Architektura SD-Access

Wprowadzenie

Miłosz Wrona, Systems Engineer

Listopad 2024

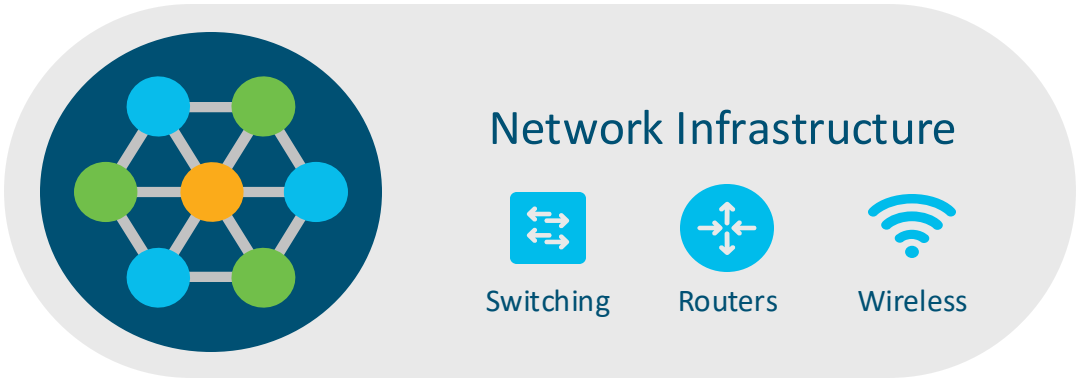
Agenda

- Wprowadzenie, czyli dlaczego SDA?
- Pojęcia podstawowe
- Segmentacja
- Demo

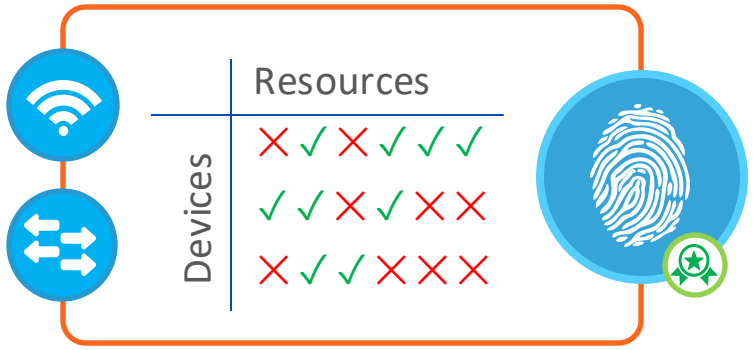
Wprowadzenie,
czyli dlaczego Cisco SD-Access?

Traditional Networks Challenges

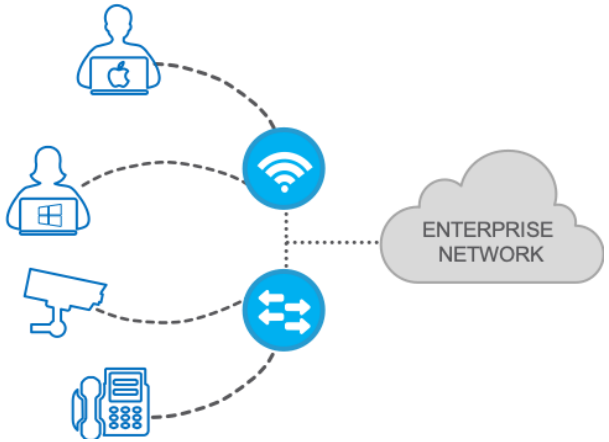
Network deployment challenges



Network security challenges



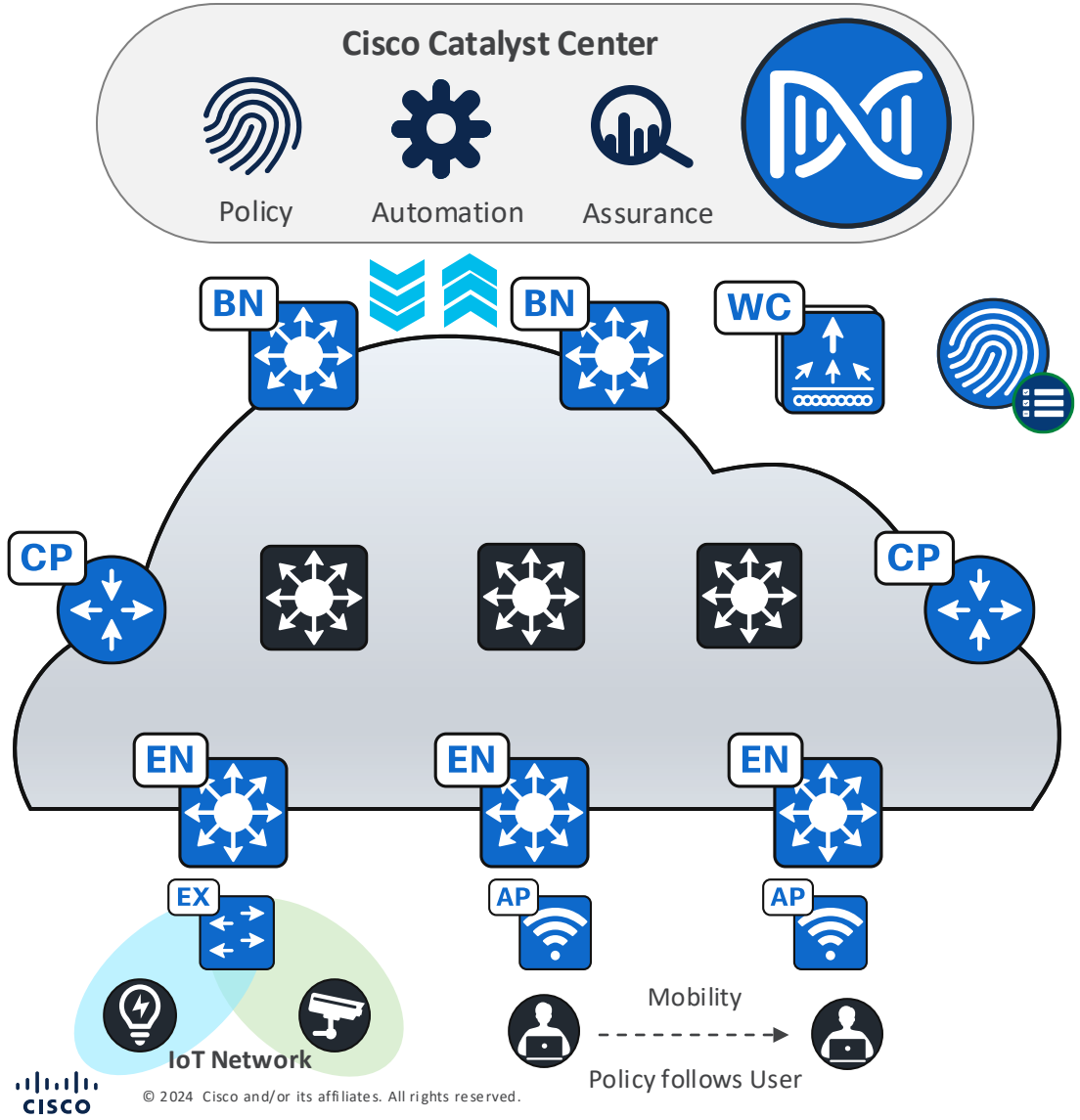
Wireless & wired network challenges



Network operations challenges

Cisco Software Defined Access

The Foundation for Cisco's Intent-Based Network



One Automated Network Fabric

Single Fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

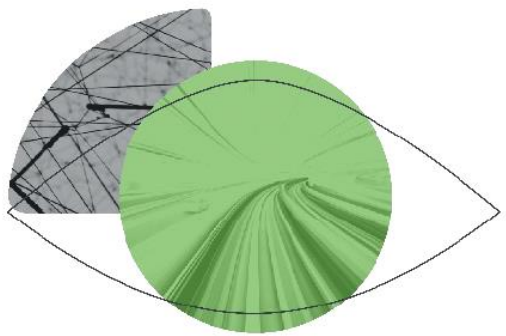
AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

Cisco Software-Defined Access

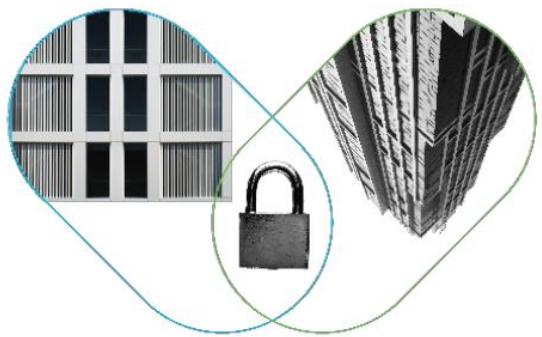
Zero Trust for the Workplace

Visibility



Grant the right level of network access to users and devices.

Segmentation



Shrink zones of trust and grant access based on least privilege.

