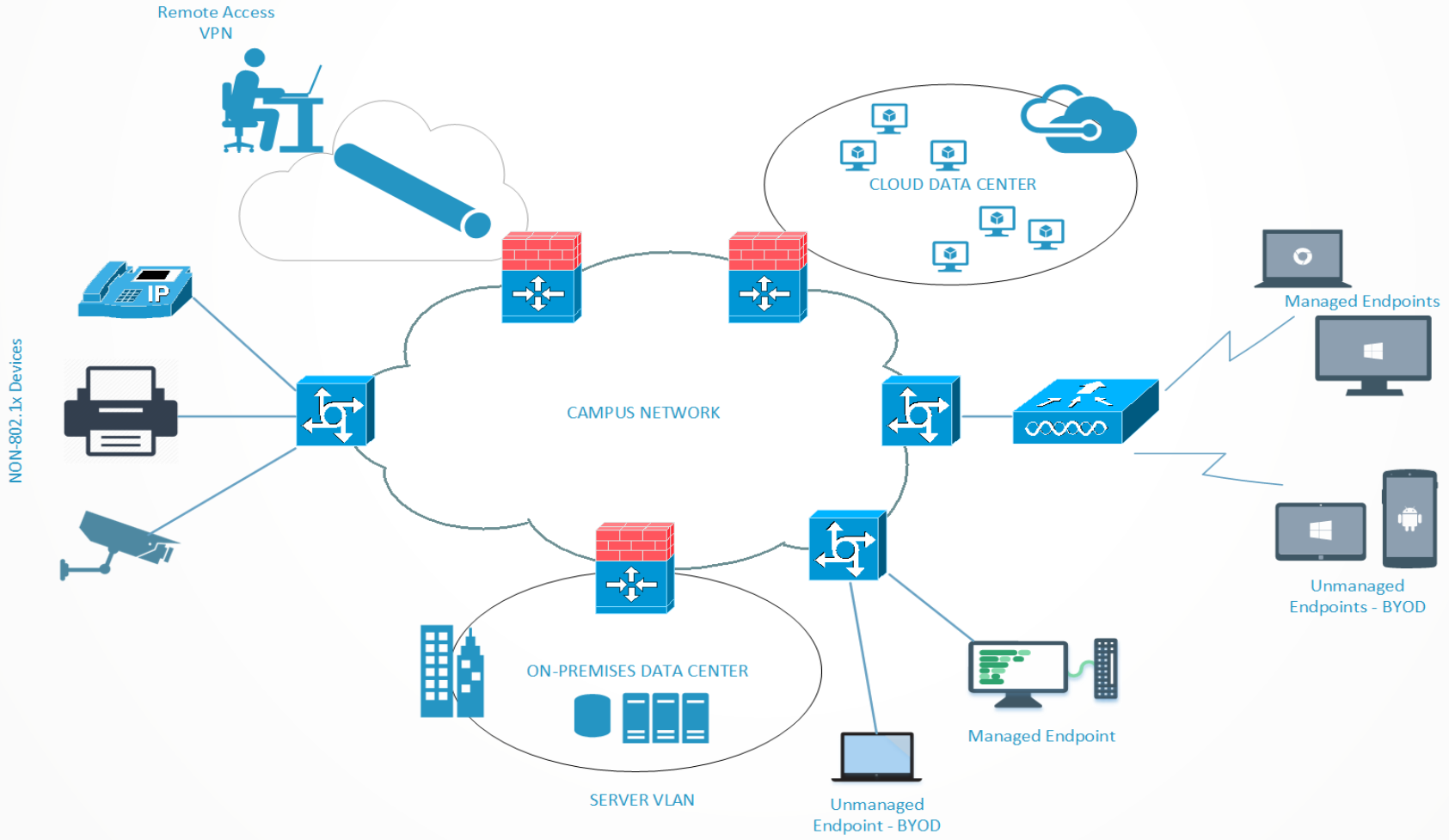
Система контролю доступу до корпоративної мережі на базі Cisco ISE

Жучко Дмитро
Comparex Ukraine

Сучасна мережева архітектура



Основні задачі, що вирішує Cisco ISE

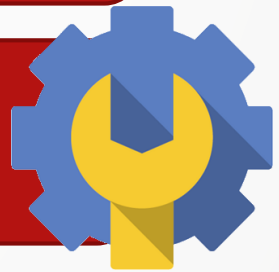
Cisco Identity Services Engine

Керування гостьовим доступом. Організаці безпечного доступу гостей до Інтернету та мережевих ресурсів.

BYOD. Визначення політики доступу BYOD пристроїв до корпоративної мережі.

Контроль доступу до мережі в цілому Визначення політик доступу через дротові, бездротові та VPN мережі.

Адміністрування мережевих пристроїв. Керування та організація доступу до мережевих пристроїв використовуючи єдину платформу

