережі, потрібно вказати в якому діапозоні адрес знаходяться пристрої, після чого вказуються параметри SNMP, які мають бути налагоджені на всіх пристроях в інфраструктурі (маршрутизатори, комутатори та інші мережеві пристрої). Після того, як дані були надані пристрою ISE, він починає автоматичний пошук пристроїв. У випадках коли пристрій не знайдено, потрібно перевірити правильність налагоджень або створювати пристрій з ручним налагодженням параметрів відповідного пристрою.

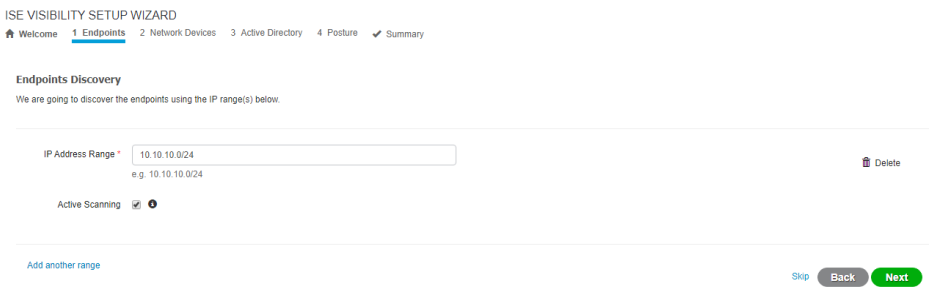


Рис. 3.33. Вказування діапазону адрес пристроїв

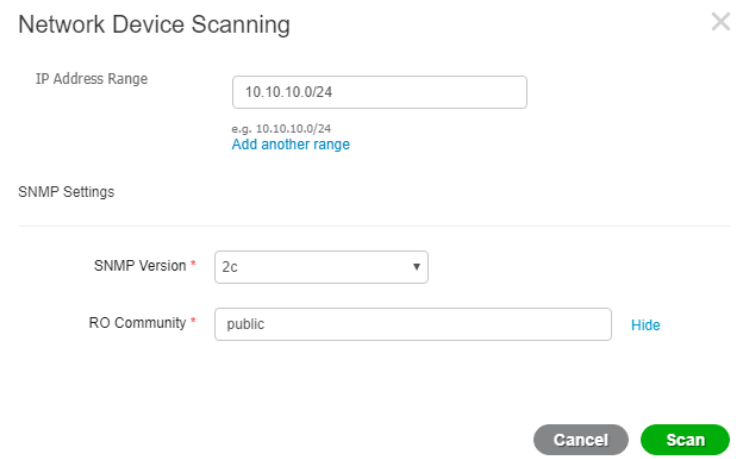


Рис. 3.34. Вказування параметрів SNMP

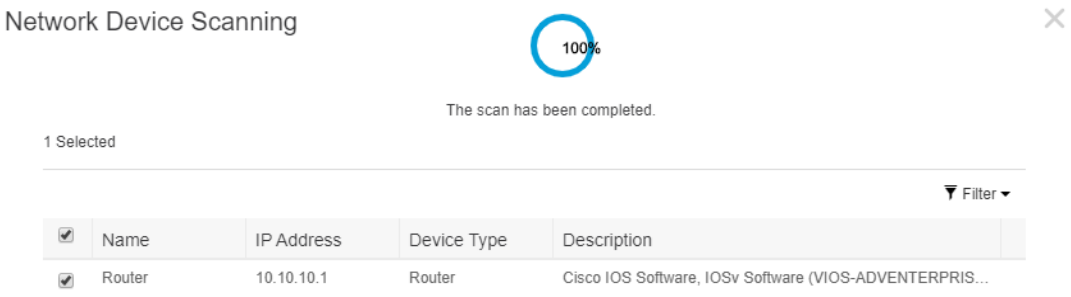


Рис. 3.35. Перший автоматичний пошук пристроїв

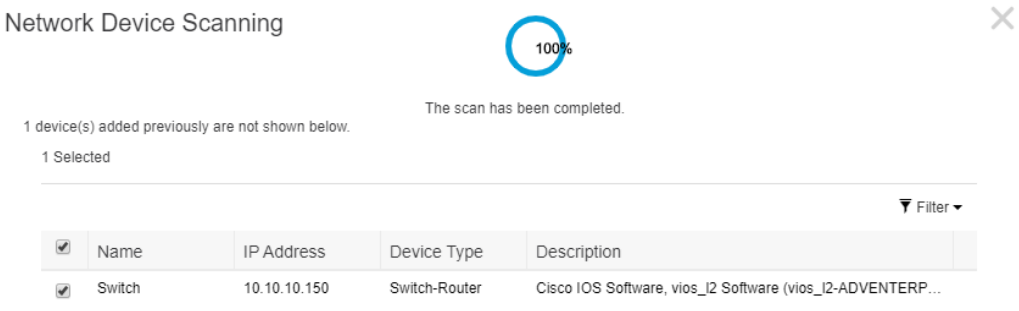


Рис. 3.36. Другий автоматичний пошук

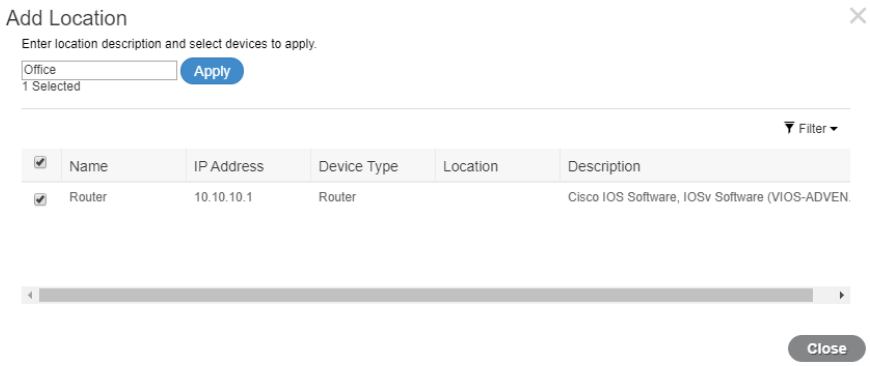


Рис. 3.37. Вказування місцезнаходження пристроя при додаванні

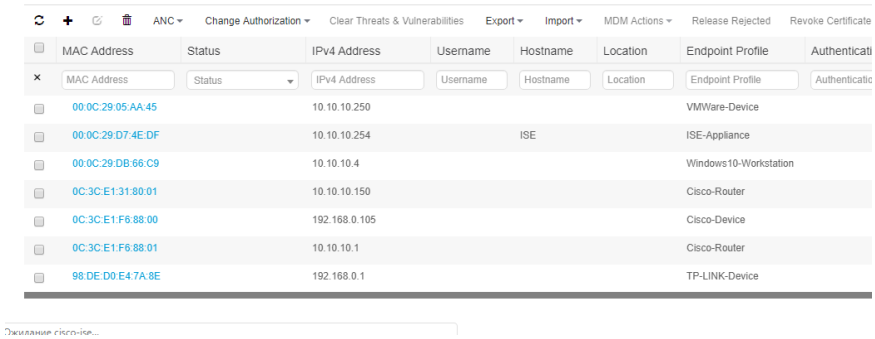


Рис. 3.38. Відображення всіх пристроїв, які були знайдені

Далі необхідно підключитися до каталогу Active Directory і провести повну інтеграцію між Cisco ISE та Windows Server, щоб користувачі мали змогу використовувати свої облікові записи, які необхідні для протоколів TACACS+ та RADIUS.

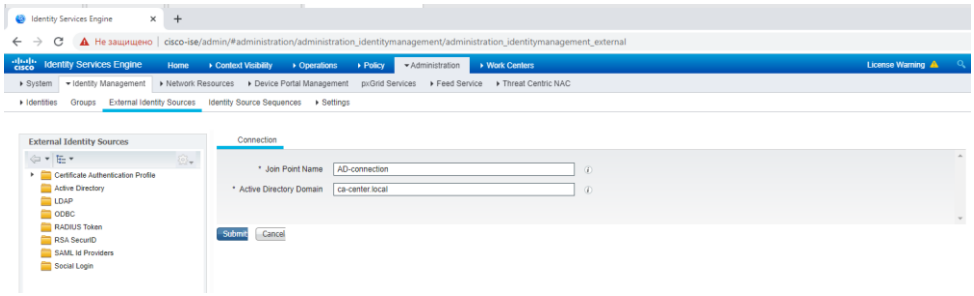


Рис. 3.39. Створення нового підключення

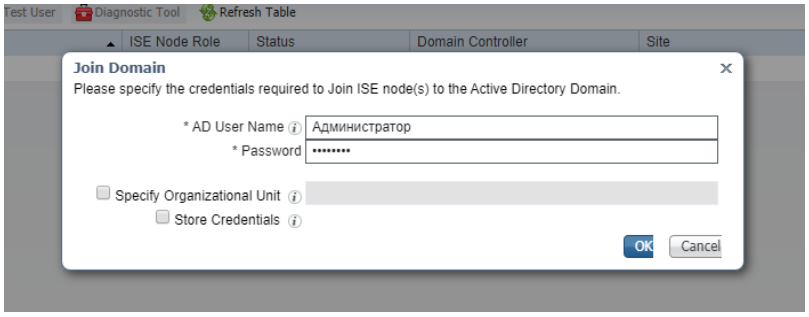


Рис. 3.40. Дані для входу у Active Directory

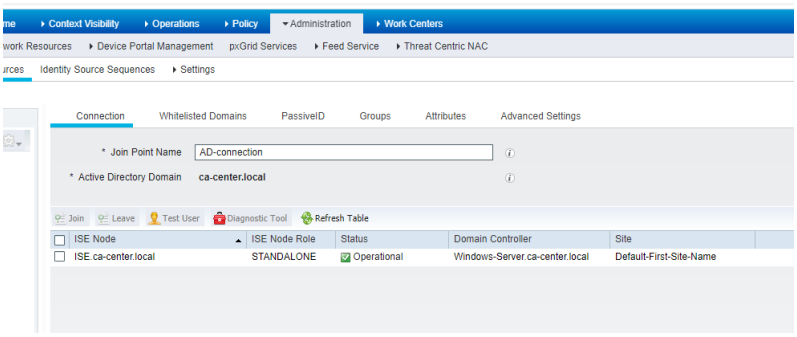


Рис. 3.41. Успішно встановлене з’єднання

Після успішної інтеграції з Windows Server та каталогом Active Directory, необхідно завантажити кореневий сертифікат серверу на пристрій ISE та додати його в сховище довірених сертифікатів. В браузері вказується адреса Windows Server для отримання сертифіката. При вході за цією адресою запитується логін та пароль адміністратора домену, після чого надається доступ для завантаження сертифікату, який потрібно імпортувати на пристрій ISE, як довірений.

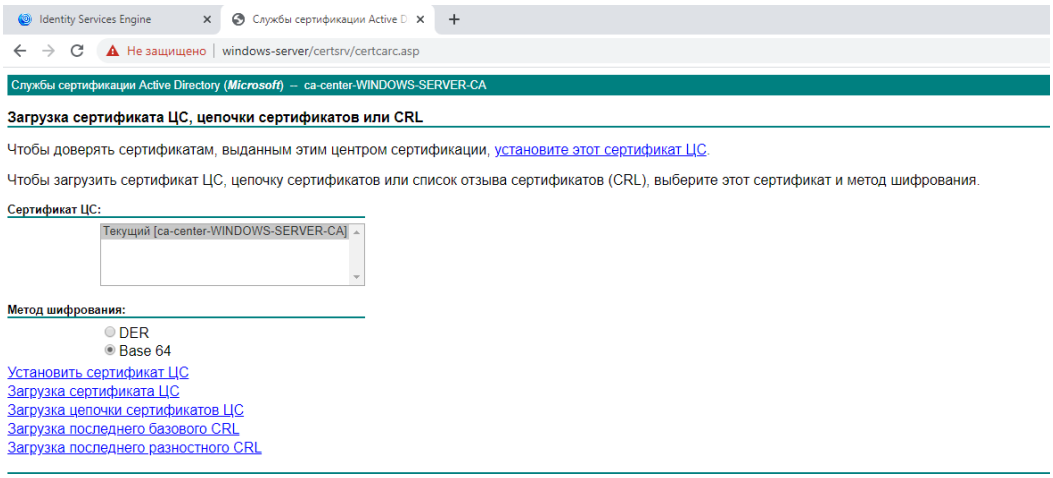


Рис. 3.42. Завантаження кореневого сертифікату с Windows Server

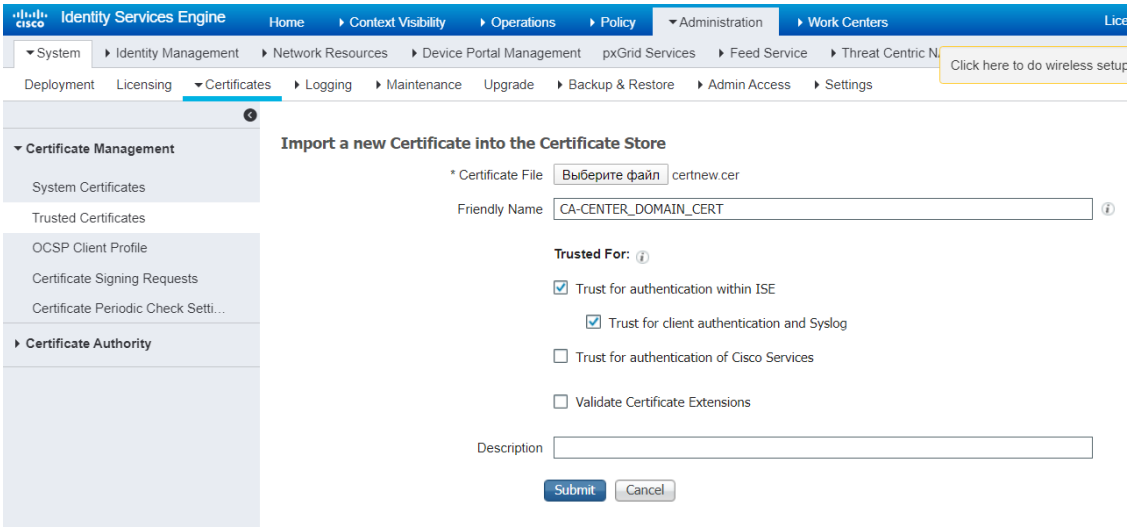


Рис. 3.43. Імпорт кореневого сертифікату на пристрій ISE

Коли кореневий сертифікат домену імпортований до сховища довірених сертифікатів ISE, можна створювати запит на підпис сертифікату. В запиті створюється новий сертифікат, який відправляється на підпис до Windows Server. Цей сертифікат надалі буде використовуватись для сертифікації адміністративної панелі ISE та при аутентифікації з протоколом 802.1X.

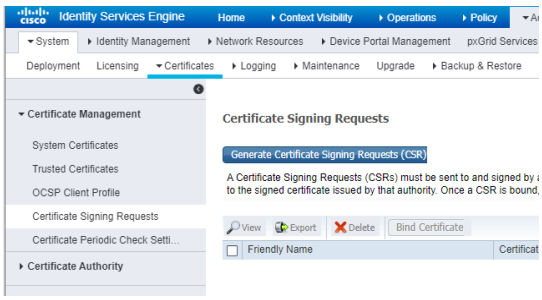


Рис. 3.44. Створення запиту на підпис сертифікату

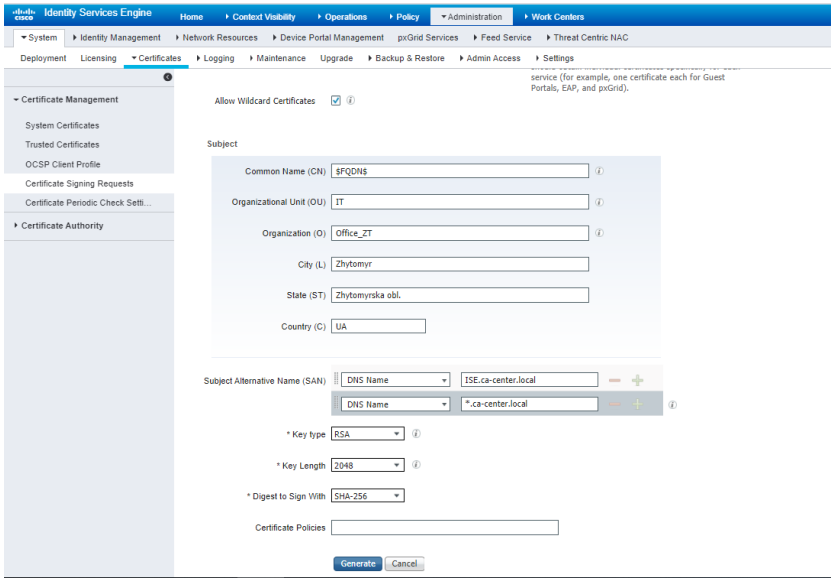


Рис. 3.45. Параметри сертифікату

При натисканні кнопки генерації, файл з створеним сертифікатом зберігається на комп'ютері. Необхідно скопіювати вміст цього файлу та знову повернутись на адресу Windows Server у браузері і підписати згенерований сертифікат.

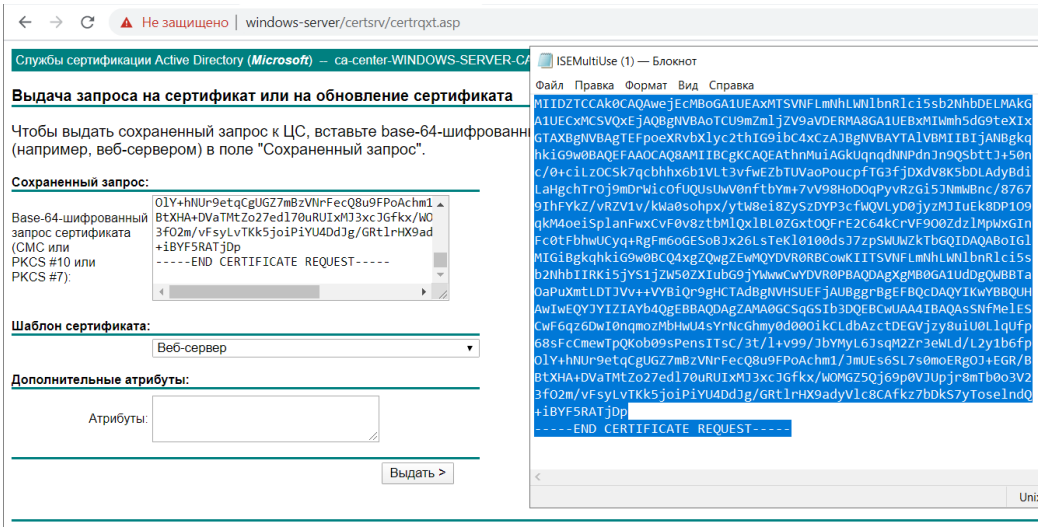


Рис. 3.46. Копіювання вмісту згенерованого файлу сертифіката та його підпис

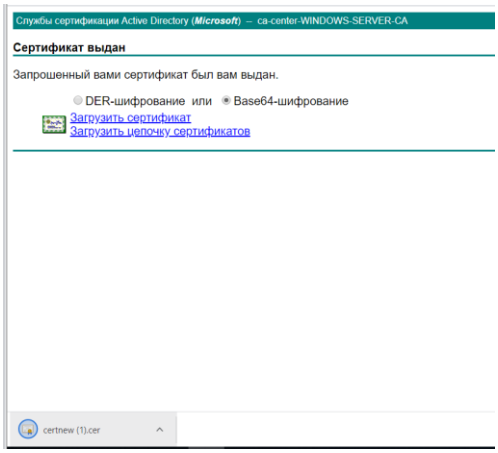


Рис. 3.47. Завантаження підписаного сертифікату

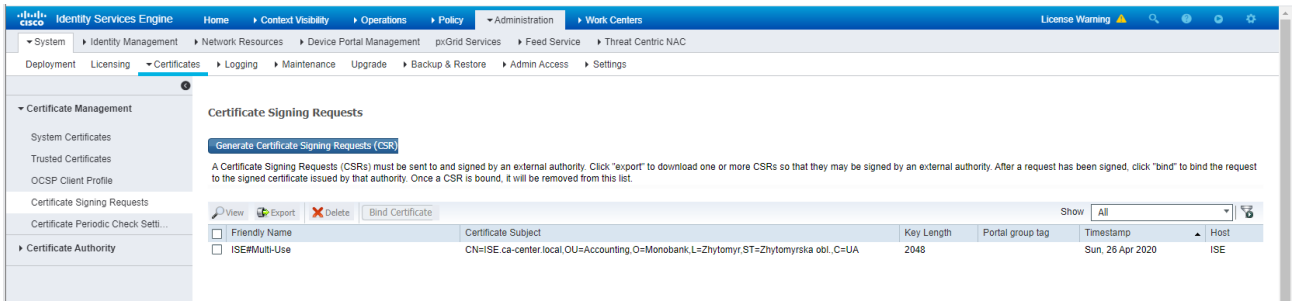


Рис. 3.48. Відображення запиту на підпис сертифікату

На етапі роботи з сертифікатами. необхідно зв’язати підписаний сертифікат з створеним запитом. Додати файл сертифікату та обрати ролі, які будуть виконуватись з використанням сертифікату. В данному випадку обирається дві ролі Admin та EAP Authentication.