Containment

Automate containment of infected endpoints and revoke network access.

Visibility, Segmentation and Containment are explored further in BRKENS-2819.

Benefits of SD-Access

Enhance Security and Compliance

Deliver consistent Experience

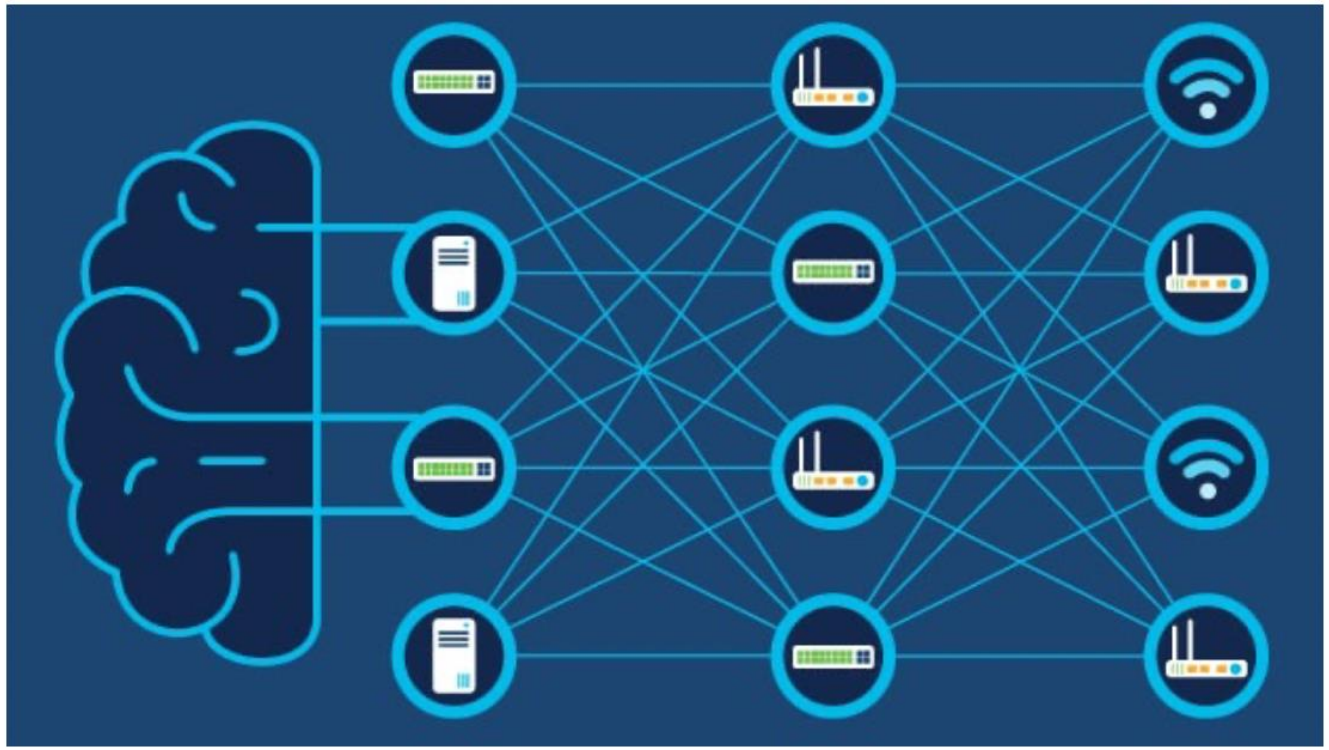
Boost operational effectiveness

Gain network insights

Pojęcia podstawowe

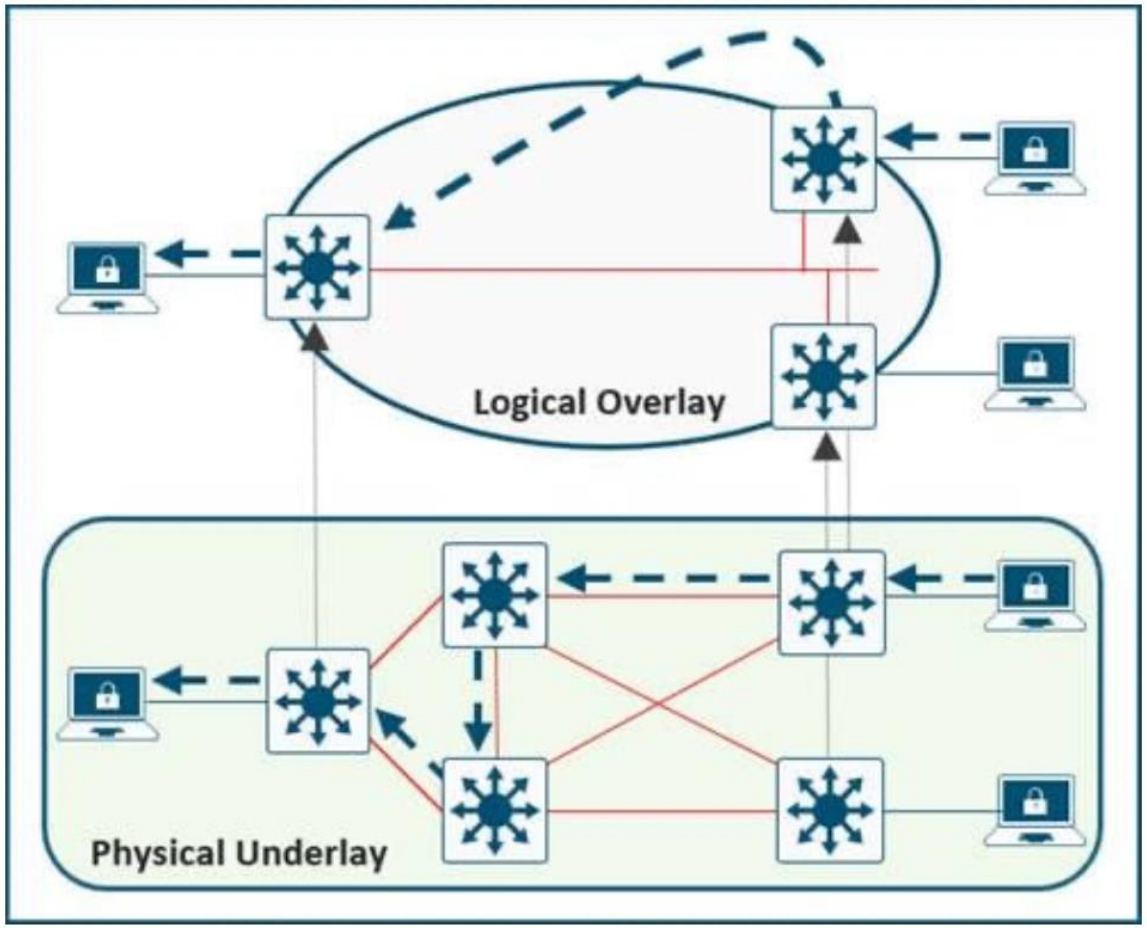
What is a Network Fabric?

- Mesh of connections between network devices.
- Transports data from source to destination.
- Usually refers to a virtualized, automated lattice of overlay connections.
- May (uncommonly) refer to physical wiring of a network .

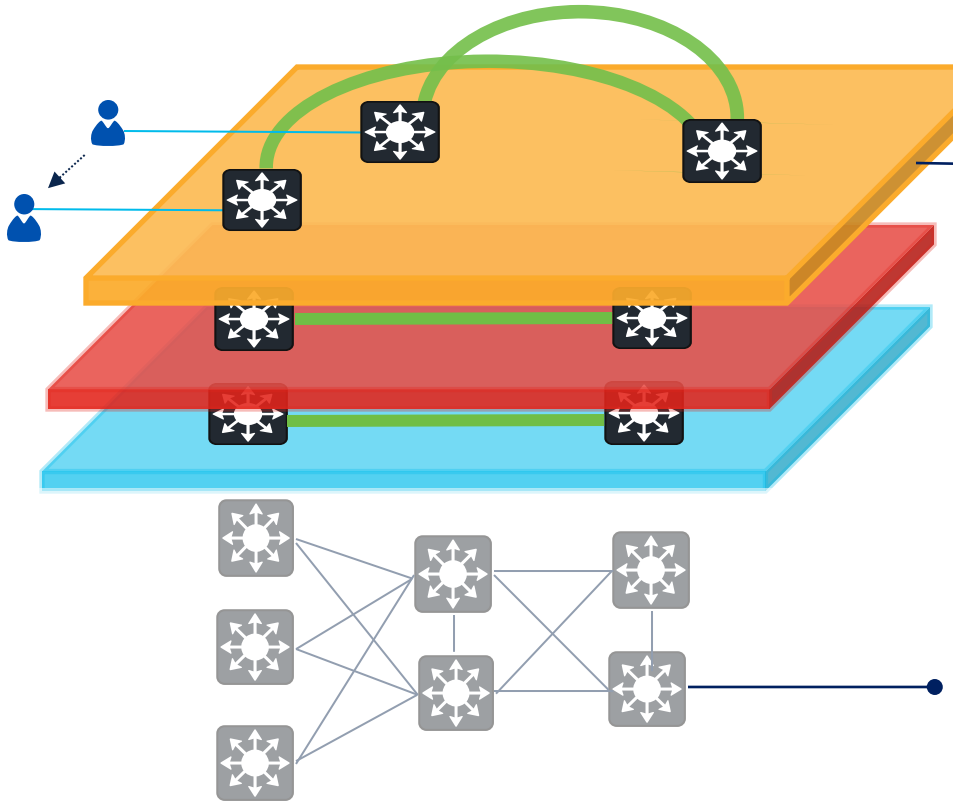


Overlay

- An Overlay network is a logical topology used to virtually connect devices, built over an arbitrary physical Underlay topology.
- Examples of overlay technologies:
  - GRE
  - MPLS
  - IPsec
  - CAPWAP
  - LISP
  - VXLAN
  - BGP EVPN
  - SD-WAN
  - ACI
  - OTV
- Services - deliver using overlay
- Mobility - map endpoints to edges
- Scalability - reduce protocol state
- Underlay is simple and manageable
- Flexible and programmable
- Maximize network reliability



Why an Overlay?

