CISCO Live!

ALL IN

#CiscoLive

Unified Identity & Policy Across Private 5G and Wi-Fi

Bhavik Adhvaryu, Sr. Technical Product Lead
@bhavik175
BRKXAR-2004

Cisco Webex App

Questions?
Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXAR-2004

Agenda

- Introduction

- Cisco's Private 5G Overview

- Identity Services Engine (ISE) Overview

- Why Unified Identity & Policy matter?

- Cisco Strategy & Solution
  - Enhanced Enterprise Experience
  - Detailed Call flows
  - Integration snapshot

- Summary

Today's Speaker

Bhavik Adhvaryu

Sr. Technical Product Lead

LinkedIn @bhavik175

CISCO Live!

Cisco's Private 5G Solution

Cisco Private 5G
Full stack subscription for success

Management
Cloud managed

Identity & Policy
Intuitively integrated into existing enterprise systems

Mobility Core
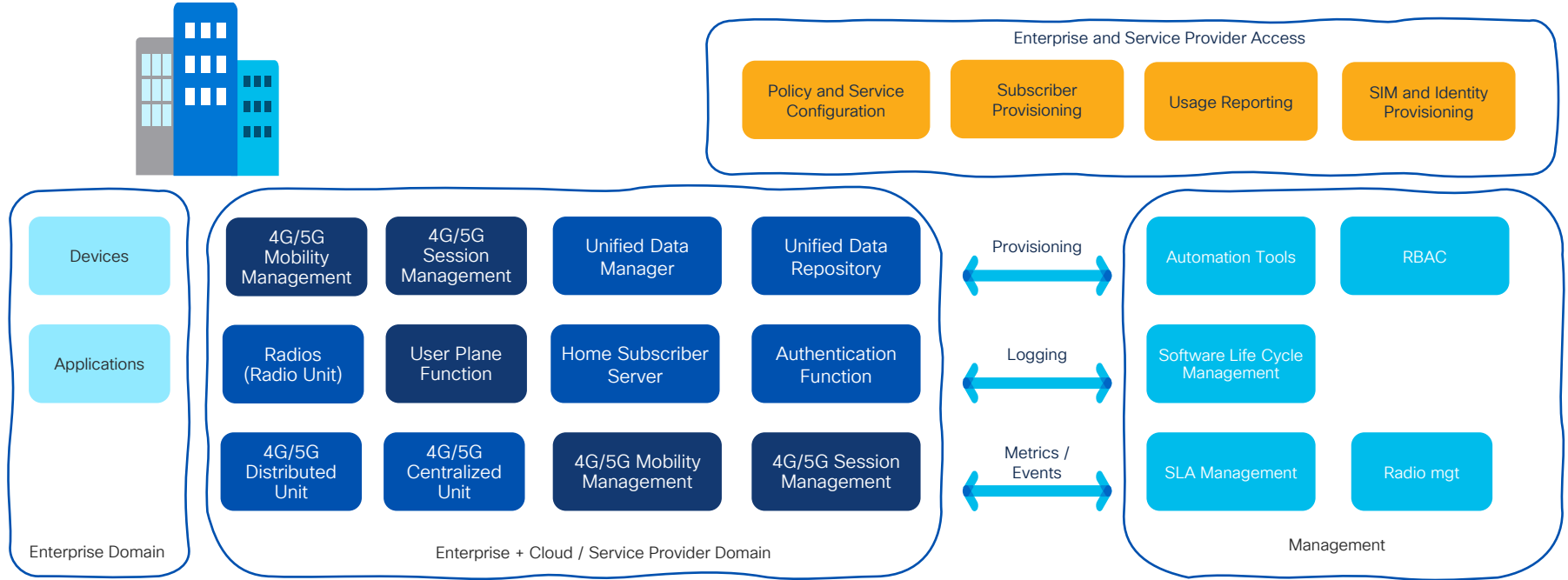Industry leading 4G/5G converged mobility core

Radios
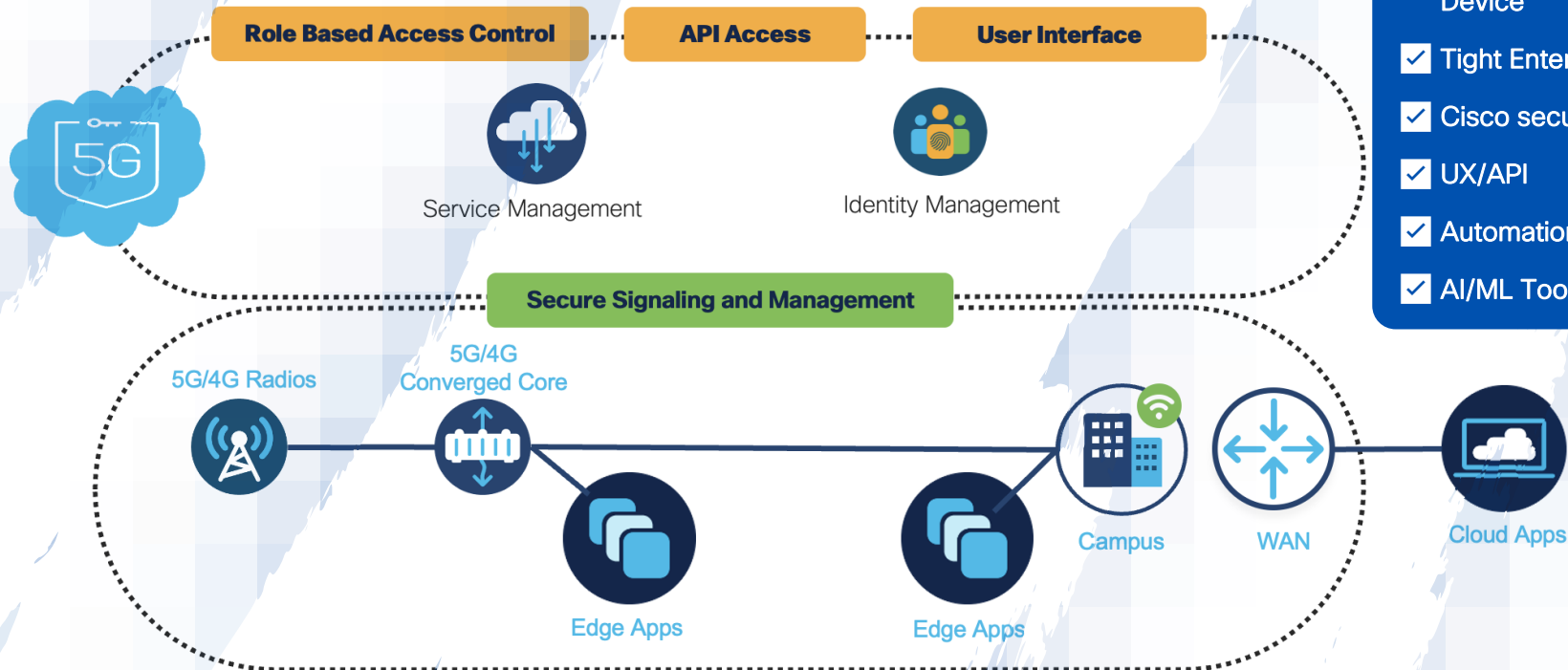Certified and validated Open RAN radio partners