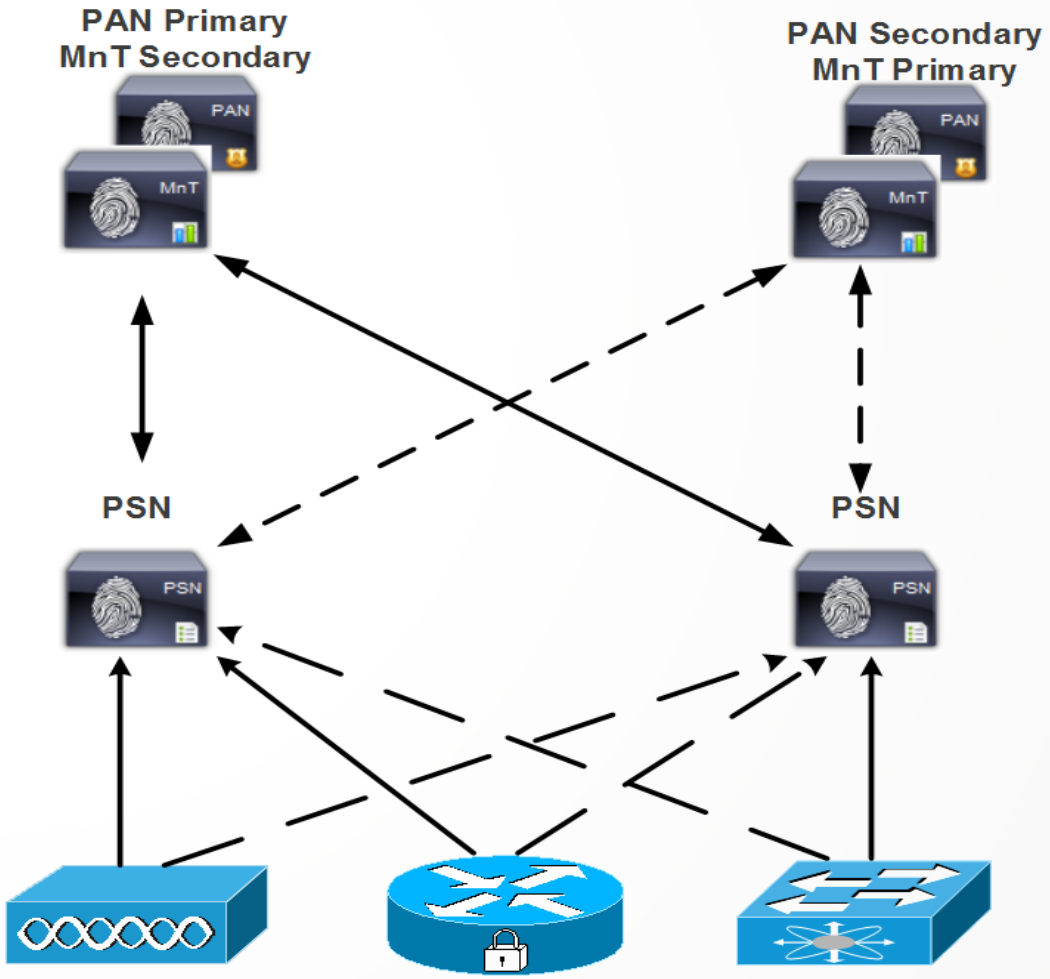


Потреба

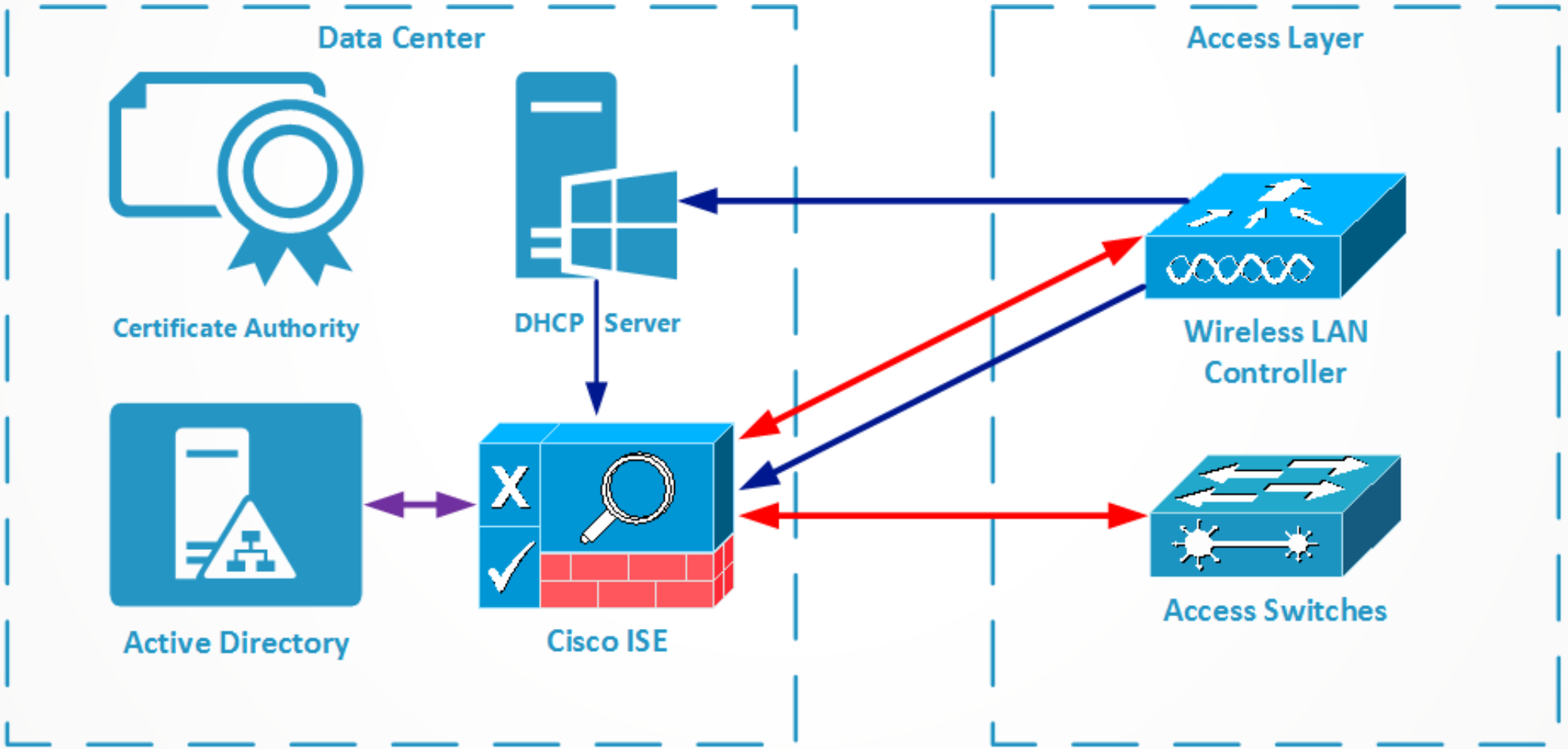
Надання повної інформації щодо пристроїв в мережі	Забезпечення повномасштабного моніторингу пристроїв, що отримують доступ до мережі та їх класифікація досягається вже на першому етапі впровадження – Monitor Mode
Контроль доступу до мережі	• Забезпечення дотримання політики підключення до дротових та бездротових мереж в масштабах усієї Компанії • Запобігання несанкціонованого доступу до мережі
Контроль відповідності та ізоляція пристроїв, що не відповідають корпоративним політикам	• Автоматичне ізолювання пристроїв, що не відповідають політикам; • Виконання операцій, направлених на приведення до відповідності комп'ютерів без залучення адміністратора
Контроль гостьового доступу	• Організація контрольованого доступу гостей до мережі Інтернет (Hotspot Portal) • Організація безпечного доступу партнерів до інформаційних ресурсів Компанії (Sponsored Portal)
Централізоване керування	Налаштування та контроль за дотриманням усіх вимог політики доступу до корпоративної мережі з єдиного інтерфейсу