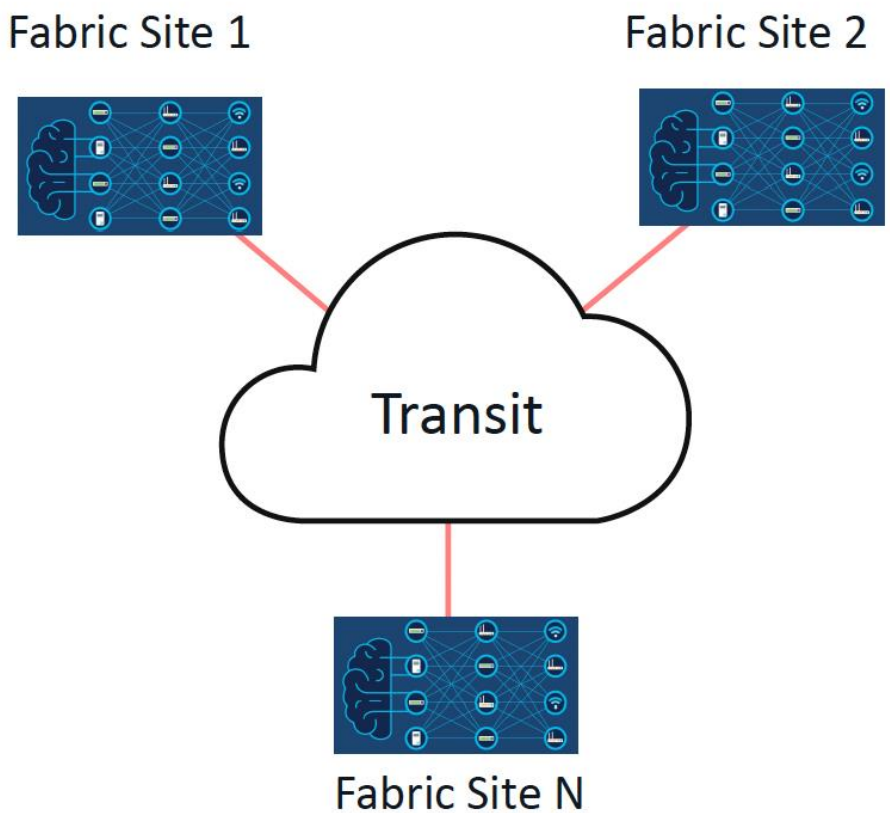


Overlay: Flexible, Scalable and Extensible. Easy to add, modify, and deliver services in virtualized overlay topologies. Optimizes mobility events.

Underlay: Build and forget!
Reliable, manageable, and simple.

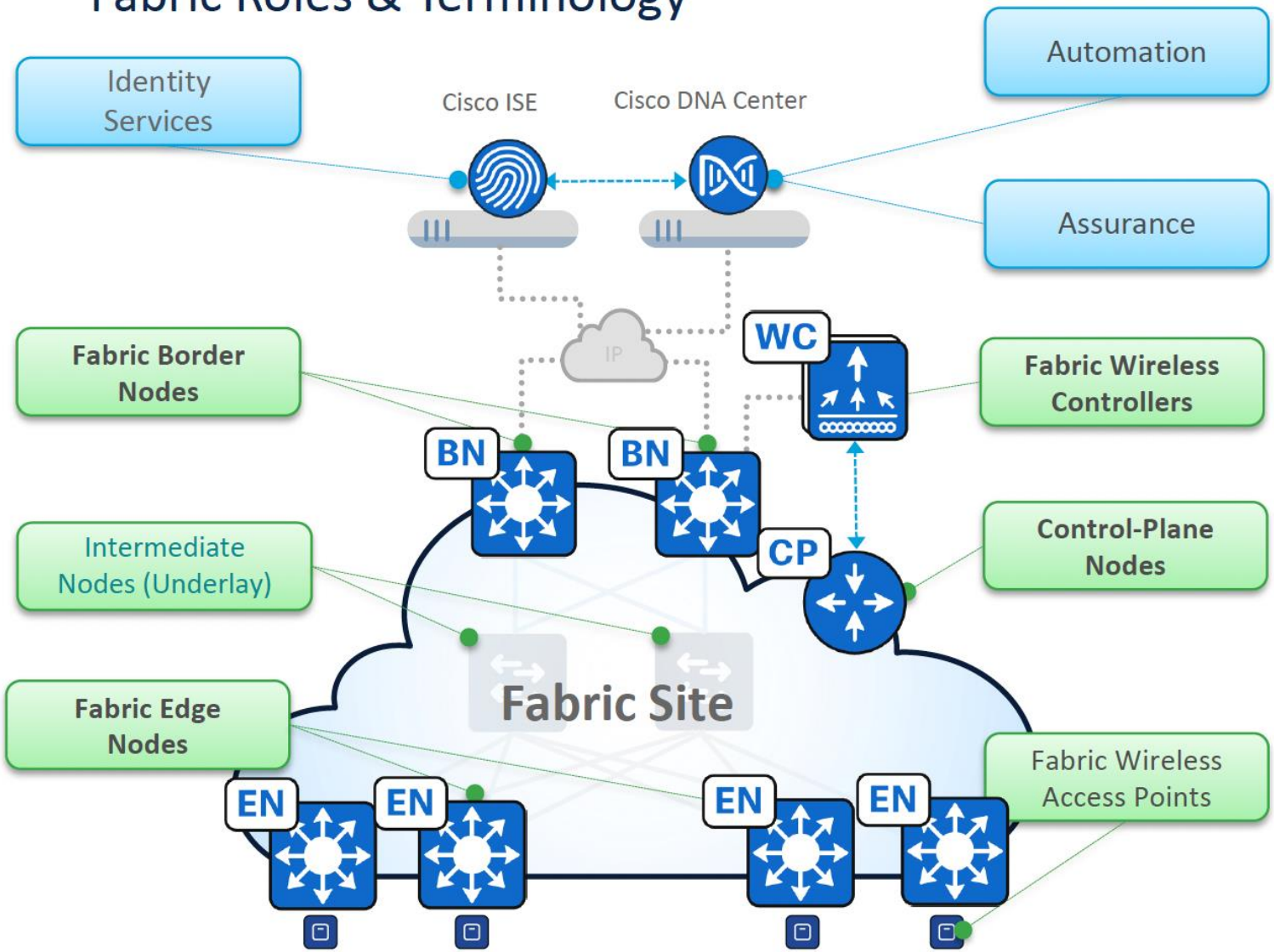
What is Fabric Site?

- An instance of an SD-Access Fabric.
- Typically defined by disparate geographical locations, but not always.
- Can also be defined by:
  - Endpoint scale.
  - Failure domain scoping.
  - RTT.
  - Underlay connectivity attributes.
- Typically interconnected by a “Transit”.



