

CISCO *Live!*



#CiscoLive



The bridge to possible

Real-World Industrial IoT SD-Access Deployment Use Cases

Lawrence Zhu, Solutions Architect
BRKIOT-2083



#CiscoLive

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://cicolive.ciscoevents.com/cicolivebot/#BRKIOT-2083>



Agenda

- Industrial IoT use case requirements
- Design and key components
- Solution implementation
- Challenges and solutions

Industrial IoT Use Case Requirements

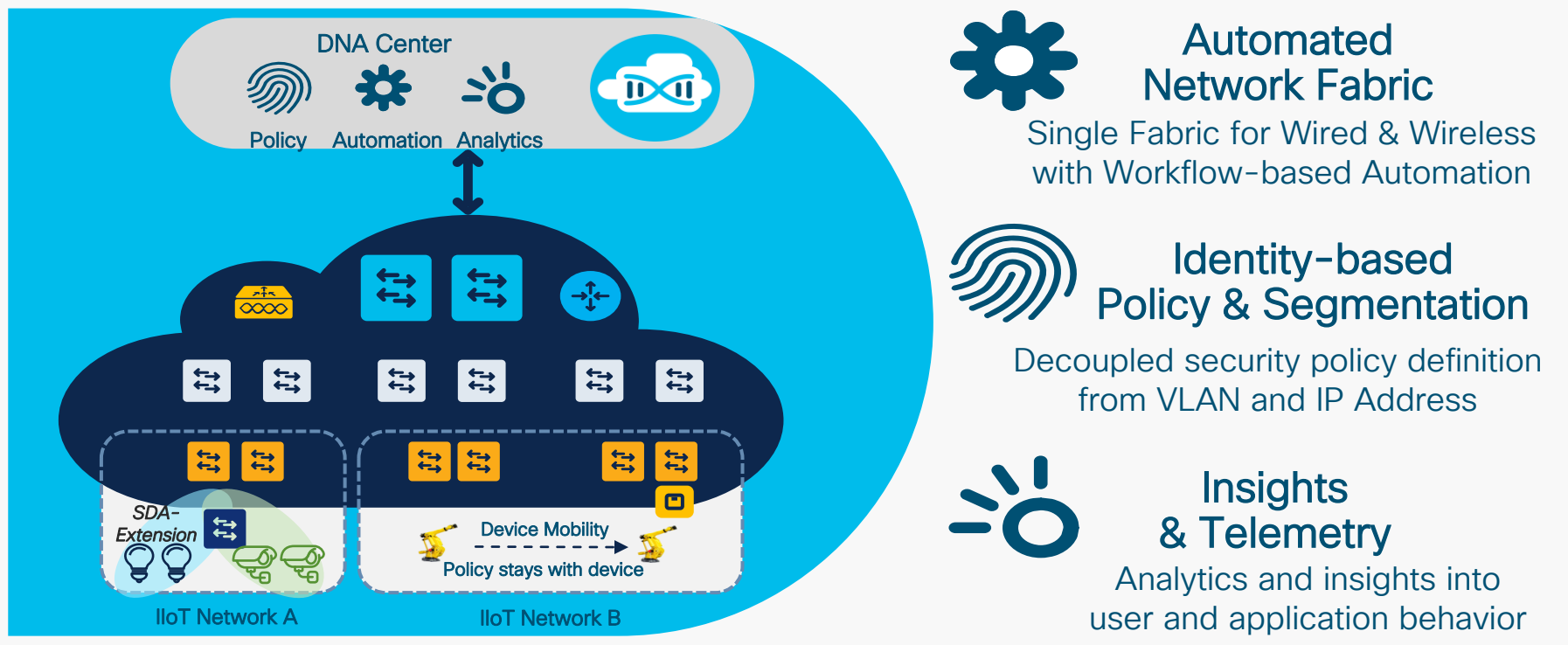
Business Drivers

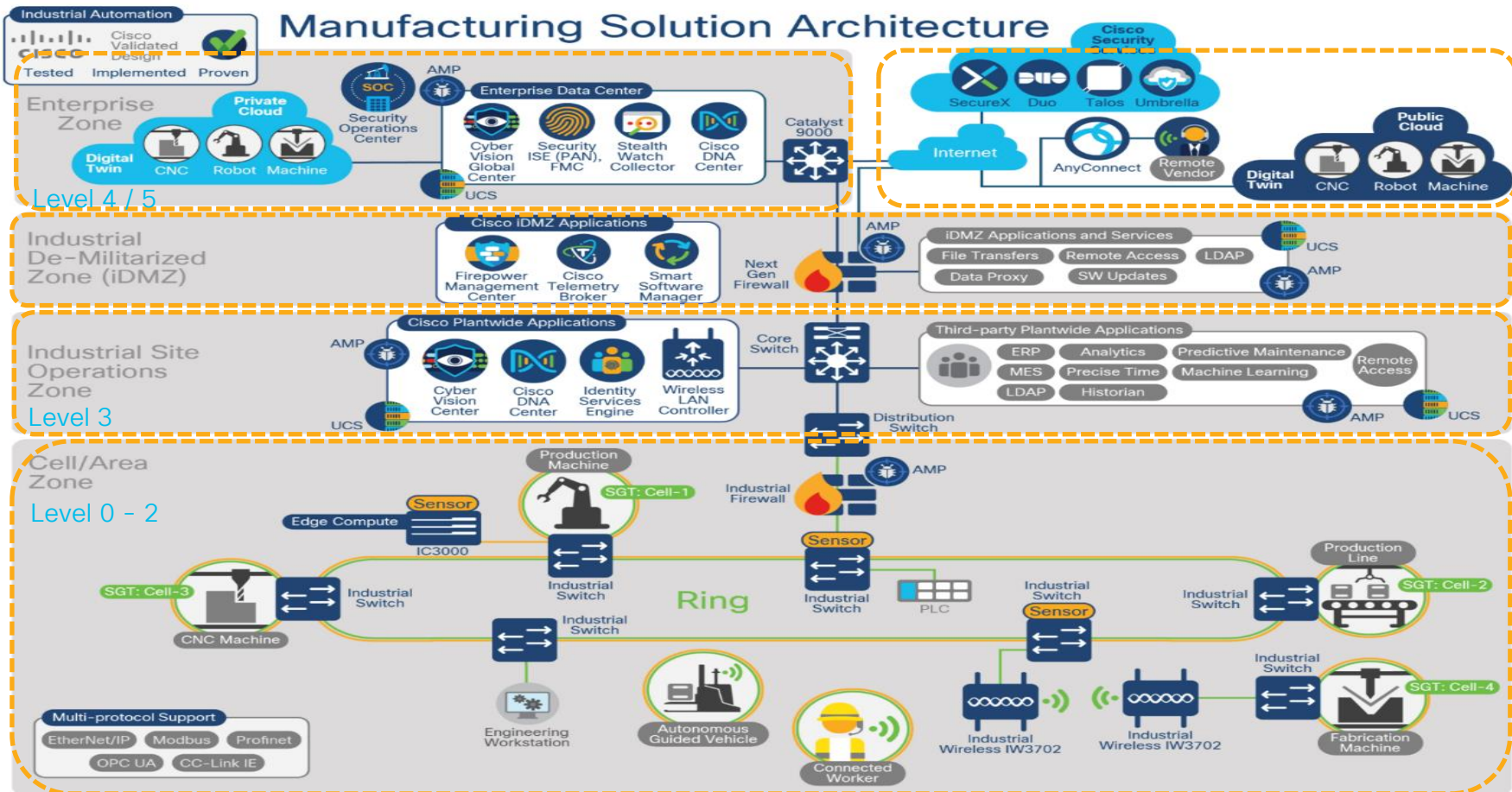