Модель впровадження

Термін	Значення
Service	Функція, яку виконує **Persona** (доступ до мережі, профілювання, моніторинг та траблшутінг).
Node	Фізичний або віртуальний пристрій Cisco ISE.
Persona	Визначає функції, що надаються **Node**. Кожна **Node** може мати наступні **Persona:** Administration, Policy Service, Monitoring.
Role	Визначає роль standalone, primary або secondary для Administration та Monitoring **Node.**



Взаємодія з наявною інфраструктурою



Профілювання пристроїв

Cisco ISE Profiler дозволяє:

- **Динамічно класифікувати кожен пристрій, що отримує доступ до мережі**
- **Надає інформацію «Що саме» підключено незалежно від користувача для побудови політик Авторизації на основі типу пристрою.**

Cisco ISE Profiler використовує для збору Інформації щодо кінцевих пристроїв:

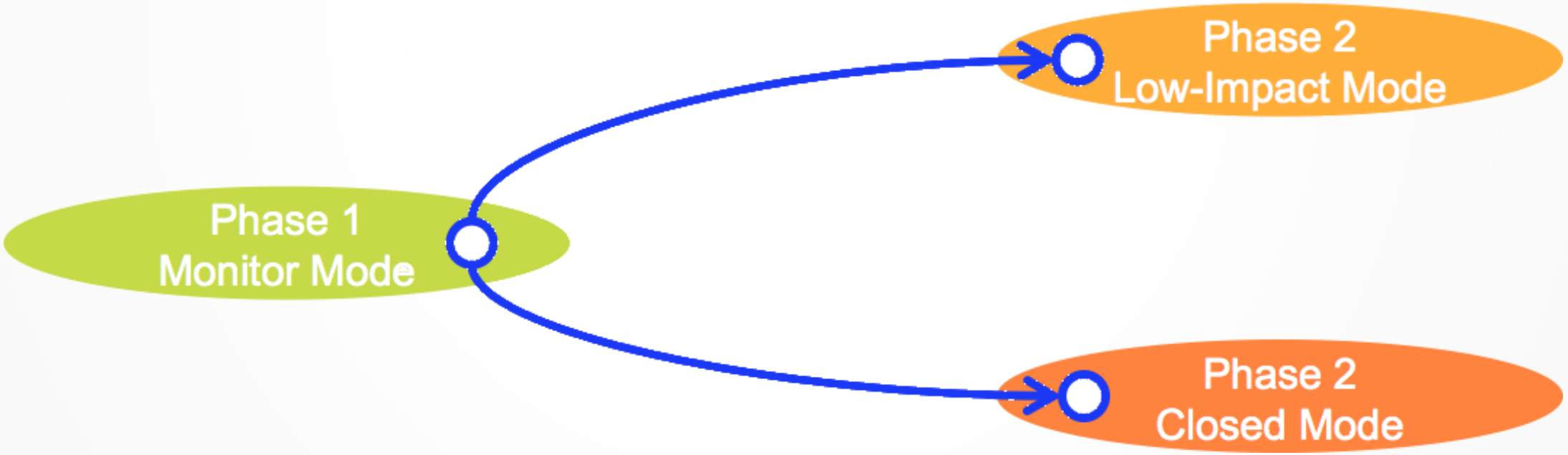
Supported ISE Probes

DHCP	HTTP	SNMP Query
RADIUS	SNMP Trap	DHCP SPAN
DNS	NMAP	NetFlow

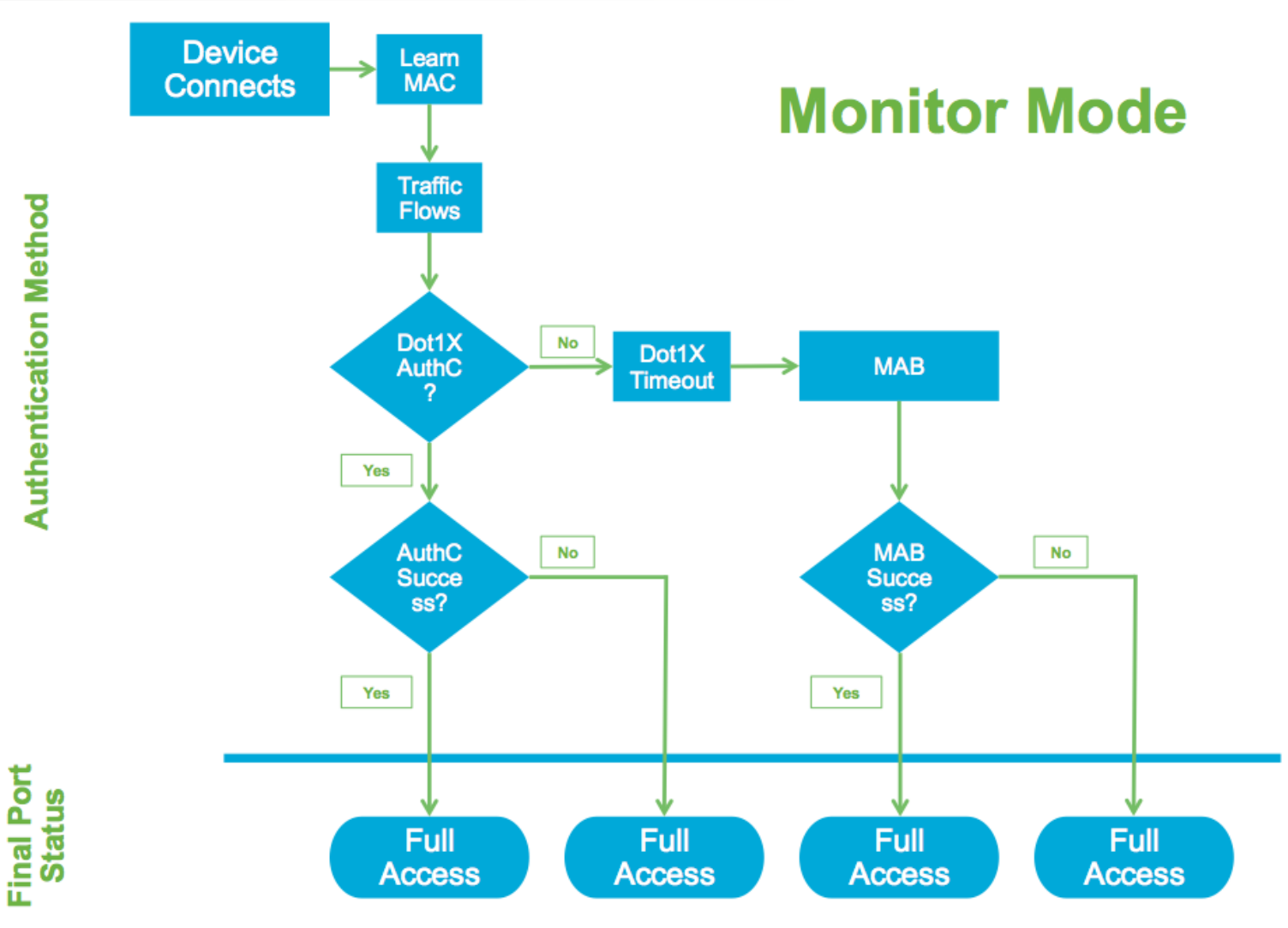
Поетапне впровадження системи

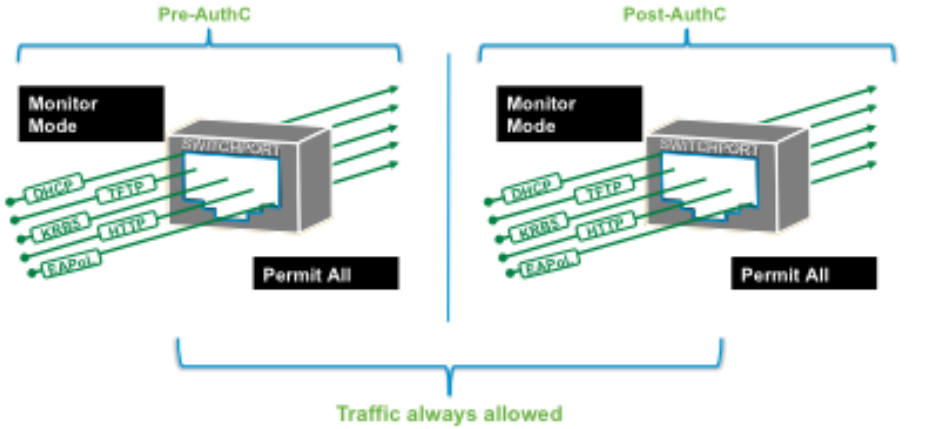
З метою мінімізації впливу на користувачів та інфраструктуру впровадження системи контролю доступу до корпоративної мережі розподіляється на 2 основні етапи.

- **Етап 1. Monitor Mode – необхідний етап, що дозволяє адміністратору системи вирішити всі проблеми, наглядно показуючи успішні та невдалі спроби автентифікації.**