Cisco SD-Access

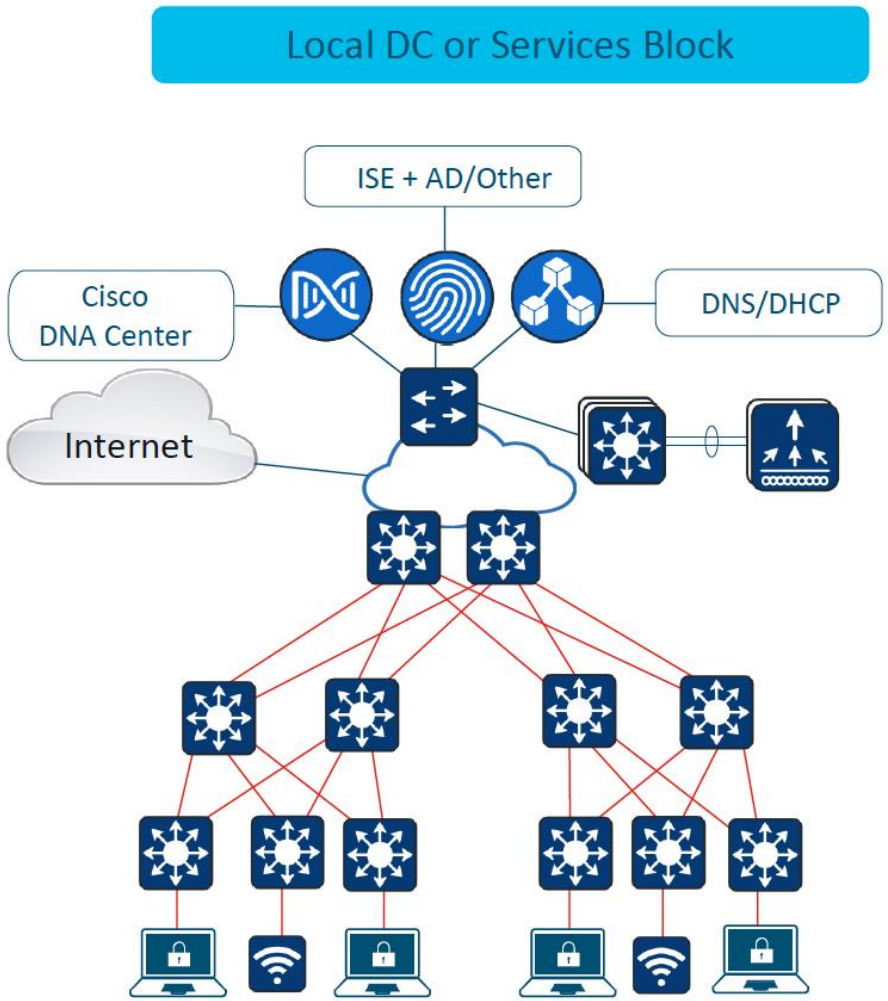
Fabric Roles & Terminology

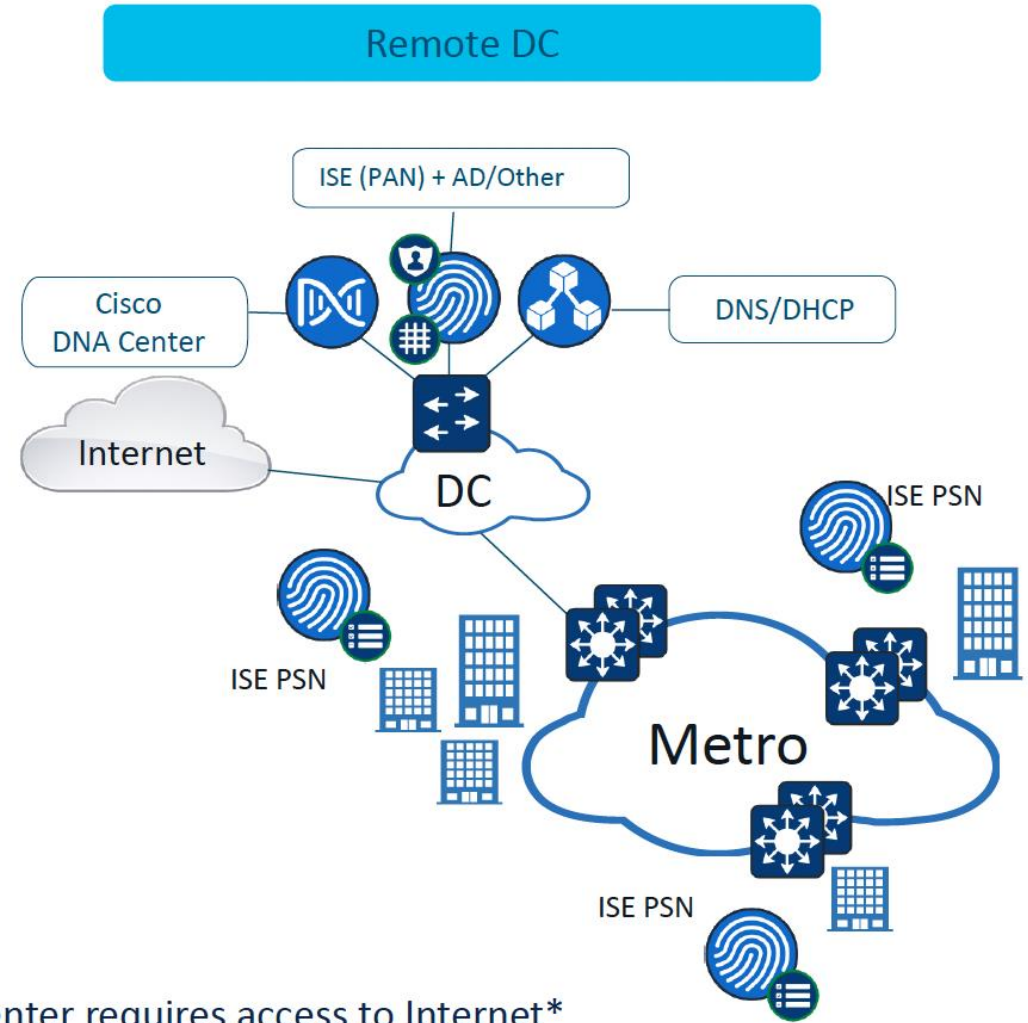


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Cisco SD-Access Architecture

Where do I place Critical/Shared Services

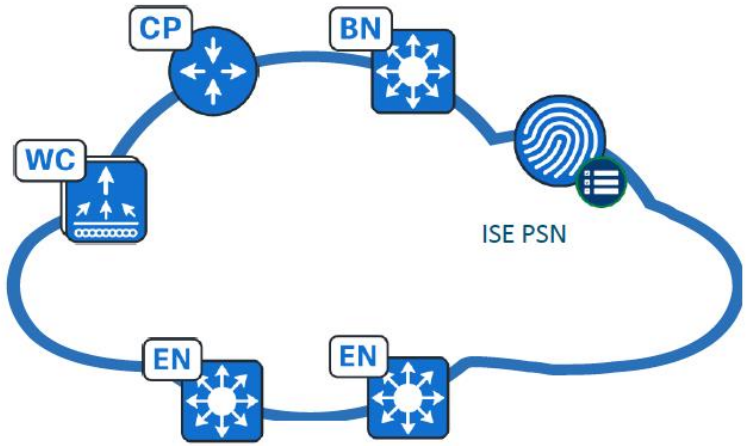




Cisco DNA Center requires access to Internet*

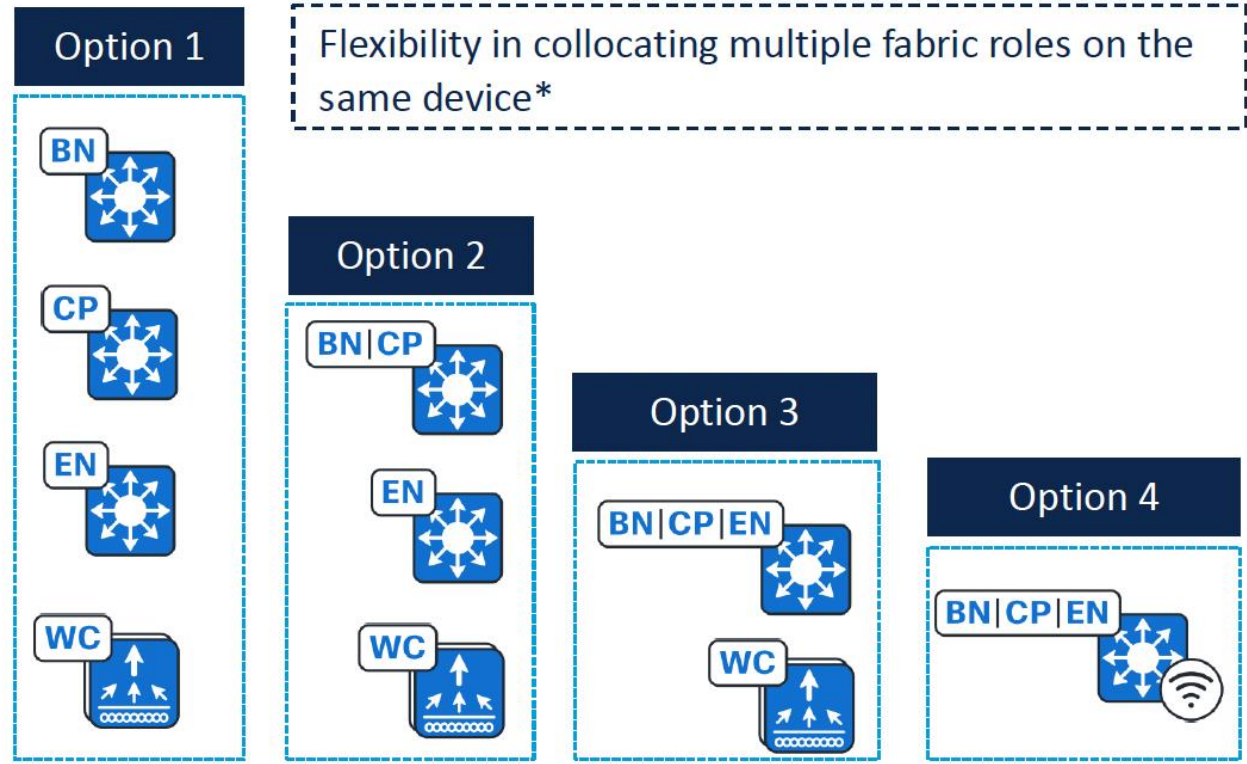
Cisco SD-Access Single-site Design Options