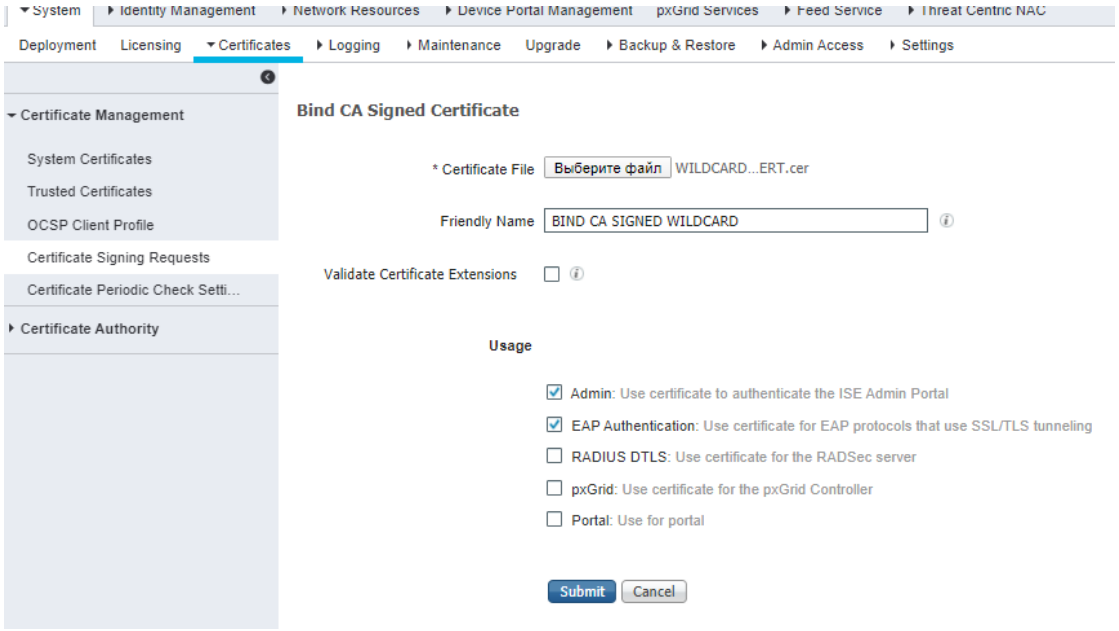


Рис. 3.49. Використання сертифікату для протоколу 802.1X

Додаємо групи користувачів з Active Directory, які будуть використовуватись при налагоджені набору політик протоколу TACACS+, для доступу до панелі адміністратор Cisco ISE та збереження резервних копій конфігурації на FTP-сервер.

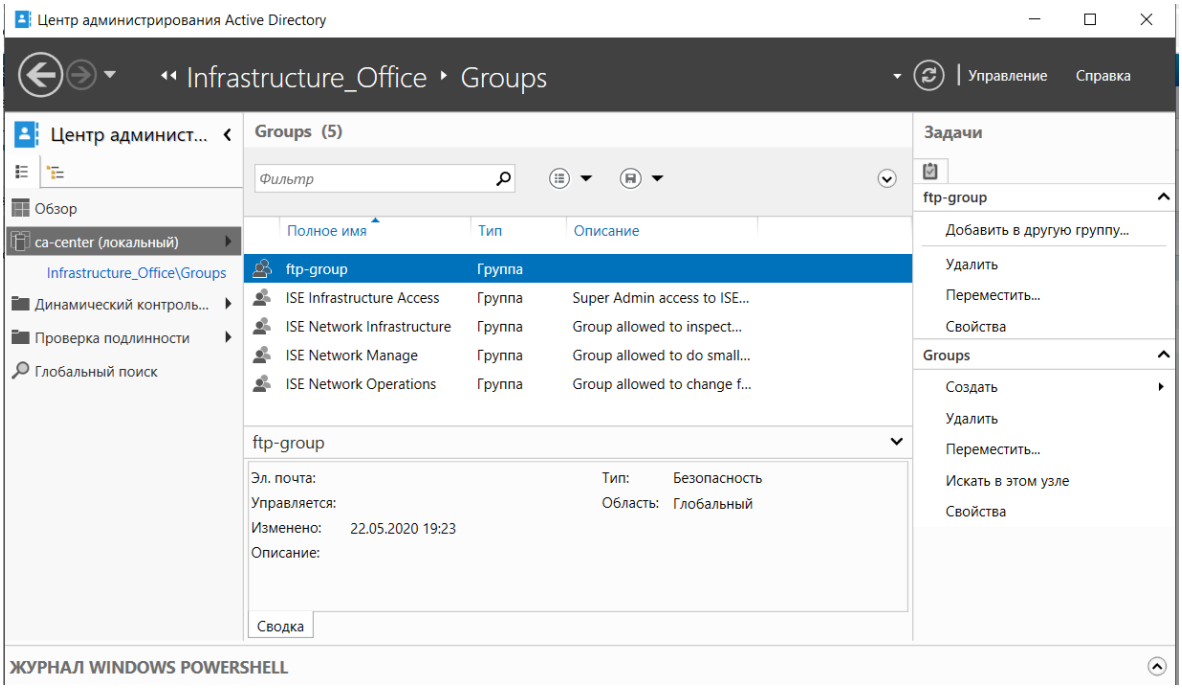


Рис. 3.50. Групи користувачів Active Directory

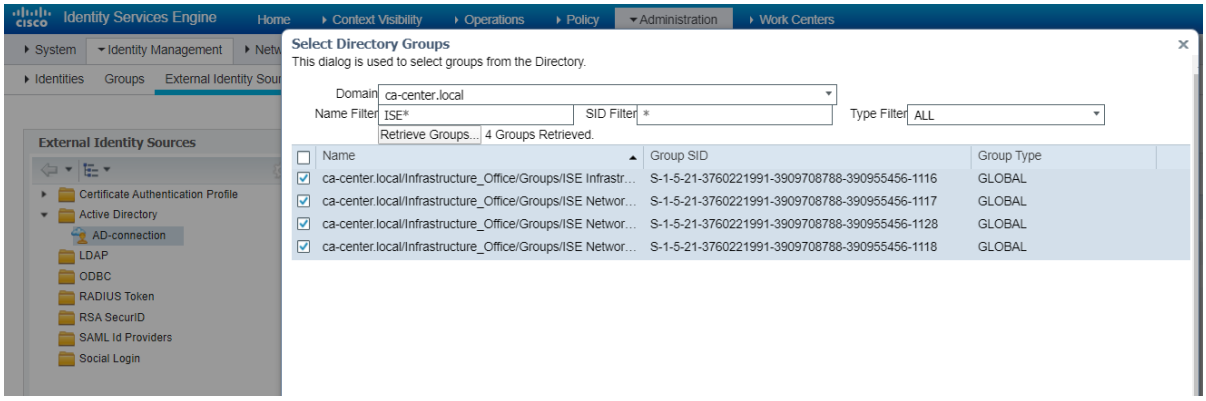


Рис. 3.51. Додавання груп користувачів до ISE

Обрані групи були успішно встановлені. Доволі важливою є налагодження можливості заходити до панелі адміністратора використовуючи облікові записи адміністраторів Active Directory і не використовувати кожний раз логін та пароль, який був налагоджений при встановленні образу ISE. Таким чином підвищується доступність і захищеність панелі адміністратора для користувачів домену.

Для аутентифікації у панель адміністратора з данними користувачів необхідно налагодити перевірку парольних даних з використанням джерела даних Active Directory.

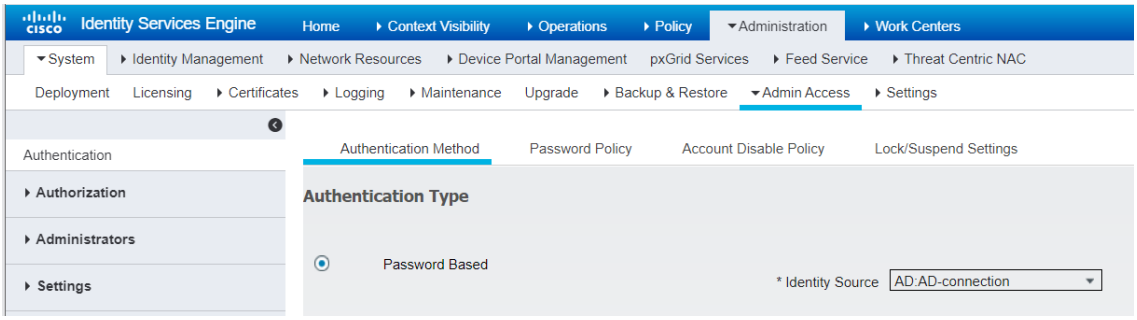


Рис. 3.52. Аутентифікація до панелі адміністратора з джерелом даних Active Directory

Далі створюється група адміністраторів домену з зовнішнім типом з'єднання, де вказується група, яка буде використовуватись для входу у панель адміністратора. Після створення групи адміністраторів домену залишається налагодити відповідні політики доступу для цієї групи.

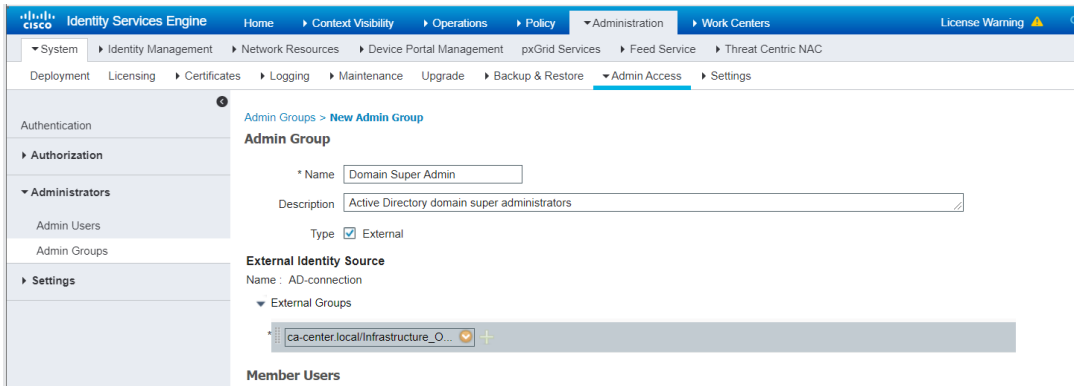


Рис. 3.53. Створення групи адміністраторів з використанням групи адміністраторів домену

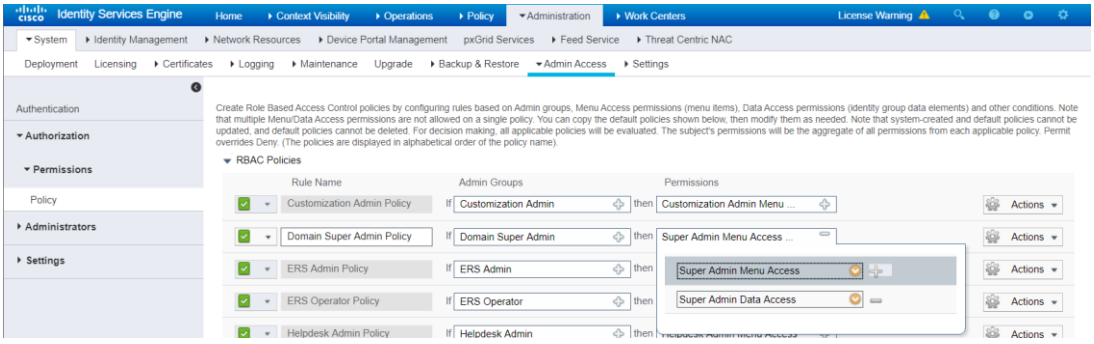


Рис. 3.54. Налагодження політики доступу для групи адміністраторів

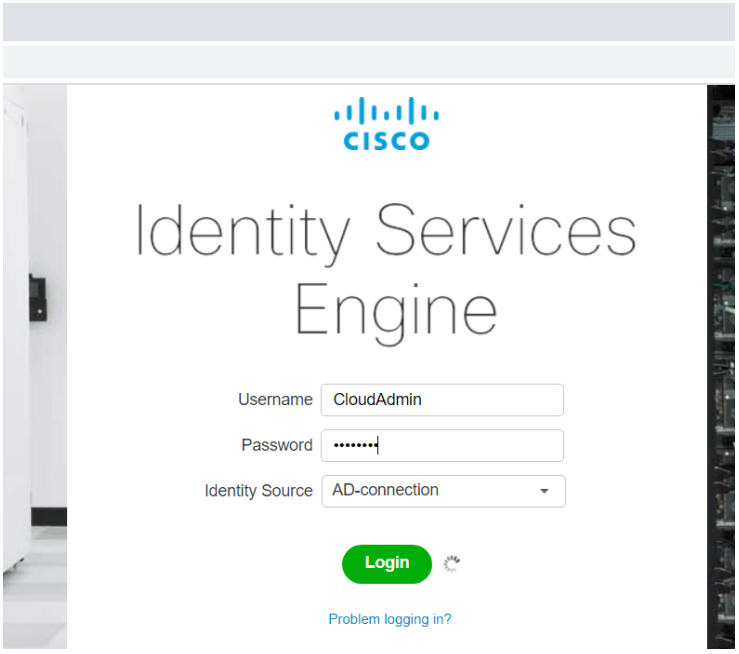


Рис. 3.55. Використання облікового запису адміністратору домену при вході у панель адміністратора ISE

Базові налагодження проведені, залишається ввімкнути протокол TACACS+, RADIUS та налагодити набори політик протоколів. Для ввімкнення протоколів необхідно перейти у вкладку адміністрування, мережеві пристрої та знайти там комутатор з нашої мережі, активувати обидва протоколи і призначити їм ключі.

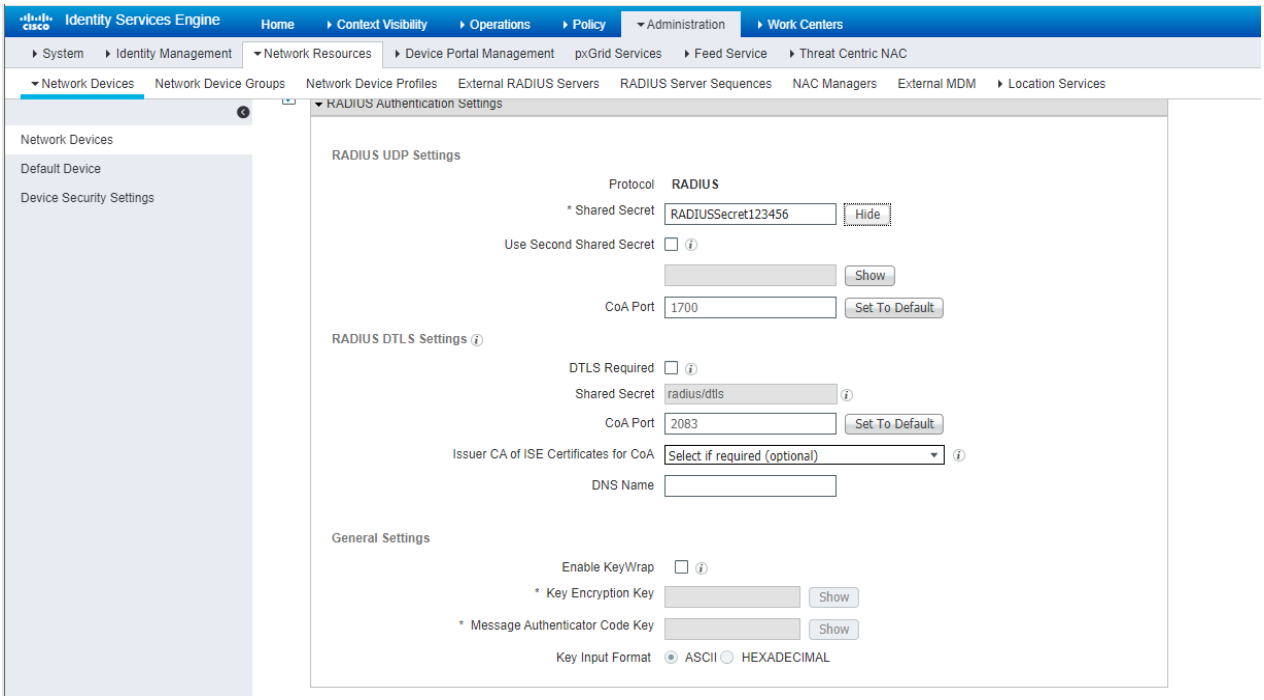


Рис. 3.56. Параметри протоколу RADIUS

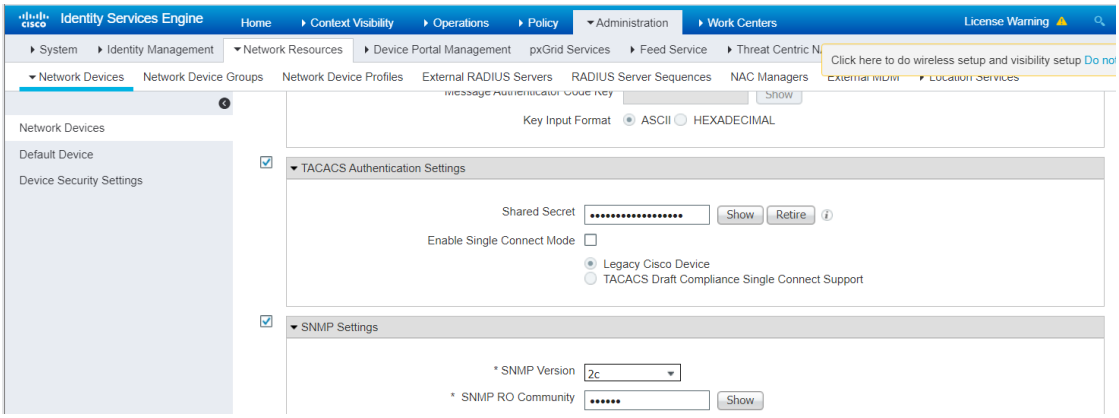


Рис. 3.57. Параметри протоколу TACACS+

Ввімкнення протоколів RADIUS та TACACS+ не достатньо для їх коректного функціювання. Поведінка протоколів за замовчуванням буде блокувати дані, тому що аутентифікація та авторизація за замовчуванням набору політик протоколів встановлені на блокуваня. Отже, потрібно додати або оновити їх під потреби підприємства для коректного функціонування.