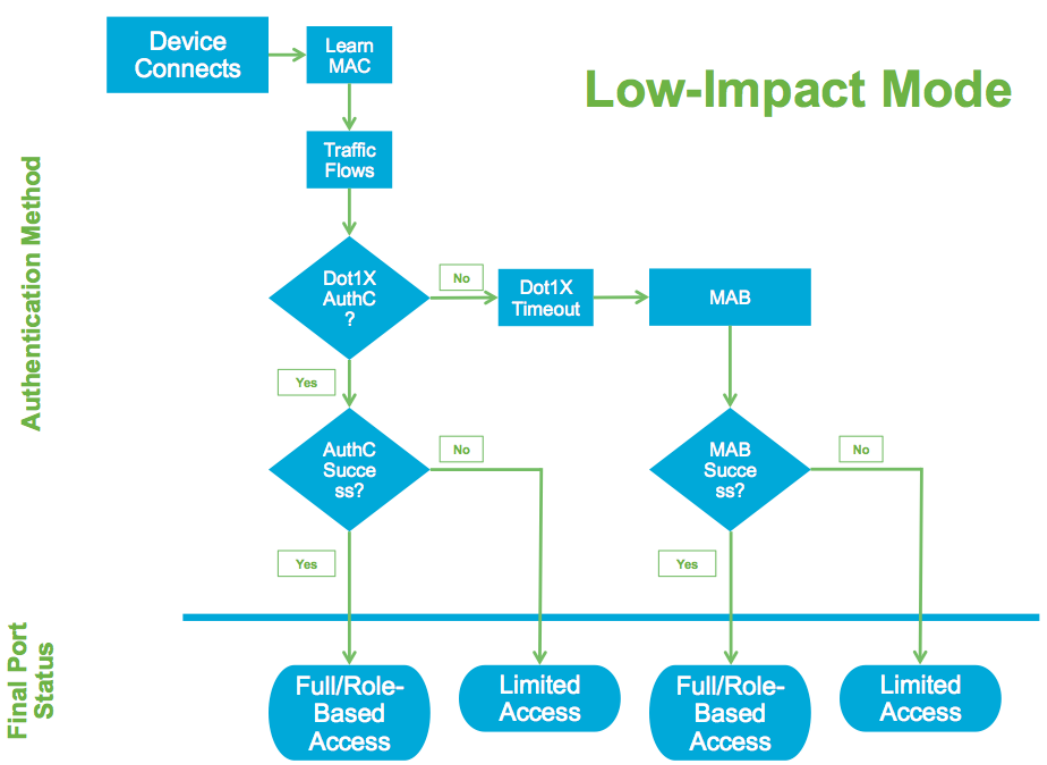
Monitor Mode



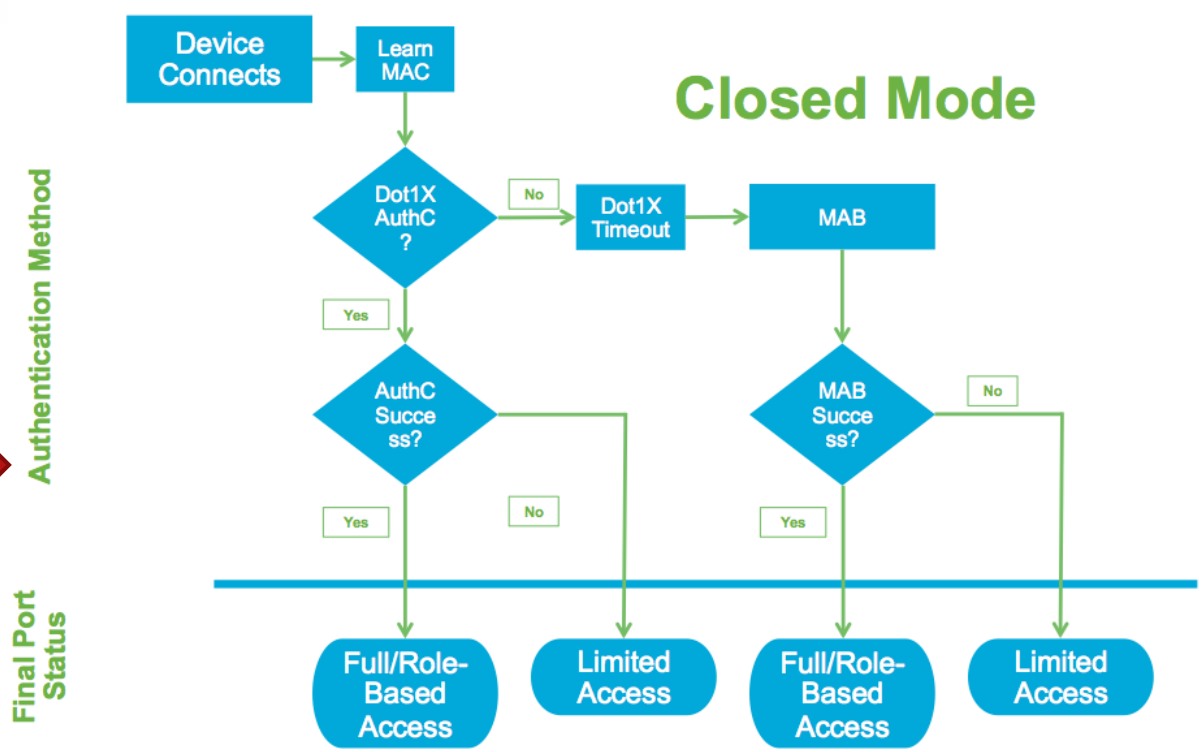


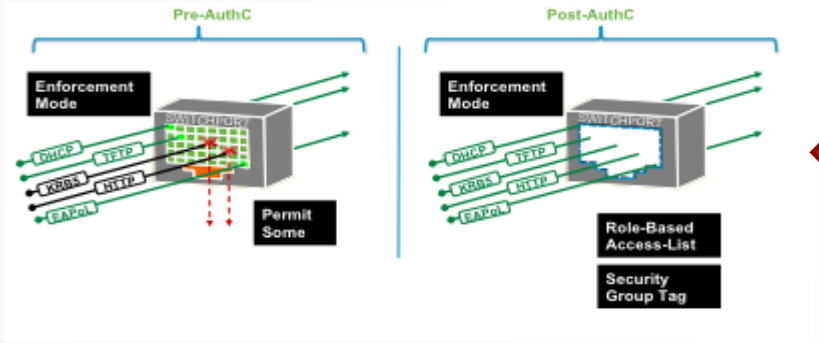
radius server **ise-3**
address ipv4 **10.4.48.43** auth-port 1812 acct-port 1813
key **[radius key]**
radius server **ise-4**
address ipv4 **10.4.48.44** auth-port 1812 acct-port 1813
key **[radius key]**
aaa group server radius **ISE_GROUP**
server name **ise-3**
server name **ise-4**
aaa authentication dot1x default group **ISE_GROUP**
aaa authorization network default group **ISE_GROUP**
aaa authorization configuration default group **ISE_GROUP**
aaa accounting dot1x default start-stop group **ISE_GROUP**
radius-server vsa send accounting
radius-server vsa send authentication