Simple

Secured

Trusted

Typical 5G Network Architecture

Enterprise and Service Provider Access

| Policy and Service Configuration | Subscriber Provisioning | Usage Reporting | SIM and Identity Provisioning |

Enterprise Domain

- Devices
- Applications

Enterprise + Cloud / Service Provider Domain

4G/5G Mobility Management	4G/5G Session Management	Unified Data Manager	Unified Data Repository
Radios (Radio Unit)	User Plane Function	Home Subscriber Server	Authentication Function
4G/5G Distributed Unit	4G/5G Centralized Unit	4G/5G Mobility Management	4G/5G Session Management

Provisioning

Logging

Metrics / Events

Management

Automation Tools	RBAC
Software Life Cycle Management	
SLA Management	Radio mgt

Not all functions shown

Cisco Private 5G in the Enterprise

Role Based Access Control

API Access

User Interface

Service Management

Identity Management

Secure Signaling and Management

5G/4G Radios

5G/4G Converged Core

Edge Apps

Edge Apps

Campus

WAN

Cloud Apps

Cisco's Private 5G

- ☑ Converged Core Architecture
- ☑ Full LCM – RAN, Core, Device
- ☑ Tight Enterprise integration
- ☑ Cisco security portfolio
- ☑ UX/API
- ☑ Automation focused
- ☑ AI/ML Tools

The Cisco Differentiator for Private 5G

Integrated Enterprise Architecture

- 5G becomes access architecture like Wi-Fi in the Enterprise
- Consistent operations and management across the Enterprise
- Intent-based policies across both Wi-Fi, 5G, and other access technologies
- Synergies with Enterprise network components (Catalyst Series, ISE, ..)

Built on Proven Technology

- Proven carrier-class 4G/5G core for the Enterprise
- Scalable SIM/IoT Device Management leveraging best in class Cisco Control Center
- Self Service / Zero-touch provisioning
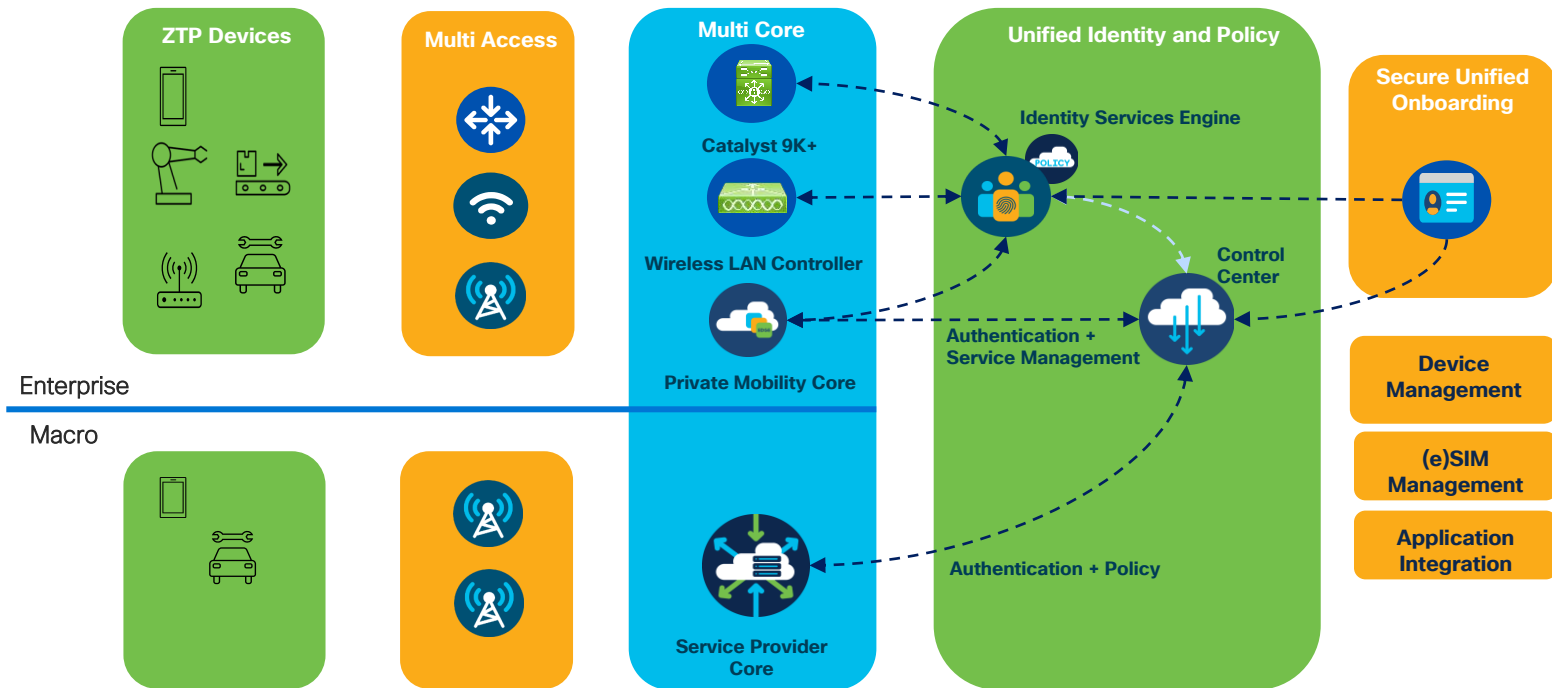- Enterprise-grade security

Managed Service Delivery

- Robust ecosystem of Certified Cisco Managed Service Partners
- MSP takes responsibility throughout solution lifecycle for operations
  - All solution components are pre-integrated and tested
  - No need to worry about infrastructure management, operations, configuration
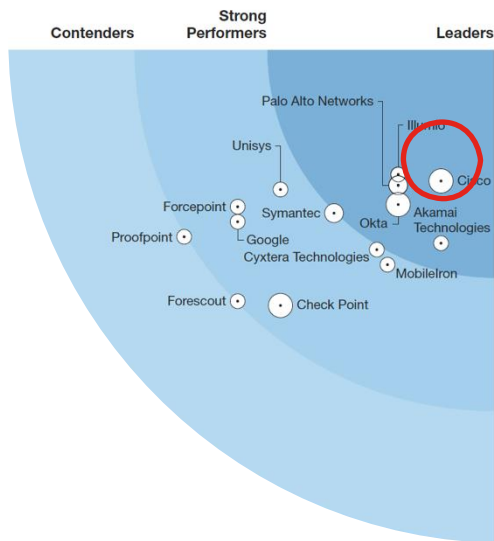
Tighter Integration into Enterprise Services

