From Chaos to Control: Practical Segmentation Strategies for Industrial Networks

Anders C Pedersen
Customer Delivery Architect, Cisco CX

Inigo Alonso
Principal Architect, Cisco CX

BRKIOT-2588

"If someone brought ransomware into your industrial network today, how many critical systems would be compromised before you could contain it?"

© 2026 Cisco and/or its affiliates. All rights reserved.



Strategic Segmentation transforms Chaos into Controlled, Resilient Operations

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Agenda

Four Essential Steps to transform Network Chaos into Control

1. **Understanding the Framework**

   Zones, Conduits, and Defense-in-Depth

2. **Gaining Visibility**

   We Can't Segment What We Can't See

3. **Implementation Strategies**

   From Macro to Micro Segmentation

4. **Operational Excellence**

   Maintaining Your Security Posture

© 2026 Cisco and/or its affiliates. All rights reserved.

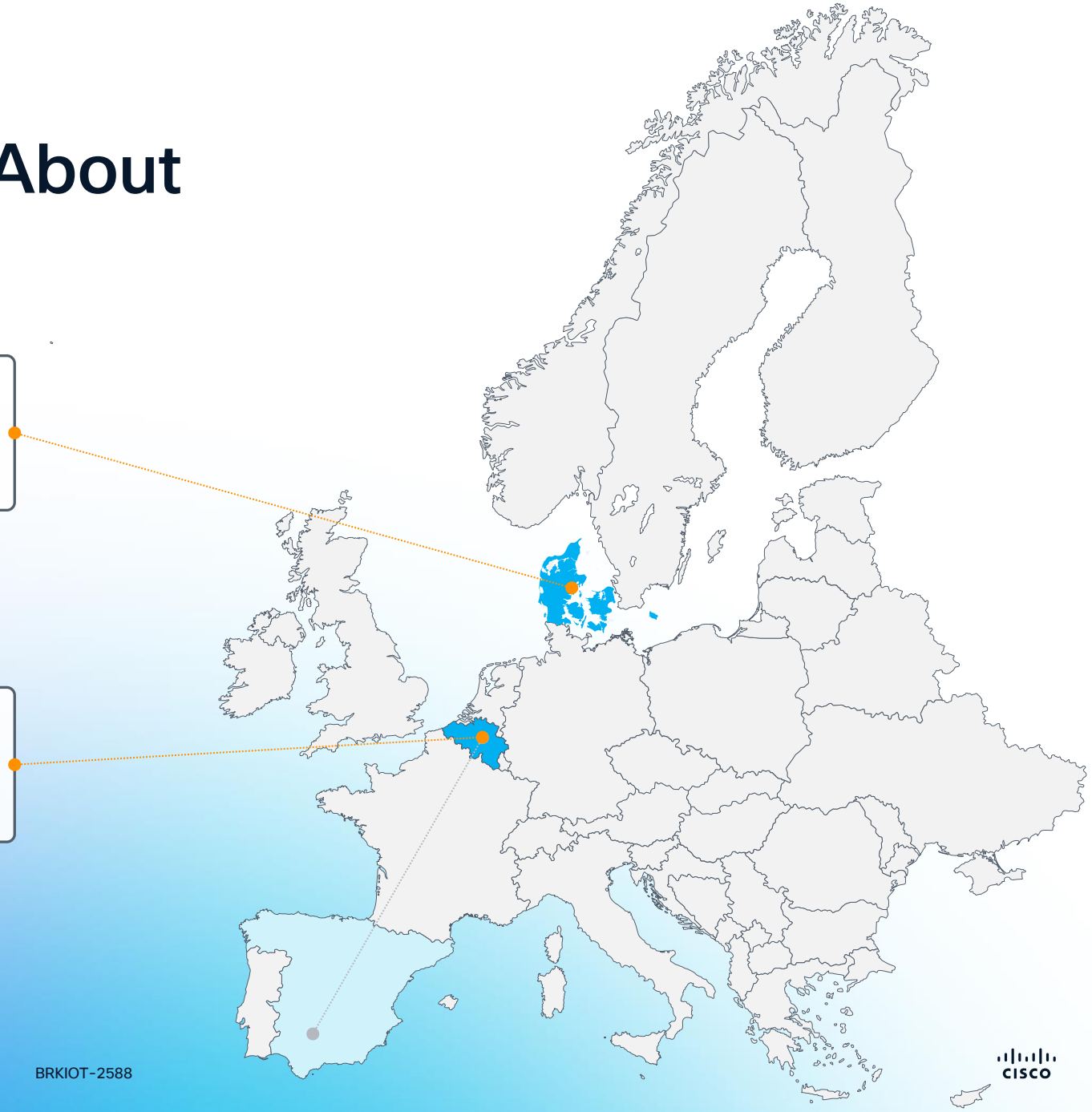
About



Anders C Pedersen
Customer Delivery Architect, Cisco CX



Inigo Alonso
Principal Architect, Cisco CX



© 2026 Cisco and/or its affiliates. All rights reserved.

"In 2024, cyberattacks on critical infrastructure surged 30%"

Cisco 2024 State of Industrial Networking Report

Countless disclosed and non-disclosed cases learned this lesson the hard way.

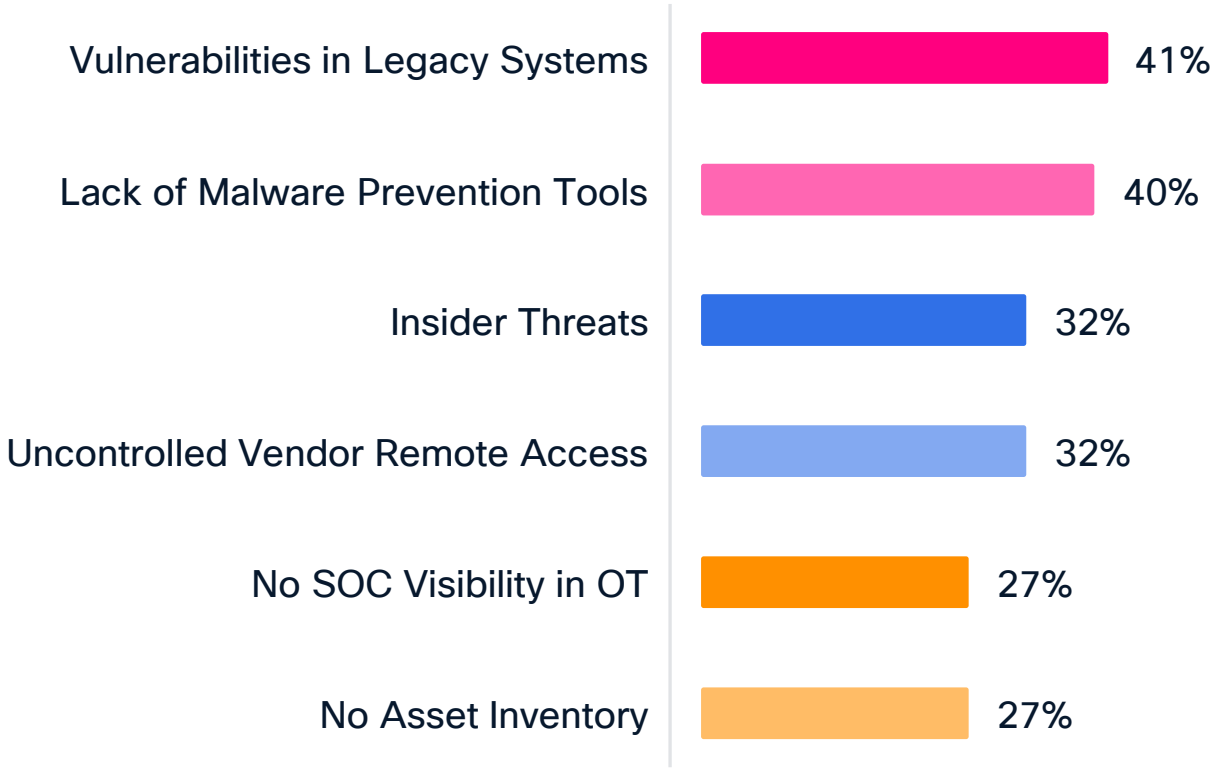
The common denominator?
Flat networks with no segmentation.

© 2026 Cisco and/or its affiliates. All rights reserved.

Challenge Statistics

OT Security Challenges – What Operators Actually Face

Top Security Challenges in Industrial Networks



Source: Cisco 2024 State of Industrial Networking Report

Segmentation mitigates 5 of 6 challenges:

Contain threats from legacy Vulnerabilities ✓

Prevents Malware spread ✓

Limits insider threat movement ✓

Restricts vendor access scope ✓

Enables SOC Visibility through policy logs ✓

© 2026 Cisco and/or its affiliates. All rights reserved.

Understanding the Framework

ISA/IEC 62443 – The Blueprint

Provides the Security Blueprint for Industrial Networks

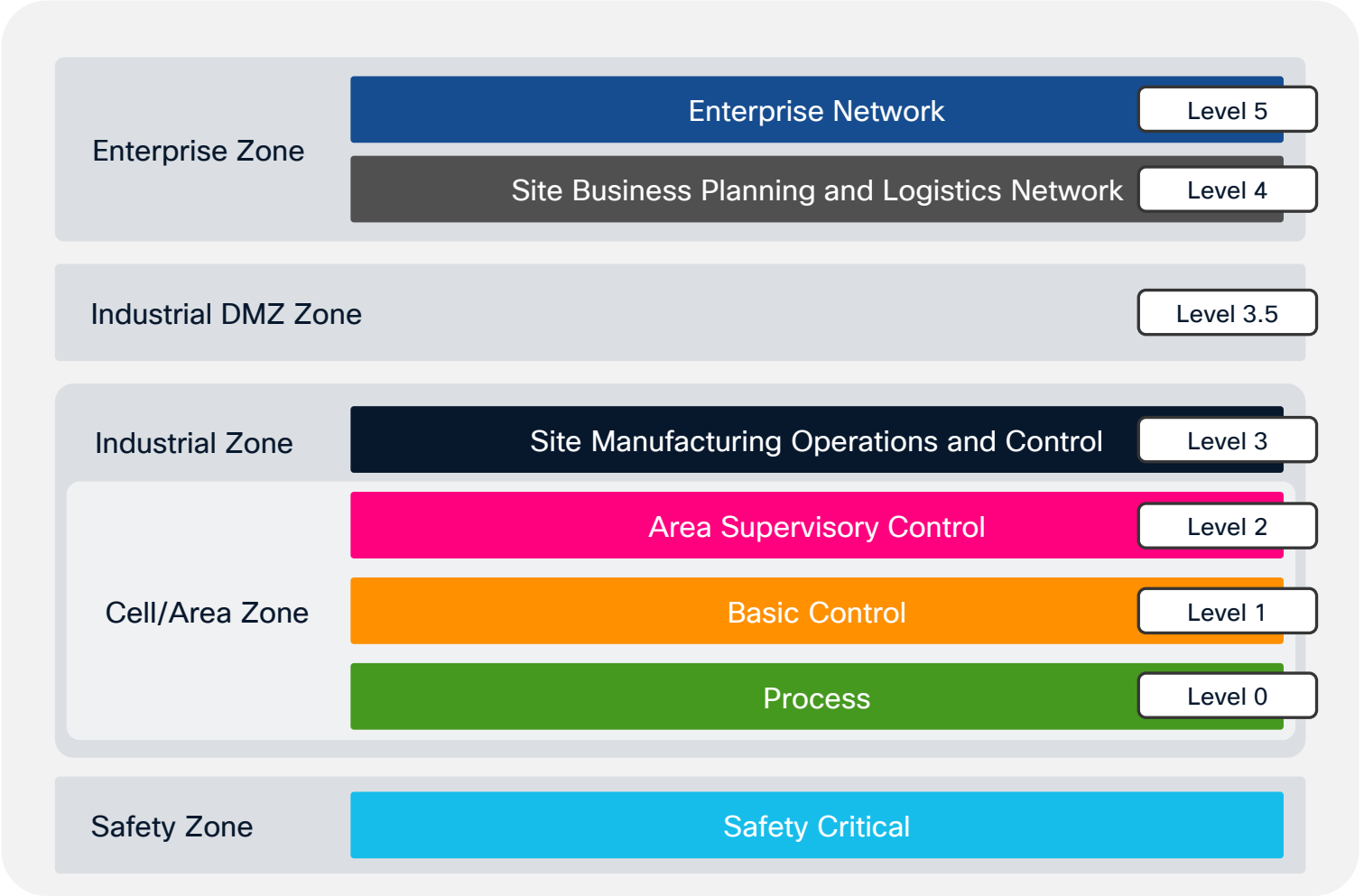
Why Standards Matter

ISA/IEC 62443 is to industrial security, what building codes are to construction.

(for example) You wouldn't build a hospital without following safety standards.

Don't build OT security without following ISA/IEC 62443.

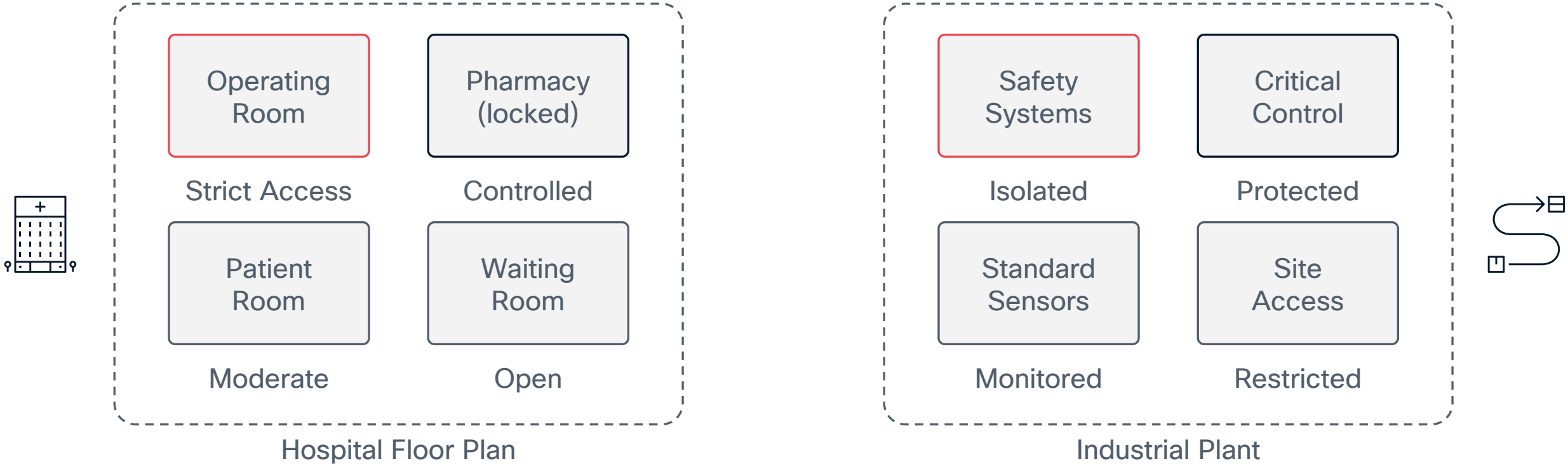
Level 0 is the closest to industrial process, ***Levels 4 and 5*** are closest to the IT network.



© 2026 Cisco and/or its affiliates. All rights reserved.