Low-Impact or Closed Mode

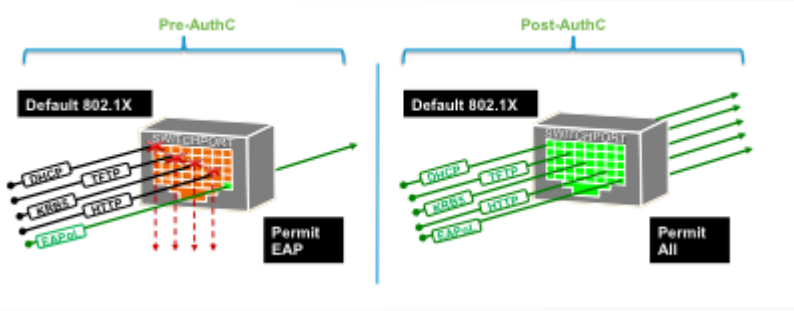


OR

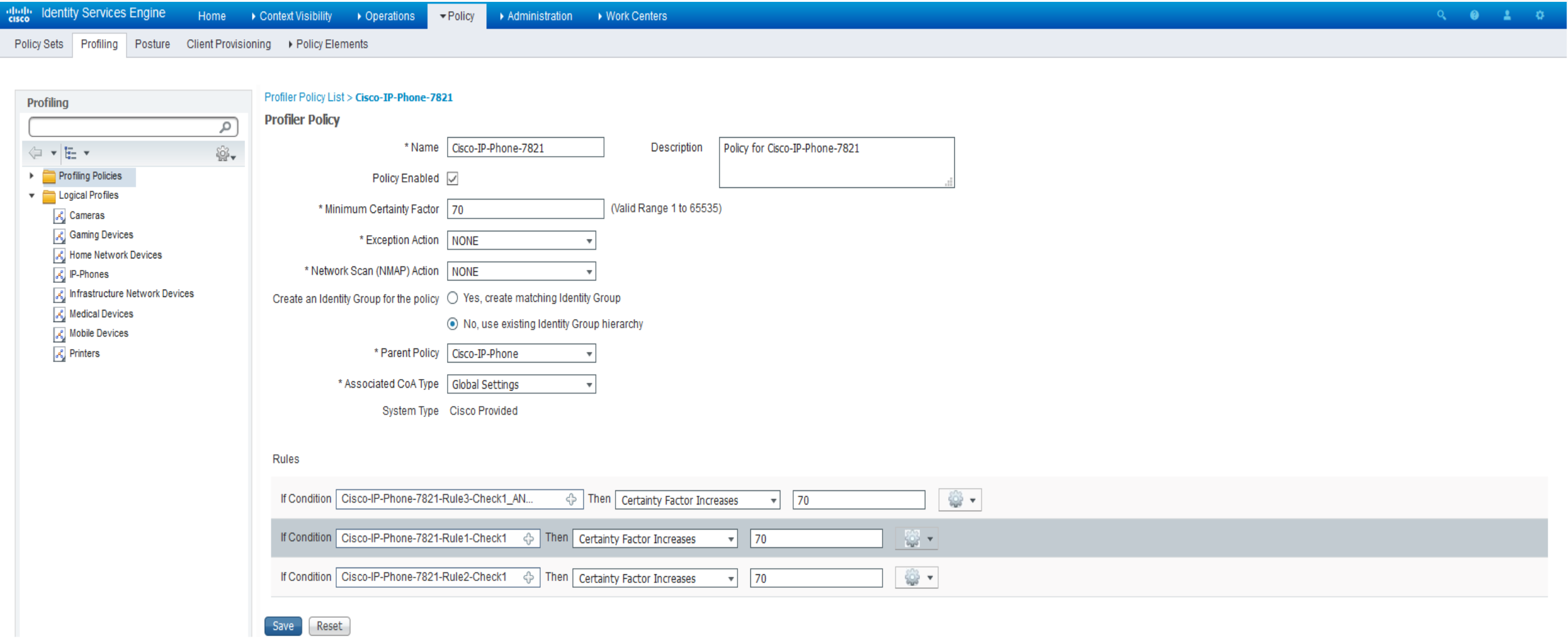




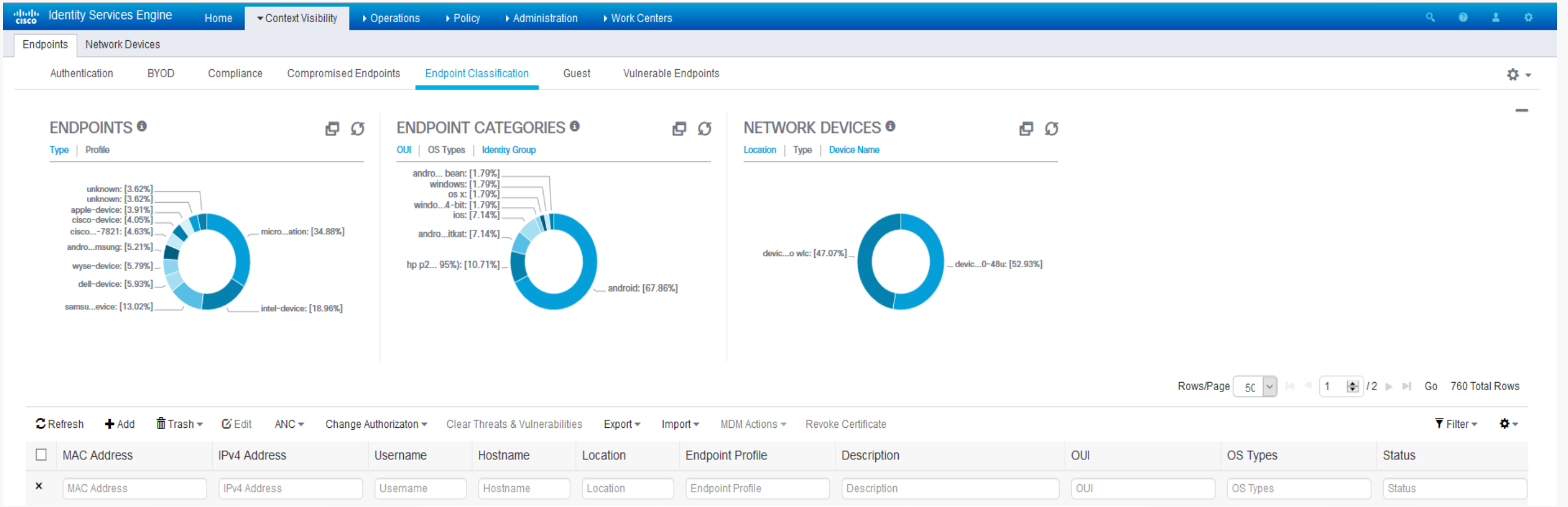
Switchport



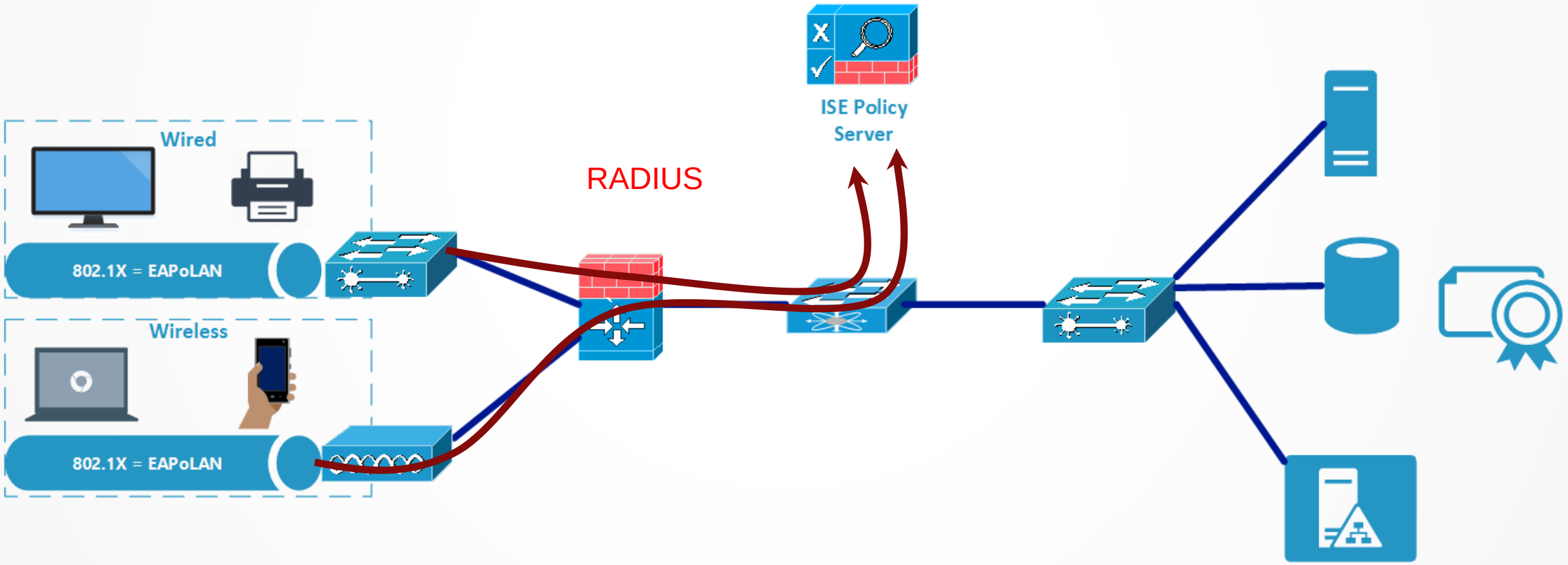