Offline Resource

ZTP Devices

Multi Access

Multi Core
- Catalyst 9K+
- Wireless LAN Controller
- Private Mobility Core
- Service Provider Core

Unified Identity and Policy
- Identity Services Engine
- Control Center
- Authentication + Service Management
- Authentication + Policy

Secure Unified Onboarding

Device Management

(e)SIM Management

Application Integration

Enterprise

Macro

ISE Overview

Cisco ISE Market Overview

#1 in Forrester Wave ZT ranking

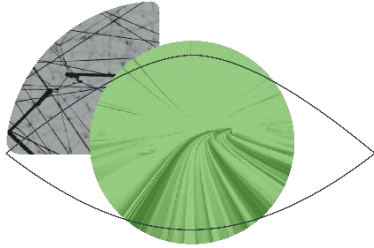**ISE continues to lead NAC market**

ISE Market Maturity

10yrs of market leadership

40,000
Deployments

41.9% Market Share
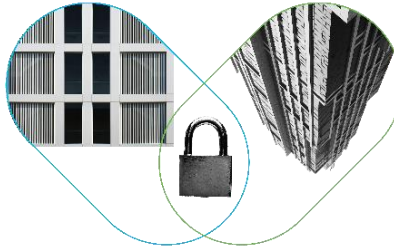–Gartner

The Pillars of Zero Trust

Visibility

Grant the right level of network access to users across domains

Segmentation

Shrink zones of trust and grant access based on least privilege

Containment

Automate containment of infected endpoints and revoke network access

ISE Enforced Zero Trust

Connecting trusted users and endpoints with trusted resources

Endpoint Request Access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically Updates access policy

Cisco ISE

Endpoint classified, and profiled into groups

- Endpoints are tagged x/SGTs
- Policy applied to profiled groups based on least privilege

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved
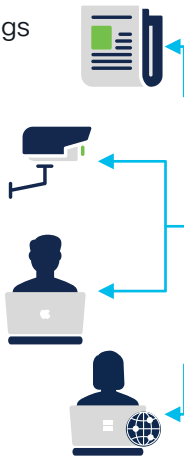
ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

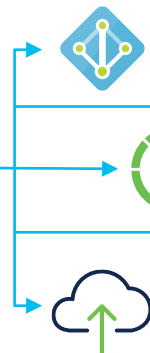- Switches
- WLCs / APs
- VPN

Cisco ISE

- Standalone ISE
- Multi-node ISE
- VM/Appliance/Cloud

Identity Services

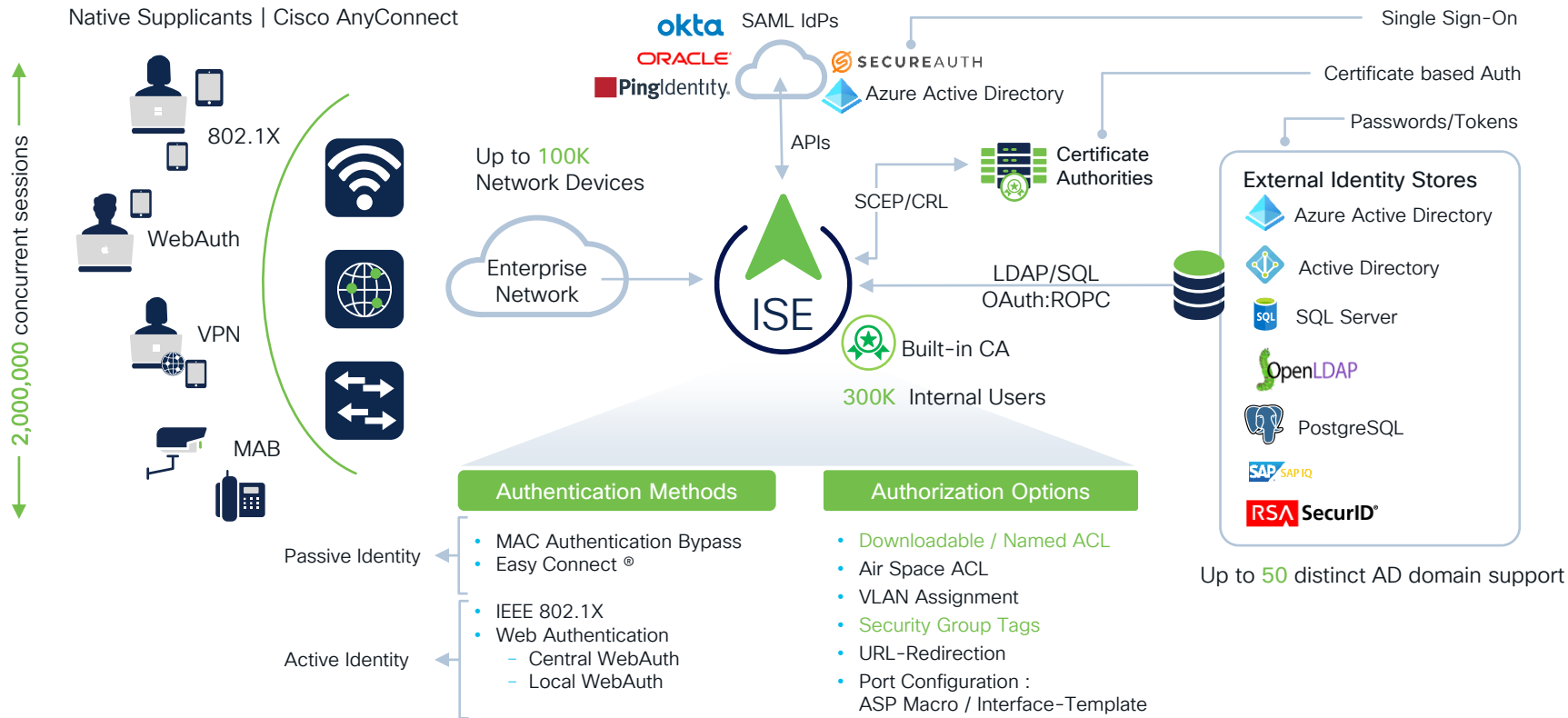- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
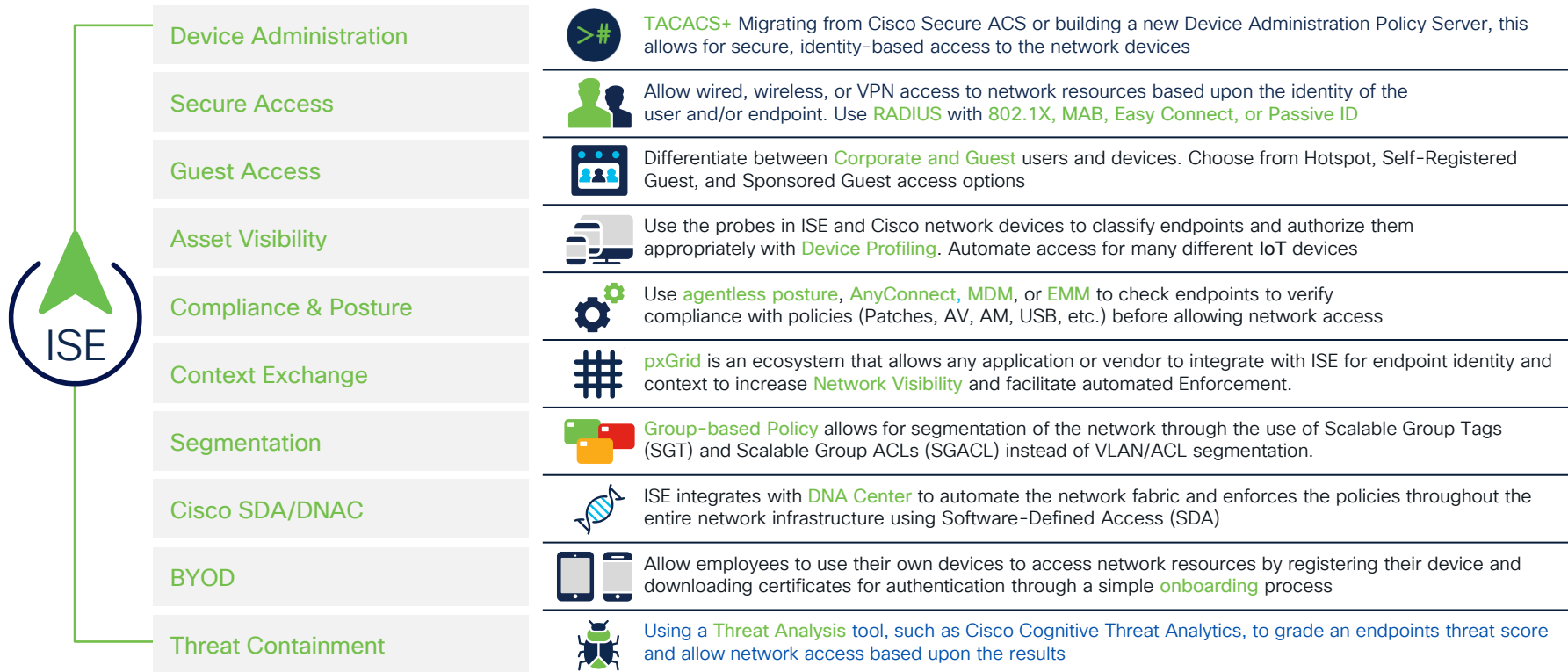- Secure Firewall
- Partners