Для протоколу TACACS+ можна змінити набір політик за замовчуванням. Перед початком роботи з політикою необхідно створити порядок перевірки особистості, так як можуть використовуватись облікові записи з Active Directory або з локальної бази даних ISE. Порядок перевірки особистості буде використовуватись під час аутентифікації користувачів на мережевих пристроях і допоможе визначити пристрою ISE в яких джерелах починати пошук користувачів.

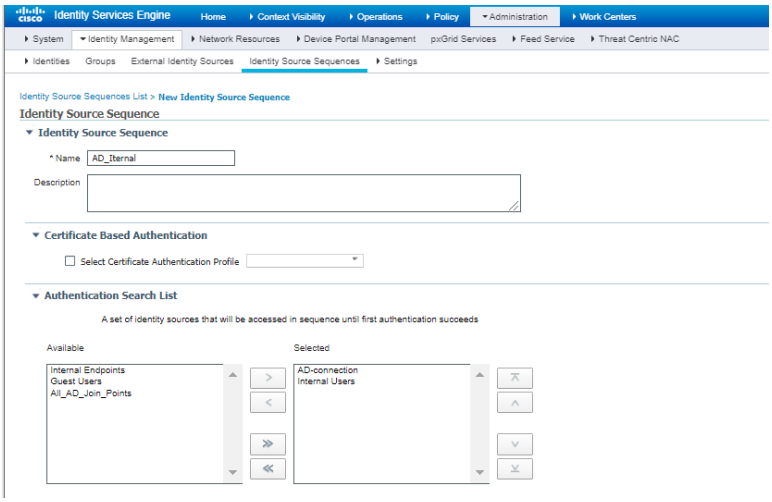


Рис. 3.58. Створення порядку перевірки особистості для використання з TACACS+

Також необхідно передбачити різний доступ всіх груп користувачів. Попередньо було створено 3 групи користувачів у каталозі Active Directory. Адміністратори матимуть найвищий рівень доступа на пристроях без обмежень, далі за ними ідуть техніки з обмеженням по використанню команд і останні працівники моніторингу з рівнем привілеїв 7, яким буде дозволено лише перегляд інформації на пристроях. Для отримання результату, потрібно створити шаблони TACACS Command Sets та TACACS Profiles для всіх груп користувачів. В TACACS Command Sets вказується перелік дозволенних і заборонених команд, а для TACACS Profiles привілеї та інші параметри. Ці шаблони в подальшому будуть використовуватись в політиці авторизації TACACS і будуть виконуватись при певних умовах.

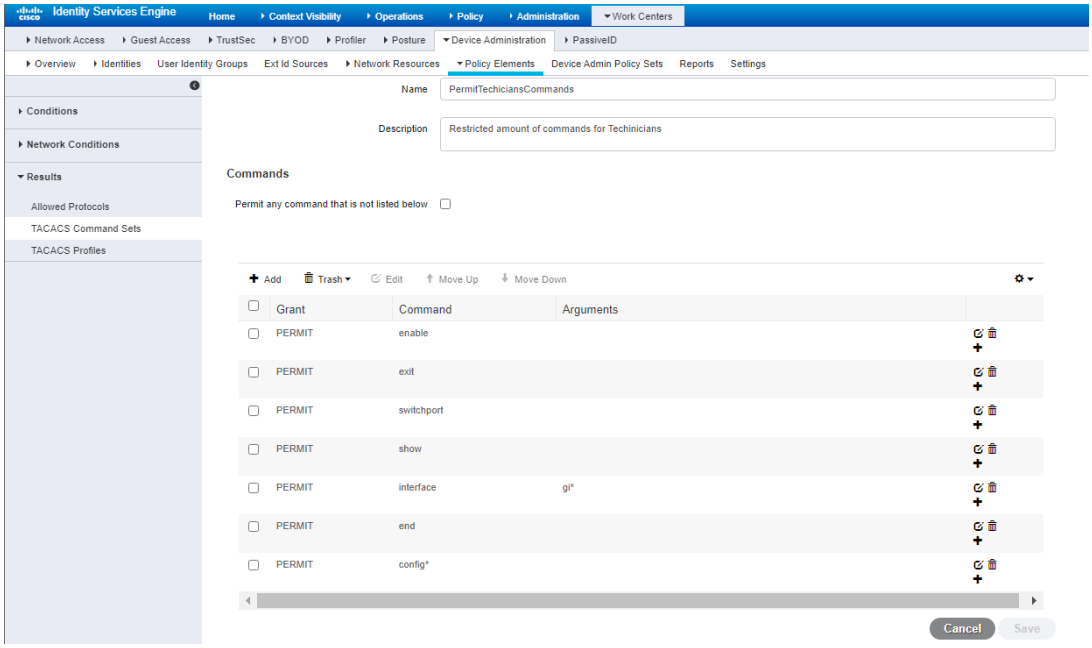


Рис. 3.59. Створення обмеженого набору команд для TACACS+

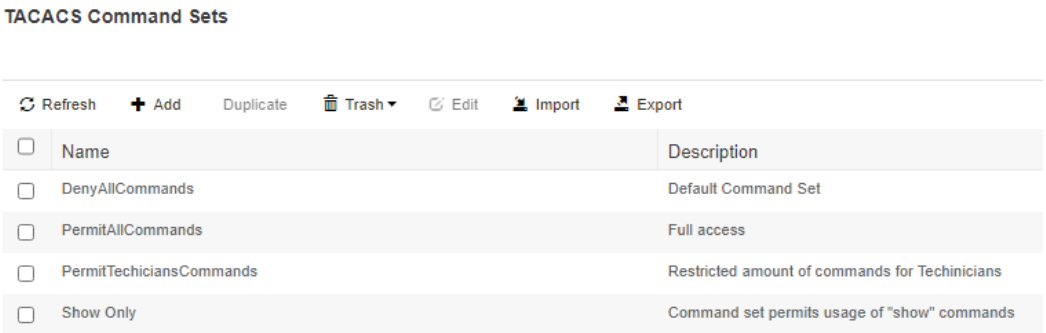


Рис. 3.60. Список створених наборів команд

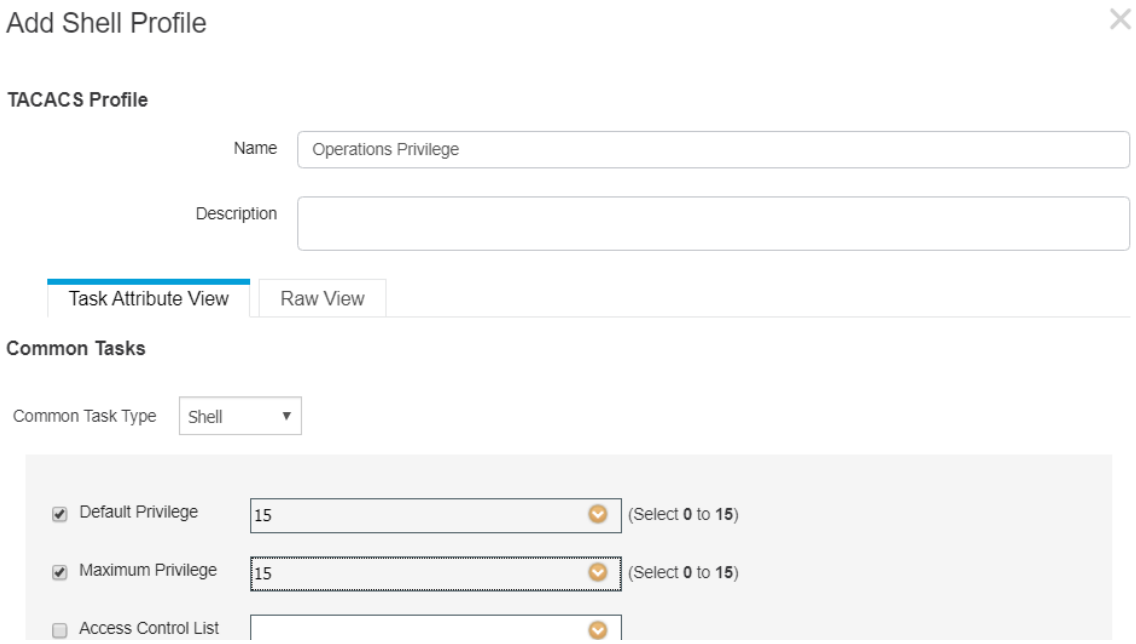


Рис. 3.61. Створення профілю для привілею

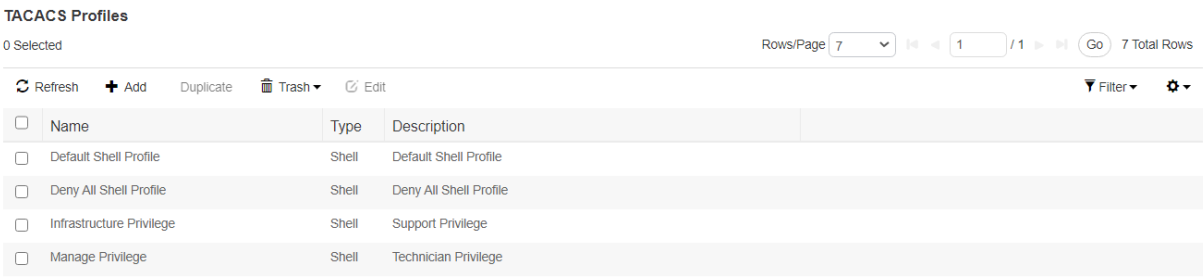


Рис. 3.62. Всі створені профілі привілеїв

Тепер можно переходити до налагодження політики, за основу візьмемо вже існуючу політику за замовчуванням, але повністю змінимо правила аутентифікації та авторизації.

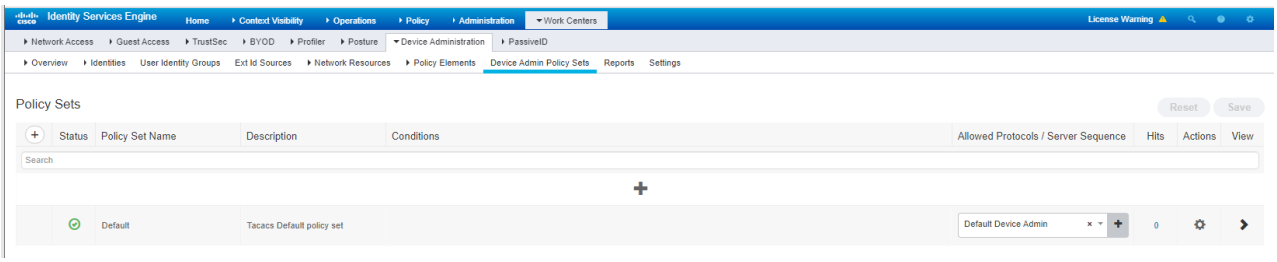


Рис. 3.63. Політика протоколу TACACS+ за замовчуванням

У вкладці аутентифікації для поля Use вказуємо джерело пошуку облікових записів, в цьому випадку це попередньо створений порядок перевірки особистості з назвою AD_Iternal.



Рис. 3.64. Встановлення джерела пошуку облікових засобів для аутентифікації

Переходимо до вкладки авторизації. Для визначення прав аутентифікованого користовача необхідно буде створити певні умови разом з якими будуть використовуватись TACACS Command Set та Profiles.

Умова перевірки доволі проста. Відбувається зв'язок з Active Directory та запит, якій групі належить користувач, якщо користувач належить до однієї з попередньо визначених груп, він отримає відповідні права та доступ, а якщо ні, тоді умова авторизації за замовчуванням відхилить його і не надасть йому жодних прав.

В Identity Services Engine присутній гнучкий редактор умов в якому будуть створені всі умови для груп. Як джерело облікового запису обираємо створене підключення AD-Connection і його параметр External Groups (зовнішні групи), якщо цей параметр дорівнює обраній групі, тоді надаємо права.

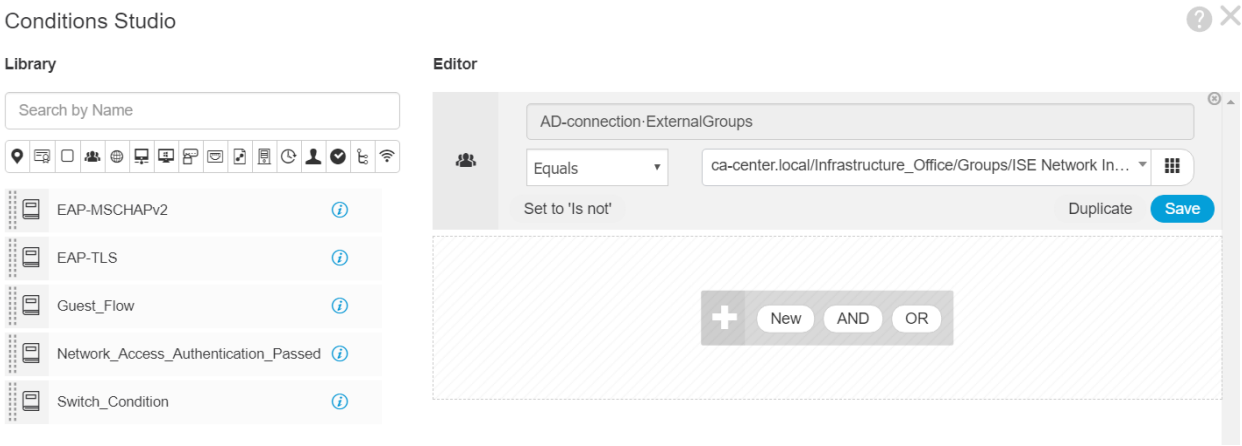


Рис. 3.65. Створення умови для авторизації

В результаті маємо чотири політики авторизації для обраних груп. Кожній групі надаються права і привілеї, якщо виконуються умови.

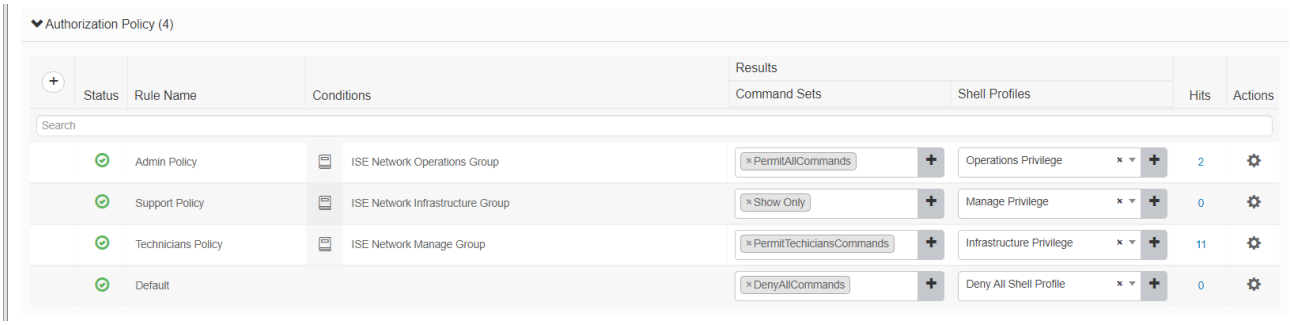


Рис. 3.66. Створені політики авторизації для протоколу TACACS+

Налагодження набору політик протоколу RADIUS відрізняється тим, що необхідно його поєднати з протоколом захисту 802.1X. Для цього ми будемо використовувати перевірки сертифікатів та облікові дані користувачів.

Почнемо з профілювання робочих станцій, це необхідно для підвищення рівня довіри даних пристроїв у системі та полегшення відстеження пристроїв.

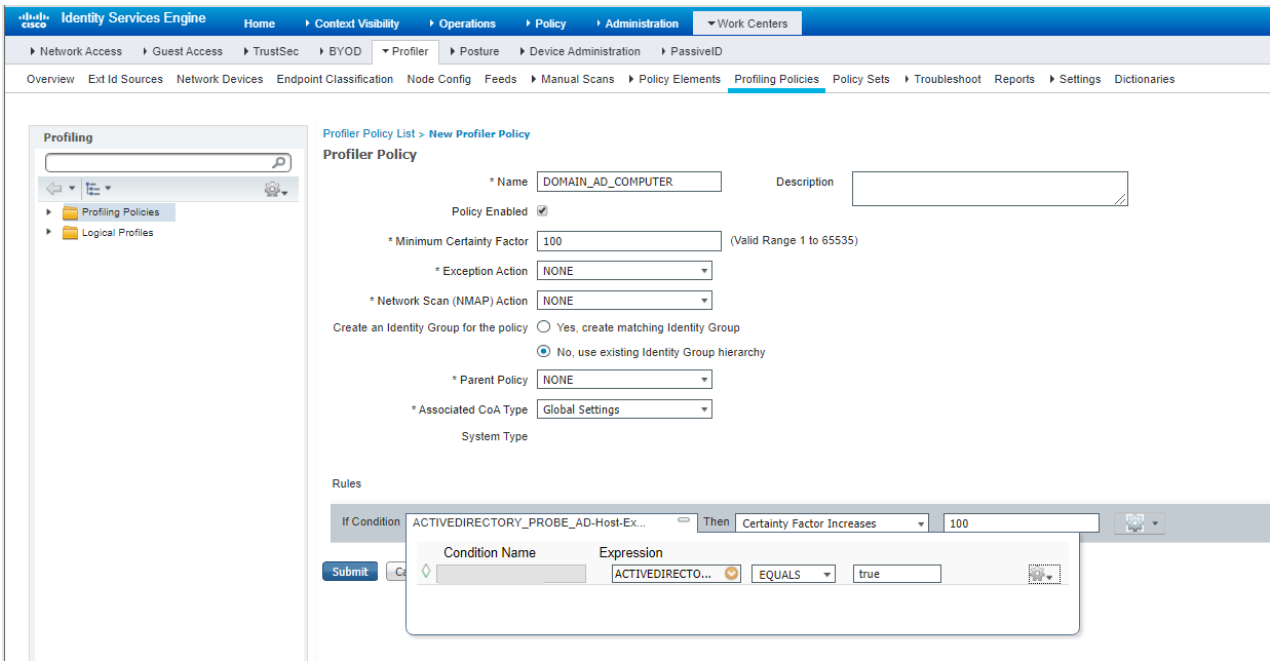


Рис. 3.67. Створення профілювання робочих станцій, які знаходяться у домені

У вкладці зовнішніх джерел особистості створюємо профіль аутентифікації за допомогою сертифікатів. Вказуємо назву, Identity Store (Сховище облікових засобів) вказуємо підключення з Active Directory, Identity From (Атрибути за якими будуть перевірятись сертифікати) обираємо перевірку “Будь який суб’єкт або альтернативні атрибути імені в сертифікаті”, яка працює тільки з AD.