Profiler Policy



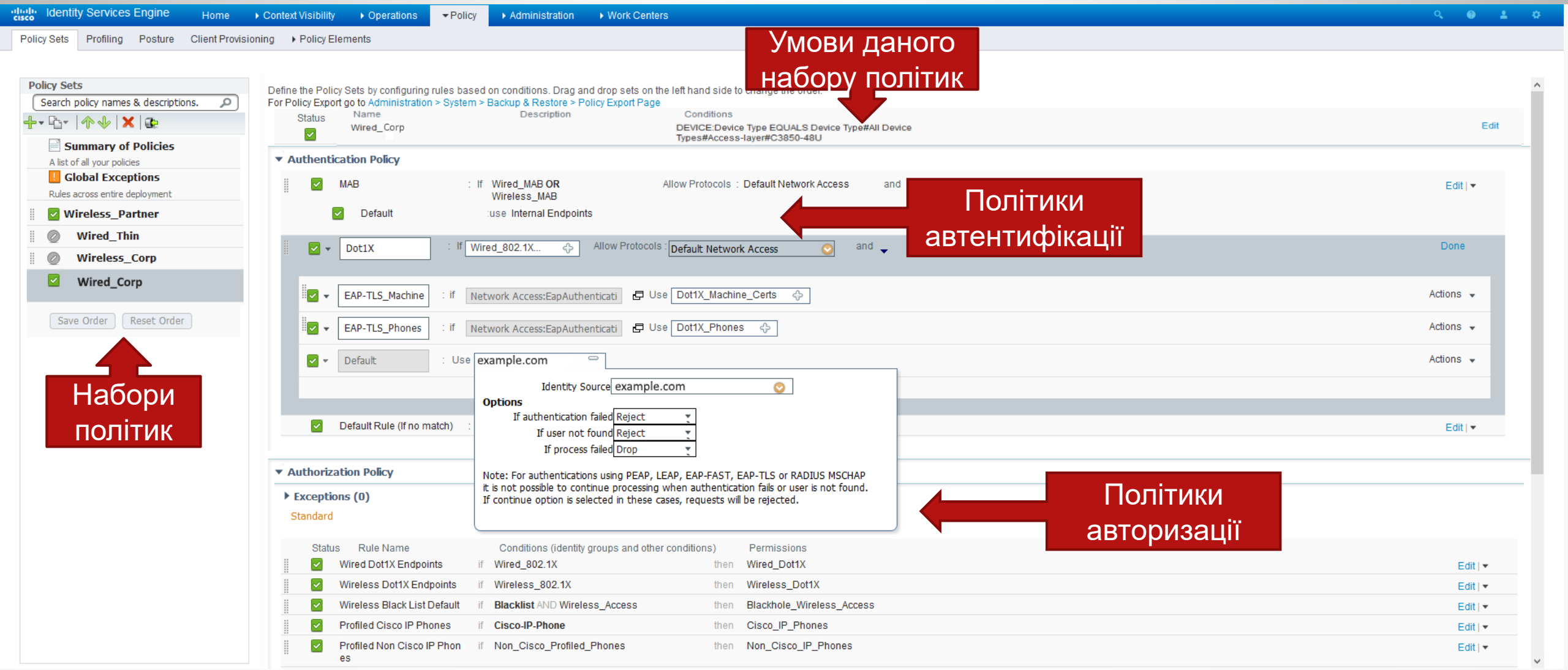
Context Visibility



Підтримка Cisco та сторонніх рішень використовуючи стандартні протоколи: RADIUS, 802.1X, EAP