Zones Defined

Zones Group Assets with Similar Security Requirements



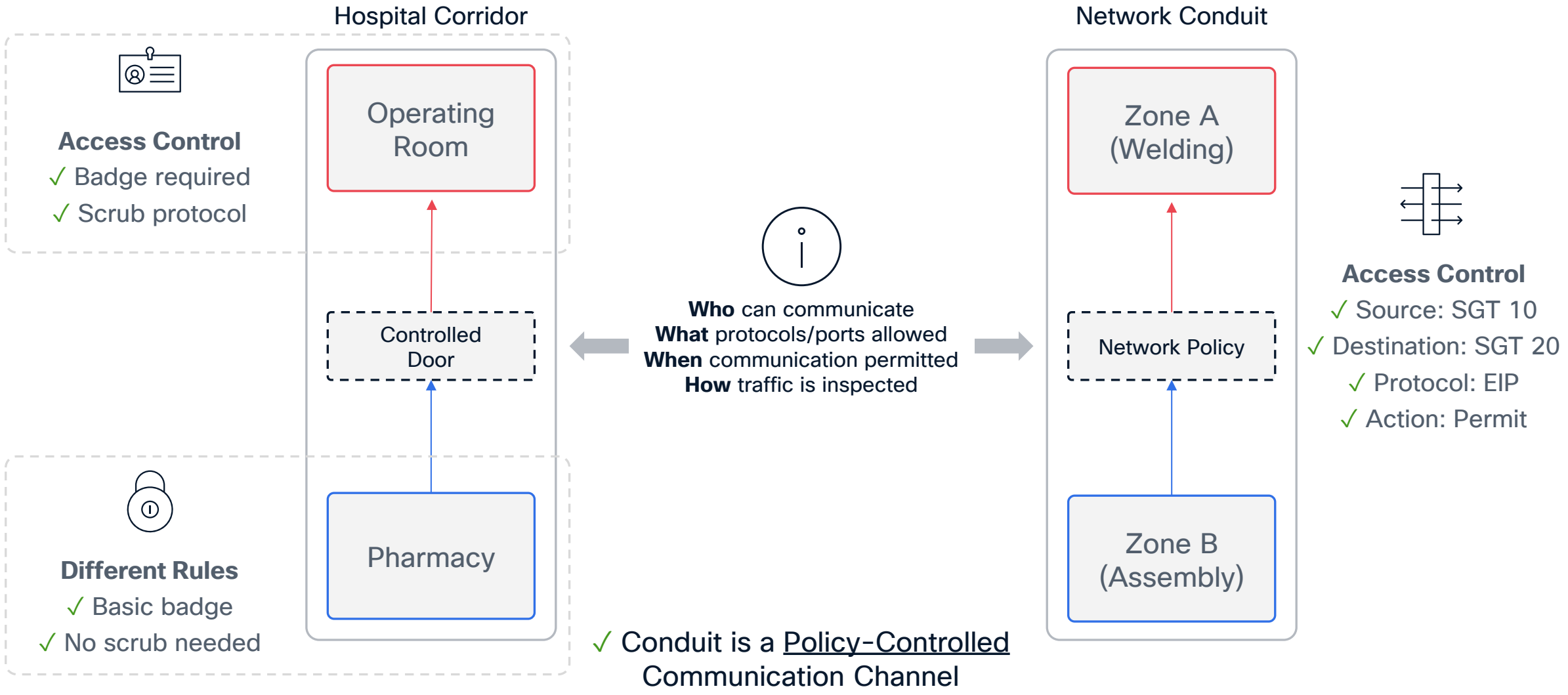
Same Principle in OT Networks

✓ Similar security requirements
✓ Shared risk profile
✓ Common function or location
✓ Defined boundaries

© 2026 Cisco and/or its affiliates. All rights reserved.

Conduits Defined

Conduits Control Communication Between Zones

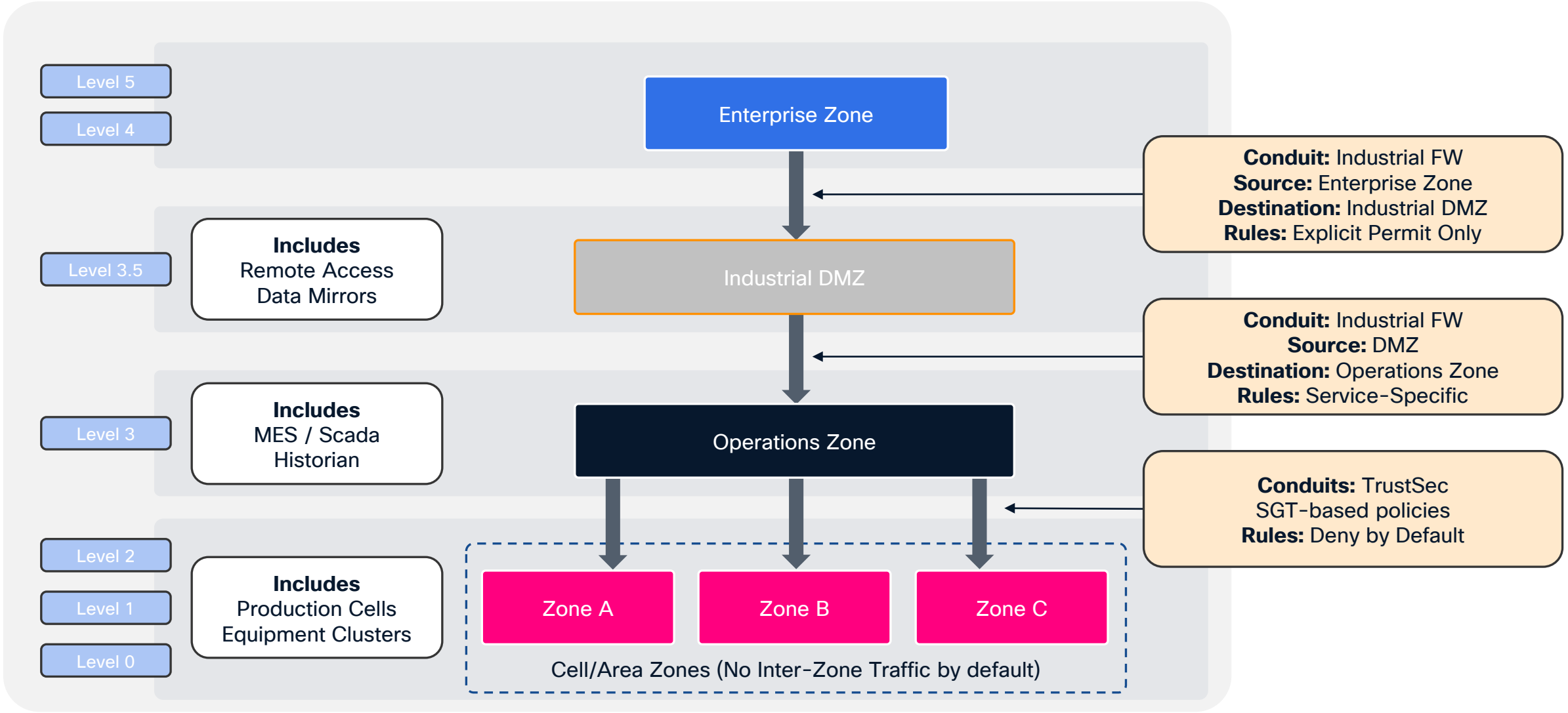


✓ Conduit is a Policy-Controlled Communication Channel

© 2026 Cisco and/or its affiliates. All rights reserved.

Zones & Conduit Model

Segmentation Creates Zones Connected by Controlled Conduits



© 2026 Cisco and/or its affiliates. All rights reserved.

Industrial Traffic Types

For your Reference

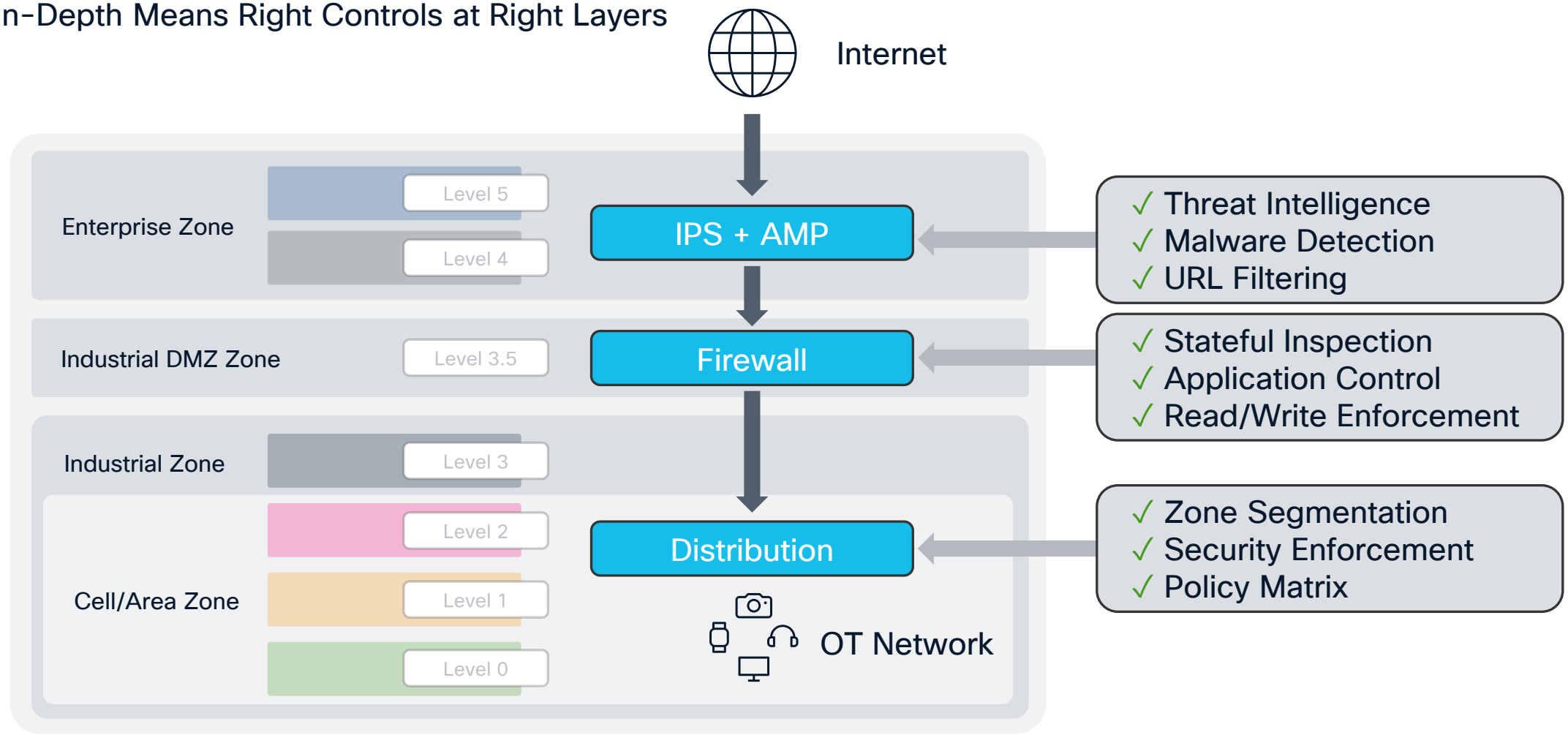
Communication Protocols used within and across Functional Levels

ISA/IEC 62264	To	Level 1	Level 2			Level 3	Level 4
From		Sensors & Actuator Functions	Monitoring Only Functions	Control & Monitoring Functions	Safety Control Functions	Operational Execution Functions	Operational Management Functions
Level 1	Sensors & Actuator Functions	IEC 61784-2 Profinet	N/A	IEC 61784-2 Profinet	IEC 61784-3 Profisafe	N/A	N/A
Level 2	Monitoring Only Functions	IEC 61784-2 Profinet, IEC 20922 MQTT	N/A	IEC 20922 MQTT	N/A	N/A	N/A
	Control & Monitoring Functions	IEC 61784-2 Profinet	N/A	IEC 61784-2 Profinet	IEC 61784-2 Profinet	IEC 62541 OPC UA	N/A
	Safety Control Functions	IEC 61784-3 Profisafe	N/A	N/A	IEC 61784-3 Profisafe	IEC 62541 OPC UA	N/A
Level 3	Operational Execution Functions	IEC 20922 MQTT	IEC 20922 MQTT	IEC 62541 OPC UA	IEC 62541 OPC UA	IEC 19464 AMQP	IEC 19464 AMQP
Level 4	Operational Management Functions	N/A	N/A	N/A	N/A	IEC 19464 AMQP	IEC 19464 AMQP

© 2026 Cisco and/or its affiliates. All rights reserved.

Defense-in-Depth Principles

Defense-in-Depth Means Right Controls at Right Layers



Multiple firewalls doing the same thing

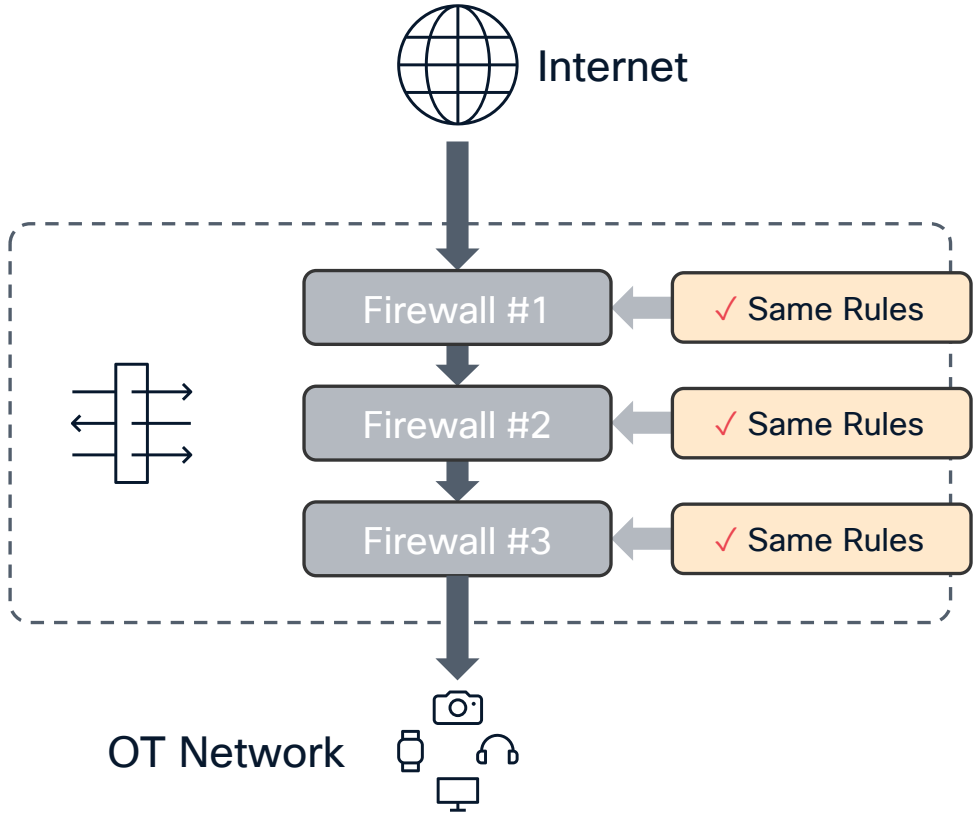
Different technologies, *Different* purposes, *Layered* protection

© 2026 Cisco and/or its affiliates. All rights reserved.

Defense-in-Depth ≠ Firewall Stacking

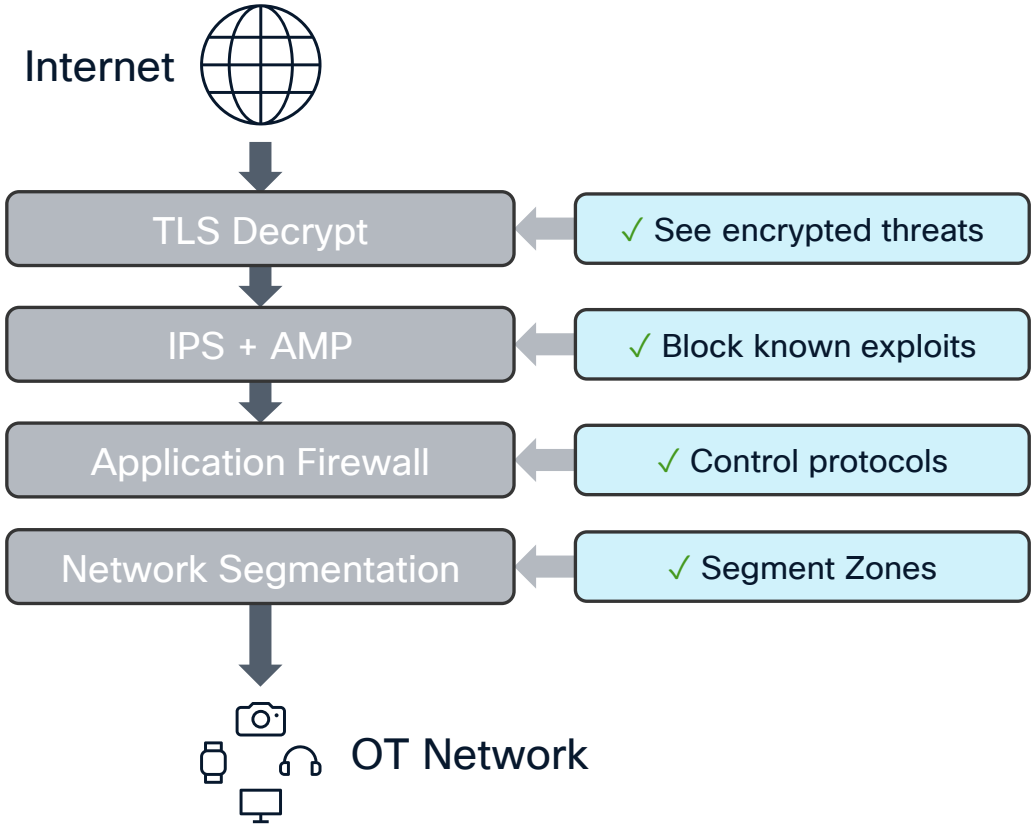
Multiple Firewalls Aren't Always Better Security

Firewall Stacking



Problem
If attacker bypasses one, they bypass all.