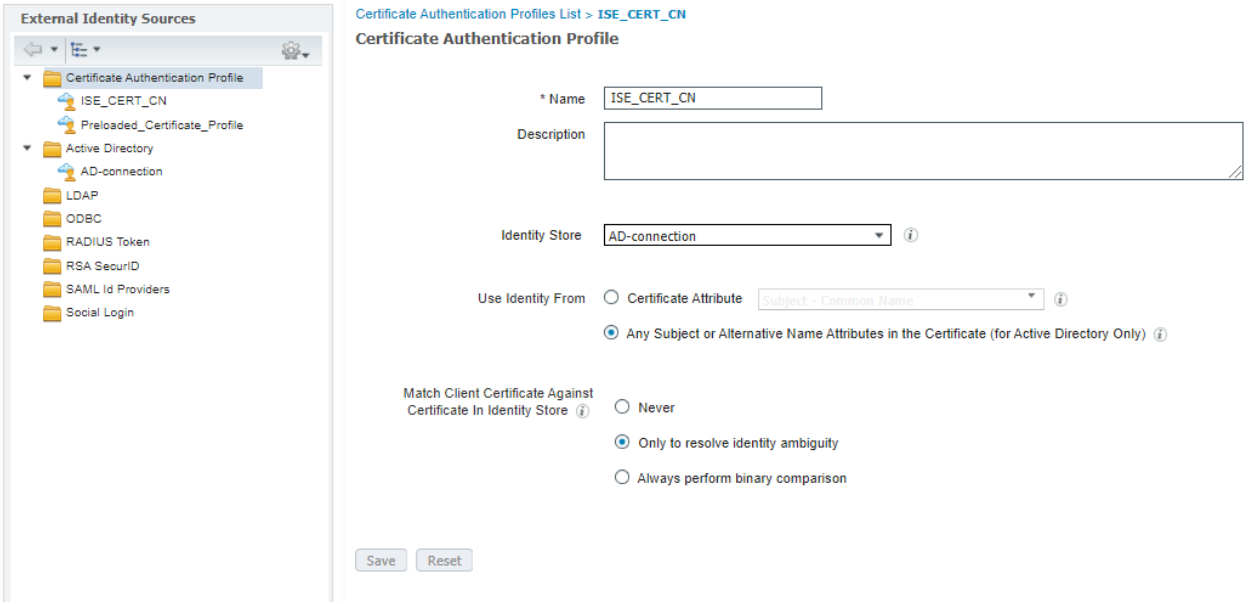


Рис. 3.68. Створення профілю аутентифікації за допомогою сертифікатів

У вкладці з зовнішнім джерелом Active Directory потрібно додати ще дві групи: користувачі домену, комп'ютери домени. Це необхідно буде в подальшому для перевірки сертифікату робочої станції та користувача під час роботи з протоколом RADIUS та 802.1X.

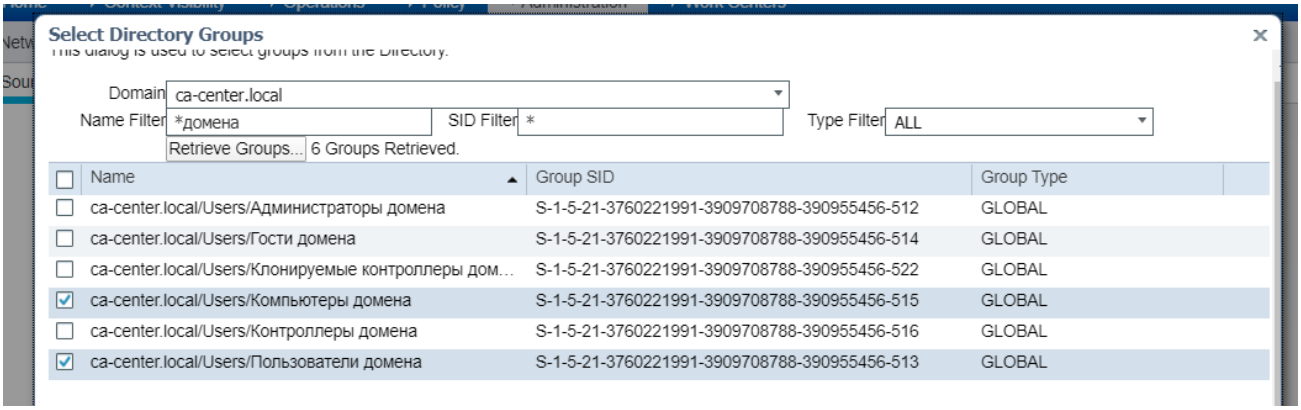


Рис. 3.69. Додавання груп з користувачами та комп'ютрами домена

Необхідно знову створюити порядок перевірки особистості, але вже для протоколу RADIUS з використанням параметру Certificate Based Authentication, в якому вказується попередньо створений профіль аутентифікації за допомогою сертифікатів.

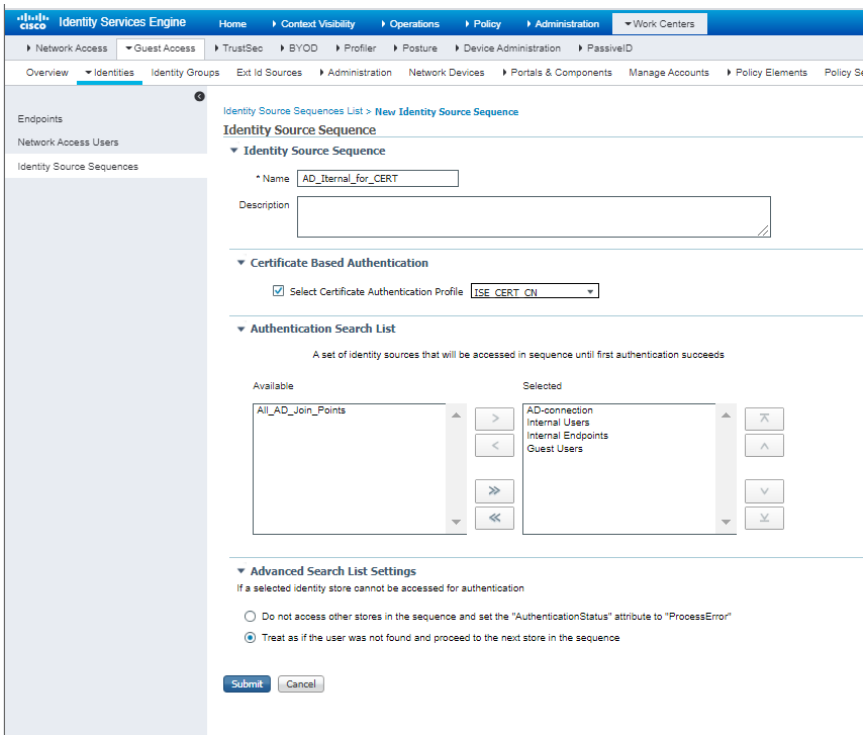


Рис. 3.70. Створення порядку перевірки особистості для політики протоколу RADIUS

Перед створенням нової політики протоколу RADIUS залишається створити новий список з дозволеними протоколами захисту. Використовуватись будуть два протоколи: EAP-TLS, PEAP.

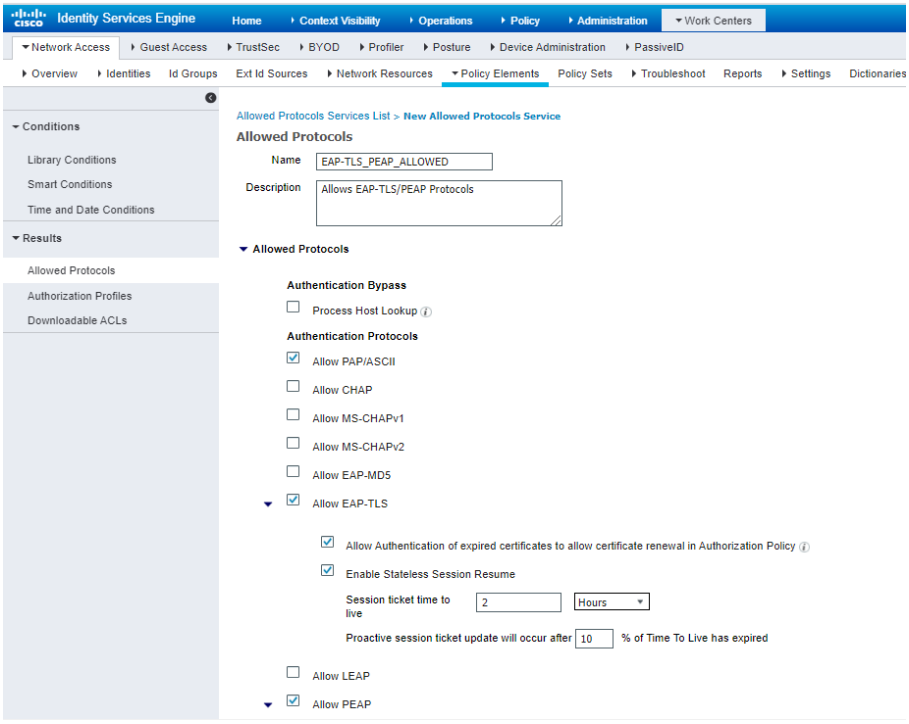


Рис. 3.71. Створення списку з дозволеними протоколами захисту

Для протоколу RADIUS створимо новий набір політик. Основні умови використання цього набору політик мають одночасно виконуватись.

1. Тип пристрою комутатор другого або третього рівня.

2. Якщо Порт NAS, який аутентифікує користувача, це порт Ethernet.

3. Умова відповідати запитам на аутентифікацію на основі 802.1X відповідно до атрибутів протоколу, визначених у профілі пристрою.

Якщо всі умови виконуються, тоді використовуються дозволені протоколи захисту EAP-TLS/PEAP.

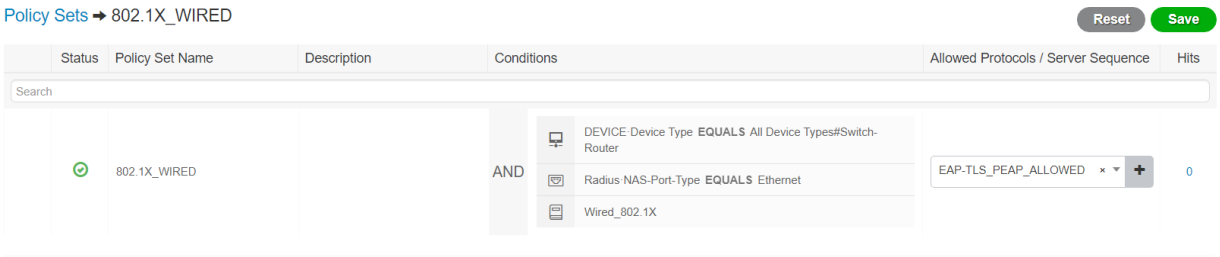


Рис. 3.72. Набір політик для протоколу RADIUS з умовами використання

Створюємо дві політики аутентифікації з умовами перевірки. Для аутентифікації за допомогою PEAP використовується умова за замовчуванням EAP-MSCHAPv2, яка визначає тип аутенфікації обраний на робочій станції. В той час для аутентифікації за допомогою EAP-TLS обрано також умову за замовчуванням для перевірки типу аутенифікації на робочій станції, але з додатковою умовою на перевірку видавця сертифікату. Якщо видавець сертифікату має назву сертифікаційного центру Windows Server, тоді виконуємо пошук у порядку перевірки особистості створеного для протоколу RADIUS з використанням сертифікату.

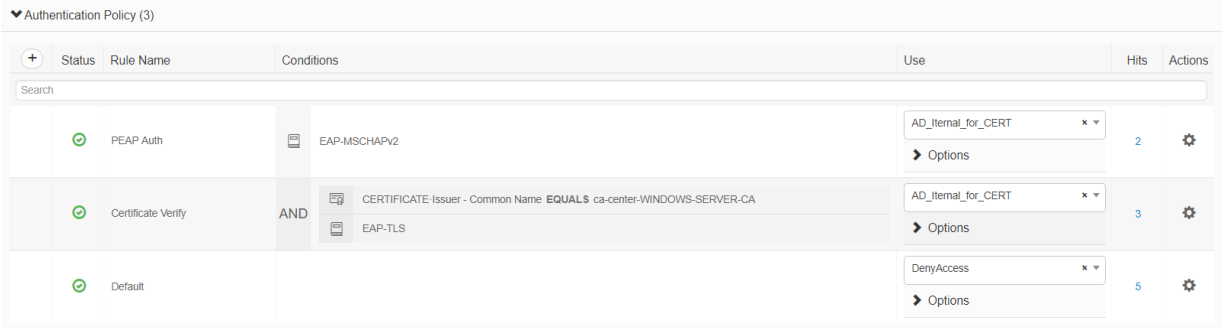


Рис. 3.73. Політика аутентифікації для протоколів EAP-TLS та PEAP

Політики авторизації відбувається в два етапи.

1. Відбувається перевірка належності робочої станції до групи робочих станцій у домені.

2. Відбувається перевірка даних користувача та чи належить він до групи користувачів у домені. Друга умова перевіряє чи попередньо робоча станція була аутентифікована, щоб не робити зайву перевірку робочої станції.

Після перевірки користувачу надається доступ до мережі інтернет, але якщо один з етапів не був виконаний, доступ до мережі інтернет забороняється. Наприклад, якщо у робочої станції відсутній сертифікат і вона не належить до групи комп'ютерів домену, але користувач ввів коректний логін і пароль, в такому випадку у робочої станції не буде доступу, адже можливий випадок викрадення інформації користувача і використання ноутбука злоумисника з викраденими даними працівника. Для інших випадків буде використовуватись політика за замовчуванням, яка відхиляє доступ до мережі. Також необхідно зазначити, що основний метод аутентифікації буде EAP-TLS, адже він надійніший, метод з використанням PEAP виступає більше в ролі запасного варіанту.

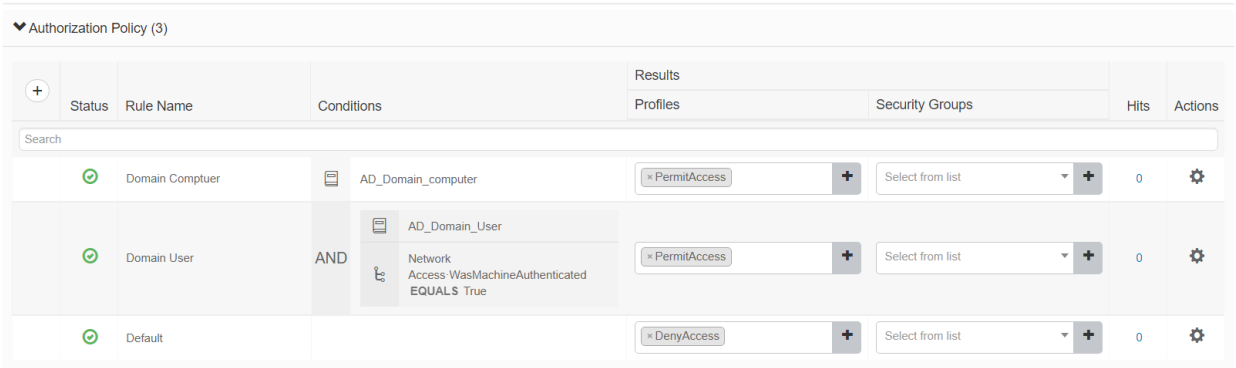


Рис. 3.74. Політики авторизації для набору політик протоколу RADIUS

Всі налагодження для протоколів RADIUS, TACACS+ та 802.1X зроблені і вони повністю готові до роботи. Останнім, що можна зробити, це налагодити систему резервного копіювання конфігураційних та моніторингових файлів Cisco ISE. Для цієї задачі на початку роботи був налагоджений FTP-сервер на

Windows сервері. У пристрої ISE залишається створити репозиторій з підключення до FTP-серверу та локальний репозиторій.

Для репозиторію будемо використовувати обліковий запис адміністратора з групи ftp-group, користувачі якою мають доступ до резервних копій з пристрою ISE.

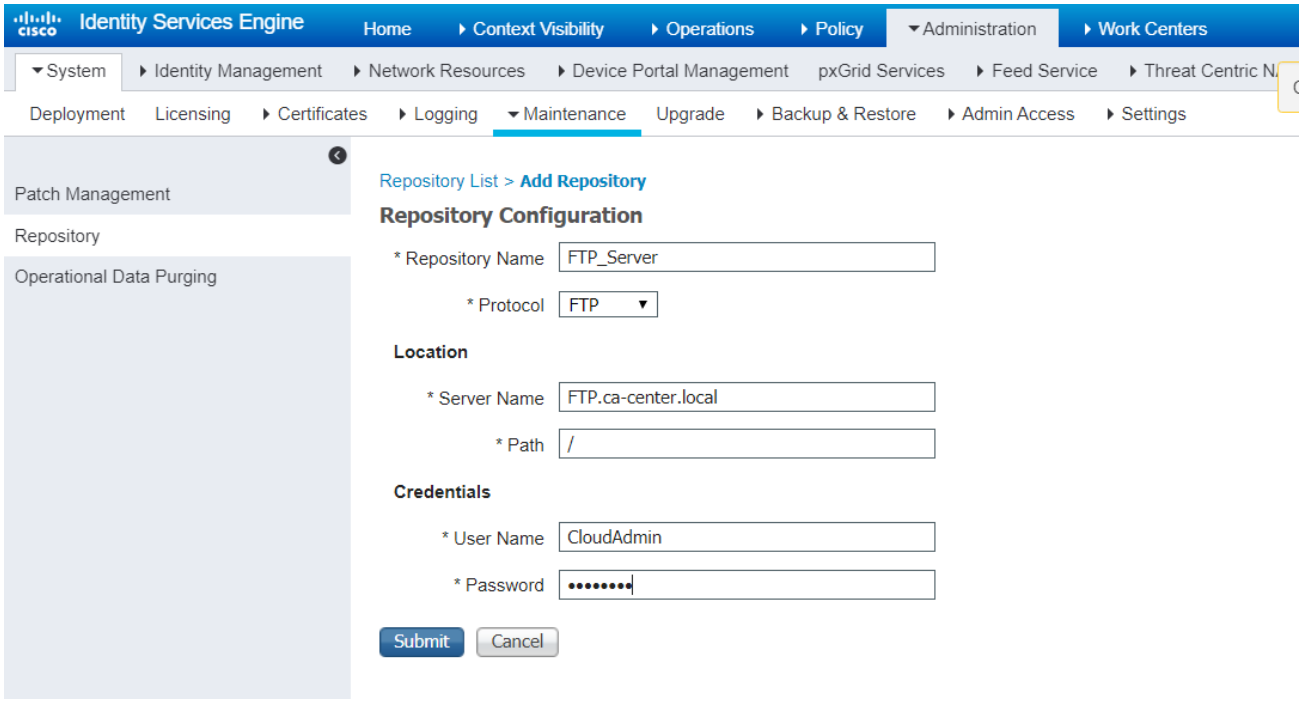


Рис. 3.75. Створення репозиторію для FTP-сервера

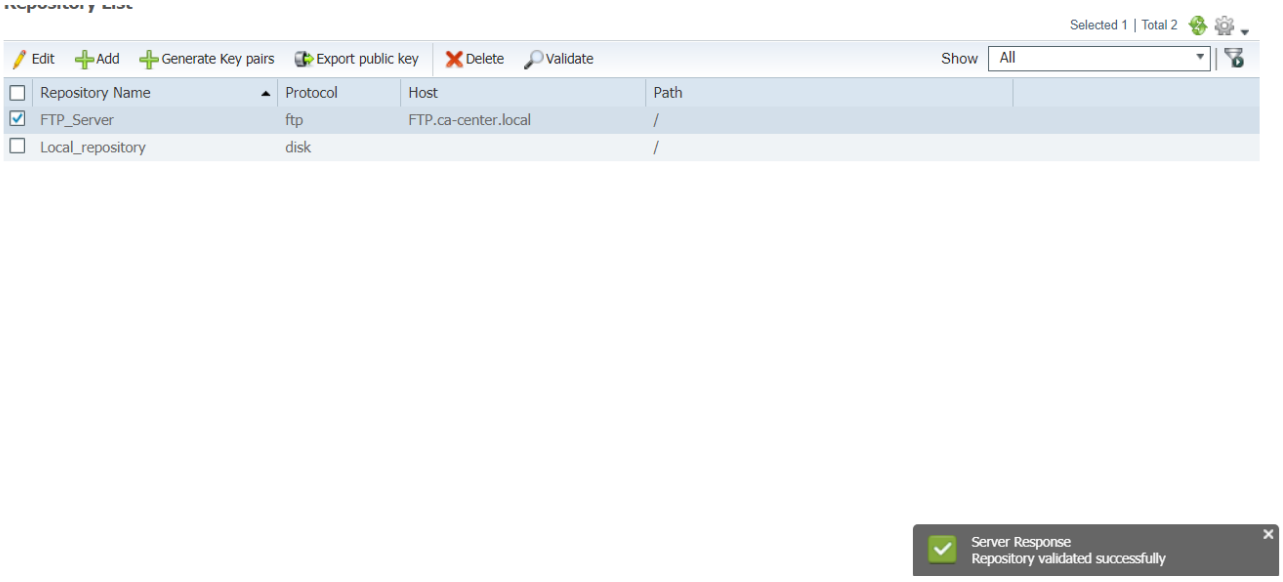


Рис. 3.76. Створені репозиторії та валідація зв’язку з FTP-сервером

При створенні резервної копії вказується пароль шифрування для захисту даних файлів конфігурації та моніторингу. Також важливо знати, що локальне

сховище сертифікатів не зберігається разом з резервною копією конфігураційних даних, тому їх рекомендовано експортувати окремо, інакше в разі пошкодження системи відновити їх буде неможливо. Процес збереження резервних копій зазвичай займає приблизно 10-15 хвилин.