Fabric Site Design Options



Fabric Site

- Logical construct that contains:
  - Fabric Edge, Border, Control Plane
  - ISE PAN/PSN Node
  - (optional) Wireless LAN Controller, Access Points
  - (optional) Extended Nodes



* Refer to Cisco SD-Access compatibility matrix for latest information

SD-Access Design Aides

- Cisco Validated Design: https://cs.co/sda-cvd
- Design Tool: http://cs.co/sda-design-tool

- Compatibility Matrix: http://cs.co/sda-compatibility-matrix

New Deployment

Release 2.3.3.6 (recommended release) Device Role Fabric Border and Control Plane

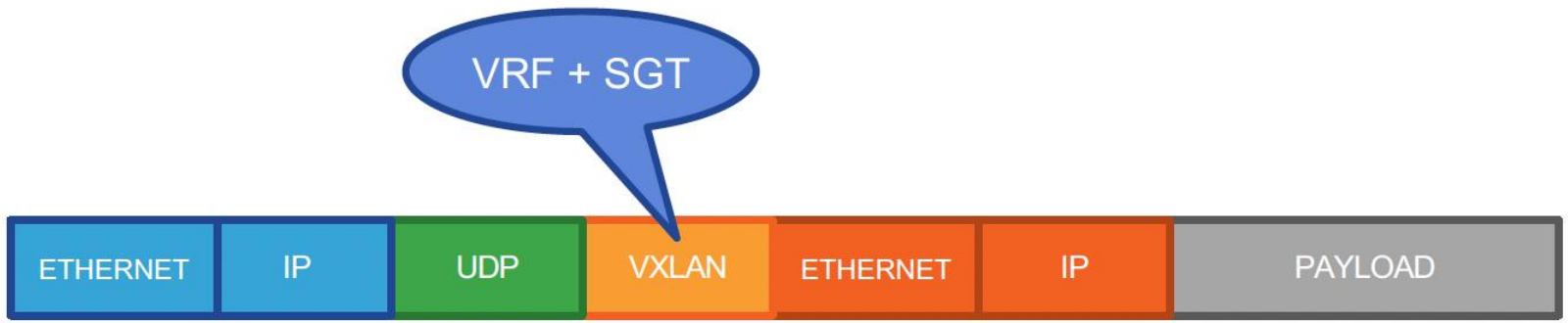
Submit Query

SD-Access Compatibility Matrix for Cisco DNA Center 2.3.3.6 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
		C9300X-12Y	IOS XE 17.6.4	IOS XE 17.9.x
		C9300X-24Y		IOS XE 17.8.x
		C9300X-24HX		IOS XE 17.7.x
		C9300X-48HXN		IOS XE 17.6.x
		C9300X-48HX		IOS XE 17.5.x

Cisco SD-Access Fabric

1. Management Plane: Cisco DNA Center
2. Control Plane: LISP
3. Data Plane: VXLAN
4. Policy Plane: Group-Based Policy based on Cisco Trustsec (CTS)



Virtual Routing & Forwarding
Security Group Tagging

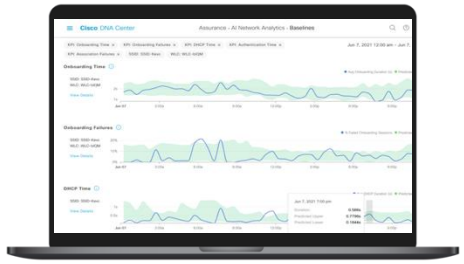
Cisco Catalyst Center – Ewolucja operacyjna

Skalowanie w odpowiedzi na potrzeby Twojego przedsiębiorstwa

Cisco Catalyst Center

Serwer Cisco UCS®

Preinstalowane oprogramowanie



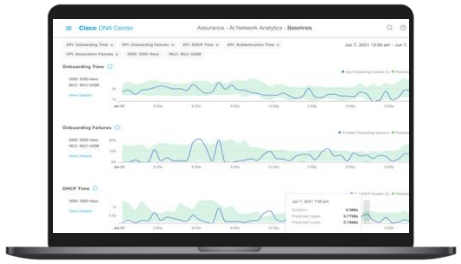
Catalyst Center fizyczny appliance

Serwer oparty na architekturze x86

Oprogramowanie dostarczone przez Cisco bez dodatkowych kosztów $0

+

Licencja ESXi



ESXi wirtualny appliance

Oprogramowanie dostarczone przez Cisco bez dodatkowych kosztów $0

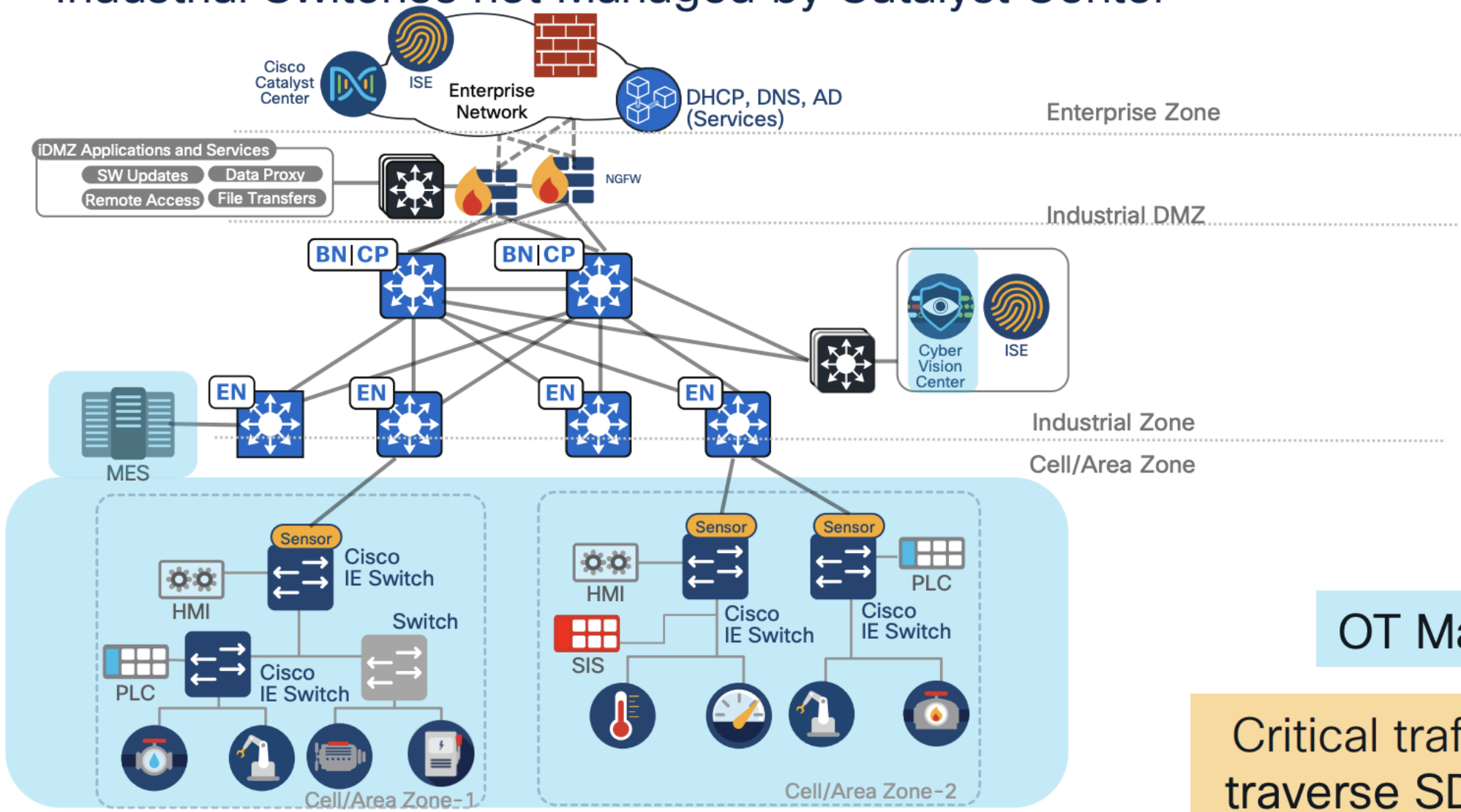
+

Subskrypcja AWS

AWS wirtualny appliance

#2 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches not Managed by Catalyst Center