ISE

Cisco DNA Center

ISE Secure Access Control Options

Native Supplicants | Cisco AnyConnect

2,000,000 concurrent sessions

- 802.1X
- WebAuth
- VPN
- MAB

SAML IdPs

okta
ORACLE
PingIdentity
SECUREAUTH
Azure Active Directory

APIs

Single Sign-On

Certificate based Auth

Passwords/Tokens

Up to 100K Network Devices

Enterprise Network

Certificate Authorities

SCEP/CRL

ISE

Built-in CA

300K Internal Users

LDAP/SQL
OAuth:ROPC

External Identity Stores

- Azure Active Directory
- Active Directory
- SQL Server
- OpenLDAP
- PostgreSQL
- SAP SAP IQ
- RSA SecurID®

Up to 50 distinct AD domain support

Authentication Methods	Authorization Options

Passive Identity
- MAC Authentication Bypass
- Easy Connect ®

Active Identity
- IEEE 802.1X
- Web Authentication
  – Central WebAuth
  – Local WebAuth

Authorization Options
- Downloadable / Named ACL
- Air Space ACL
- VLAN Assignment
- Security Group Tags
- URL-Redirection
- Port Configuration :
  ASP Macro / Interface-Template

Why Customers Buy ISE

ISE

Device Administration
TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices

Secure Access
Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use RADIUS with 802.1X, MAB, Easy Connect, or Passive ID

Guest Access
Differentiate between Corporate and Guest users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options

Asset Visibility
Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with Device Profiling. Automate access for many different IoT devices

Compliance & Posture
Use agentless posture, AnyConnect, MDM, or EMM to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access

Context Exchange
pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase Network Visibility and facilitate automated Enforcement.

Segmentation
Group-based Policy allows for segmentation of the network through the use of Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation.

Cisco SDA/DNAC
ISE integrates with DNA Center to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)

BYOD
Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple onboarding process

Threat Containment
Using a Threat Analysis tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results

Why Unified Policy & Identity is critical?

Enterprise Problem Statement

How can Enterprise IT/OT admin have common policies and identity across various enterprise domains such as Wi-Fi, Wired and Cellular (4G & 5G)?

Why Unified Policy & Identity is critical?

Intent
Unified Business goals across the enterprise domains driven by ISE

Use Cases

Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint.

Differentiate between Corporate and Guest users and devices

Classify the endpoints and authorize them appropriately with Device Profiling

Group-based Policy allows for segmentation of the network using access control lists (ACLs)

Identity based policy allows the unified policy to users and devices

VLAN tagging on data plane traffic matching with rest of the campus logic

Security Group Tagging (SGT)

QoS Profile

Uplink & Downlink Aggregate Maximum Bit Rate (AMBR)

PDU Type

New in P5G

Authorization Enforcement Options

VLANs
Dynamic VLAN Assignments

Employees
VLAN 3

Printers
VLAN 5

Guest
VLAN 4
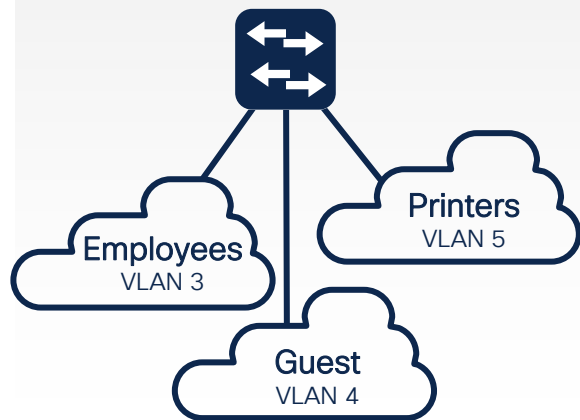
Per port / Per Domain / Per MAC