Політики авторизації та автентифікації



Контроль відповідності

	ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Умови відповідності	Operating System/Service Packs/Hotfixes Service Check Registry Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation Patch Management Check Windows Update Running Windows Update Configuration WSUS Compliance Settings	Operating System/Service Packs/Hotfixes Service Check Registry Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation Windows Update Running Windows Update Configuration WSUS Compliance Settings	Service Check File Check Application Check Antivirus Installation Antivirus Version/ Antivirus Definition Date Antispyware Installation
Дії, направлені на приведення до відповідності	Message Text (Local Check) URL Link (Link Distribution) File Distribution Launch Program Antivirus Definition Update Antispyware Definition Update Patch Management Remediation Windows Update WSUS	Message Text (Local Check) URL Link (Link Distribution) File Distribution	Message Text (Local Check) URL Link (Link Distribution) Antivirus Live Update Antispyware Live Update

Бездротовий доступ до мережі

Автентифікація ноутбуків працівників використовуючи цифрові сертифікати Microsoft CA

SSID: CORP

Миттєвий доступ без паролю через Hotspot Portal

SSID: Guest

Контрольований доступ партнерів за допомогою Self-registration та Sponsor Portals

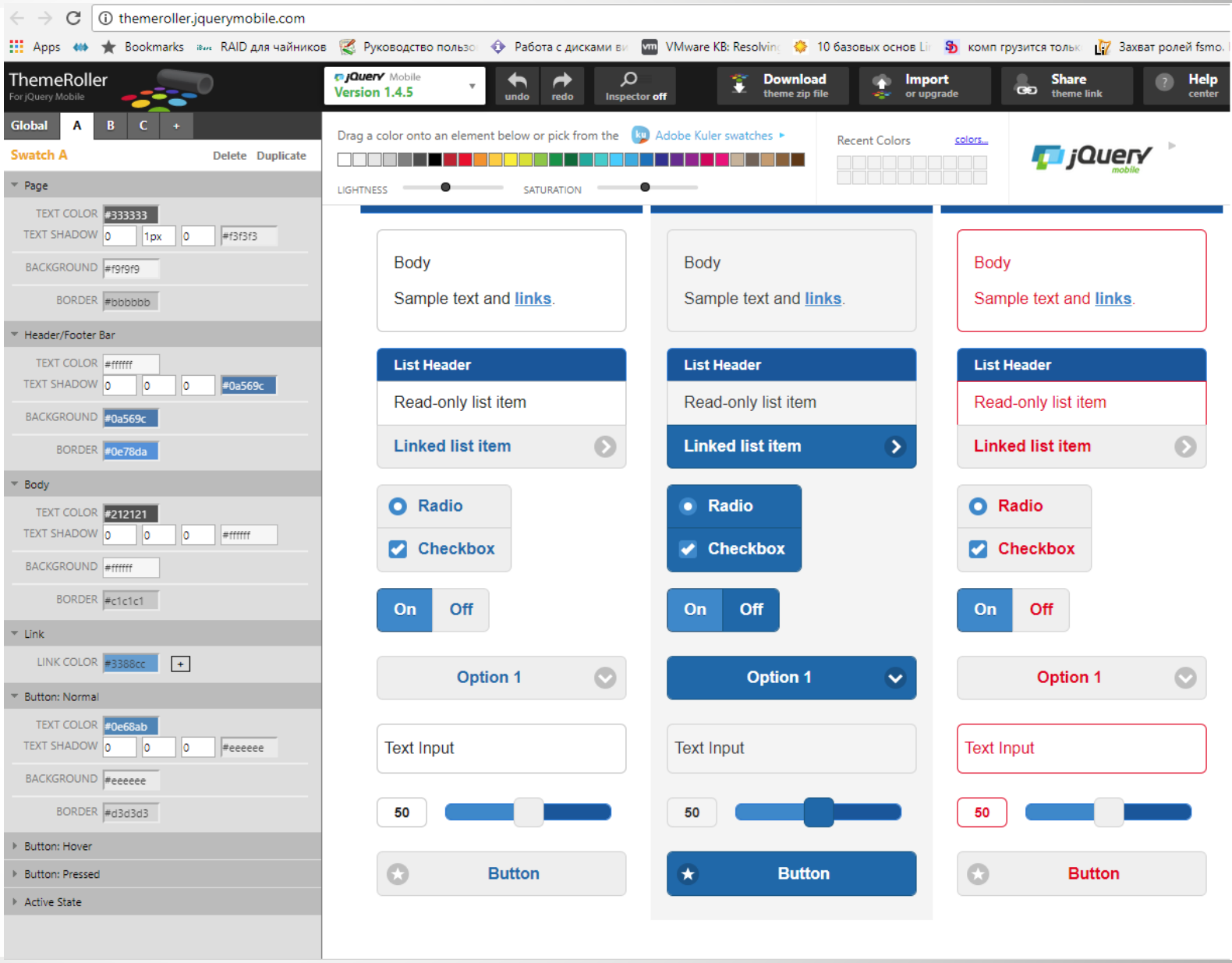
SSID: SPONSORED

Налаштування зовнішнього вигляду користувацьких порталів

Swatch A – вигляд за замовчуванням

Swatch B – вигляд елементів при наведенні на них (наприклад, кнопка Accept)

Swatch C – визначає елементи, такі як сповіщення, повідомлення про помилки, недійсні поля введення тощо



Результати впровадження

Надано інформацію в реальному часі щодо того «хто», «що», «коли», «звідки» та «яким чином» отримав доступ до мережі

Реалізовано гнучкий механізм контролю доступу до мережі та механізм захисту від неконтрольованого доступу

Забезпечено контроль відповідності пристроїв до мережі заданим критеріям, автоматизовано ізоляцію пристроїв, що не відповідають їм та процес приведення до відповідності

Забезпечено ефективну сегментацію мережі

Надання механізму керування життєвим циклом гостьового та партнерського WI-FI доступу

Дякую за увагу!

Visit us at: **www.comparex.com**