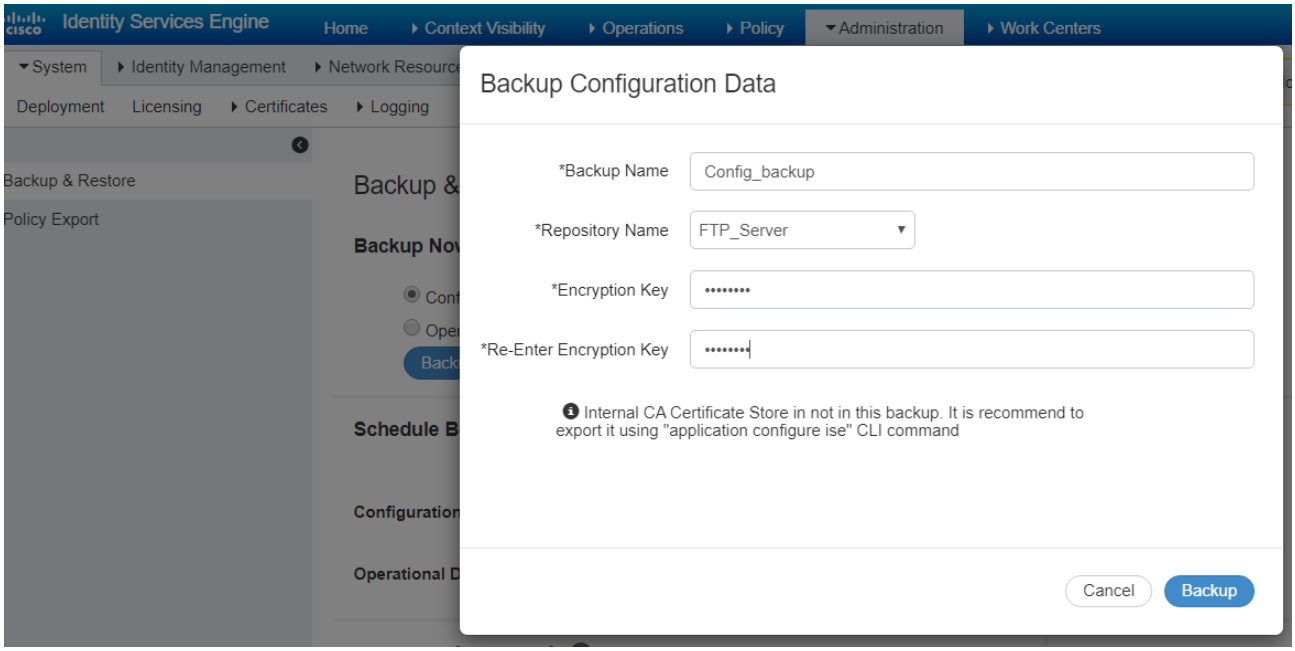


Рис. 3.77. Створення резервної копії конфігураційних даних

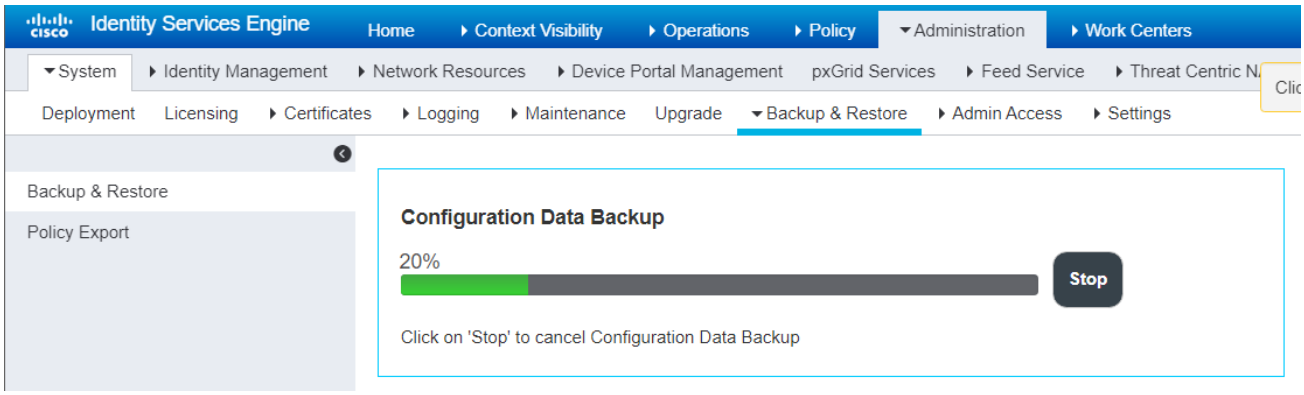


Рис. 3.78. Процес збереження резервної копії на FTP-сервер

Якщо резервні копіювання файлів конфігурації і моніторингу успішні, при натисканні на репозиторій мають з’явитись дані про останні файли у репозиторії з датою, коли вони були зроблені.

В данному випадку резервні копії були зроблені для демонстрації в ручному режимі, можливе також їх налагодження в автоматичному режимі в обрані години, дні або місяці.

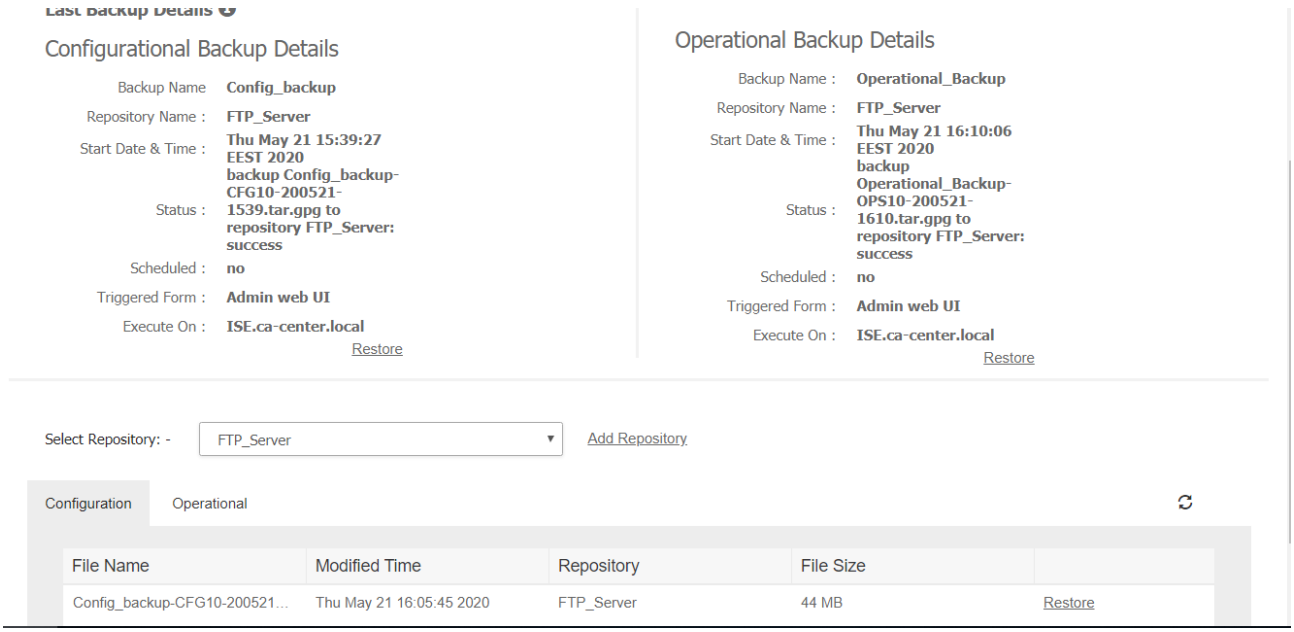


Рис. 3.79. Інформація про останні резервні копії

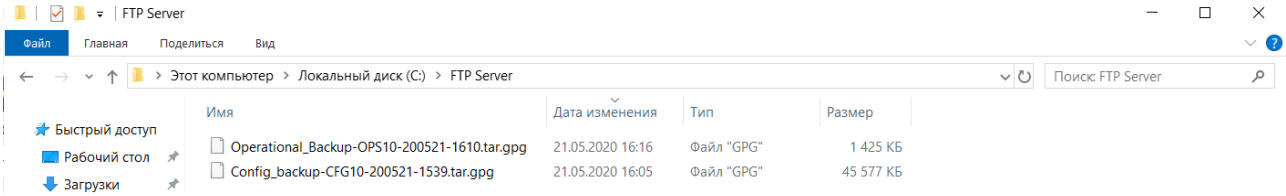


Рис. 3.80. Відображення резервних у каталозі налагодженому для FTP-серверу

На данному етапі виконані всі необхідні налагодження для коректного функціонування пристрою Cisco Identity Services Engine та протоколів RADIUS, TACACS+, 802.1X. Проведено повну інтеграцію з Windows сервером та службою каталогів Active Directory з використанням сертифікатів та підрозділів з групами користувачів. Визначено та налагоджено всі можливі умови аутентифікації та авторизації користувачів для протоколів. Методи аутентифікації були налагодженні з передбаченням можливих дій злоумисників. Налагоджено допоміжний функціонал пристрою для підвищення захисту та стабільності роботи пристрою у мережі підприємства.

3.4. Перевірка працездатності підсистеми аутентифікації

В данному пункті виконується перевірка роботи рішення Cisco Identity Services Engine з налагодженими протоколами та робочими станціями.

Для перевірки роботи протоколу TACACS будемо використовувати дані користувачів з обраних груп, які мають різні права доступу під час віддаленого підключення SSH з використанням програми Putty.

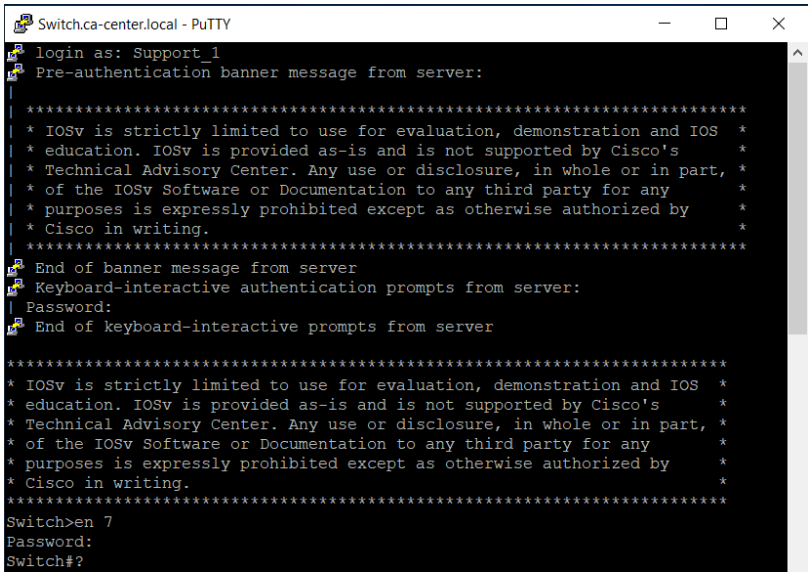


Рис. 3.81. Вхід на пристрій з використанням користувача підтримки

Вхід з користувача підтримки Support_1 успішний як і вхід у привілейований режим з рівнем 7. Після цього користувачу підтримки мають бути доступні лише команди show, а всі інші заборонені, тому це необхідно перевірити.

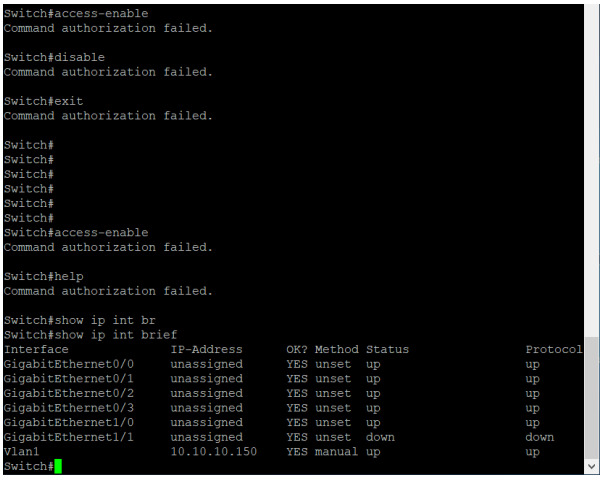


Рис. 3.82. Використання команд show дозволяються, всі інші забороняються

Користувачі групи підтримки налагоджені правильно, тепер перейдемо до перевірки користувачів з групи техніків, їм встановлено початковий рівень привілею 1 і максимальний 15, але 15 рівень привілеїв не надає їм всі права, як адміністраторам. Вони можуть робити деякі зміни на інтерфейсах пристроїв, спробуємо це перевірити.

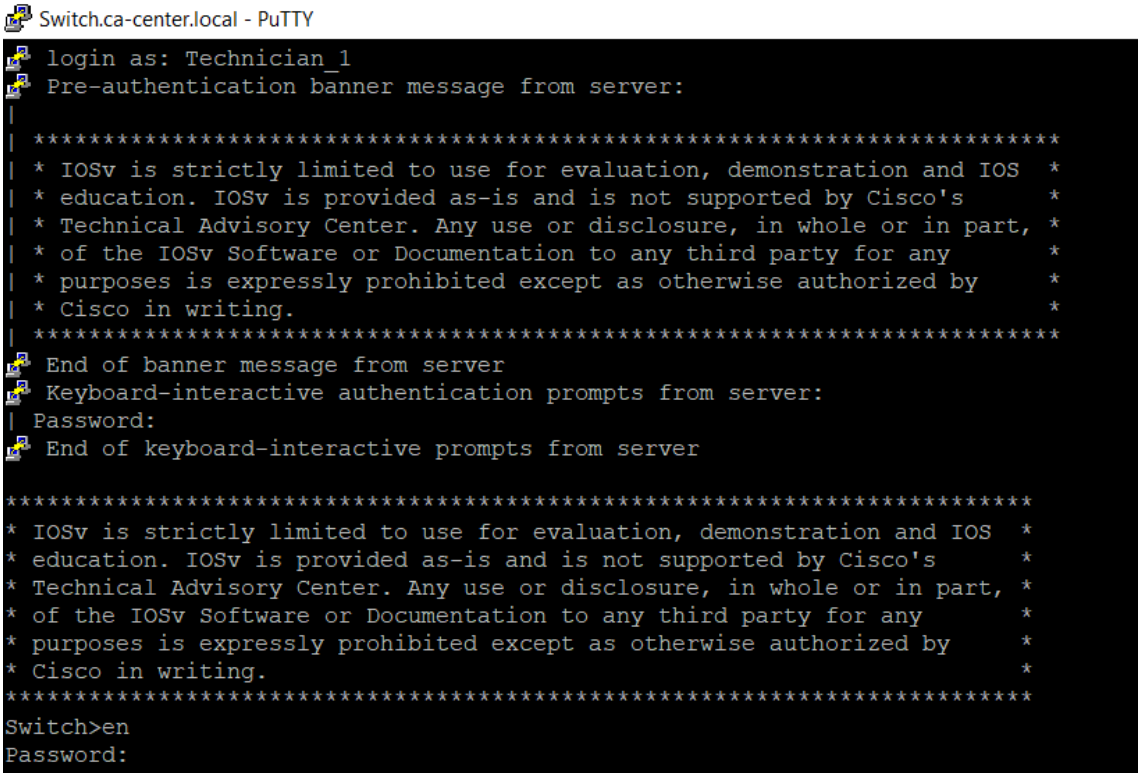


Рис. 3.83. Вхід на пристрій з використанням користувача техніка

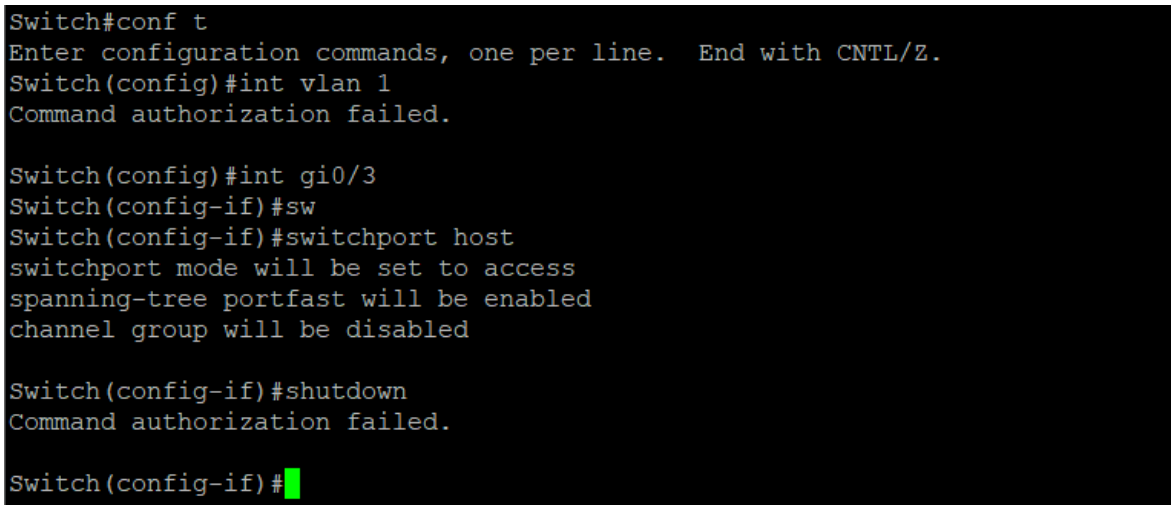


Рис. 3.84. Перевірка дозволених команд для користувачів з групи техніків

Перевіримо вхід користувачів з групи адмністраторів. Для них дозволені всі команди на пристроях.