ACLs
Access Control Lists

Employee
`permit ip any any`

Contractor
`deny ip host <critical>`
`permit ip any any`
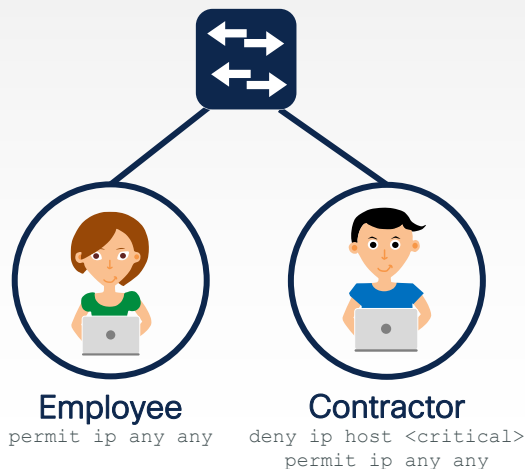
Scalable Group Tags*
Cisco Group-Based Policy

16-bit SGT assignment and
SGT based Access Control

* Future P5G Integration Phase

P5G & ISE Integration
Overview

1 Request SIM cards and assign Policy Group

P5G Portal

SIM Mgmt.

Internet

Admin

Cloud

Enterprise Prem

2 Insert Cisco delivered SIM in devices

3 Admin Assigns QoS Policy Profile to device

ISE

TLS

Enterprise Facility

Devices

RAN

P5G Edge

Application Services

QoS Policy Profiles

A B C
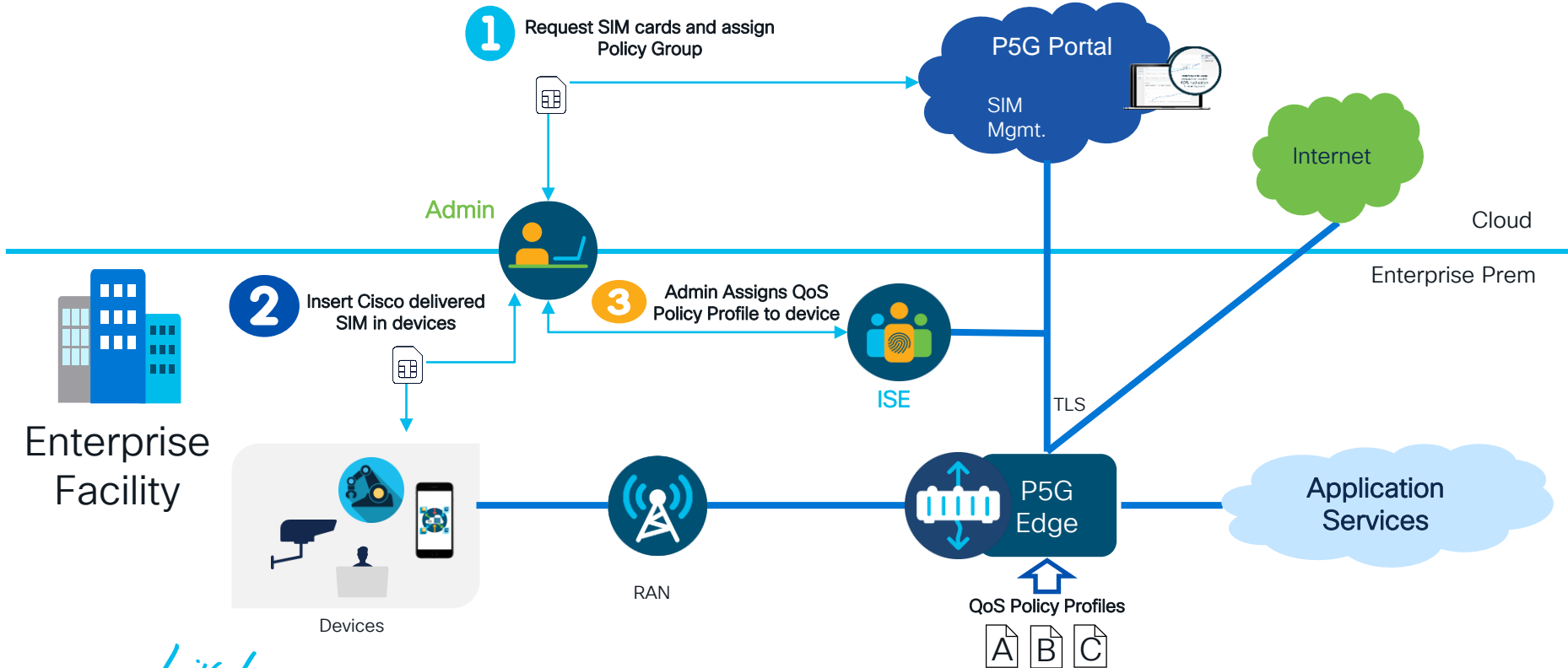
ISE Authorisation & Policy Integration Flow
(Authentication & Registration)

Offline Resource

P5G Portal

SIM Mgmt.