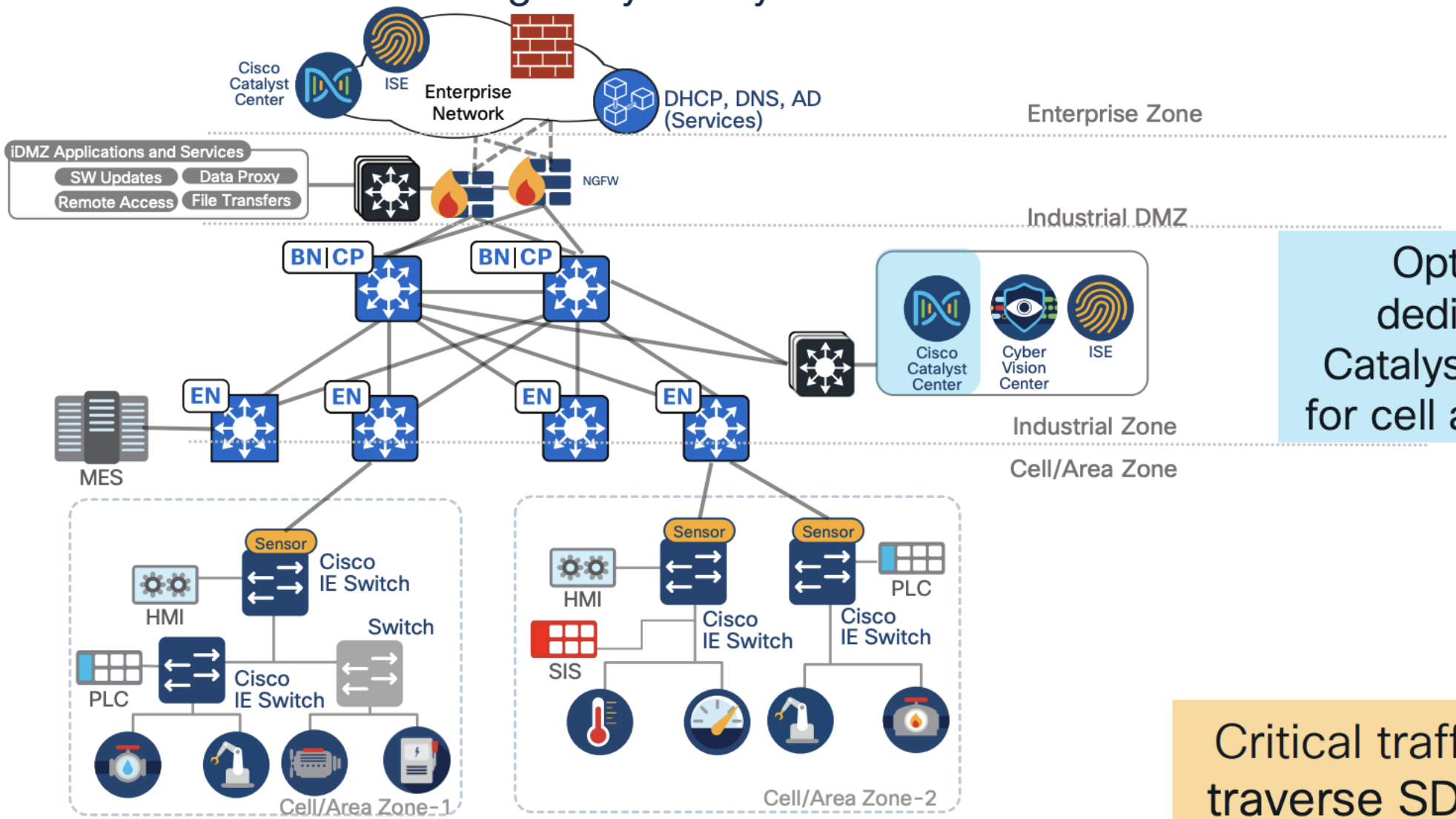


OT Managed

Critical traffic doesn't traverse SDA network

#3 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches Managed by Catalyst Center



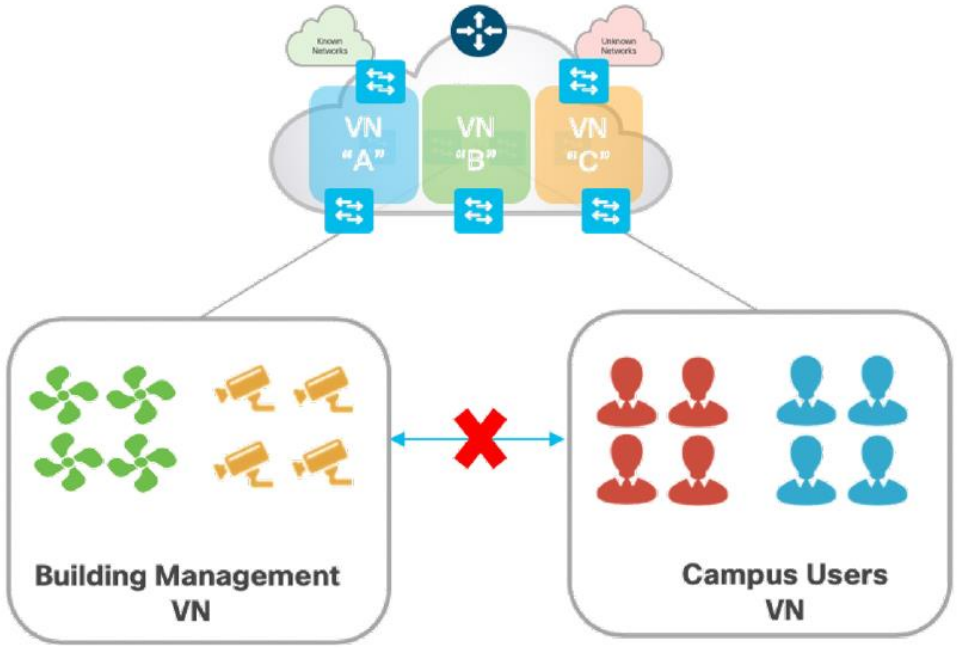
Optional dedicated Catalyst Center for cell area zone

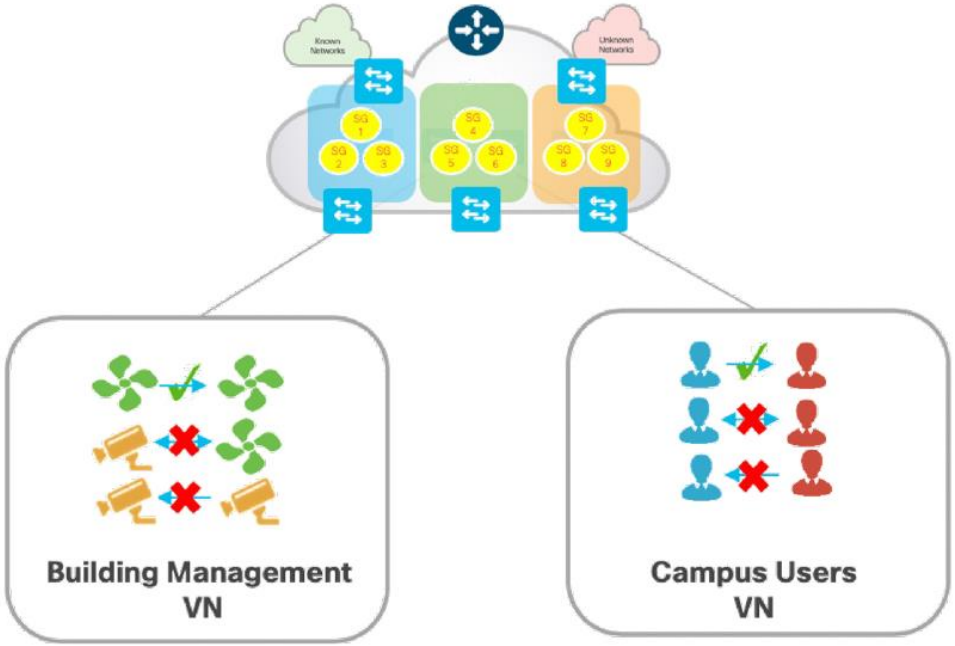
Critical traffic doesn't traverse SDA network

Segmentacja

SD-Access Policy

Macro-Segmentation and Micro-Segmentation





Virtual Network (VN)