Layered Defense

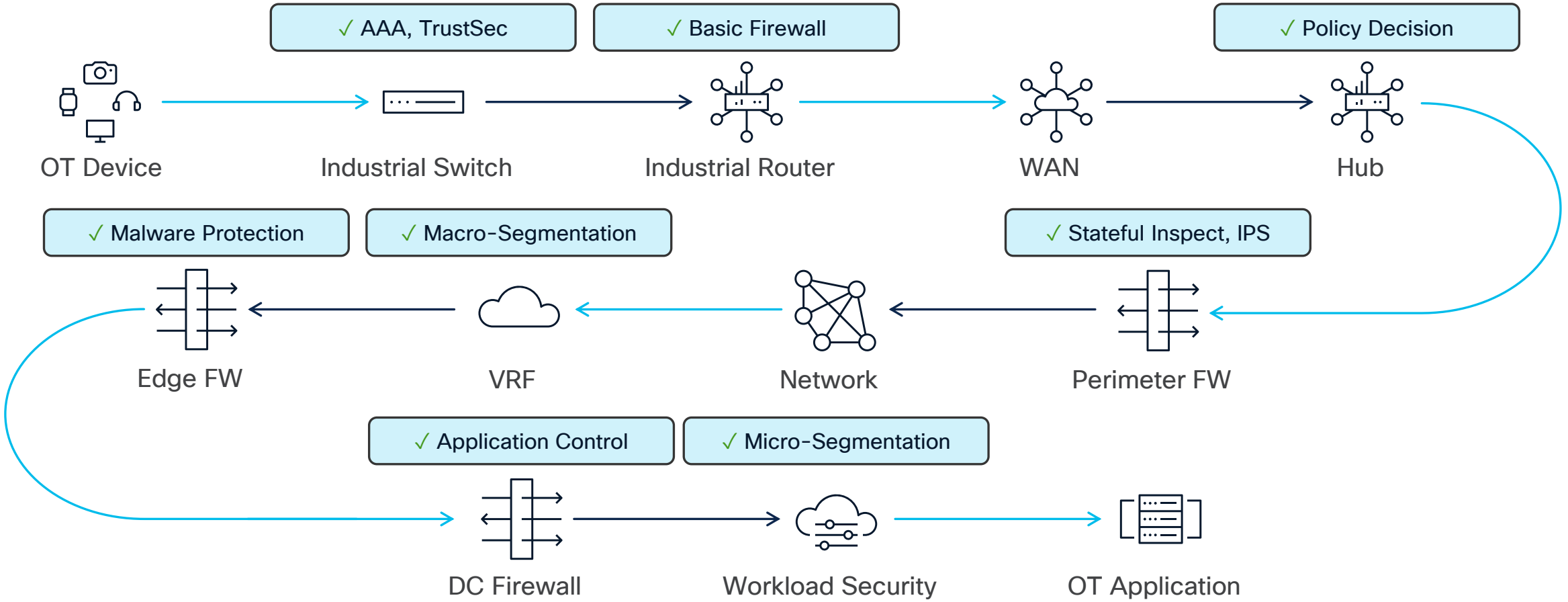


Benefit
Each layer catches different attack types.

© 2026 Cisco and/or its affiliates. All rights reserved.

The Real Defense-in-Depth Stack

Example: Enforcement Points from Field to Data Center

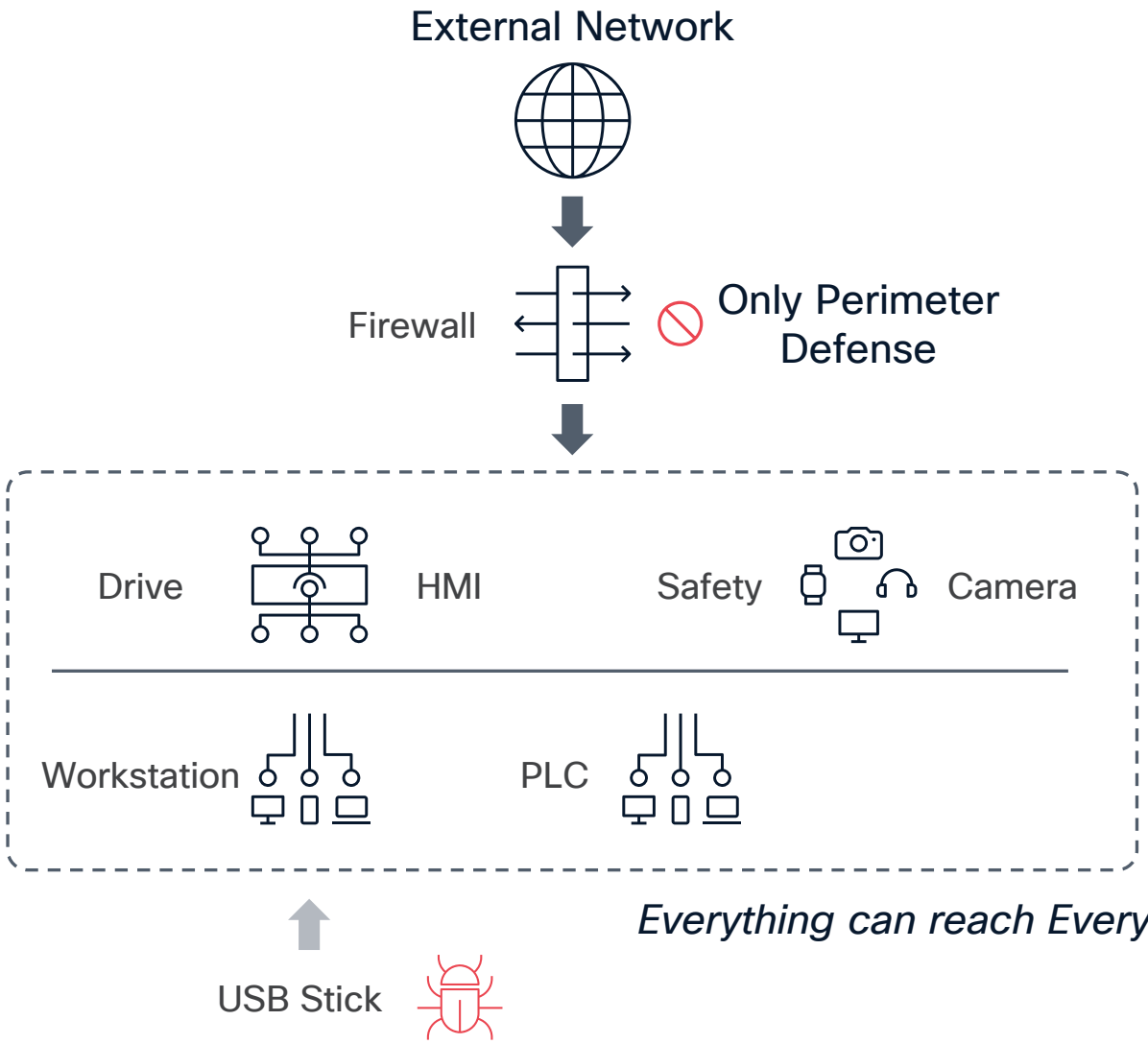


Each hop enforces different policies for different threats.

© 2026 Cisco and/or its affiliates. All rights reserved.

Common Anti-Pattern #1

The Flat Network of Chaos



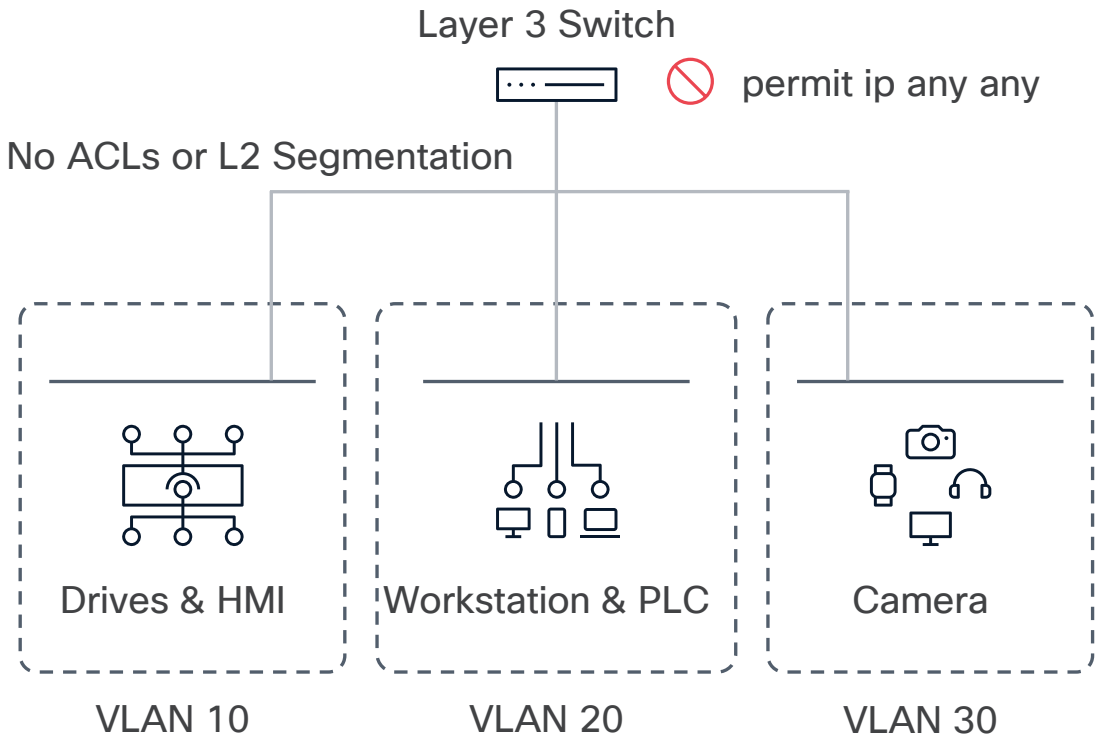
- Single Compromised Device = Full Network Access
- Malware spreads unchecked
- No containment boundaries
- Lateral movement takes minutes

Everything can reach Everything!

© 2026 Cisco and/or its affiliates. All rights reserved.

Common Anti-Pattern #2

VLANs Without Enforcement



Problem
VLANs provides isolation at Layer 2...
But unrestricted routing defects the purpose!

"We have VLANs, so we're secure..."

Reality
VLANs are *just* speed bumps, not roadblocks.

Without routing enforcement malware just take a different path.

© 2026 Cisco and/or its affiliates. All rights reserved.

Common Anti-Pattern #3

Over-Segmentation Without Visibility

Premature Policy Matrix

	A	B	C	D	E	F	…
A	✓	⊘	✓	?	⊘	?	?
B	⊘	✓	?	✓	?	⊘	?
C	✓	?	✓	⊘	?	✓	?
D	?	✓	⊘	✓	?	?	⊘
…	?	?	?	?	?	?	?



Guessing at policies

Breaking legitimate flows

Emergency “permit any” rules

Constant firefighting



“We deployed the segmentation last Friday.

Operations called Monday morning.

Half of our applications stopped working...”

Root Cause

Policy without Visibility

© 2026 Cisco and/or its affiliates. All rights reserved.



Strategic Segmentation transforms Chaos into Controlled, Resilient Operations

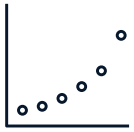
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The Approach

Starts with Comprehensive Documentation and Visibility









Step 1 **Discover**	Step 2 **Baseline**	Step 3 **Zones & Policy**	Step 4 **Enforce**
Identify all Assets and Flows	Collect normal communication patterns	Design segmentation and policy rules based on identified assets	Enable blocking gradually with validation
Cyber Vision Active & *Passive Discovery;* *Interviews*	Validated Profiles; *Recommended* to run over several weeks	Mode **Monitor Only** (log, no block)	Timeline **Zone by Zone**
Result **Profiling & Inventory**	Result **Understand the normal**	Result **Confident Policies**	

✓ Controlled Production Disruptions

✓ Policies match Reality

✓ OT Team Confidence

© 2026 Cisco and/or its affiliates. All rights reserved.

Gaining Visibility

Why Visibility Comes First

Segmentation Without Visibility Causes Operational Chaos

Blind Segmentation

Policy defined Friday afternoon.

Monday Morning

“Half our application stopped working!”

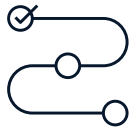
Common Mistakes:

- Blocked interlocked PLCs
- Broke data collection
- Disconnected HMI from Controllers
- Severed MES/TOS connections

Result

Emergency Rollback, lost credibility, wasted effort.

Visibility-Driven Segmentation



Discovery

Map Flows

Segmentation & Policy

Monitor Mode

Enforce

Result

Controlled Production disruptions, confident policies, OT buy-in.

Gartner Finding:

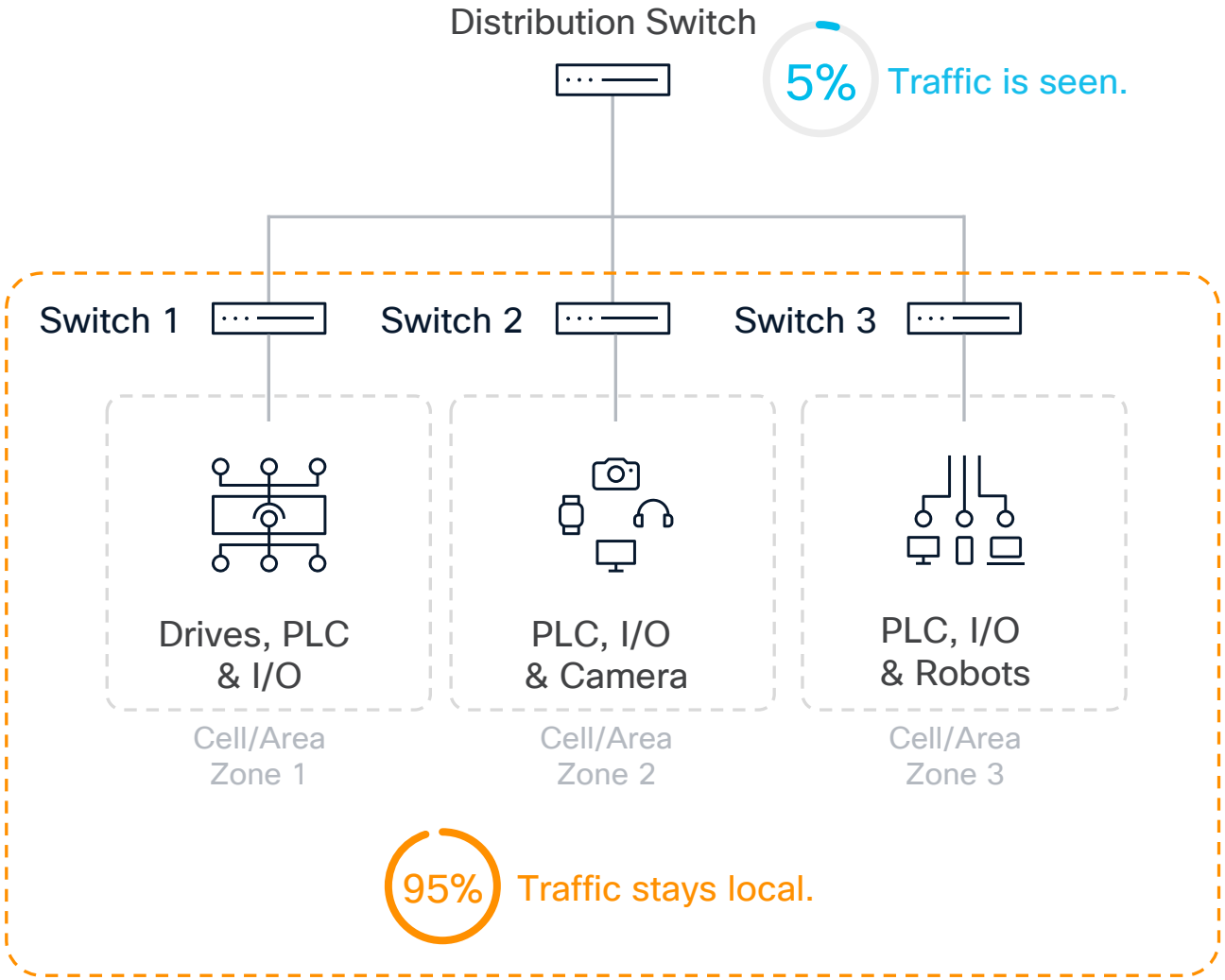
99% of firewall breaches stem from misconfigurations, not flows.