- Support **Industry 4.0** digital transformation
- **Secure resilient scalable** with industrial protocols support
- **Automate** deployment and expansion
- **Simplify** operation support with improved **visibility**
- Identity-based access control and group-based **segmentation**
- Flexible and secure **vendor remote VPN access**

Design and Key Components

Industrial IoT Secure Fabric Design

SD-Access Key Benefits



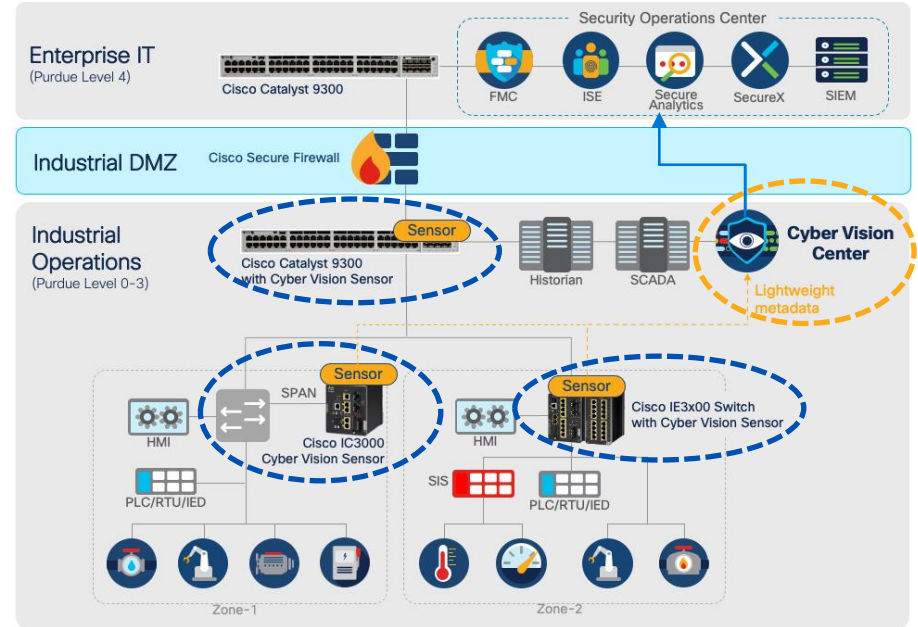


<https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-industry-solutions/industrial-automation-networks.html>