Internet

Internet

Cloud

Enterprise Prem

Admin

Authenticate & Secure

2

Registration Request/Accept

4

ISE

Enterprise Facility

1

Registration Request

Authenticate & Secure

2

ID Request/Response

3

Registration Complete

5

P5G Edge

QoS Policy Profiles

A B C

Application Services
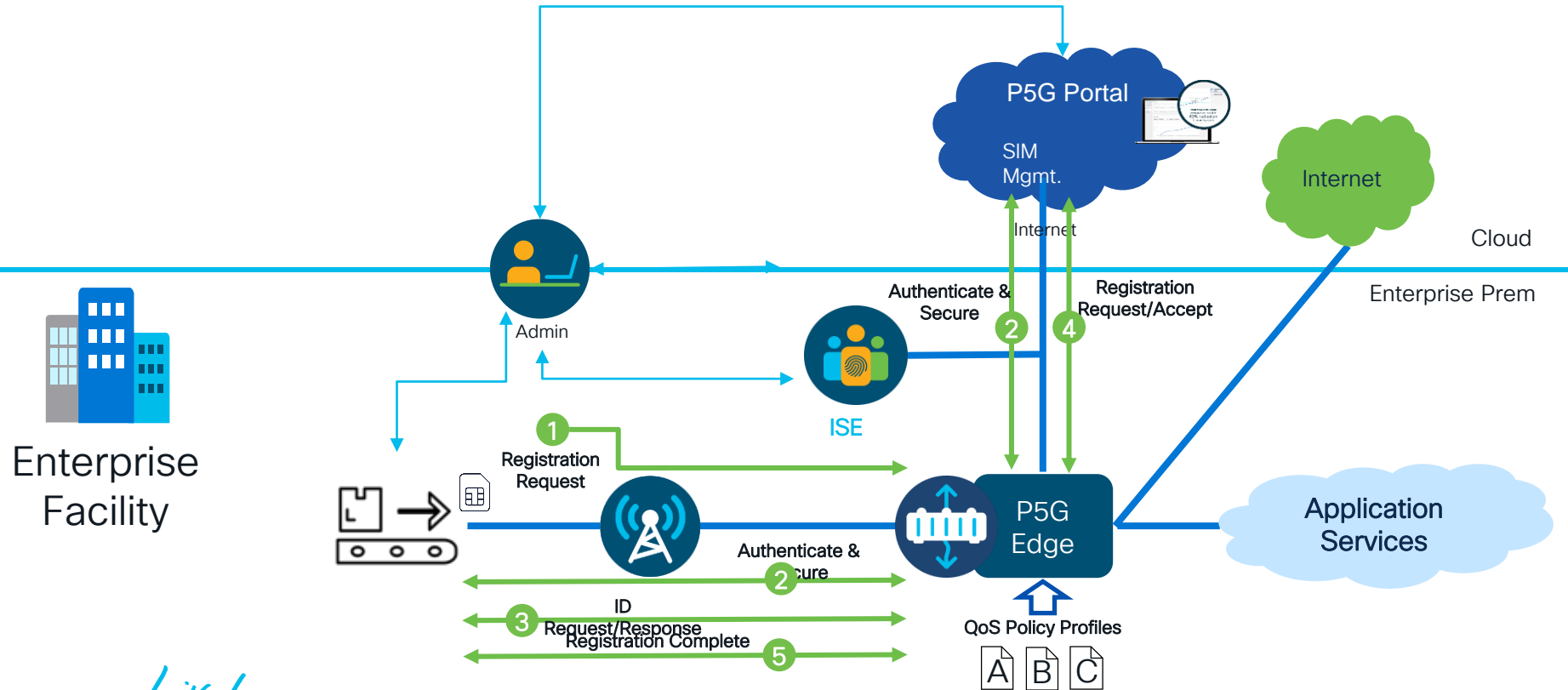
P5G & ISE Integration
Secondary Authorization Workflow

P5G Portal

SIM Mgmt.

2 RADIUS Access Request
IMSI

3 RADIUS Access Accept
Policy Profile Name

Internet

Cloud

Enterprise Prem

Admin

ISE

3 RADIUS Access Accept

2 RADIUS Access Request

4 AUTH Status

7 RADIUS Accounting Start

Enterprise Facility

1 PDU Session Establishment Request

P5G Edge

Application Services

6 PDU Establishment Response

Devices

QoS Policy Profiles

A B C **5** QoS Policy Profile "C" indicated in ISE response and used to establish PDU Session

P5G & ISE Detailed Integration Call Flows

5G Call Flow
Authentication Authorization Focused
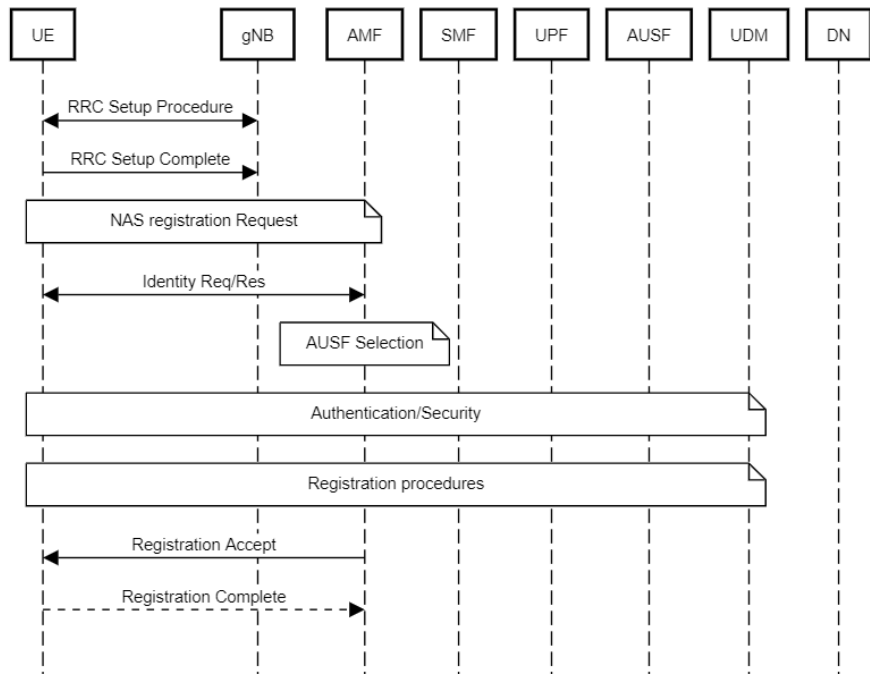
UE Registration
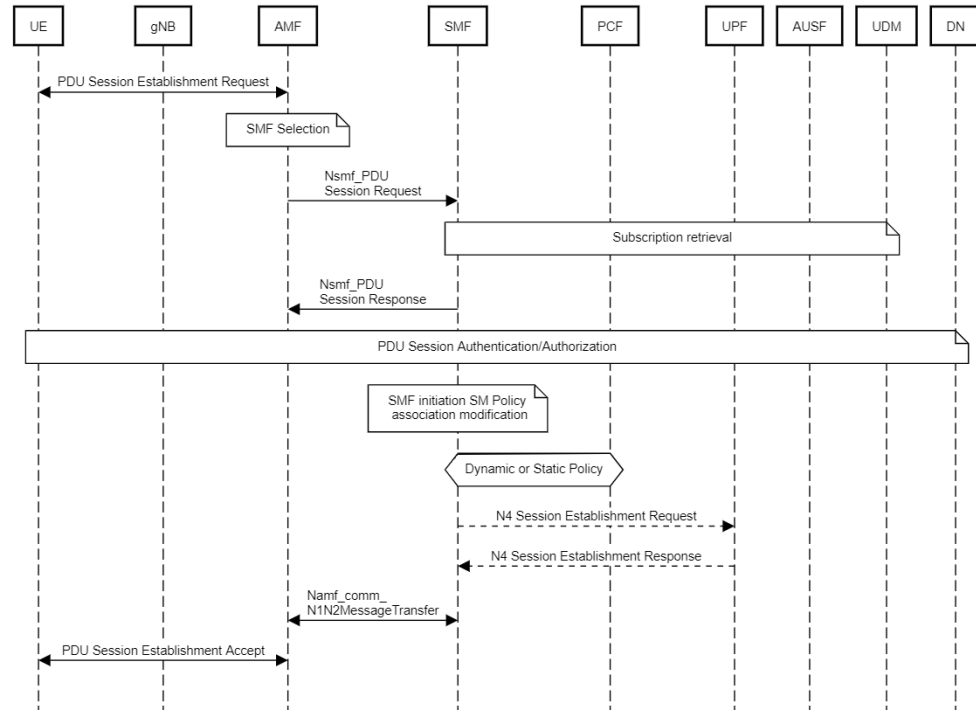
PDU Session Establishment