Root Cause: *Deploying policies without understanding the actual traffic flow.*

© 2026 Cisco and/or its affiliates. All rights reserved.

The Visibility Challenge

Most Industrial Traffic Never Reaches Distribution Switches



The Visibility Gap

Traditional Monitoring:

- TAPs on distribution = miss up to 95% of traffic
- Centralized Sensors = can't see intra-zone traffic
- RSPAN = doubles the traffic, can cause jitter

Real Visibility requires:

✓ Sensors at the edge

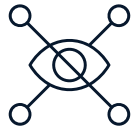
✓ Distributed throughout cell/area zones

✓ Minimal bandwidth overhead

© 2026 Cisco and/or its affiliates. All rights reserved.

Discovery Methods Compared

Passive and Active Discovery Are Complementary Techniques

	 **Passive Discovery**	 **Active Discovery**
How it works?	Listens to network traffic using Deep Packet Inspection	Sends targeted queries using protocol-specific commands
What you discover?	• Active Devices • Communication Flows • Protocols in Use • Some attributes	• Dormant Devices • Firmware Versions • Serial Numbers • Rack Configurations
Pros (advantage)	✓ Zero Risk ✓ See actual behavior ✓ No device change	✓ Complete details ✓ Finds offline/silent devices ✓ On-demand refresh
Cons (disadvantage)	• Devices must be communicating. • Takes time to build complete picture	• Requires careful implementation. • Can't cross NAT without edge sensors.

Best Practice: Use both methods together

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

The NAT Boundary Problem

Centralized Discovery Can't See Through NAT Boundaries

Automotive Manufacturing Example

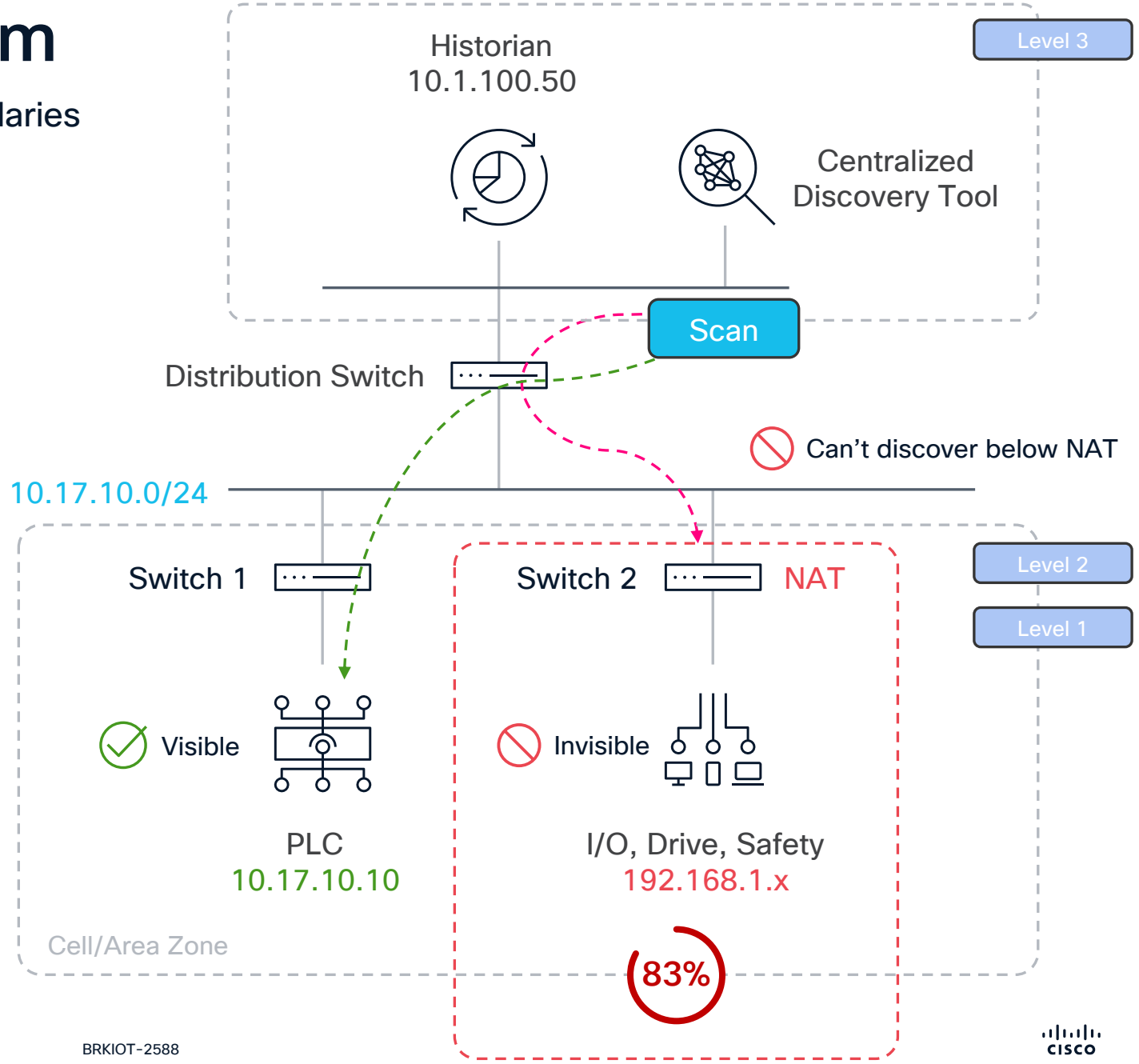
17% of devices have translated IPs

(Visible to central discovery)

83% of devices behind NAT

(Invisible to central discovery)

Devices typically invisible: I/O modules, drives, safety controllers, relays, field instruments, local HMIs

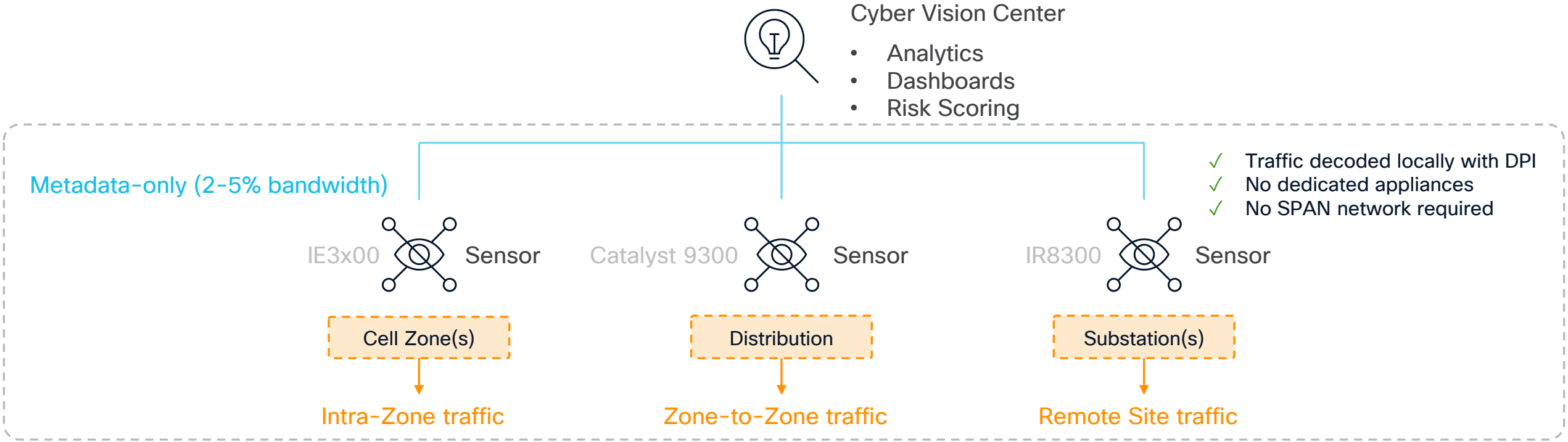


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Cyber Vision Architecture

See BRKIOT-2846
for more on Cisco Cyber Vision

Embed Sensors Where Devices Connect for Complete Visibility



- ✓ Sensors embedded in Switches/Routers (IOx application)
- ✓ 100% visibility – even behind NAT
- ✓ Minimal Bandwidth-only metadata sent
- ✓ No additional hardware – activate a feature
- ✓ Distrusted DPI - scales naturally

Traditional Monitoring is lacking

TAPs on distribution = miss up to 95% of traffic

Centralized Sensors = can't see intra-zone traffic

RSPAN = doubles the traffic, can cause jitter

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Asset Discovery

Complete Asset Inventory with Risk Context

See BRKIOT-2846
for more on Cisco Cyber Vision

Automatic Detection:

- ✓ Vulnerabilities
- ✓ Risk scores
- ✓ Communication patterns
- ✓ Baseline deviations

Cyber Vision Center – Asset Inventory

Total Components: 847 Sensors: 12

High Risk: 23 Medium Risk: 104 Low Risk: 720

Vendor	Count	Vulnerabilities
Rockwell	347	12 High, 34 Med
Siemens	256	8 High, 21 Med
Scheider	198	5 High, 18 Med
Mitsubishi	46	2 High, 7 Med

Top Vulnerabilities (CVEs):

- CVE-2023-1234 (CVSS 9.8) – 23 devices
- CVE-2023-5678 (CVSS 8.1) – 17 devices

Devices communicating with Public IPs: 8

Default Credentials Detected: 12

Cleartext protocols in use: 34

Every Device Detail:

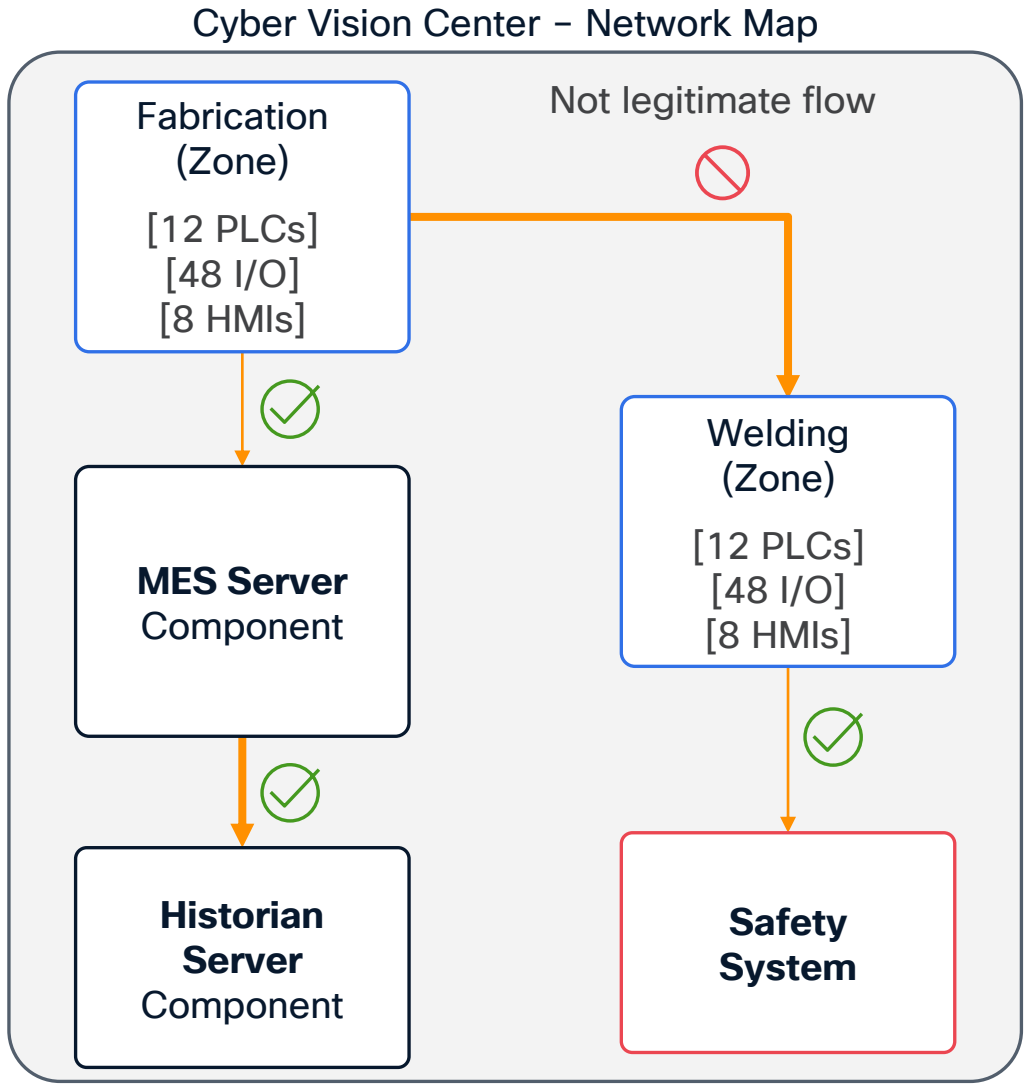
- ✓ Make/Model
- ✓ Firmware version
- ✓ Serial Number
- ✓ Rack slot config
- ✓ Last Activity

© 2026 Cisco and/or its affiliates. All rights reserved.

Network Map & Communication Flows

See BRKIOT-2846
for more on Cisco Cyber Vision

Visualize Communication Patterns to Inform Segmentation Policy



High Traffic volume

Low Traffic Volume

Expected Flow (baseline)

Unexpected Flow (investigate)

Captured Flows (24h period):

- ✓ Intra-Zone: 1.247.890 (94%)
- ✓ Inter-Zone: 78.234 (6%)
- ✓ External: 412 (<1%)
- ⚠ Unexpected: 3 flows flagged

© 2026 Cisco and/or its affiliates. All rights reserved.

Baselines & Monitoring

See BRKIOT-2846
for more on Cisco Cyber Vision

Baselines Define Normal to Detect Anomalies

Baseline Recommendations:
Collect for 2-4 weeks minimum
Include normal *AND* abnormal states
(weekday, weekend, maintenance windows)

Don't baseline public IP traffic
(too dynamic – creates noise)

Create separate baselines for:
Critical Control zones
Safety Systems
High-Value assets

Review deviations with OT team
before assuming they're threats

Week 1-2: Collection Period

Continuous passive monitoring

Capturing: Communication flows, Device behavior & Protocol usage

Baseline saved

Week 3+: Monitoring Mode

Normal Activity	Deviation
PLC → I/O	PLC → ?
Known flow Expected Protocol	New Destination Unexpected Flow
No Alert	Alert Generated

Typical Alerts:
- New devices appeared in zone
- Device communicating with public IP
- Firmware upload detected outside maintenance window
- Protocol change (was Modbus, now HTTPs)
- Communication pattern shift

© 2026 Cisco and/or its affiliates. All rights reserved.