First-level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

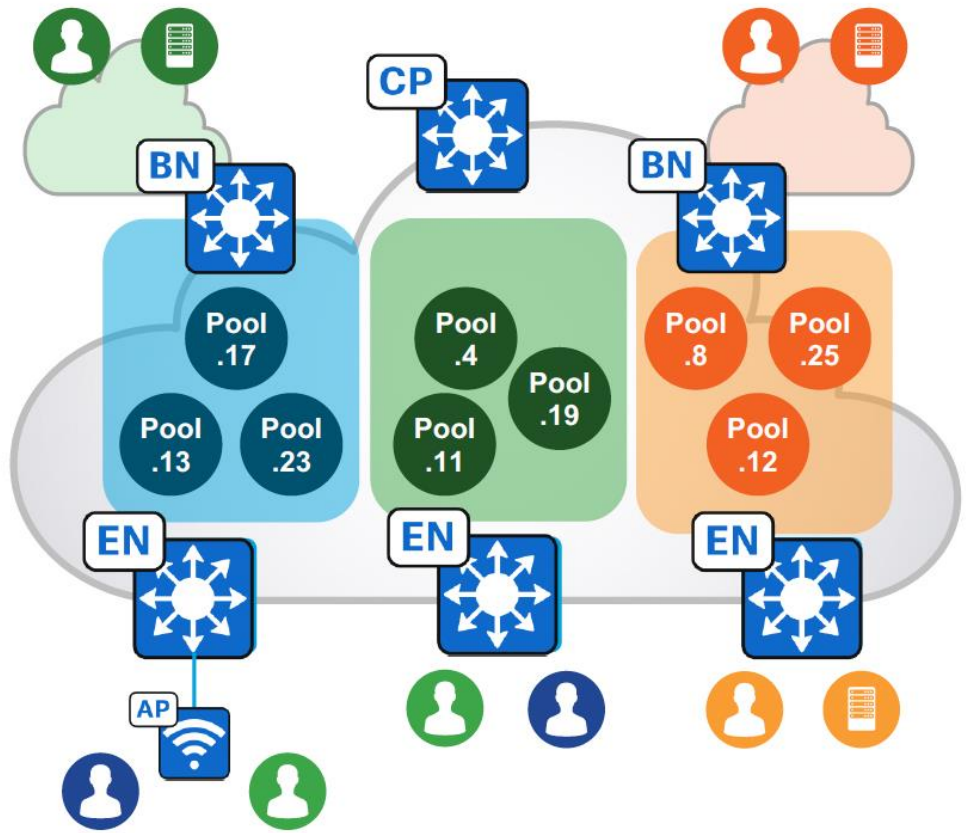
Security Group Tag (SGT)

Second-level Segmentation ensures **role-based access control** between groups in a VN. Ability to segment the network into lines of business or functional blocks.

Cisco SD-Access Fabric

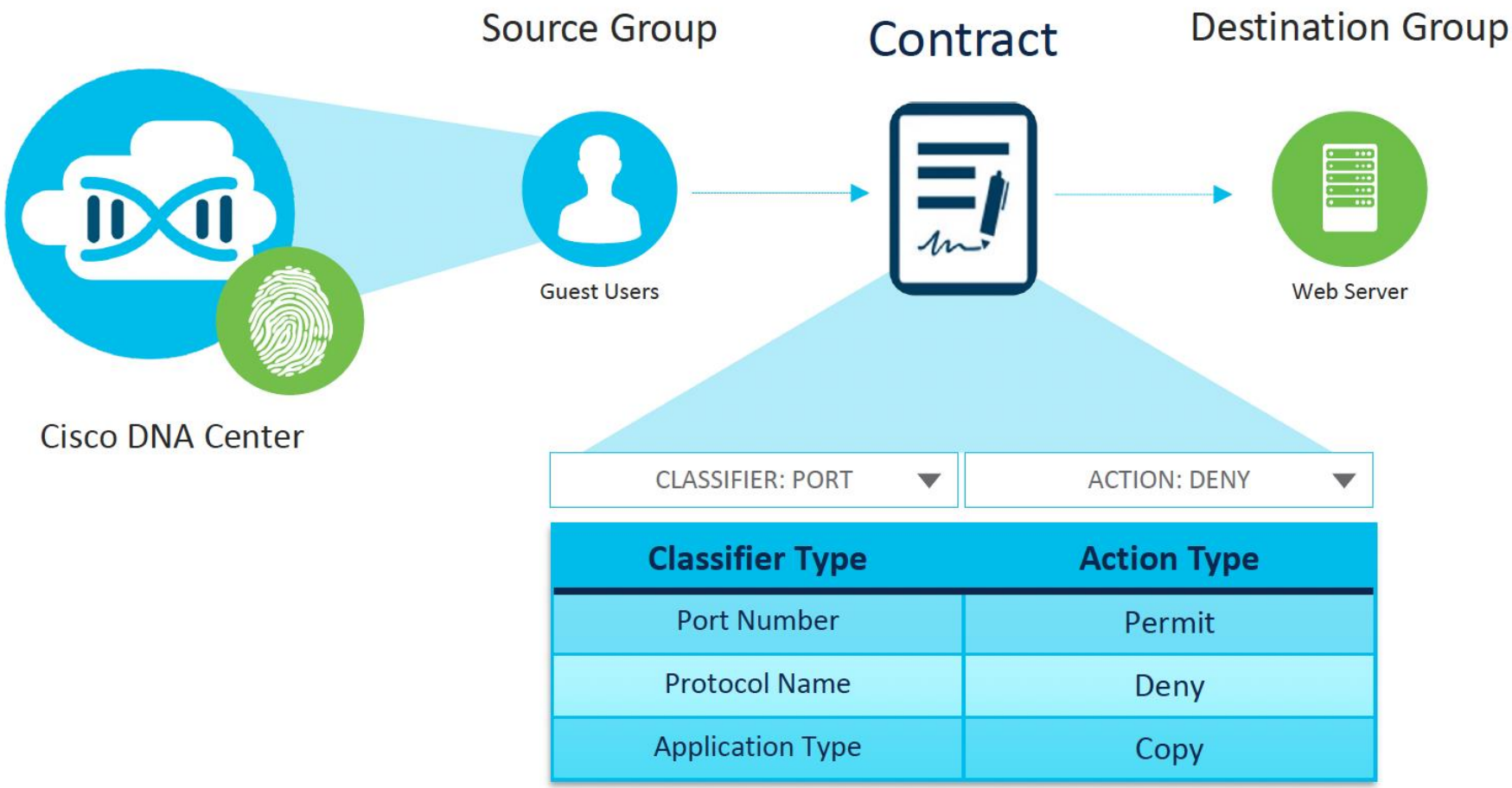
Host Pools

- Provide a Default Gateway and Basic IP Services for Endpoints
- Host pools are assigned to endpoints dynamically by AAA or statically per port