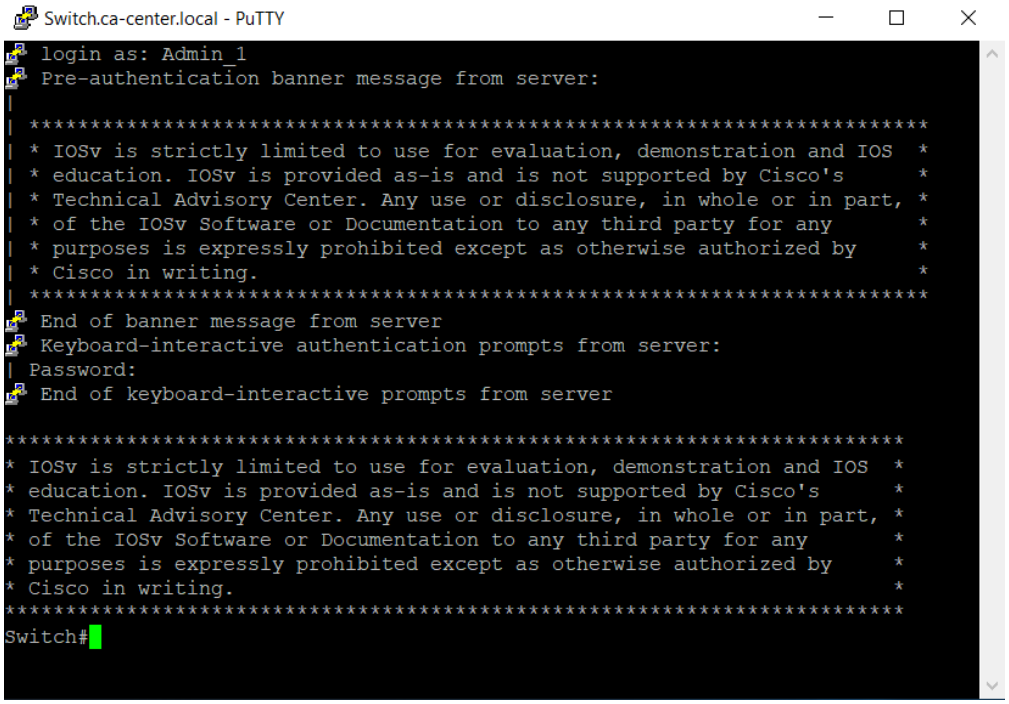


Рис. 3.85. Вхід на пристрій з використанням користувача адміністратора

На початку роботи комутатор було налагоджено на випадок непередбачуваної ситуації. Спробуємо імітувати, що пристрій Cisco ISE аварійно завершив свою роботу і відповідно TACACS+ не працює, тоді в нагоді будуть локальні облікові записи мережевих пристроях. Комутатор був налагоджений так, що використання локальних облікових записів мережевих пристроїв неможливе, якщо працює TACACS+, а у випадку коли він не відповідає, використання локальний облікових записів дозволяється.



Рис. 3.86. Заборона входу під локальними обліковими записами, якщо TACACS+ працює

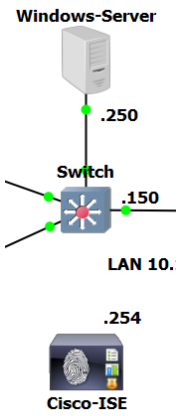


Рис. 3.87. Відключення Cisco ISE від комутатора

Після того як пристрій ISE відключено від комутатора, всі облікові записи для протоколу TACACS+ з Active Directory не будуть працювати.

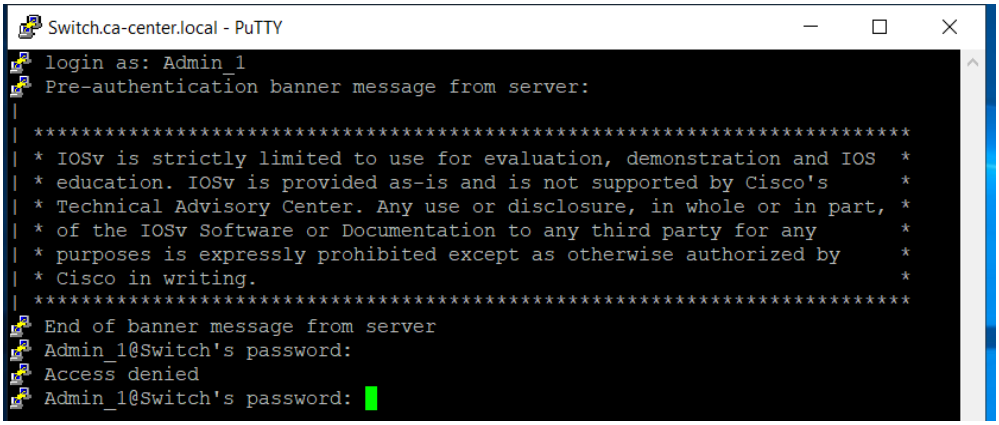


Рис. 3.88. Вхід на пристрій з використанням користувача адміністратора

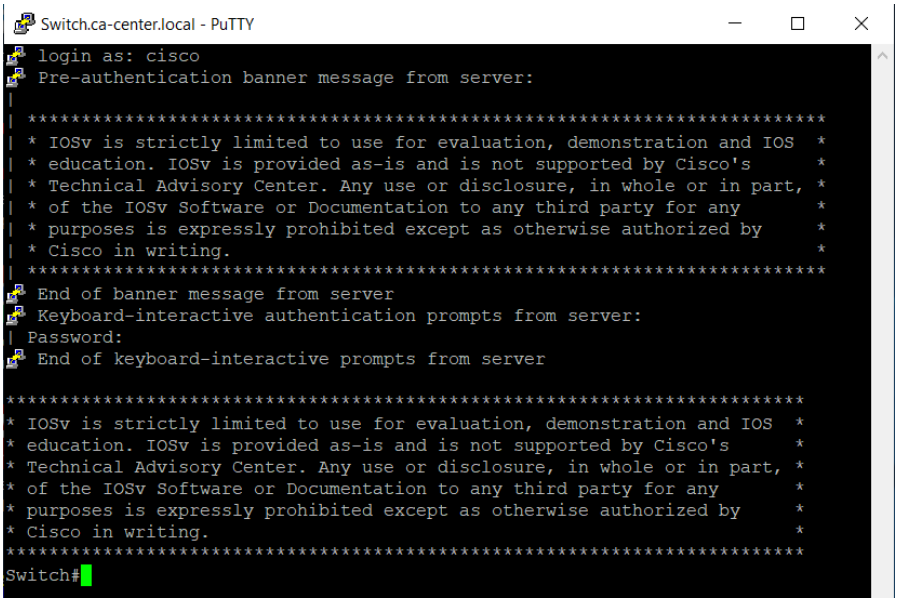


Рис. 3.89. Вхід на пристрій з використанням локального облікового запису

Всі групи користувачів перевірені і коректно працюють відповідно до зроблених налагоджень на пристрої ISE. Пристрій ISE контролює кожну спробу входу і зберігаю цю інформацію. Переглянемо всі спроби.

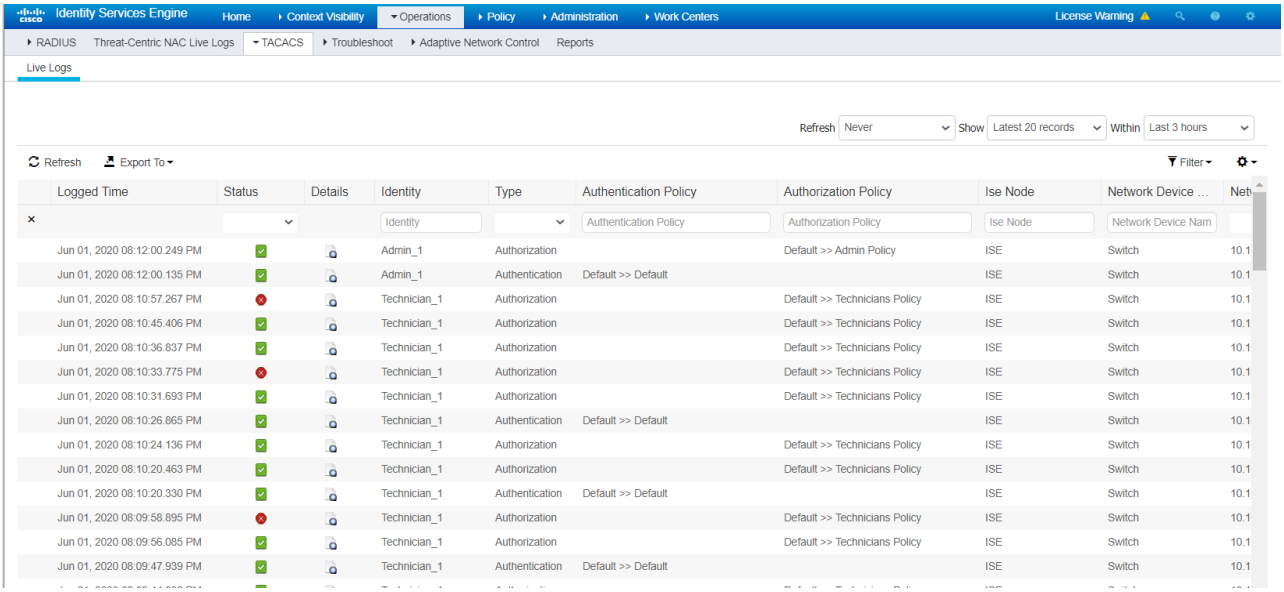


Рис. 3.90. Відображення спроб аутентифікації та авторизації у систему TACACS+

Окрім списку з усіма спробами аутентифікації та авторизації є можливість переглянути кожну спробу детально.

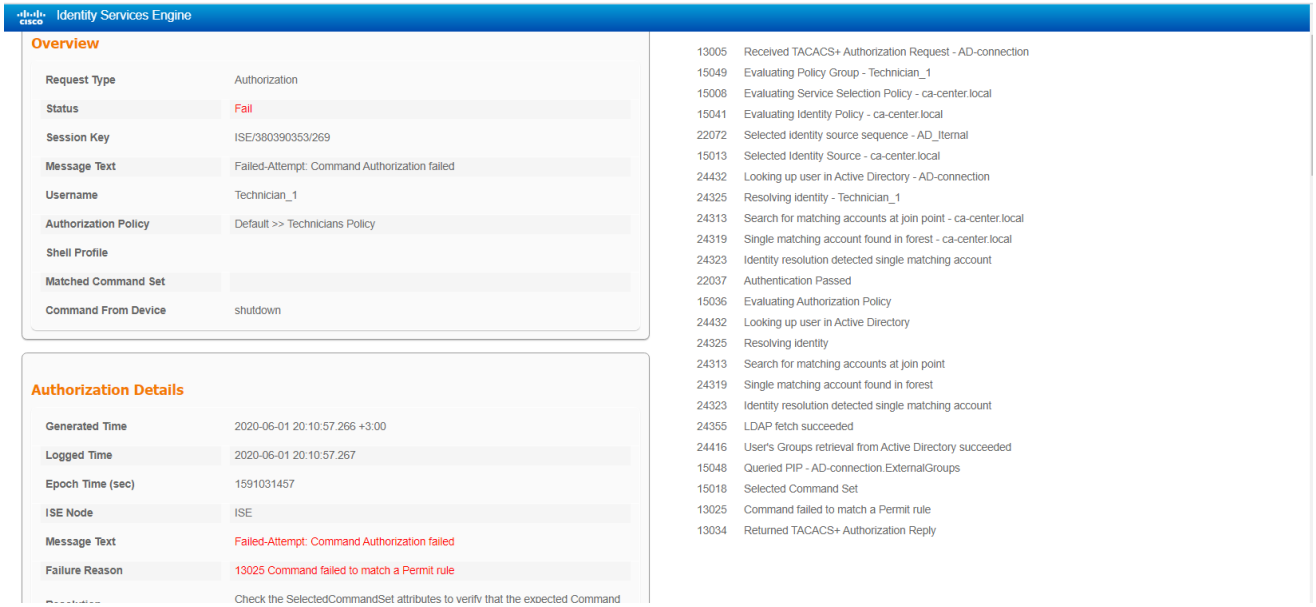


Рис. 3.91. Детальна інформація про невдалу спробу авторизуватися на мережевий пристрій

Можемо побачити, що спрацювала політика авторизації для користувача з групи техніків. Доступ був заборонений через те, що було використану команду shutdown, яка заборонена для цієї групи.

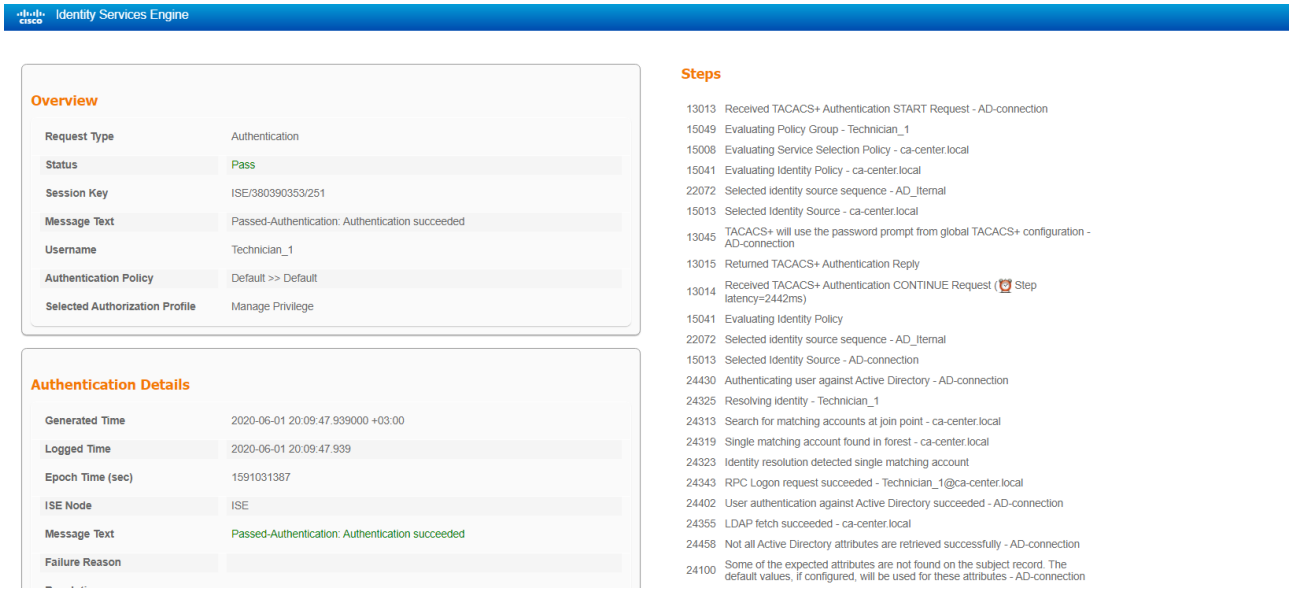


Рис. 3.92. Детальна інформація про аутентифікацію на мережевий пристрій

Тестування протоколу TACACS+ успішне. Переходимо до тестування протоколу RADIUS. Під час його тестування мають виконуватись деякі умови. Робочі станції мають знаходитись у домені, на Windows сервері виділені два сертифікати від сертифікаційного центра для робочої станції та користувача, щоб дозволити використання EAP-TLS. Попередньо на Windows сервері була налагоджена політика для встановлення на робочих станціях за замовчуванням EAP-TLS, як основного засобу входу у мережу (зазвичай практика налагодження доменої політики для автоматичного встановлення захищенного з'єднання або перевірки справжності використовується на підприємствах), але на період тестування вона була відключена для того щоб перевірити роботу EAP-TLS та PEAP окремо. Результатом перевірки має бути вільний доступ у мережу підприємства.

Перший крок, це налагодити перевірку справжності в ручному режимі після чого бажано перезавантажити машину. Перевірка справжності налагоджена на одному комп'ютері за допомогою EAP-TLS, а на другом PEAP

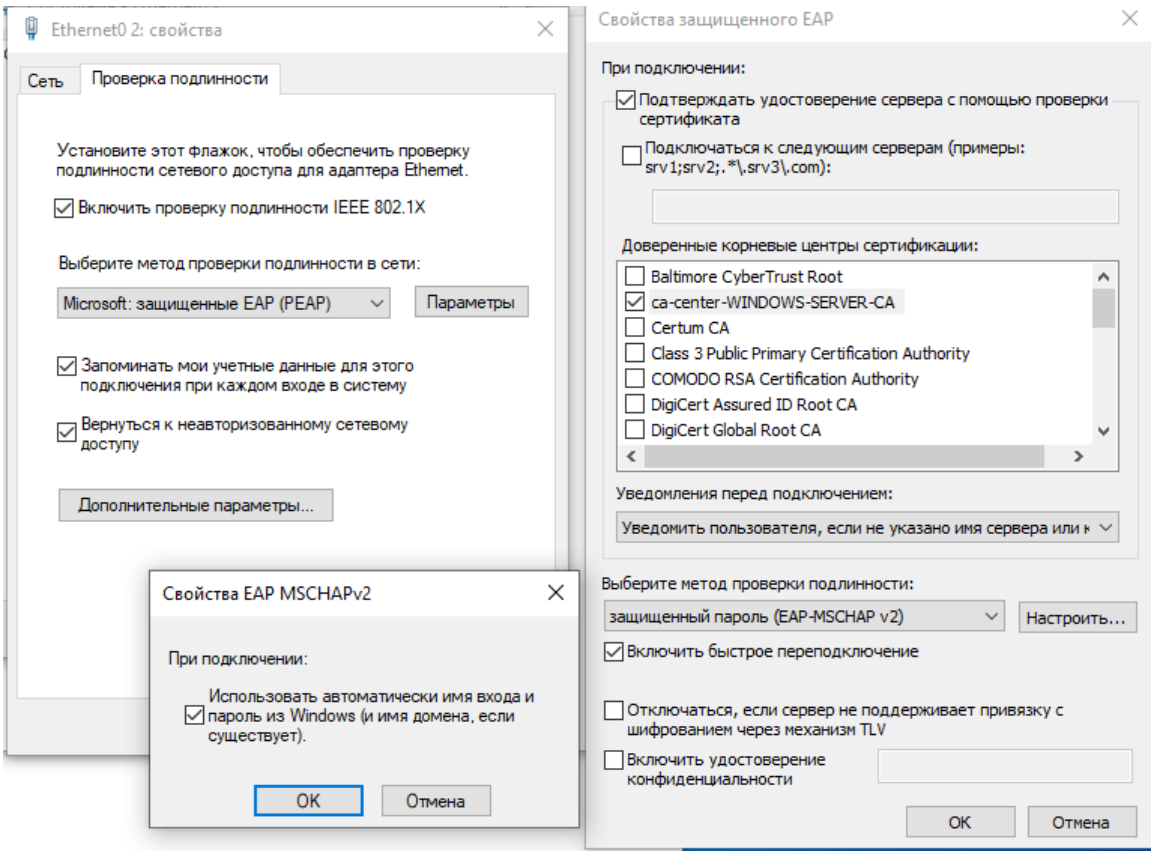


Рис. 3.93. Налагодження необхідні для роботи PEAP на робочій станції

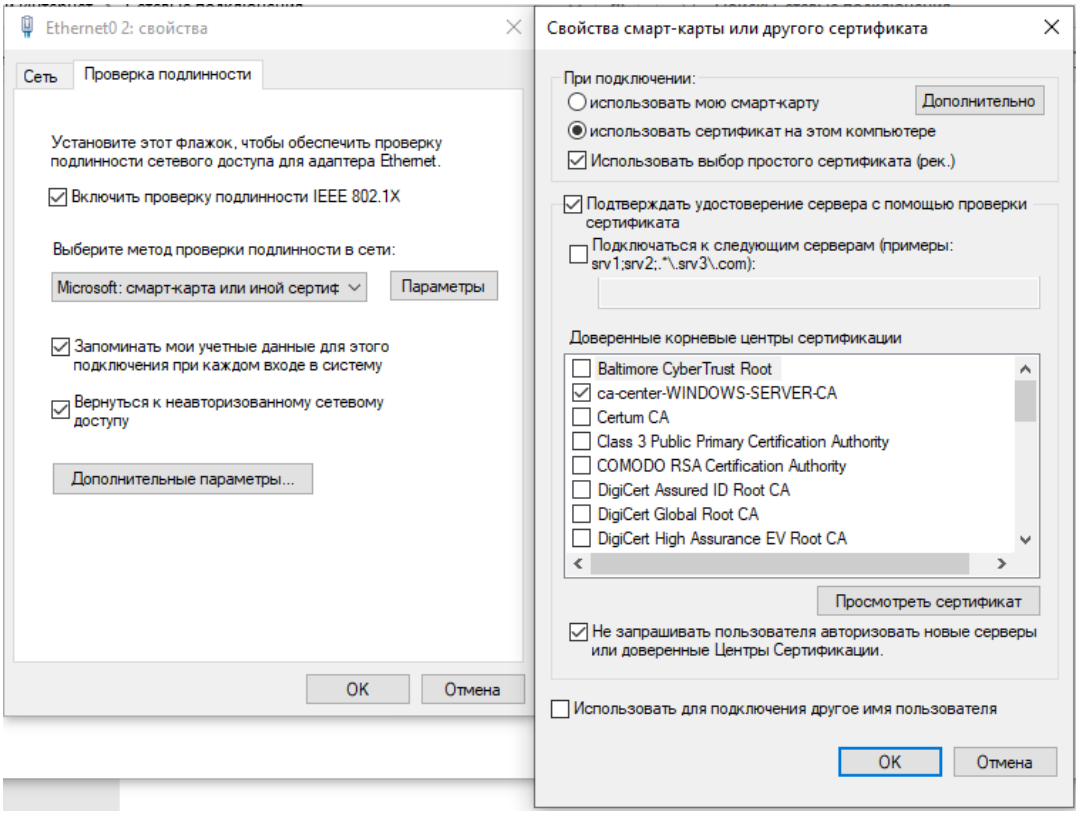


Рис. 3.94. Налагодження необхідні для роботи EAP-TLS на робочій станції

При використанні обох методів аутентифікації спочатку відбувається аутентифікація робочої станції і тільки якщо умова виконується, дозволяється вхід користувача. Різниця цих методів лише у роботі. EAP-TLS використовує сертифікати комп'ютера та користувача, як додакову перевірку, а PEAP використовує лише дані комп'ютера та користувача, тому він виступає, як запасний варіант.