Strategic Segmentation transforms Chaos into Controlled, Resilient Operations

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Implementation Strategies

Technology Selection Matrix

For your Reference

Choose the Right Segmentation Tool for Your Use Case

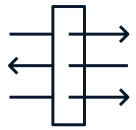
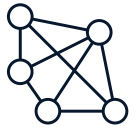
Method	Best Use Case	Complexity	Benefits	Scales to
VLANs + Static ACLs	• Starting Point • 5-10 zones • Legacy Gear • Limited budget • “Need Now”	Low	• Universal • Well-Known approach • Simple to Understand • Low Cost	• ~ 10 zones (max)
Private VLANs	• Intra-Zone isolation • 10-100 devices • Tactical wins • Asset isolation	Low to Medium	• No routing needed • No IP-changes • Wire-Speed performance • Simple-Config	• ~ 10 devices per zone
TrustSec (SGT + SGACL)	• Large Sites or Plants • 10+ zones • Multi-Zone • 100+ Devices • Need to Scale	Medium	• Centralized Policy (ISE) • Full Logging • Policy follows Identity • Updates in Minutes	• 1000+ devices
Firewalls	• Critical Boundaries • Industrial-DMZ • Industrial-DC • Deep inspection	Medium to High	• Deep Packet Inspection • Application Layer Control • Protocol analysis • Virtual Patching	• Boundary Protection

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Phased Deployment Roadmap

Deploy Segmentation in Four Manageable Phases

Week 1-3	Week 3-8	Week 8-16	Week 16-24+
1 Secure the Boundary	2 Gain Visibility	3 Macro-Segmentation	4 Micro-Segmentation
Industrial Firewall 	Cyber Vision 	Zone-to-Zone isolation 	Device-to-Device control 
Establish IT/OT Boundary Controls.	Identify assets, vulnerabilities, communication patterns.	Deploy Zone-to-Zone Isolation	Create Granular Policies <u>within</u> Zone
Stops 80%+ of external threats at the perimeter	Complete Inventory, communication flows & vulnerabilities visibility	90% reduction in lateral movement attack surface	99% attack surface reduction for critical assets

Continuous Monitoring (never stops)

Golden Rules

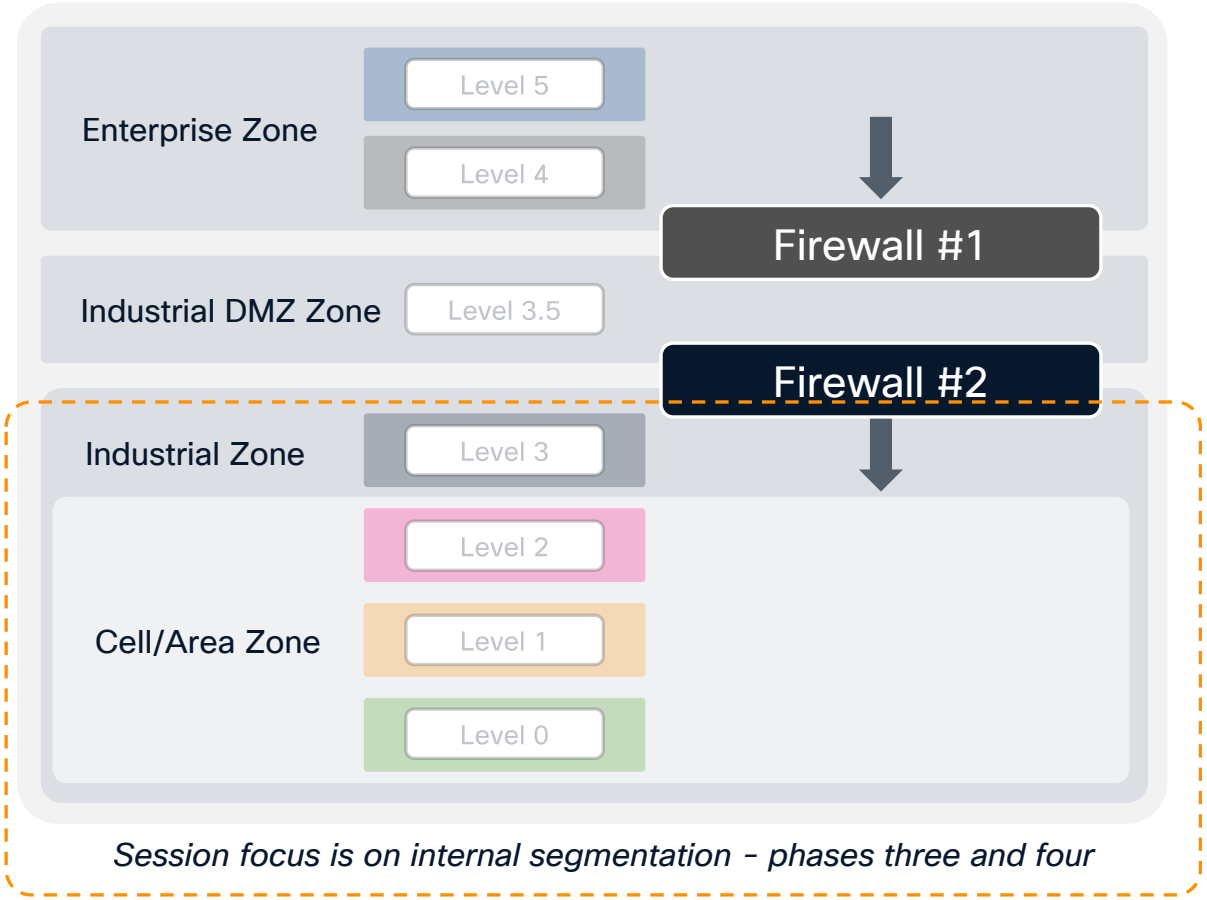
- ✓ Phase 1 & 2 run in <u>Parallel</u>.
- ✓ <u>Always</u> Monitor Mode before Enforce Mode.
- ✓ <u>Get</u> OT Sign-Off at each phase.
- ✓ <u>Can Stop</u> at any phase.
- ✓ <u>Never</u> enforce without observing first.

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Phase 1 – Industrial DMZ Overview

Secure the IT/OT Boundary First



Week 1: Design

- ✓ Document allowed services with OT stakeholders
- ✓ Define applications that cross boundary
- ✓ Create initial firewall rule set

Week 2: Monitor Mode

- ✓ Deploy firewall in logging-only mode
- ✓ Observe traffic patterns
- ✓ Refine rules based on actual traffic

Week 3: Enforcement

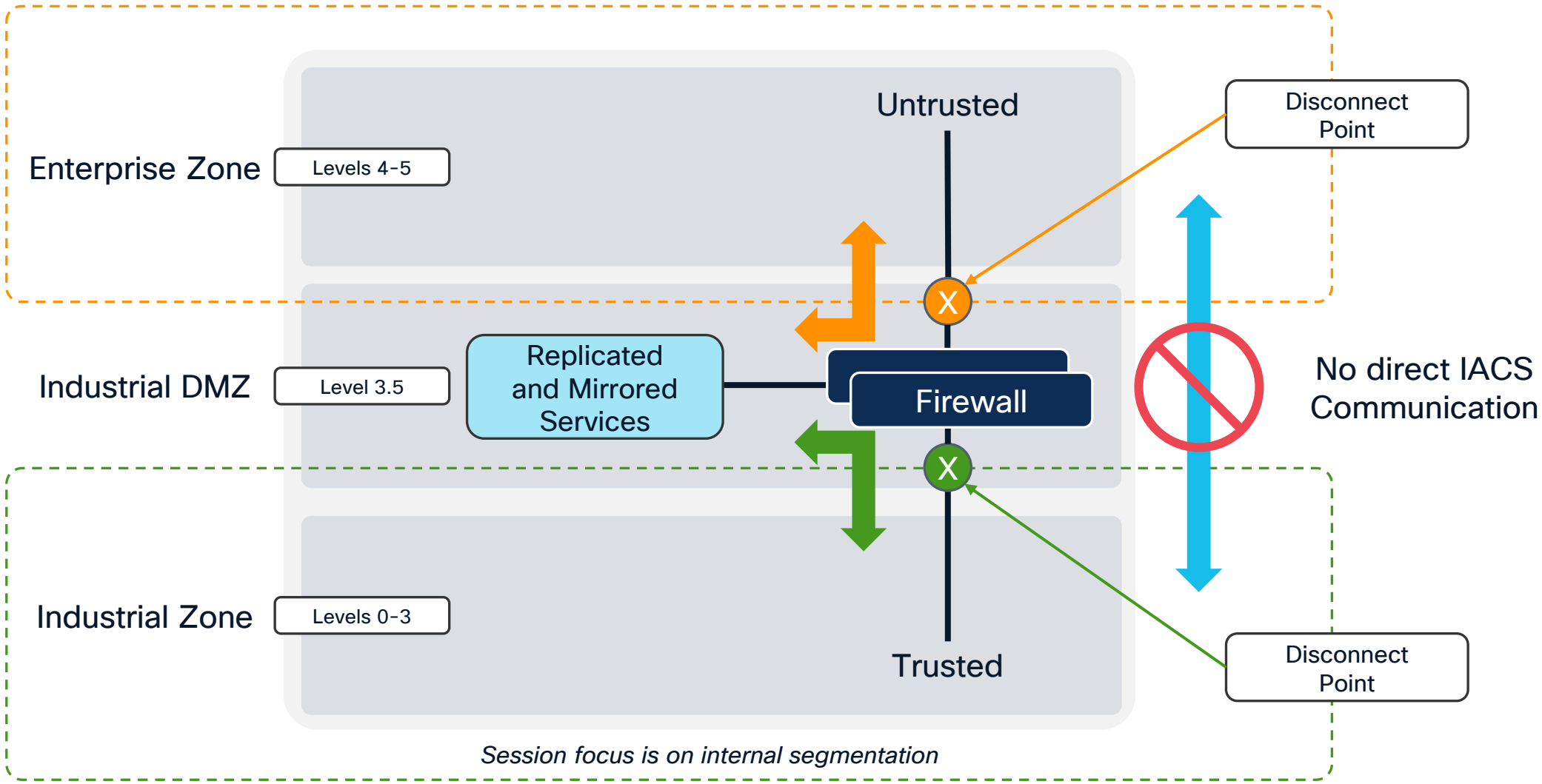
- ✓ Enable blocking after validation
- ✓ Monitor closely for false positives
- ✓ OT hotline on standby

Immediate Benefit: 80%+ of external attack vectors blocked

© 2026 Cisco and/or its affiliates. All rights reserved.

Phase 1 – Industry Best Practices

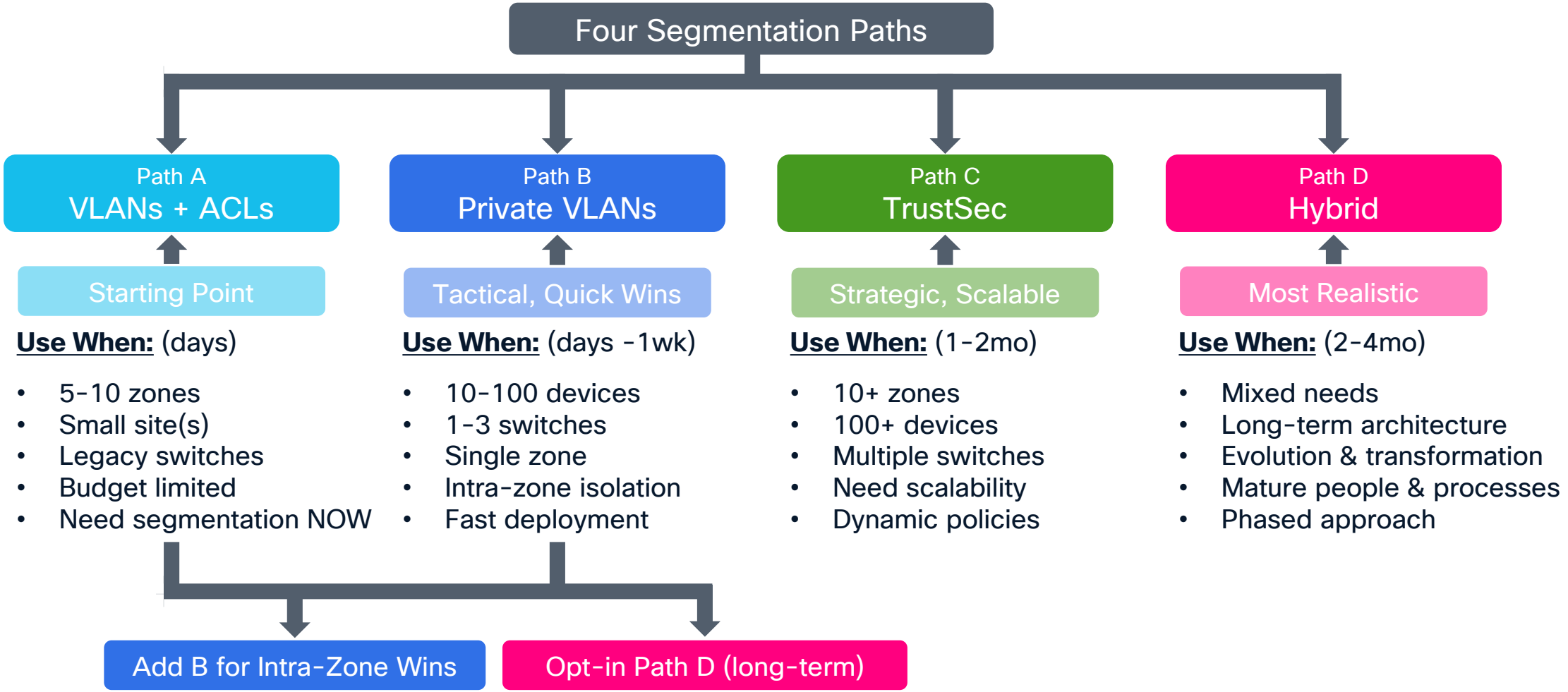
ISA/IEC 62443 Approach – Industrial DMZ



© 2026 Cisco and/or its affiliates. All rights reserved.

Phase 3 and 4 Decision Point

Choose Your Segmentation Path Based on Scale and Needs



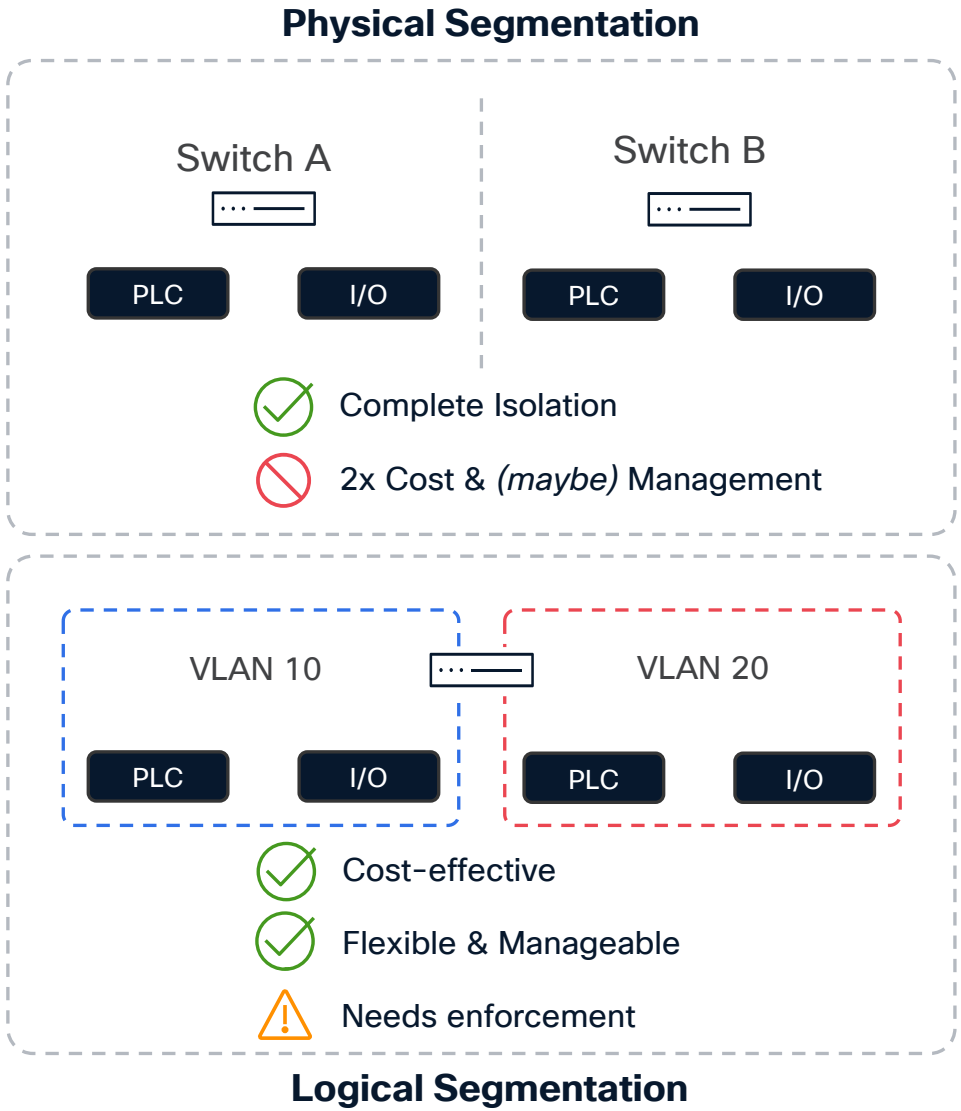
90% of organizations eventually go for Path D (Hybrid)

© 2026 Cisco and/or its affiliates. All rights reserved.