SD-Access Policy

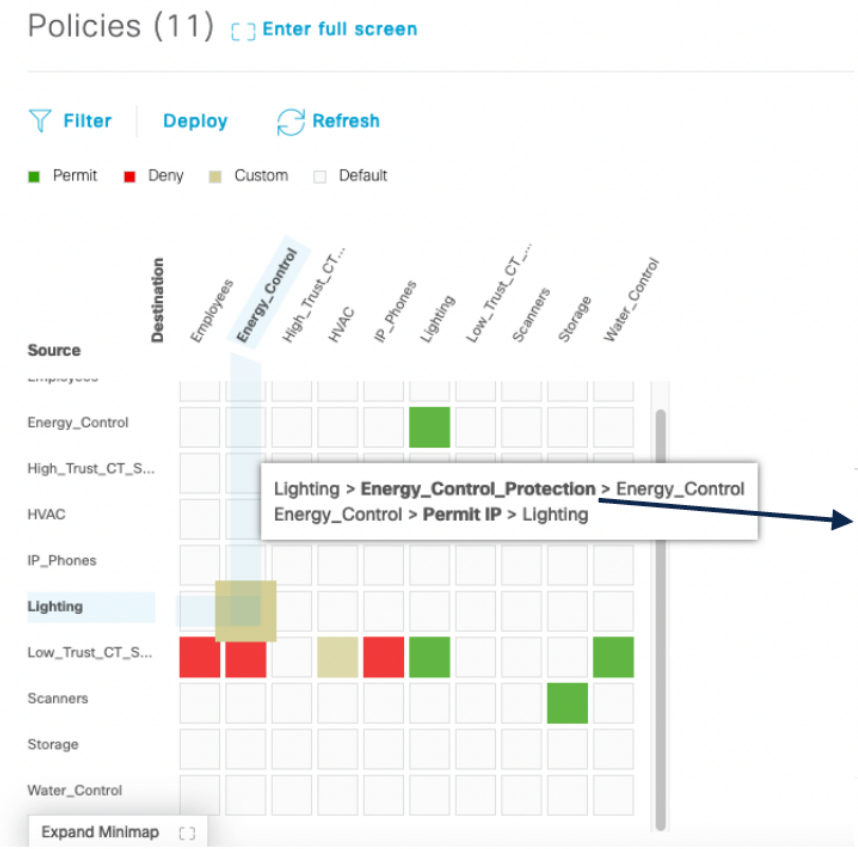
Access Control Policies



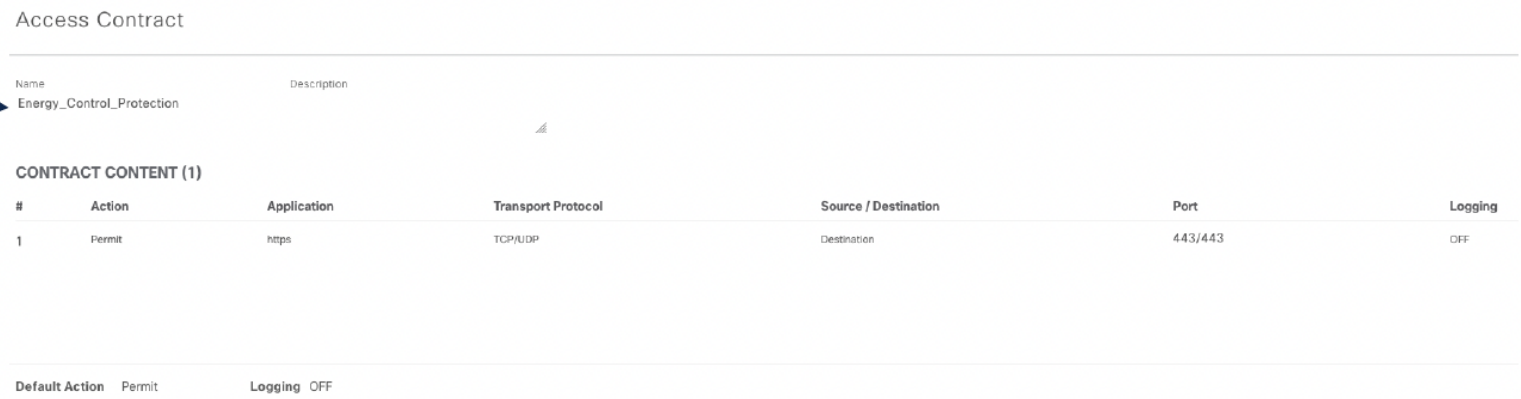
Classifier Type	Action Type
Port Number	Permit
Protocol Name	Deny
Application Type	Copy

SD-Access Policy

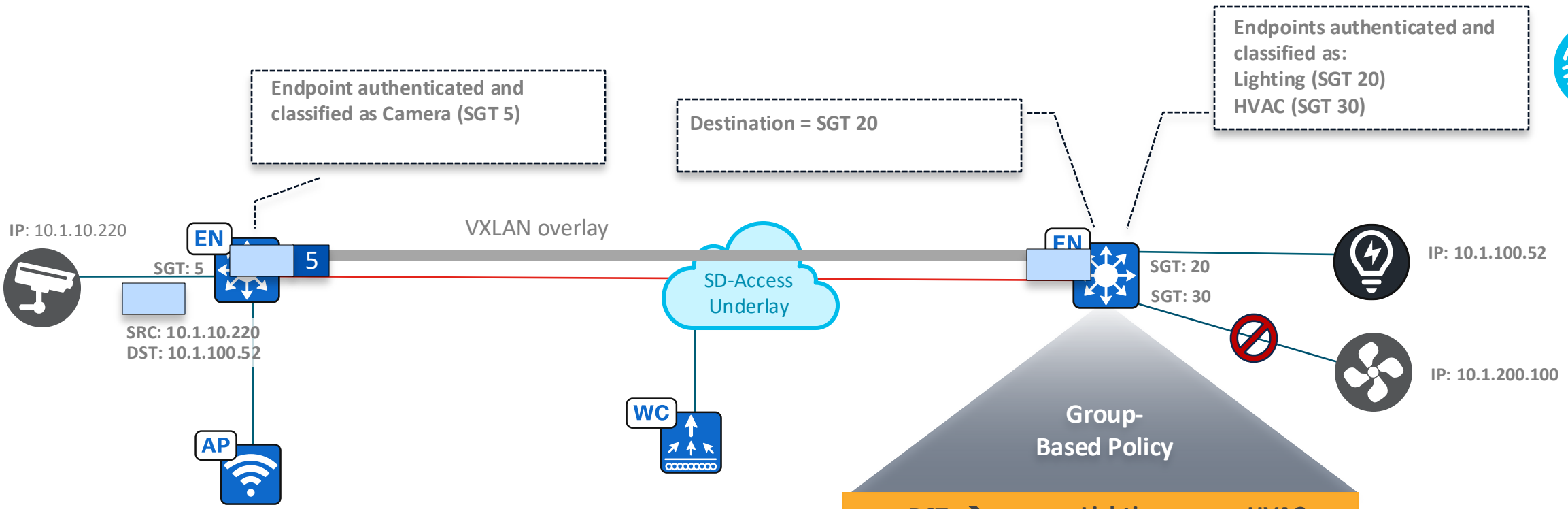
Group-Based Access Control Policy



1. Select **Source Group**(s)
2. Select **Destination Group**(s)
3. Select **Access Contract**(s)



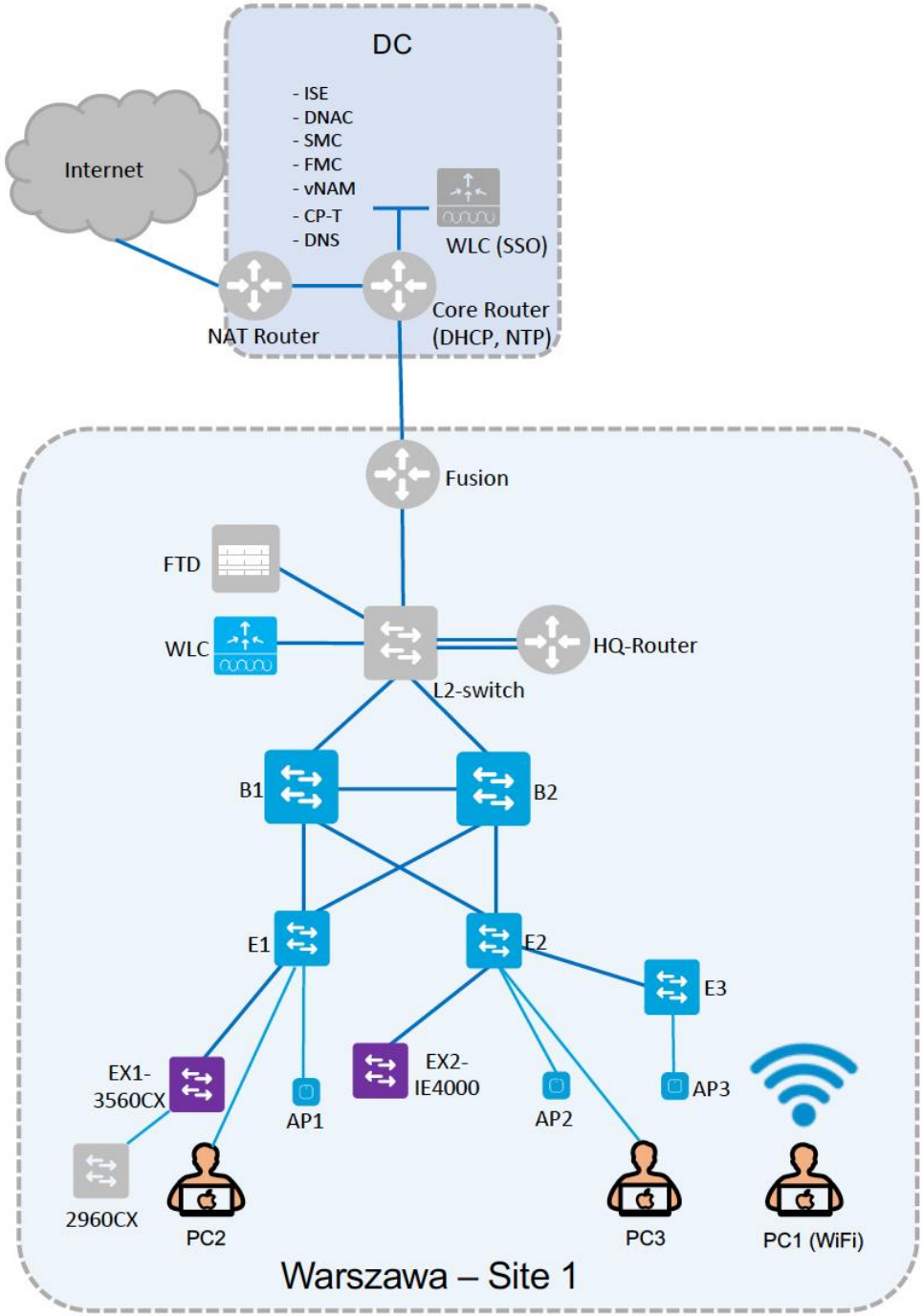
What is Security Group Tag and Group-Based Policy?



DST → / ↓ SRC	Lighting (20)	HVAC (30)
Camera (5)	Permit	Deny
BYOD (7)	Deny	Permit

Demo

LAB Topology



The bridge to possible

Dziękuję za uwagę