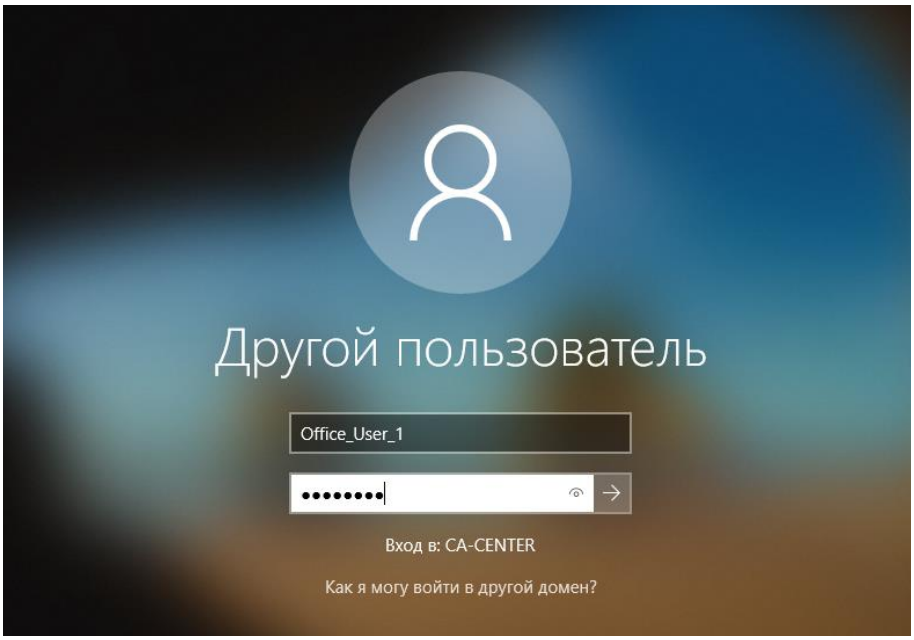


Рис. 3.95. Вхід користувача для перевірки

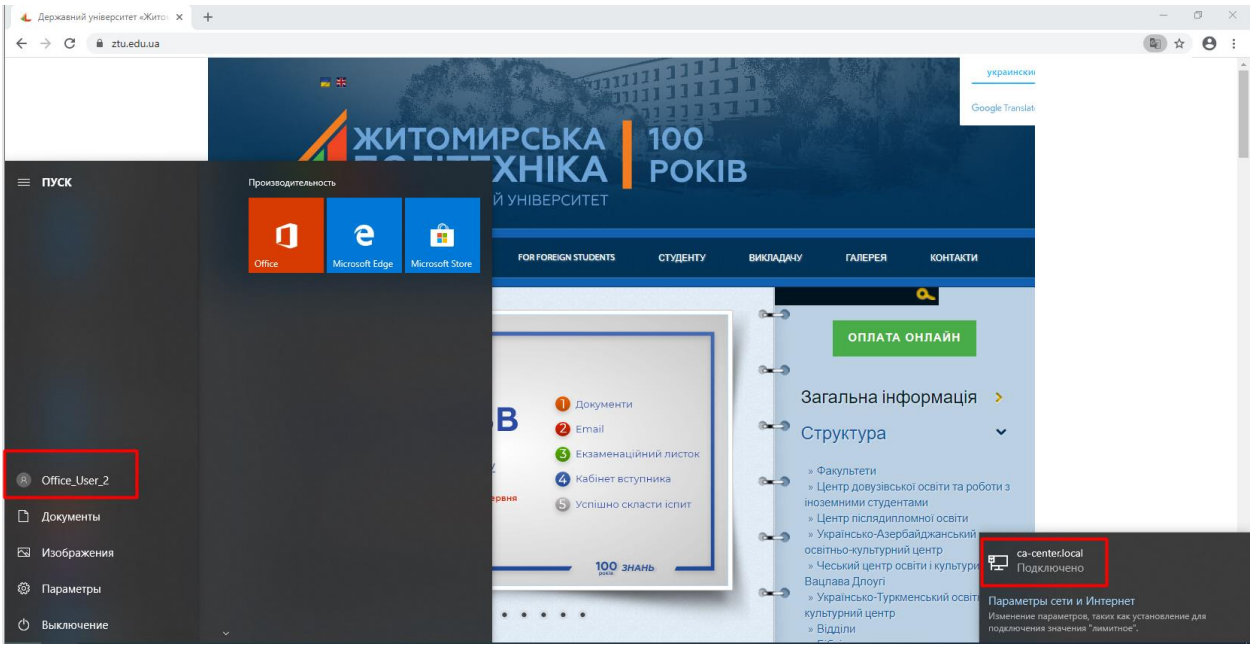


Рис. 3.96. Доступ до інтернету, якщо користувач пройшов перевірку

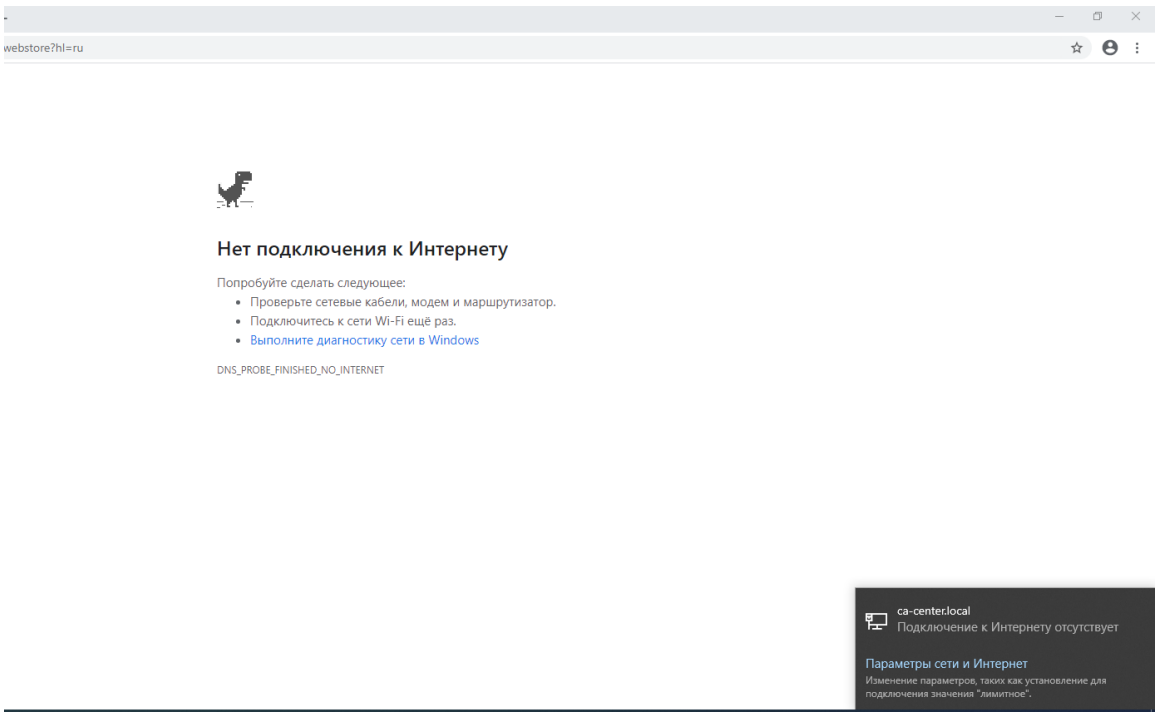


Рис. 3.97. Відсутність доступу до інтернету, якщо користувач не пройшов перевірку

Політики аутентифікації та авторизації перевірені. Додатково можно переглянути повідомлення на комутаторі для протоколу RADIUS у процесі відладки та моніторингові дані на самому пристрої ISE.

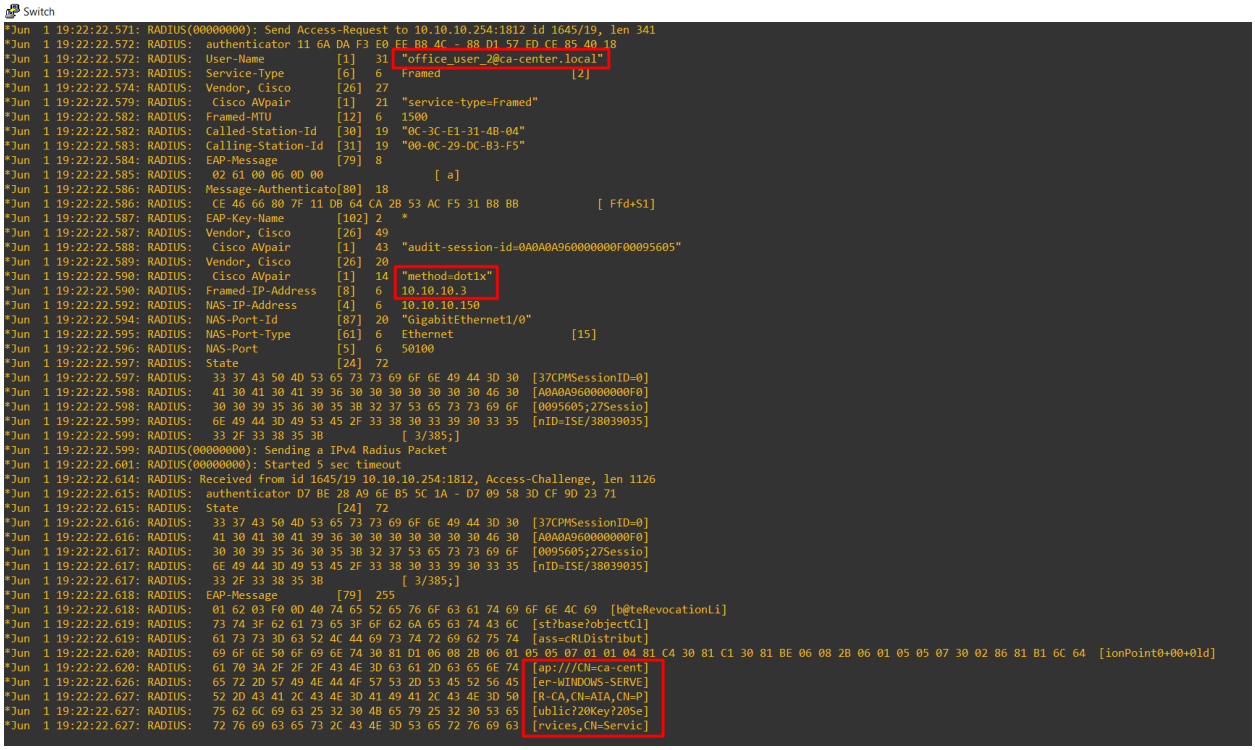


Рис. 3.98. Протокол RADIUS під час відладки на комутаторі

У вкладці RADIUS Live Logs мають з’явитись відомості про нові пристрої, які були успішно аутентифіковані і сессії, що відбуваються. Після того, як робочі станції аутентифіковані, вони відображаються у списку. Так само відбувається, якщо аутентифікація була не пройдена, з’являються спроби невдалої аутентифікації у списку.

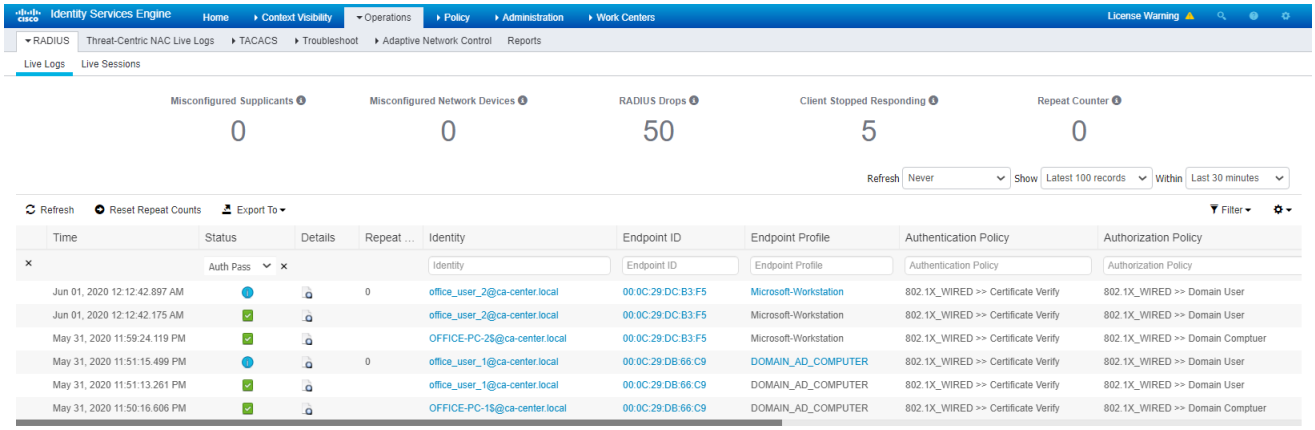


Рис. 3.99. Інформація про пристрої з яких був здійснений вхід з EAP-TLS

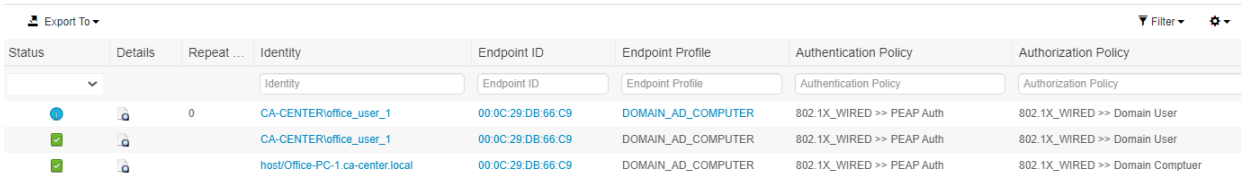


Рис. 3.100. Інформація про пристрої з яких був здійснений вхід з використанням PEAP

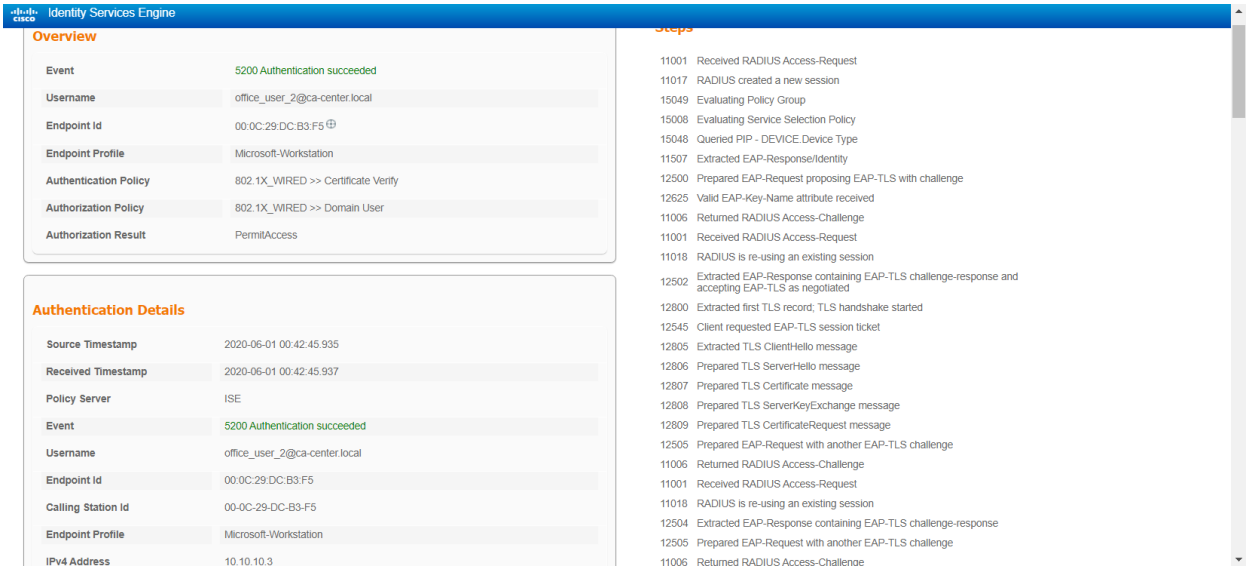


Рис. 3.101. Інформація про пристрої з яких був здійснений вхід з використанням PEAP