P5G & ISE Integration
Enhanced Call Flow
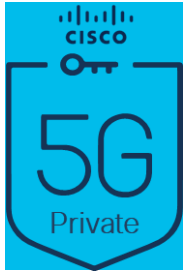
Secondary Authorization

Grant the right level of network access through unified policies across domains based on common business objectives
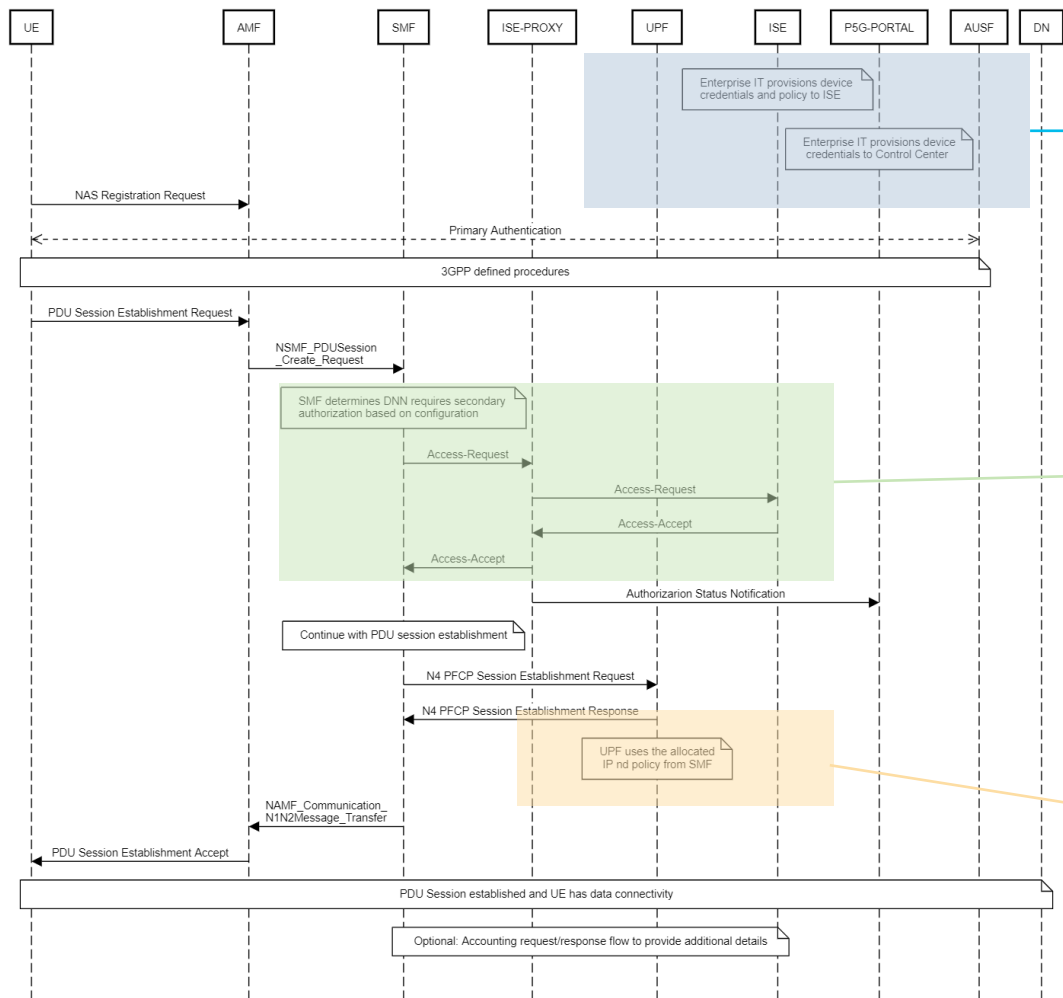
Pre-requisite
- Required device credentials and policies on ISE
- Required device credentials on P5G-Portal

- ISE-Proxy is the secret recipe to facilitate the ISE integration
- SMF sends radius access requests to ISE via ISE-Proxy
- Based on the policy configuration, ISE will take one of the following actions
  - Deny the request
  - Accept the request
  - Accept the request with specific policy details such as Auth Profile Index, PDU type, VLAN tagging, AMBR, etc.

- SMF gets the policy details from ISE and send it to UPF
- UE will have enhanced policies applied as defined in ISE

P5G & ISE Integration
Visualization

Admin

Service Admin
- Ise Instances
- Device Group
- Device Type
- Device Profile

All fields required unless marked otherwise.

Account Name	CC-ISE-BXB
Endpoint Name	BXB-ISE-01
Admin Host (Primary)	10.218.1.30
Admin Host (Secondary)	10.218.1.20
Authentication	Y
User Name	admin
Password	•••••••••
Radius Host (Primary)	10.218.1.30
Radius Host (Secondary)	10.218.1.20
Radius Authentication Port	1812

Device Group Name ▲

☐ 5GDevice_List_VLAN_895
☐ 5GDevice_List_VLAN_896
☐ 5Gdevices_Allow_list
☐ 5G_Devices_Default_VLAN_1
☐ 5Gdevices_Deny_list
☐ Employee_Default

Devices

ICCID	IMSI	Device Profile	Device ID
2001111403110002012	200111112502012	Apple-iDevice_Employee_Default	Employee-Apple-Device
2001111403110002011	200111112502011	Employee_Default	Employee 5
2001111403110002002	200111112502002	5G_Devices_Allow_profile	Michael Shay (Use-Case-1)
2001111403110002004	200111112502004	5G_Devices_Deny_profile	Faulty-Camera
2001111403110002008	200111112502008	Employee_Default	Employee 4
2001111403110002006	200111112502006	Employee_Default	Employee 3
2001111403110002007	200111112502007	5G_Devices_Allow_profile	Employee 2
2001111403110002010	200111112502010		Non-ISE-provisioned-device
2001111403110002001	200111112502001	5G_Devices_VLAN_895	John Thompson (Use-Case-3)
2001111403110002003	200111112502003	5G_Devices_VLAN_896	Scarlet Fiero (Use-Case-2)
2001111403110002005	200111112502005	5G_Devices_Allow_profile	Employee 1
2001111403110002009	200111112502009	5G_Devices_Deny_profile	Faulty-Sensor

Edit

SIM Status (Required)	Activated ▼
SIM Barred	No ▼

Services

Communication Plan	5GaaS-ISE-DEMO Plan ▼
Device Profile	5G_Devices_Allow_profile ▼