Industrial IoT Secure Fabric Design

Cyber Vision (CCV) – Context Visibility

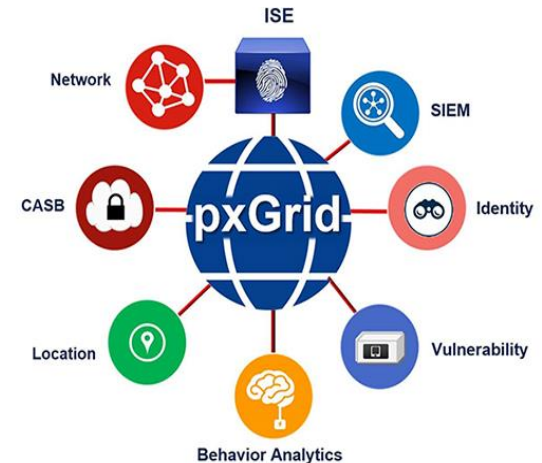
- **Visibility** into industrial assets
- Centralized analytics platform
- Sensors embedded in infrastructure, only lightweight metadata flow to center
- CCV device **host group** can be 'translated' into **SGT** (Security Group Tag) in ISE



Industrial IoT Secure Fabric Design

Platform Exchange Grid (pxGrid)

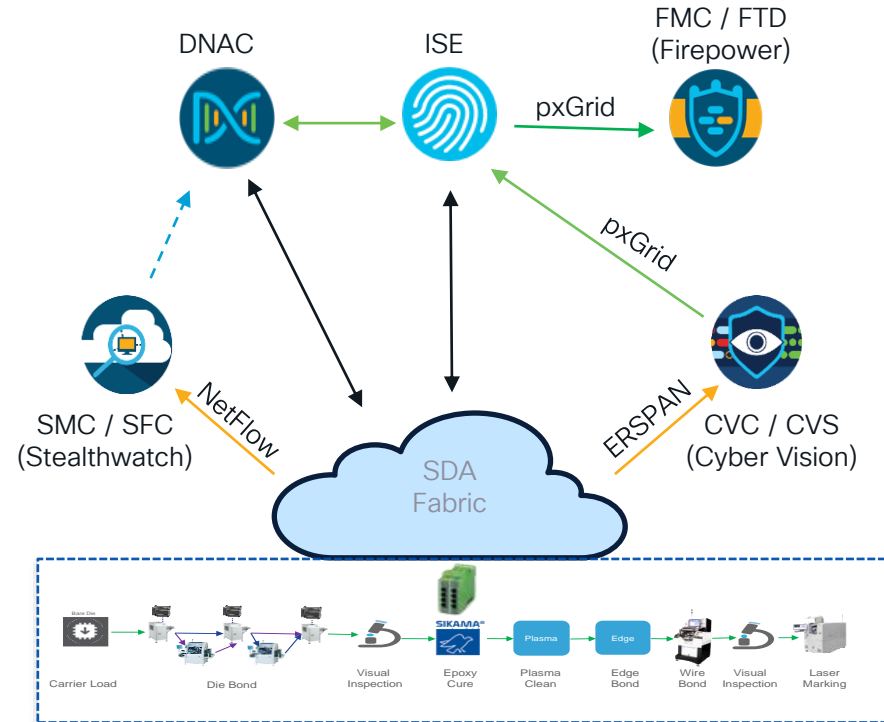
- Open, scalable, IETF-approved **internet standard**
- Grid for **context sharing**
- Identity Service Engine (ISE) as **controller**
- **Publisher** client shares context
- **Subscriber** consumes context
- Customize and secure what context gets shared and with which platforms