Path A: VLAN + Static ACLs

VLANs (quickly) Explained

Logical Segmentation on Shared Physical Infrastructure



What VLANs Provide:

- Layer 2 isolation
- Separate subnets
- Bandwidth optimization
- Logical grouping

What VLANs don't Provide:

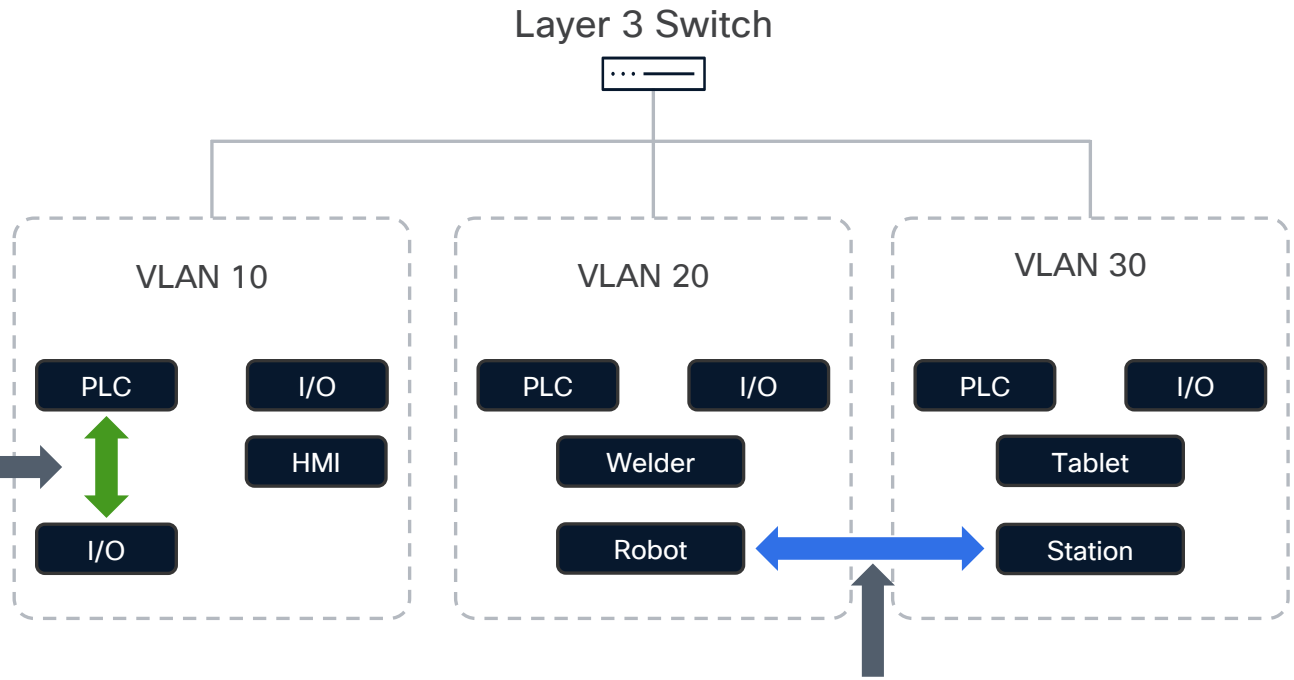
- Routing security
- Inter-VLAN prevention
- Application control
- Automatic policy

A VLAN creates separate broadcast domain on shared infrastructure

© 2026 Cisco and/or its affiliates. All rights reserved.

VLAN Architecture with Routing

VLANs Create Zones, Routing Connects Them



Intra-VLAN (Layer 2)

PLC > I/O

- ✓ Fast, Local
- ✓ No policy needed

Inter-VLAN (Layer 3)

VLAN 20 > Layer-3 > VLAN 30

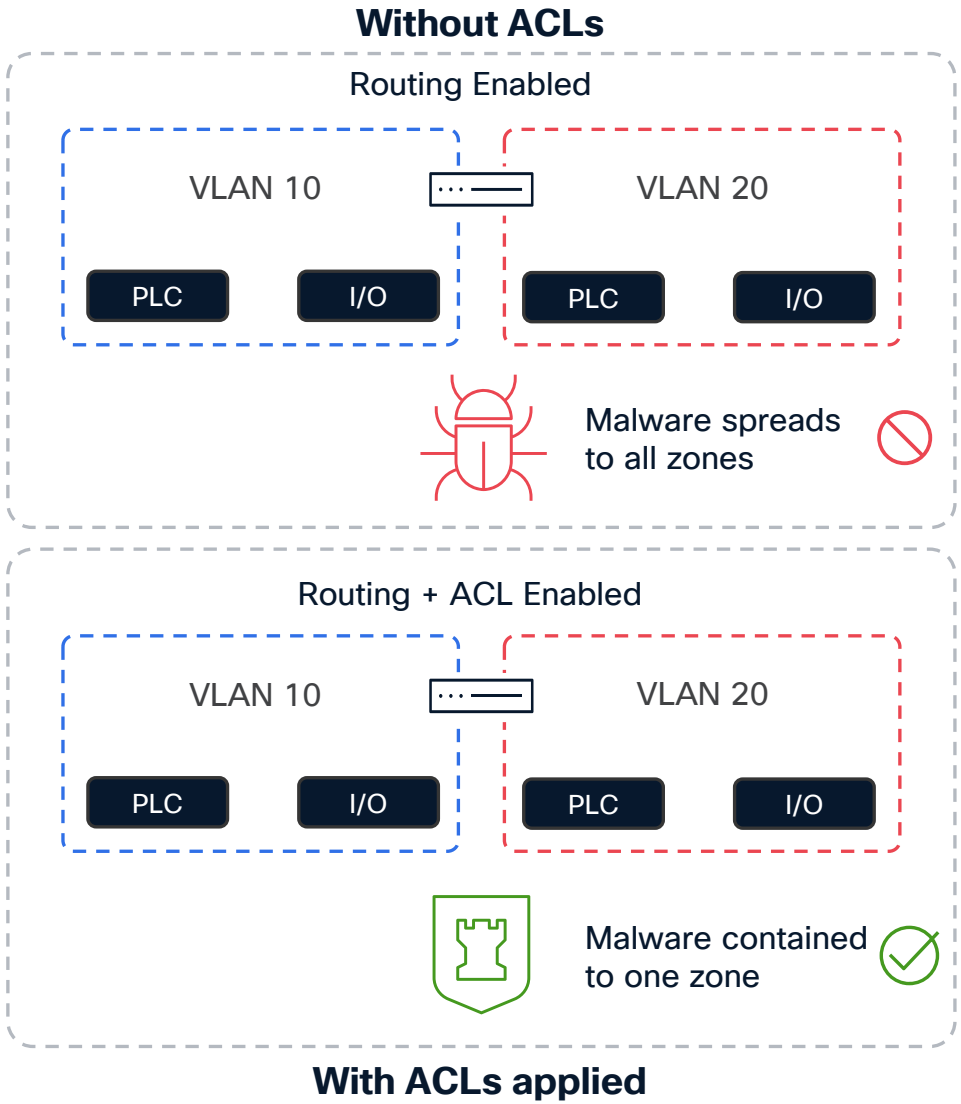
- Without ACLs: Allowed
- With ACLs: Controlled

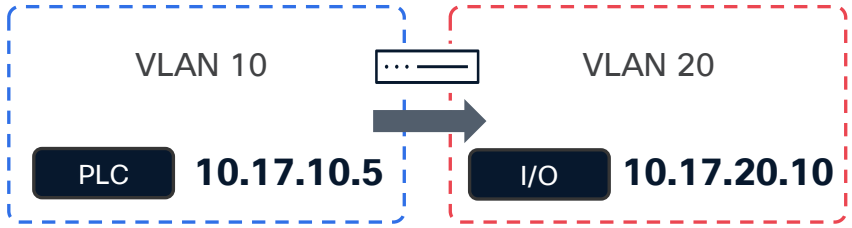
Layer 3 routing between VLANs enables communication between separate VLAN broadcast domains.

© 2026 Cisco and/or its affiliates. All rights reserved.

ACL Enforcement Concept

ACLs Enforce Policy at Layer 3 Boundaries





How an Access-List process Packets:

Example: Packet: 10.17.10.5 > 10.17.20.10

ACL evaluates (top to bottom - always):

Example 1

10: permit specific > Match ✓

20: permit subnet > (not checked)

30: deny any > (not checked)

Example 2

10: permit subnet > Match ✓

20: permit specific > (not checked)

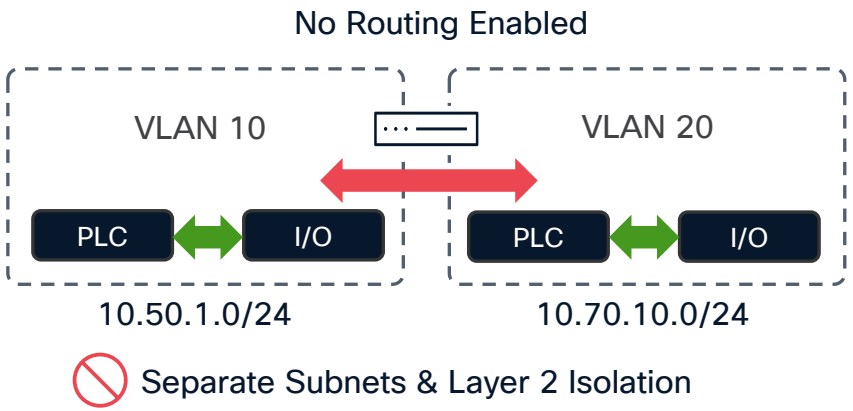
30: deny any > (not checked)

© 2026 Cisco and/or its affiliates. All rights reserved.

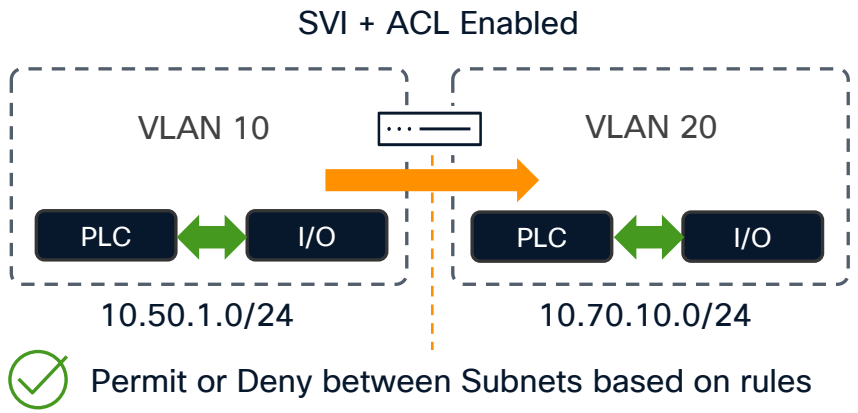
VLANs and Static ACLs – Starting Point

VLANs and ACLs: Foundation for Zone Segmentation

Step 1: VLANs creates Zones



Step 2: ACL Enforce Policy



Pattern: Named ACL

- Permit only what is needed
- Deny rest & Log denies

```
ip access-list extended MAINTENANCE-TO-PRODUCTION
  permit tcp 10.50.1.0 0.0.0.255 10.17.10.0 0.0.0.255 eq 22
  permit tcp 10.50.1.0 0.0.0.255 10.17.10.0 0.0.0.255 eq 443
  deny ip any any log

interface Vlan20
  ip access-group MAINTENANCE-TO-PRODUCTION in
```

© 2026 Cisco and/or its affiliates. All rights reserved.

VLANs and Static ACLs - Limitations

Three Scaling Limitations

⚠ Limitation 1: Management Overhead

- 10 zones = 10 ACLs = 2 hours per policy change
- 20 zones = 20 ACLs = 1 day per policy change

Human error: 10 ACLs = 40% chance of mistakes

⚠ Limitation 2: Location-Based Policies

- ACLs tied to IP address, not device identity
- Device moves → ACL doesn't follow
- Mobile devices (AGVs, tablets) break ACL assumptions

⚠ Limitation 3: Visibility vs. Performance

- No logging = Blind to security events
- Logging = Risk of Switch CPU overhead

Trade-off: Security visibility or network performance

When to migrate to TrustSec?

- ✓ Exceed >10 zones
- ✓ Policy changes takes >1-hour regularly
- ✓ Mobile devices common (AGVs, tablets)
- ✓ Need logging without performance impact
- ✓ Ready for Centralized Policy Management

© 2026 Cisco and/or its affiliates. All rights reserved.

Path B: Private VLANs

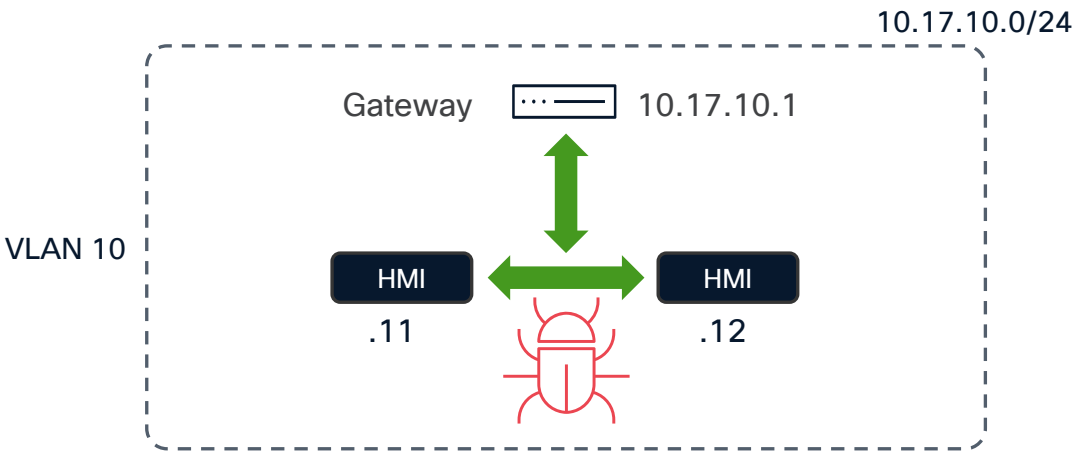
Private VLANs Explained

Subdivide a Single Subnet Without Routing

Key Insight

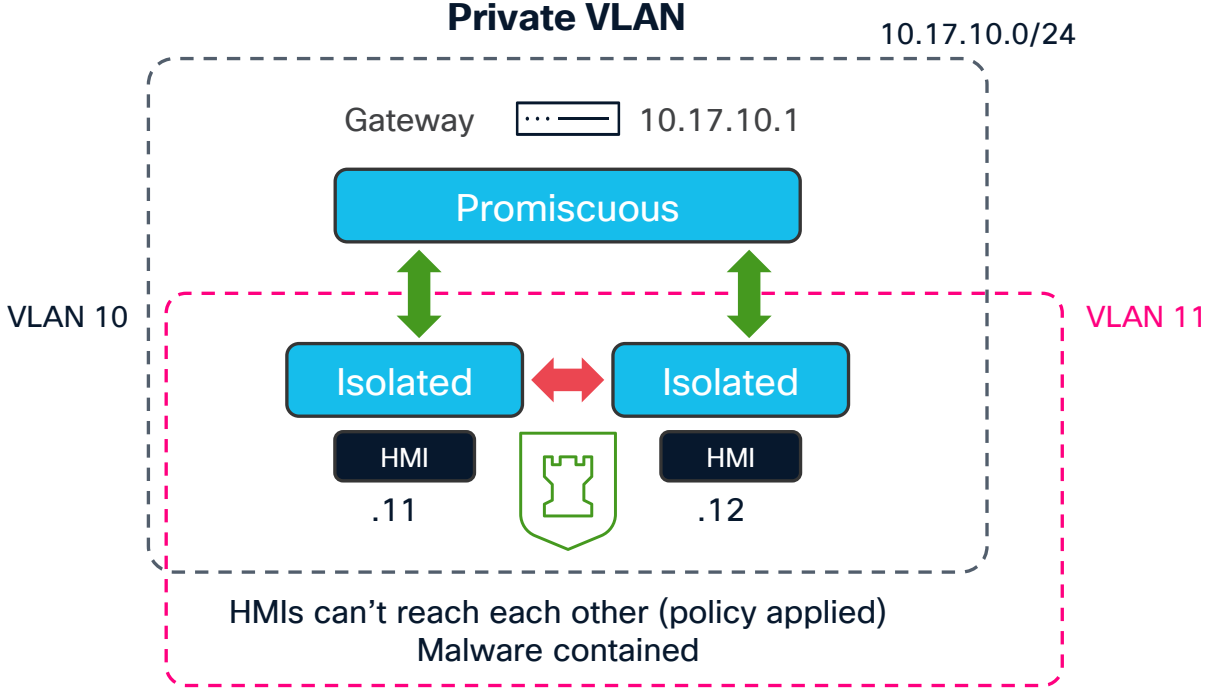
- Same Subnet (10.17.10.0/24)
- Same Gateway (10.17.10.1)
- Isolated at Layer 2 by Switch enforcement

Traditional VLANs



All able to communicate (no policy)
Malware spreads free

Private VLAN



HMIs can't reach each other (policy applied)
Malware contained

Promiscuous
Talks to everyone

Use for:

- Gateways
- Servers
- Monitoring

Isolated
Talks to gateway ONLY

Use for:

- Untrusted devices
- Cameras
- Vendor laptops

Community
Able to talk to "team"

Use for:

- Vendor equipment
- Equipment clusters
- Departmental teams

© 2026 Cisco and/or its affiliates. All rights reserved.