Rating

Device ID

Rate Plan

Usage Limit Override

- 5G_Devices_Allow_profile
- 5G_Devices_Default_VLAN_1
- 5G_Devices_Deny_profile
- 5G_Devices_VLAN_895
- 5G_Devices_VLAN_896
- Android_Guest_Default
- Apple-iDevice_Employee_Default
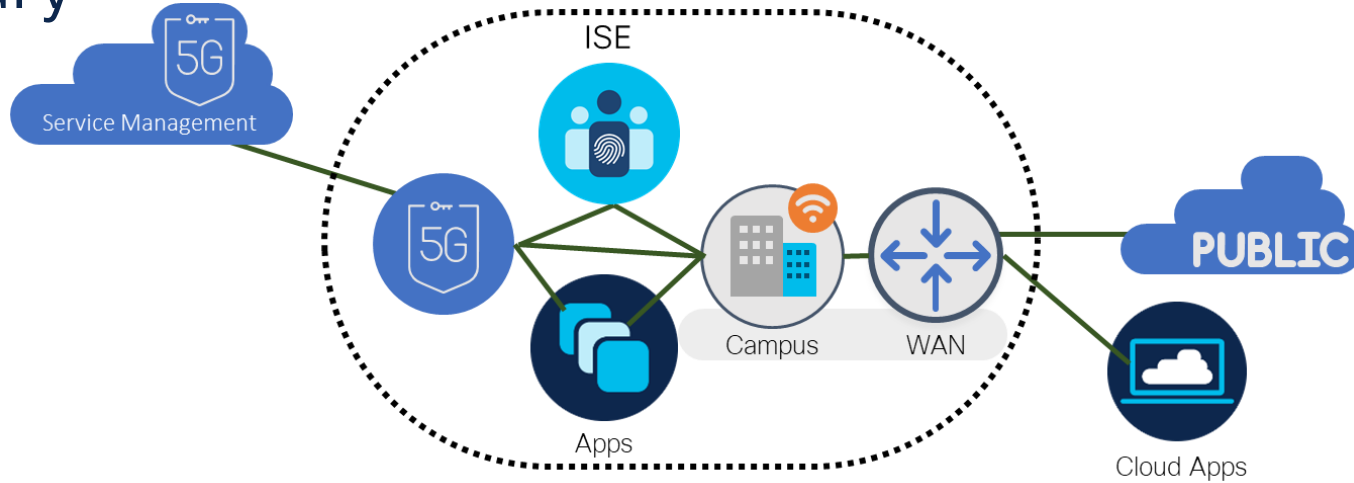- Employee_Default
- Guest_Default

Summary

Summary

Service Management

ISE

Apps

Campus   WAN

PUBLIC

Cloud Apps

Intent based policies across Wi-Fi & P5G

Enterprise known and trusted policy platform

Secured network regardless of access type or location

Consistent & reliable experience via VLAN tagging, IP pools etc.

Enhanced Private 5G experience delivered with unified identity and policy

Cloud Apps

Cisco Private 5G Learning Map
Learn More about Technical Seminars & Breakouts

Start

June 12 | 2:00 pm
TECSPG-2432
New Adventures in Wireless: The Journey of WiFi6 and Private 5G Networks for the Enterprise

June 13 | 11:00 am
BRKSPG-1003
Evolution of Private 5G Networks Standards

June 13 | 4:00 pm
BRKSPM-2842
Industry enablers making Private 5G a viable private networking option

June 14 | 4:00 pm
BRKXAR-2004
Unified Identity & Policy Across Private 5G and Wi-Fi

June 16 | 8:00 am
BRKEWN-2030
WiFi6 and Private 5G for the Enterprise – a 'Better Together' Journey

Continue

June 16 | 8:45 am
BRKSPM-3169
Customer Challenges and Practical Design Consideration for 5G Transformation

Cisco Private 5G Learning Map

Learn more about Solution Overviews and Interactive Design Sessions

Start

June 14 | 2:00 pm
PSOGEN-1029
Private 5G as-a-Service is Here: Get Ready

June 15 | 11:00 am
PSOIND-1004
Private 5G and it's role in Healthcare Infrastructure

June 14 | 4:00 pm
PSOIND-1003
Private 5G in Education: Innovation and Opportunity

June 16 | 4:00 pm
PSOSPG-1002
Leading Your Digital Transformation with Cisco Private 5G Network Offer

June 14 | 10:30 am
IBOSPG-2004
5G Customer Success Story: US Marine Corps Smart Warehouse

June 13 | 4:00 am
IBOSPG-2010
Getting Started with Enterprise Private 5G: An Interactive Design Workshop

June 15 | 4:00 pm
IBOSPG-2004
5G Customer Success Story: US Marine Corps Smart Warehouse

Finish

June 16 | 11:00 am
IBOSPG-2010
Getting Started with Enterprise Private 5G: An Interactive Design Workshop

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers
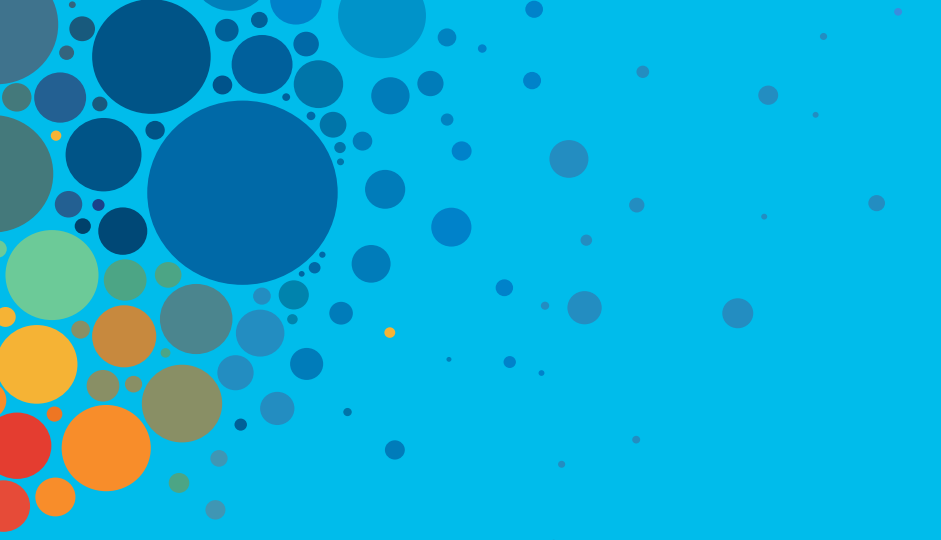
Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue
your education

- Visit the Cisco Showcase
  for Cisco Private 5G Demo

- Book your one-on-one
  Meet the Engineer meeting

- Attend the interactive education
  with DevNet, Capture the Flag,
  and Walk-in Labs

- Visit the On-Demand Library
  for more sessions at
  www.CiscoLive.com/on-demand

Thank you

CISCO *Live!*

ALL IN

#CiscoLive