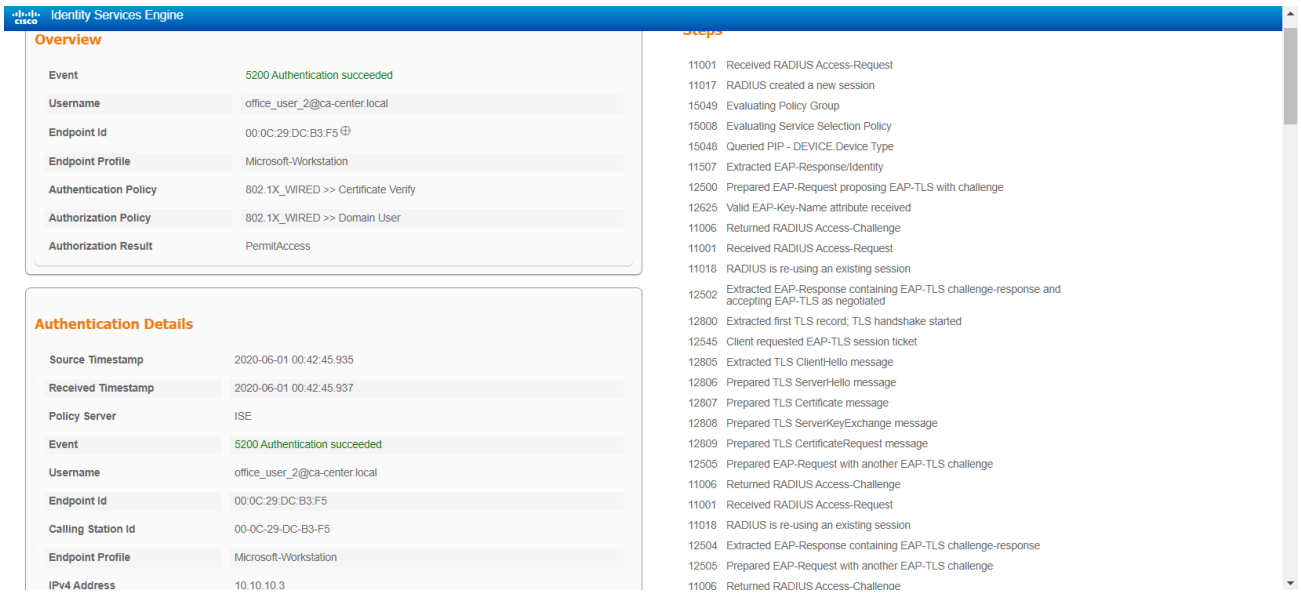


Рис. 3.102. Детальна інформація про успішну аутентифікацію на мережевий пристрій

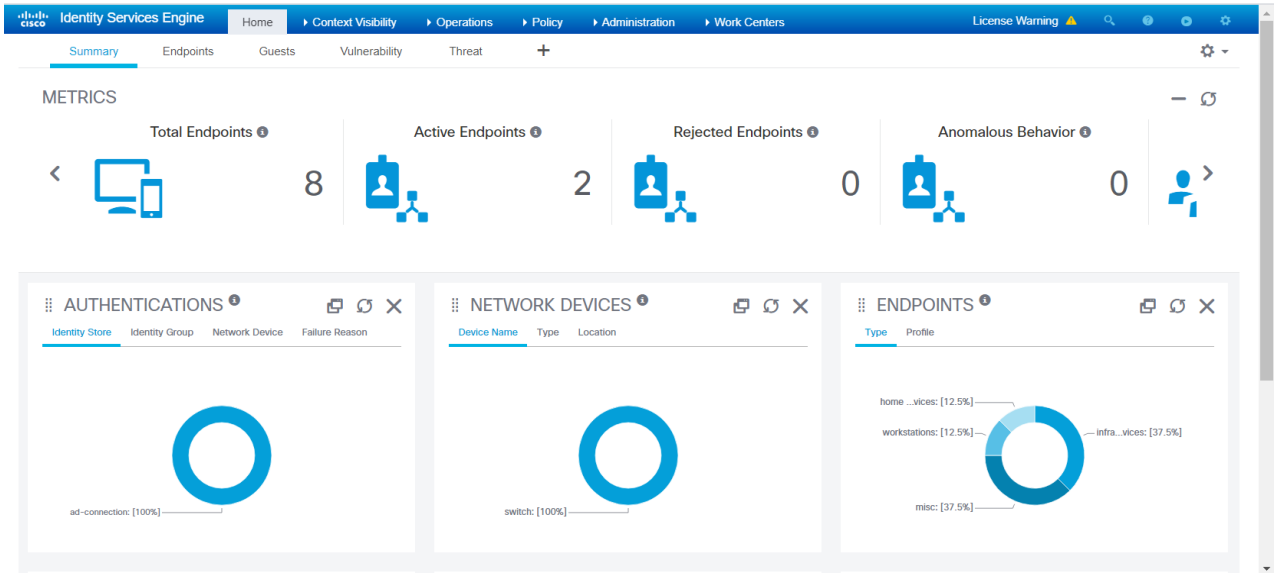


Рис. 3.103. Статистика пристроїв на головній сторінці

Після всіх налагоджень на головній сторінці відображається оновлена загальна кількість пристроїв у мережі, активні кінцеві пристрої, які пройшли аутентифікації, та додаткова інформація статистика про джерело перевірки аутентифікації, мережеві пристрої та типи мережевих пристроїв, які “бачить” пристрій ISE.

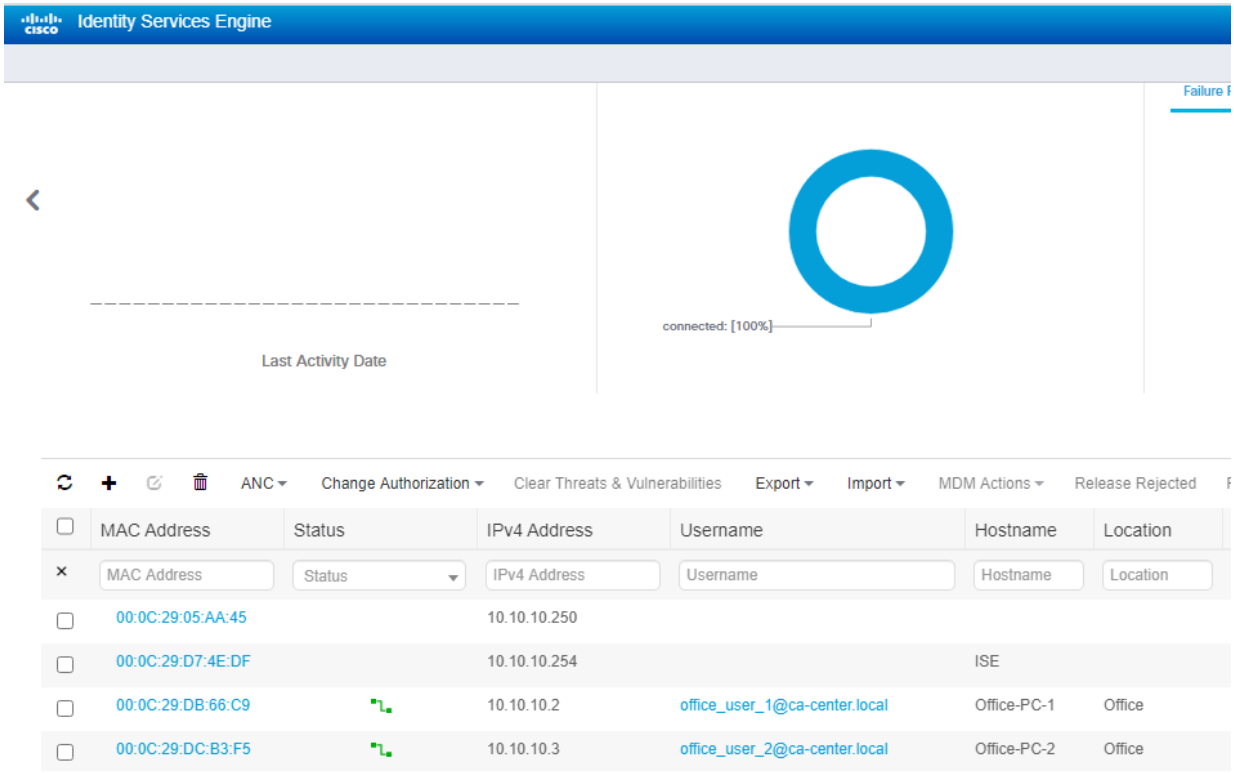


Рис. 3.104. Перелік всіх пристроїв та активні сесії

Висновки до третього розділу

В данному розділі було проведено роботу з налагодження мережевого обладнання для роботи з протоколами AAA, TACACS+, RADIUS, стандартом 802.1X та можливістю виходу у мережу інтернет. Windows Server був налагоджений та підготовлений для інтеграції з рішенням від Cisco Identity Services Engine. Рішення Cisco Identity Services Engine повністю налагоджене для адміністрування мережевих пристроїв та надання доступу до мережі. Перевірено працездатність мережі при використанні віддаленого доступу до пристроїв та робочих станцій для аутентифікації.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було спроектовано та реалізовано підсистему аутентифікації на базі рішення Cisco Identity Services Engine:

1. Проведено аналіз протоколу AAA. Розглянуто архітектуру, сферу застосувань, принцип роботи та його основні компоненти: аутентифікація, авторизація, аудит. Було розглянуто основне призначення, особоливості та принцип роботи протоколів RADIUS, TACACS+. Проведено порівняння протоколів TACACS+ та RADIUS, розглянуто переваги та недоліки кожного. Проаналізовано принцип роботи і процедуру передачі EAP-повідомлень сервером доступу стандарту IEEE 802.1X в комп'ютерних мережах. Досліджено рішення Cisco Identity Services Engine, принцип його роботи, для яких цілей використовується та переваги його використання у великих інфраструктурах. В результаті аналізу протоколів та засобів забезпечення підсистеми аутентифікації сформовано розуміння принципу роботи протоколів, стандарту 802.1X, сфери використання та необхідності рішення Cisco Identity Services Engine для реалізації та застосування у проекті.

2. При проектуванні підсистеми аутентифікації було проведено аналіз необхідного програмного забезпечення для реалізації проекту. Було обрано графічний емулятор мереж GNS3, проведено короткий аналіз можливостей та порівняння з Cisco Packet Tracer. Проаналізовано програмний продукт засобів віртуалізації VMWare Workstation, який буде забезпечувати поєднання віртуальної та фізичної мережі. Наведено сценарій встановлення зображення віртуальної машини на базі рішення Cisco Identity Services Engine для використання у проекті. Розроблено адресацію майбутньої комп'ютерної мережі, з врахуванням кількості всіх пристроїв. В результаті виконаної роботи маємо всі інструменти для побудови проекту у віртуальному середовищі.

3. Після побудови проекту у віртальному середовищі виконано роботу з налагодження мережевого обладнання. Маршрутизатор налагоджено для доступу до фізичної мережі з віртуальної мережі, на комутаторі другого-третього

рівня було налагоджено протоколи AAA, RADIUS, TACACS+ та стандарт 802.1X. Встановлено всі необхідні компоненти Windows Server розгорнуто домен, сертифікаціний центр, налагоджено видачу сертифікатів робочим станціям і користувачам, DHCP-сервер, FTP-сервер. Налагоджено політику домену для встановлення підлкючення на робочих станціях за стандартом 802.1X, створено підрозділи з користувачами підприємства. Основні налагодження були виконані на Cisco Identity Services Engine, такі як: підключення до служби каталогів Active Directory і повна інтеграція з Windows Server, ідентифікація всіх пристроїв мережі, імпорт та створення сертифікатів, ввімкнення протоколів RADIUS та TACACS+. Налагоджено політики доступу протоколів з врахуванням привілеїв та режимів доступу користувачів. Реалізовано резервне копіювання конфігураційних та моніторингових файлів на віддалений FTP-сервер. Перевірено працездатність підсистеми з використанням віддаленого підключення SSH та робочими станціями для аутентифікації користувачів. Проаналізовано моніторингові дані про аутентифікацію і авторизацію користувачів на робочих станціях та на мережевих пристроях.

Результатом кваліфікаційної роботи є повністю функціональний проект підсистеми аутентифікації на базі рішення Cisco Identity Services Engine з інтегрованим Windows Server, проект може застосовуватись на підприємствах у реальному житті.

В подальшому дана підсистема може бути покращена шляхом налагодження інших функцій рішення Cisco Identity Services Engine, технології TrustSec та впровадженням нових пристроїв у проект мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Документація по протоколу RADIUS[Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-7-0E/wireless/configuration-guide/b_37e_4500sup8e_cg/configuring_radius.pdf
2. The RADIUS Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://networkradius.com/doc/3.0.10/introduction/RADIUS.html
3. Как работает RADIUS? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.pdf
4. Протоколы AAA: RADIUS и Diameter. Книга 9. Телекоммуникационные протоколы/ Б.С.Гольдштейн, В.С.Елагин, Ю.Л. Сенченко. СПб.: Питер, 2014.. 352 с.
5. Authorization, Authentication, Accounting [Електронний ресурс] – Режим доступу до ресурсу: https://networkradius.com/doc/3.0.10/concepts/introduction/AAA.html
6. Аутентификация в Cisco IOS [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/pt/blog/192668/
7. CCNP Security Secure 642-637 Official Cert Guide / Sean Wilkins, Franklin H. Smith. Cisco Press. 228 с.
8. Neumann J. The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More / Jason Neumann., 2015. – 272 с.
9. Carroll B. Cisco access control security : AAA administration services / Brandon Carroll. – Indianapolis, IN: Cisco Press, 2004. – 172 с. – (2nd ed).
10. Афанасьев А.А, Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012. - 550 с.

11. Документація по Cisco Identity Services Engine [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/security/identity-services-engine-2-4/model.html
12. Платформа Cisco Identity Services Engine [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/dam/global/ru_ru/downloads/broch/ISE_data_sheet_c78-656174_RUS.pdf
13. Cisco ISE (Identity Services Engine): Beyond the Data Sheet [Електронний ресурс] – Режим доступу до ресурсу: https://www.aspiretransforms.com/2018/02/15/aspire-webinar-cisco-identity-services-engine-ise/
14. Cisco ISE Blog [Електронний ресурс] – Режим доступу до ресурсу: https://www.lookingpoint.com/blog/topic/cisco-ise
15. Документація по протоколу TACACS[Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/xe-16/sec-usr-tacacs-xe-16-book.pdf
16. The TACACS+ Protocol [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-08.html
17. Документація по протоколу 802.1X [Електронний ресурс] – Режим доступу:https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_58_se/configuration/guide/3750scg/sw8021x.pdf
18. What is 802.1x and how does it work [Електронний ресурс] – Режим доступу до ресурсу: https://www.securew2.com/solutions/802-1x/
19. Документація по SNMP [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html
20. TACACS+ and RADIUS Comparison [Електронний ресурс]. – 2008. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html
21. VMware vs VirtualBox: what is the best software for Desktop Virtualization [Електронний ресурс] – Режим доступу до ресурсу:

https://www.iperiusbackup.net/en/vmware-vs-virtualbox-what-is-the-best-software-for-desktop-virtualization/

22. Getting Started with GNS3 [Електронний ресурс] – Режим доступу до ресурсу:https://docs.gns3.com/1PvtRW5eAb8RJZ11maEYD9_aLY8kkdhgaMB0wPCz8a38/index.html
23. RFC 1492 (TACACS+) [Електронний ресурс] – Режим доступу: https://tools.ietf.org/html/rfc1492
24. RFC 2866 (RADIUS Accounting) [Електронний ресурс] – Режим доступу: https://tools.ietf.org/html/rfc2866
25. RFC 2865 (RADIUS) [Електронний ресурс] – Режим доступу: https://tools.ietf.org/html/rfc2865
26. RFC 3579 (RADIUS EAP) [Електронний ресурс] – Режим доступу: https://tools.ietf.org/html/rfc3579
27. RFC 3580 (IEEE 802.1X RADIUS) [Електронний ресурс] – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc3580
28. RFC 2903 (AAA Architecture) [Електронний ресурс] – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc2903

ДОДАТКИ

```
Router#show run
Building configuration...

Current configuration : 7984 bytes
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ethernet lmi ce
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
ip name-server 192.168.0.1
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface GigabitEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
!
ip forward-protocol nd
no ip http server
no ip http secure-server
ip nat inside source list 1 interface
GigabitEthernet0/0 overload
!
snmp-server community public RO
```

snmp-server chassis-id
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps diameter
snmp-server enable traps auth-framework sec-violation auth-fail
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bfd
snmp-server enable traps bgp cbgp2
snmp-server enable traps bstun
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dlsw
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps entity-ext
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmobile
snmp-server enable traps ipmulticast
snmp-server enable traps isis

snmp-server enable traps mempool
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps stun
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps pw vc
snmp-server enable traps waas
snmp-server enable traps event-manager
snmp-server enable traps lisp
snmp-server enable traps firewall serverstatus
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pki
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps gdoi ks-role-change
snmp-server enable traps gdoi ks-gm-deleted
snmp-server enable traps gdoi ks-peer-reachable
snmp-server enable traps gdoi ks-peer-unreachable
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps ethernet cfm alarm

```
snmp-server enable traps rf
snmp-server enable traps bulkstat collection
transfer
snmp-server enable traps mpls vpn
snmp-server enable traps vrfmib vrf-up vrf-
down vnet-trunk-up vnet-trunk-down
snmp-server host 10.10.10.254 version 2c
public
snmp mib nhrp
!
access-list 1 permit 10.10.10.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
 transport input none
!
no scheduler allocate
!
end

Switch#show run
Building configuration...
Current configuration : 8980 bytes
!
! Last configuration change at 10:59:03 UTC
Sun Jun 7 2020 by cisco
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$.D5e$POKL/SkhSV6P4kDhPaZUb/
!
username cisco privilege 15 password 7
060506324F41
aaa new-model
!
!
aaa group server tacacs+ default
 server name TACACS-ISE
 ip tacacs source-interface Vlan1
!
aaa group server radius radius-group
 server name radius-ise
 ip radius source-interface Vlan1
!
aaa authentication login default local group
tacacs+
aaa authentication enable default group
tacacs+ enable
aaa authentication dot1x default group radius-
group
aaa authorization config-commands
aaa authorization exec default group tacacs+
local if-authenticated
aaa authorization commands 0 default group
tacacs+ local if-authenticated
```

```
aaa authorization commands 1 default group
tacacs+ local if-authenticated
aaa authorization commands 7 default group
tacacs+ local if-authenticated
aaa authorization commands 15 default group
tacacs+ local if-authenticated
aaa authorization network default group
radius-group
aaa accounting update newinfo periodic 5
aaa accounting dot1x default start-stop group
radius-group
aaa accounting exec default start-stop group
tacacs+
aaa accounting commands 0 default start-stop
group tacacs+
aaa accounting commands 1 default start-stop
group tacacs+
aaa accounting commands 7 default start-stop
group tacacs+
aaa accounting commands 15 default start-
stop group tacacs+
aaa accounting system default start-stop group
radius-group
!
aaa server radius dynamic-author
 client 10.10.10.254 server-key 7
107C283D2C2221380907382E30796166764
651
!
aaa session-id common
!
no ip domain-lookup
ip domain-name ca-center.local
ip cef
no ipv6 cef
!
!
dot1x system-auth-control
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
lldp run
!
interface GigabitEthernet0/0
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/1
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/2
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 switchport mode access
 media-type rj45
 negotiation auto
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
```

```
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0
 switchport mode access
 media-type rj45
 negotiation auto
 authentication event fail action next-method
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/1
 media-type rj45
 negotiation auto
!
interface Vlan1
 ip address 10.10.10.150 255.255.255.0
 ip helper-address 10.10.10.254
 no ip redirects
 no ip proxy-arp
!
ip forward-protocol nd
!
ip http server
ip http secure-server
!
ip ssh version 2
!
snmp-server community public RO
snmp-server enable traps snmp authentication
linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific
state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific
state-change shamlink interface
snmp-server enable traps ospf cisco-specific
state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific
errors
snmp-server enable traps ospf cisco-specific
retransmit
snmp-server enable traps ospf cisco-specific
lsa
snmp-server enable traps ethernet cfm cc
mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm
crosscheck mep-missing mep-unknown
service-up
snmp-server enable traps auth-framework sec-
violation
snmp-server enable traps energywise
snmp-server enable traps pw vc
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire
status
snmp-server enable traps ether-oam
```

```
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps ethernet evc status
create delete
snmp-server enable traps bridge newroot
topologychange
snmp-server enable traps stpx inconsistency
root-inconsistency loop-inconsistency
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap
delete
snmp-server enable traps ipsec cryptomap
attach
snmp-server enable traps ipsec cryptomap
detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps bfd
snmp-server enable traps bgp cbgp2
snmp-server enable traps cef resource-failure
peer-state-change peer-fib-state-change
inconsistency
snmp-server enable traps dlsw
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps msdp
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-
change rp-mapping-change invalid-pim-
message
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps slb real virtual csrp
snmp-server enable traps syslog
snmp-server enable traps event-manager
snmp-server enable traps pki
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps mpls vpn
snmp-server enable traps vrfmib vrf-up vrf-
down vnet-trunk-up vnet-trunk-down
snmp-server host 10.10.10.254 version 2c
public
tacacs server TACACS-ISE
 address ipv4 10.10.10.254
 key 7
08156D6D283A362417081E013E7D717C60
6773
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request
include
radius-server attribute 31 mac format ietf
upper-case
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 30 tries 3
```

```
!
radius server radius-ise
 address ipv4 10.10.10.254 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 3
 key 7 107C283D2C2221380907382E30796166764651
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 60 0
 transport input ssh
line vty 5 15
 exec-timeout 60 0
 transport input ssh
!
!
end
```