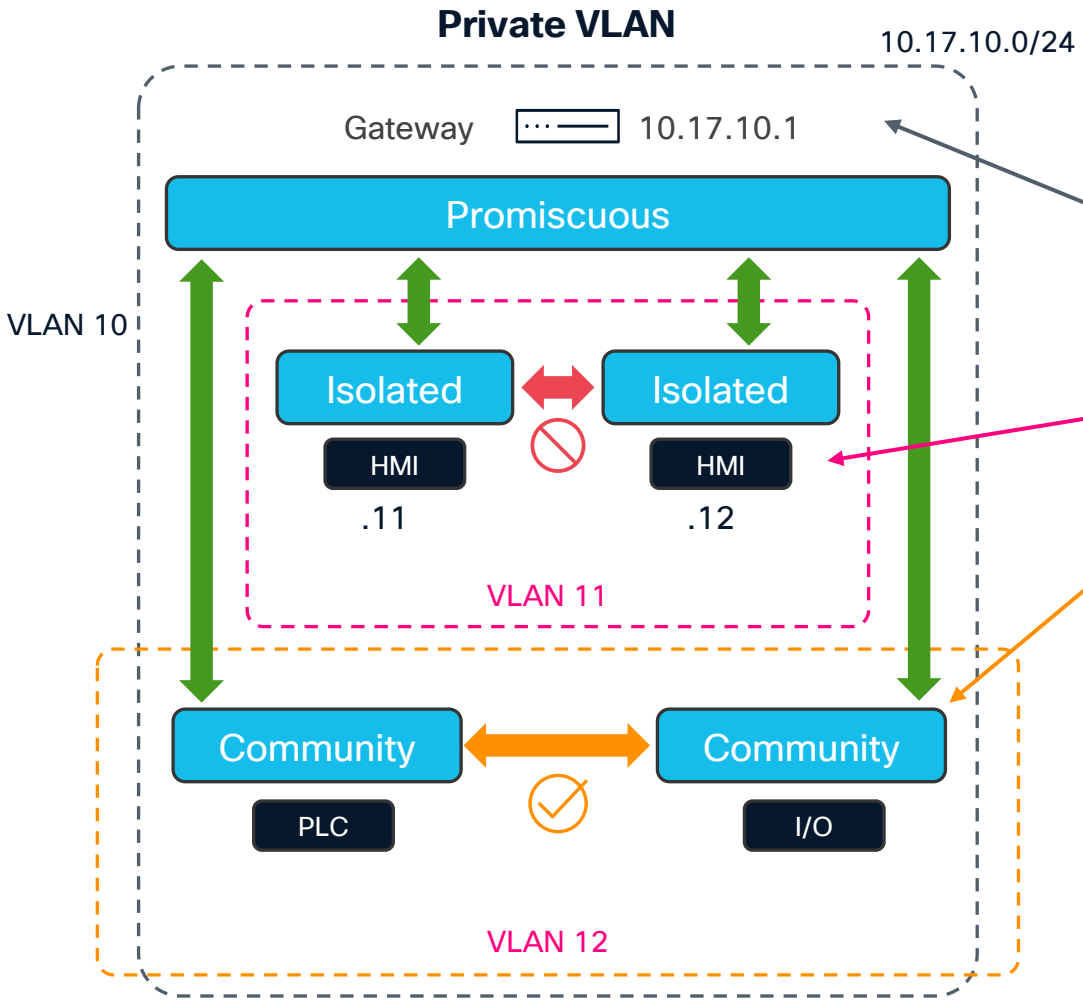
Private VLAN – Starting Point

Quick Intra-Zone Isolation

Promiscuous
Talks to everyone

Isolated
Talks to gateway ONLY

Community
Talks to gateway + “team”




```
vlan 10
  private-vlan primary
  private-vlan association 11

vlan 11
  private-vlan isolated

vlan 12
  private-vlan community

interface Vlan10
  ip address 10.17.10.1 255.255.255.0
  private-vlan mapping 11

interface range GigabitEthernet1/0/1-20
  switchport mode private-vlan [host | community]
  switchport private-vlan host-association 10 [11 | 12]
```

© 2026 Cisco and/or its affiliates. All rights reserved.

Private VLANs – Limitations

Three Limitations to Understand

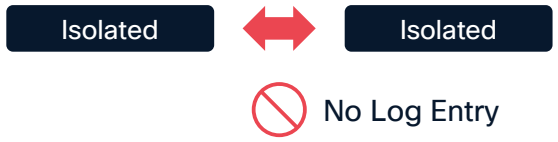
Limitation 1: Usually Single Switch

- Doesn't extend across switches easily



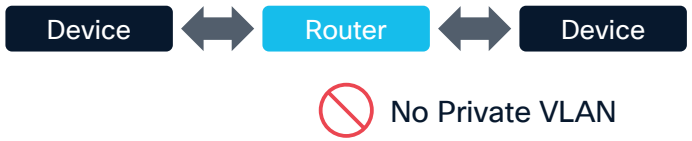
Limitation 2: No Logging of Denied Traffic

- Silent Drops – can't see attempted lateral movement



Limitation 3: Layer 2 Only

- Can't enforce policy across different VLANs



When to use Private VLANs

- 10–100 Devices in a single zone
- 1–3 switches maximum
- Quick tactical Isolation needs
- HMIs, Vendors, Cameras
- Fast Wins

© 2026 Cisco and/or its affiliates. All rights reserved.

Path C: TrustSec

TrustSec – Starting Point

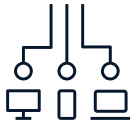
Identity-Based Segmentation at Scale using three steps

See BRKENS-1852 for more on TrustSec find it on the Cisco Live On-Demand Library

Step 1: Classification

Assign Identity Tag to Device

Device



Assigns SGT 10

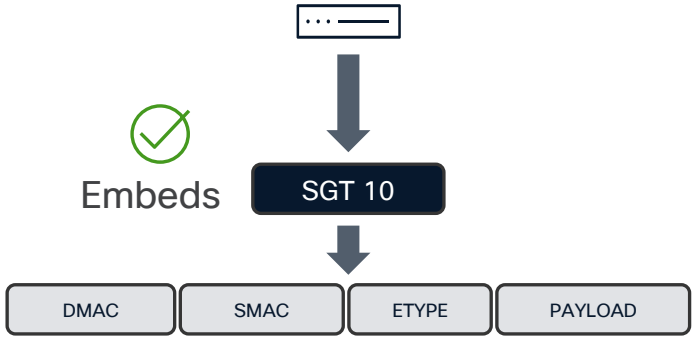
Based on:

- IP address
- Subnet
- VLAN
- ISE Authentication

Step 2: Propagation

Carry Identity Tag Through Network

Access Switch



Methods:

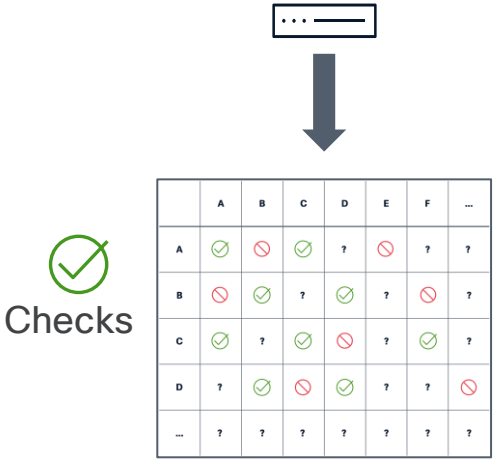
- Inline Tagging
- SXP Protocol

Frame carries:
- Source: SGT 10
- Destination: 10.3.1.5

Step 3: Enforcement

Apply Policy at Boundary

Distribution Switch



Policy Matrix

Decision:
- Source: SGT 10
- Destination: SGT 30
- Action: Permit or Deny

© 2026 Cisco and/or its affiliates. All rights reserved.

TrustSec – Policy Matrix

Define Zone-to-Zone Communication

- Within zone (traffic stays local, not enforced)
- Permitted (explicit SGACL configured)
- Denied (falls to default deny policy)

	Fabrication (10)	**Welding** (20)	**Painting** (30)	**Maintenance** (50)	**Infrastructure** (60)	**...**
Fabrication (10)	-	⊘	⊘	✓	✓	
Welding (20)	⊘	-	⊘	✓	✓	
Painting (30)	⊘	⊘	-	✓	✓	
Maintenance (50)	✓	✓	✓	-	✓	
Infrastructure (60)	✓	✓	✓	✓	-	

Fabrication to Welding: Deny
(no business need)

Maintenance to Fabrication: Permit
(ssh (port 22), https (port 443), deny all else)

Infrastructure to All: Permit
(ntp (port 123), dns (port 53), deny all else)

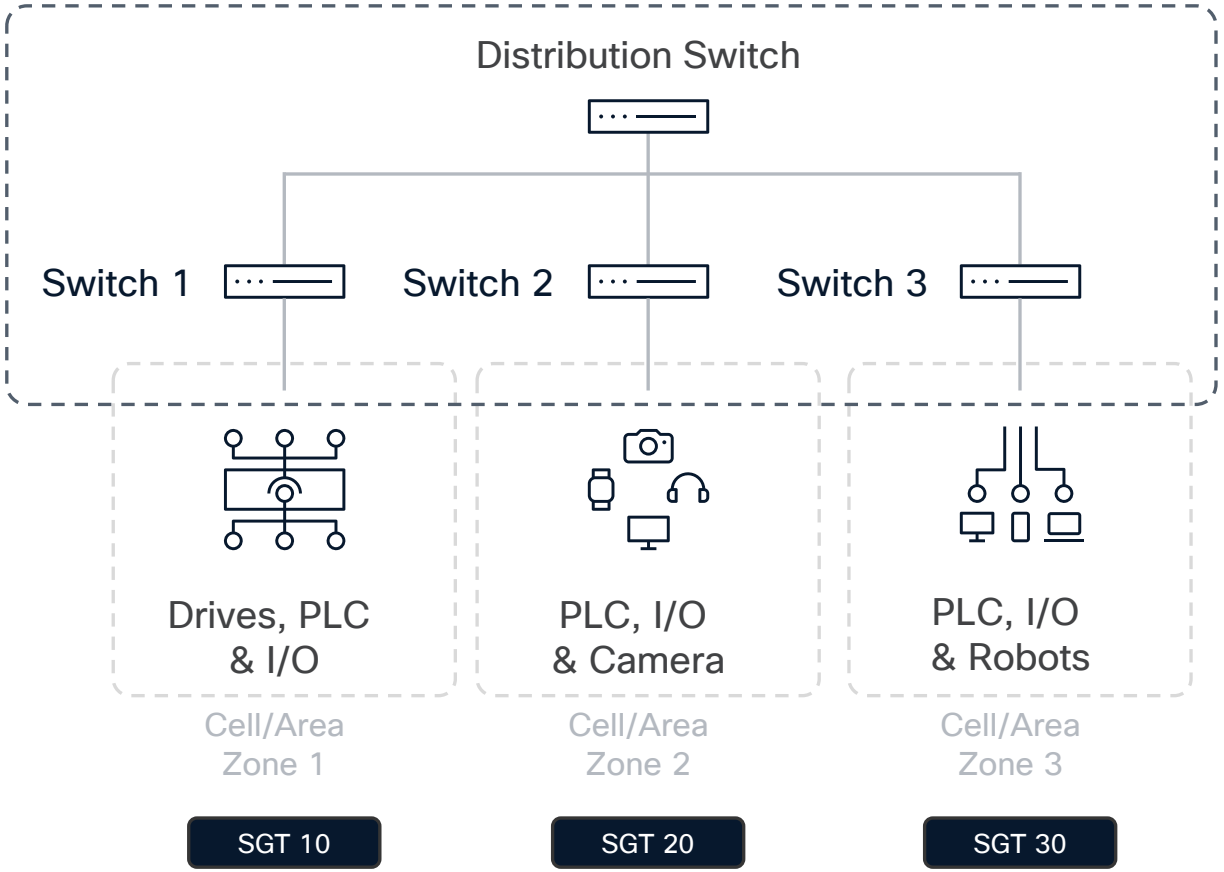
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

TrustSec – Classification

Assign SGTs at TrustSec Domain Ingress

See BRKENS-1852 for more on TrustSec find it on the Cisco Live On-Demand Library



Static (subnet-based)

Based on Source Subnet:

- 10.17.10.0/24 = SGT 10
- 10.17.20.0/24 = SGT 20

✓ Use for Zones
✓ Simple, predictable
✓ No ISE Authentication needed

Dynamic (Identity-based)

Based on Authentication:

- ISE Profiles Device
- Assigns SGT dynamic

✓ Use for Exceptions
✓ Flexible, per-device
✓ Integrate with Cisco Cyber Vision

Static Subnet to SGT Mapping

```
cts role-based sgt-map 10.17.10.0/24 sgt 10

cts role-based sgt-map 10.17.20.0/24 sgt 20

cts role-based sgt-map 10.17.30.0/24 sgt 30
```

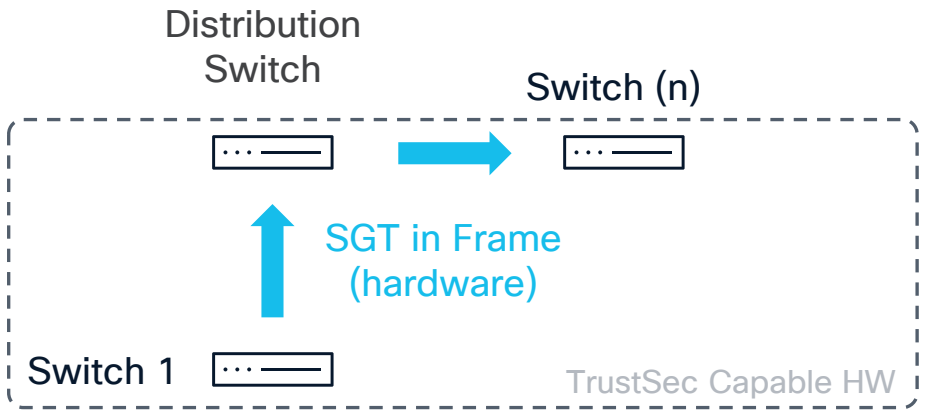
© 2026 Cisco and/or its affiliates. All rights reserved.

TrustSec – Propagation

Ability to carry SGT Through the Network

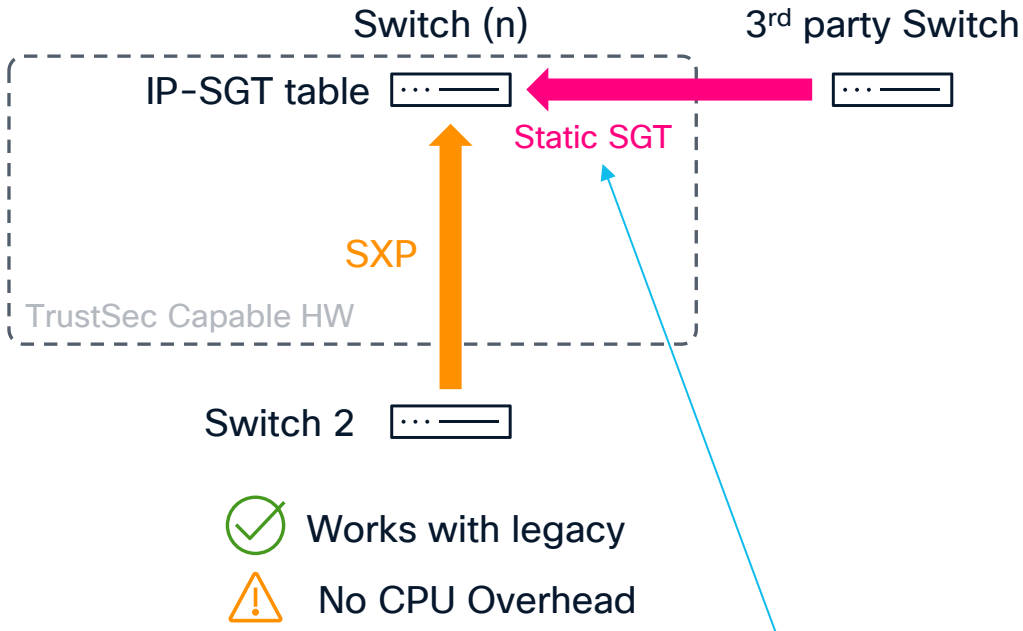
See BRKENS-1852 for more on TrustSec find it on the Cisco Live On-Demand Library

Inline Tagging
(Preferred)



- Line-Rate
- No CPU Overhead

SXP Protocol
(Fallback)



- Works with legacy
- No CPU Overhead

```
interface GigabitEthernet1/3
 cts manual
  policy static [tag]
```

- Inline tagging: Between Core, Distribution & Access
- SXP: Access to Distribution

© 2026 Cisco and/or its affiliates. All rights reserved.

TrustSec – Enforcement

See BRKENS-1852 for more on TrustSec find it on the Cisco Live On-Demand Library

Policy Applied at Zone Boundaries

⚠ **Do NOT enable enforcement until:**

- ✓ 2+ weeks of Visibility data collected
- ✓ Monitor Mode validated with OT Team
- ✓ Rollback Plan Prepared

```
! STEP 1: Enable enforcement globally
cts role-based enforcement

! STEP 2: Specify which VLANs to enforce
cts role-based enforcement vlan-list 10,20,30

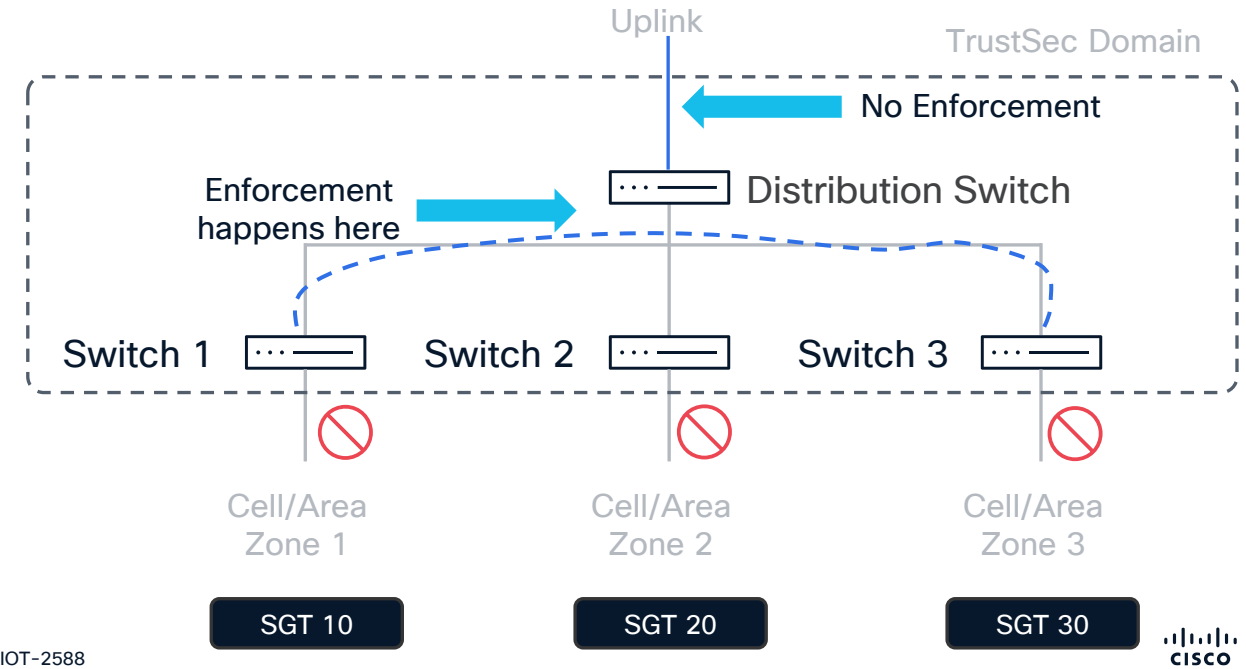
! STEP 3: Disable on uplinks (CRITICAL!)
interface TenGigabitEthernet1/1/1
 description Uplink to Core
 cts manual
  policy static [tag] trusted
 no cts role-based enforcement
 ! Don't block northbound traffic

! STEP 4: Monitor mode first
cts role-based monitor all
 ! Logs matches, doesn't block
 ! Then remove command for full enforcement
```

PACKET FLOW TRACE

Device in Zone 1 tries to reach Zone 2:

- Packet leaves Zone 1 (**source**: 10.17.10.5, **destination**: 10.17.20.3)
- Enters Access Switch 1, gets classified: Source SGT = **10**
- Reaches Distribution Switch, classified as Source SGT = **10**
- Distribution Switch determines destination is in 10.17.20.0/24 = SGT **20**
- Checks matrix: SGT **10** → SGT **20** = ?
- Policy says: DENY
- Packet dropped at Egress, Syslog Created



© 2026 Cisco and/or its affiliates. All rights reserved.

TrustSec – Deployment Guidance

Critical Gotchas and Best Practices

See BRKENS-1852 for more on TrustSec find it on the Cisco Live On-Demand Library

Fallback SGACL in the event of ISE communication is Lost

```
ip access-list role-based FALLBACK
 permit ip

cts role-based permissions from 10 to 10 FALLBACK
```

✓ Start with static subnet-to-SGT (*simpler*)

✓ Use Monitor Mode before enforcement (*always*)

✓ Disable Enforcement on Uplinks (*critical*)

✓ Tag Infrastructure services (*don't forget*)

✓ Test failover scenarios (*ring reconvergence*)

✓ Have rollback plan (*know how to disable quickly*)

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco



Strategic Segmentation transforms Chaos into Controlled, Resilient Operations

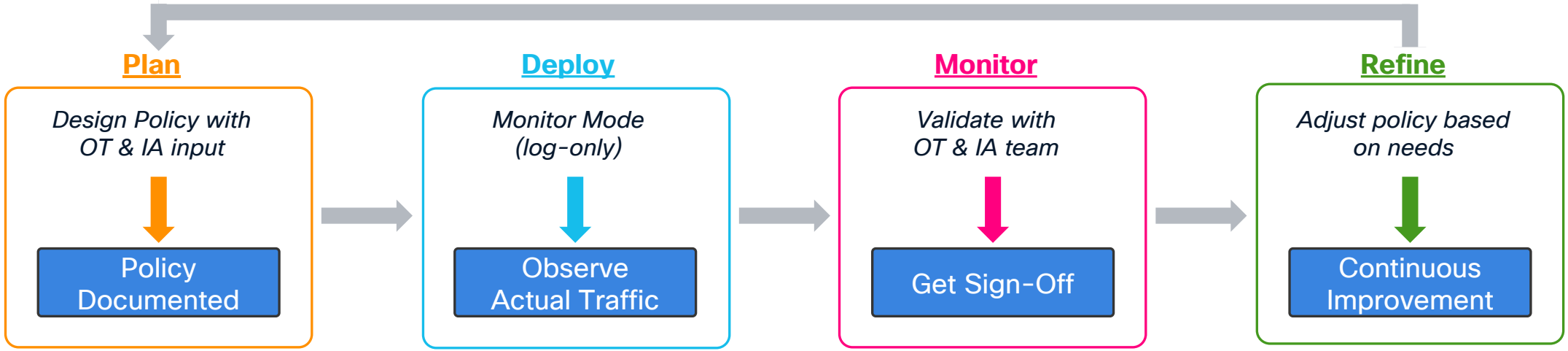
© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Operational Excellence

Policy Lifecycle Management

Segmentation Is a Continuous Process, Not a One-Time Project



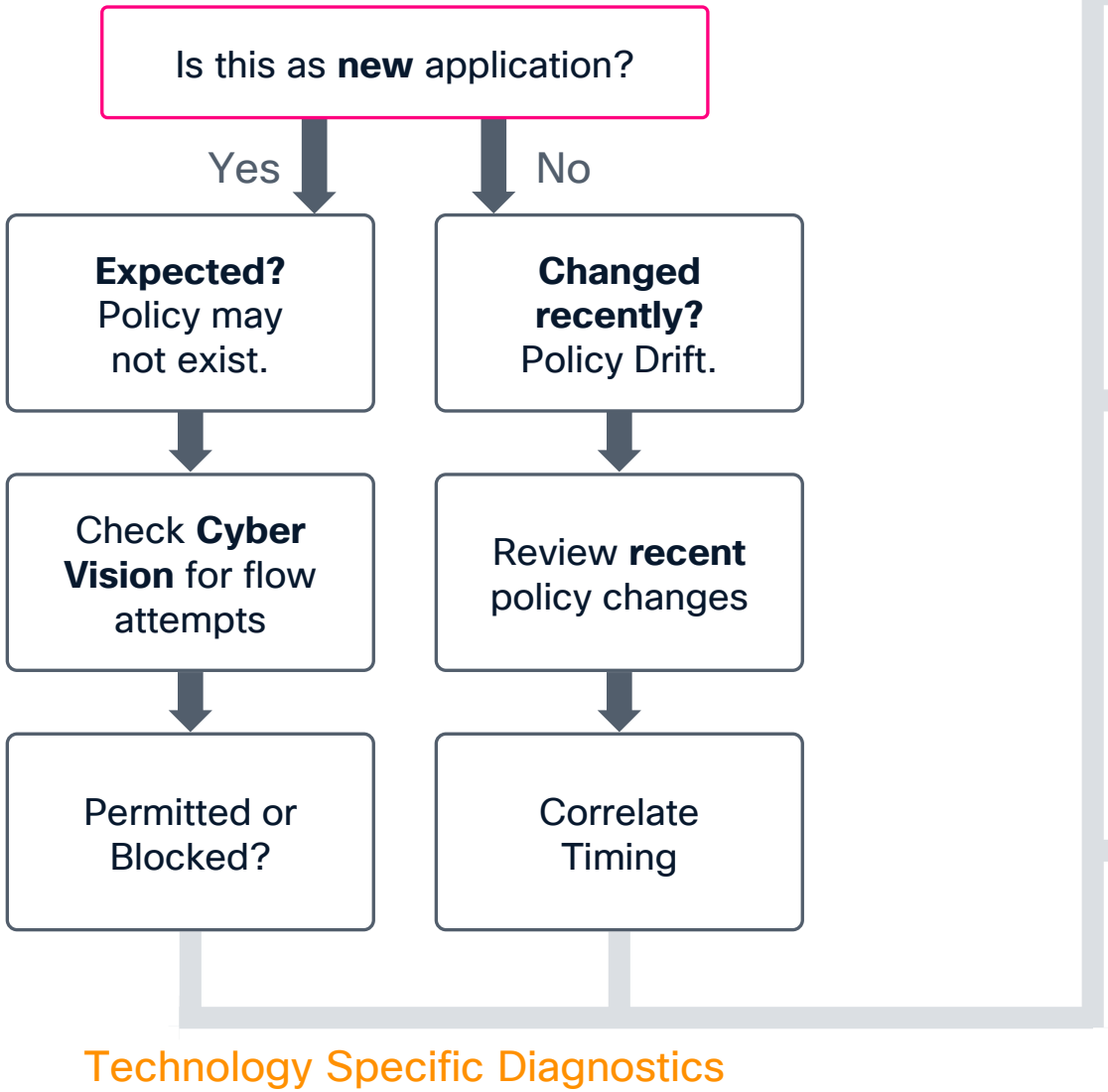
- ✓ Document all policy changes (change log)
- ✓ Require business justification (why is this needed?)
- ✓ Test in lab or non-production first
- ✓ Deploy in monitor mode before enforcement
- ✓ Review deny logs weekly (security posture)
- ✓ Quarterly policy review (remove unused rules)

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Troubleshooting Workflow

Systematic Troubleshooting Prevents Firefighting



Using VLAN + Static ACLs?

1. Check ACL hit-counters
2. Review Syslog for denies
3. Verify ACL is applied to interface
4. Check ACL sequence order

Using Private VLANs?

1. Verify Private VLAN Configuration
2. Check Port-Type (Isolated/Community)
3. Verify Promiscuous Port Configuration
4. Check if VLANs are on trunk (using multi-switch)

Using TrustSec?

1. Check SGT Assignment (source)
2. Check destination SGT mapping
3. Verify Policy Matrix entry
4. Check SGACL enforcement enabled
5. Review SGACL counters and Syslog for denies

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Measuring Success

Track Metrics to Prove Segmentation Value

	Before Segmentation	After Segmentation	Target
Attack Surface	All 400+ devices reachable	<20 devices per zone	Isolate critical assets
Incident Containment	48+ hours	4-6 hours	<8 hours
Lateral Movement	Unlimited	Zone-Contained	90%+ reduction
Policy Change Time	2-3 days (ACL)	30 minutes (TrustSec)	<1 hour
Compliance Audit	Manual Evidence Gathering	Automated Logging	Full Audit Trail

Typical Ransomware/Malware Incident



Without Segmentation:
Single breach → plant-wide spread
All production zones at risk
Extended recovery time



With Segmentation:
Breach contained to single zone
Other zones continue production
Faster isolation and remediation

Result: Business continuity + reduced risk

© 2026 Cisco and/or its affiliates. All rights reserved.

Agenda Recap

Four Essential Steps to Transform Network Chaos into Control

01 **Understanding the Framework**

ISA/IEC 62443 zones & conduits

Defense-in-Depth

Common Anti-Patterns to avoid

02 **Gaining Visibility**

Why Visibility must come first

Passive & Active discovery

Cyber Vision Architecture

Baselines for detecting anomalies

03 **Implementation Strategies**

Four technology paths

- VLANs + Static ACLs (foundation)
- Private VLANs (tactical wins)
- TrustSec (strategic scale)
- Firewall (critical boundaries)

Phased deployment roadmap

Gotchas and Best Practice

04 **Operational Excellence**

Policy Lifecycle Management

Troubleshooting Workflow

Metrics to prove Success

Continuous Improvement

© 2026 Cisco and/or its affiliates. All rights reserved.

cisco

Webex App

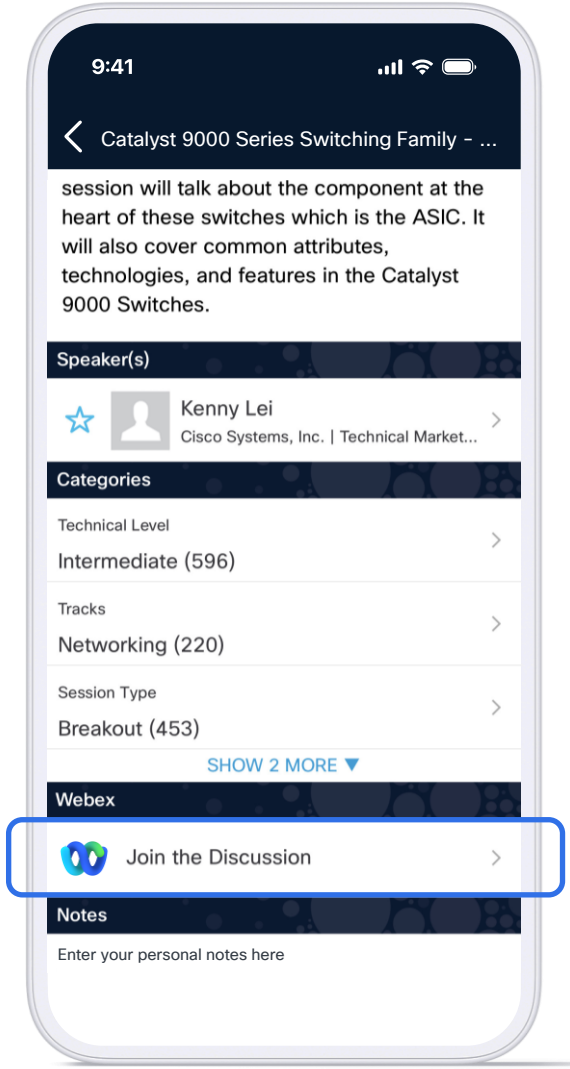
Questions?

Use Webex App to chat with the speakers after the session

How

1. Find this session in the Cisco Events 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 February 27, 2026.



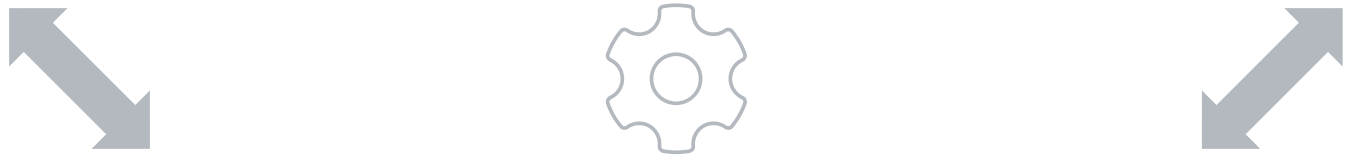
© 2026 Cisco and/or its affiliates. All rights reserved.

Next Steps

Your Segmentation Journey Starts Today

If you are a Network Engineer/Architect
✓ Deploy Visibility in OT
✓ Design Segmentation Policies
✓ Implement Monitor Mode validation

If you are a Security Engineer/Architect
✓ Define Zone Security Policies
✓ Design Policy Matrix with OT input
✓ Establish Continuous Monitoring



If you are an OT Manager
✓ Identify Critical Zones to Protect
✓ Collaborate on Policy Validation
✓ Approve Enforcement Deployment

All Roles: Start conversations *NEXT WEEK*

© 2026 Cisco and/or its affiliates. All rights reserved.

Complete your session surveys



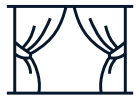
Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

© 2026 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



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



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

© 2026 Cisco and/or its affiliates. All rights reserved.

Thank you

cisco Live !


CISCO