Industrial IoT Secure Fabric Design

Integration among Key Components

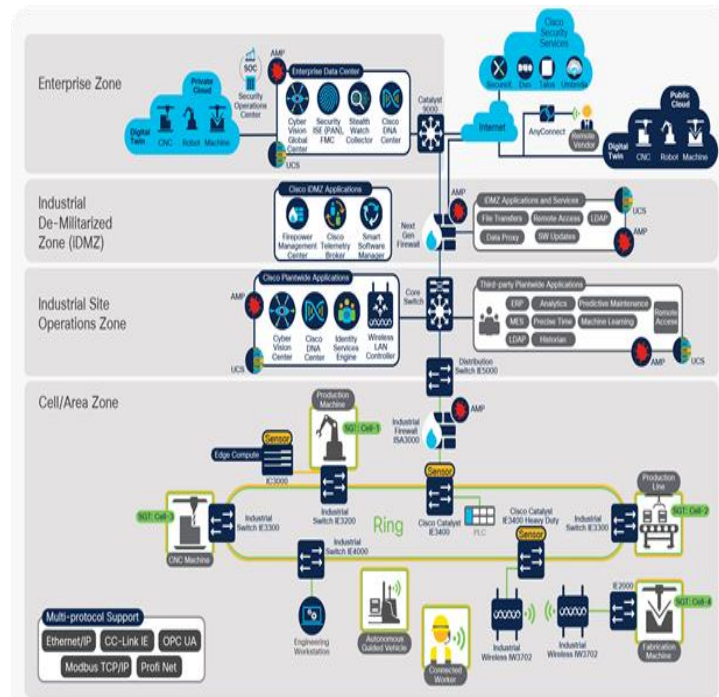
- Catalyst 9000 switching fabric
- DNA Center network orchestrator / assurance platform
- ISE identity / security policy management
- CCV OT assets visibility
- FMC/FTD north-south and Inter-VN security policy enforcement
- SMC/SFC data flow analysis



Industrial IoT Secure Fabric Design

Key Design Considerations

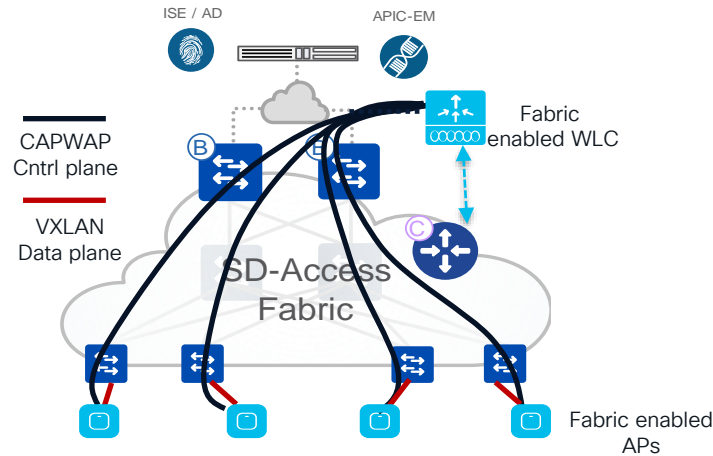
- Keep OT/IT network boundary
- Observe Purdue Model for Control Hierarchy
- Enterprise-wide architectural design
- Site sizing and model selection
- VRF/VLAN/IP Schema/Underlay routing
- Critical VLAN
- WAN Transit Options (IP-Transit, SD-WAN, SDA-Transit)



Industrial IoT Secure Fabric Design

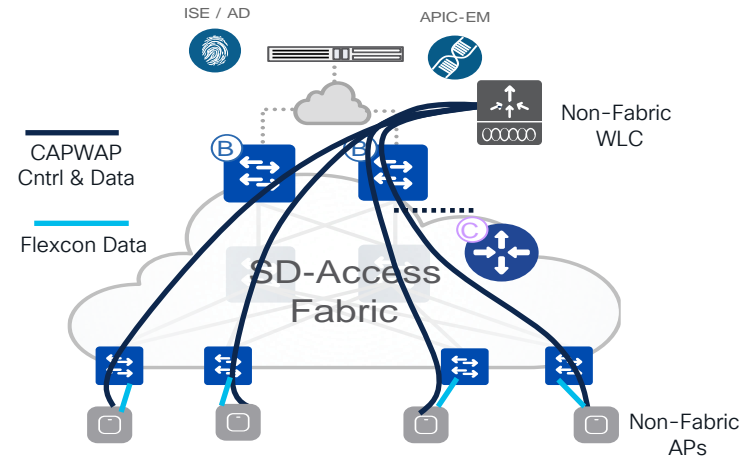
Wireless – FEW / OTT / FlexCon OTT / Mixed mode

SD-Access Wireless



- Fabric enabled wireless (**FEW**)
- WLC/APs integrated in Fabric
- **Same policy** applies to Wireless & Wired

CUWN wireless Over The Top (OTT) / FlexCon



- SDA Fabric is just a transport
- Support any WLC/AP software and hardware
- **FlexCon OTT roaming latency / SGT support**

Policy Design Considerations

-
- Production Matrix
- Applied rules: 62
- Firewall Policy Rule Configuration:
- Destination:** Web_Scal
 - Action:** Deny
 - Log:** ☒
 - Log Message:**

```

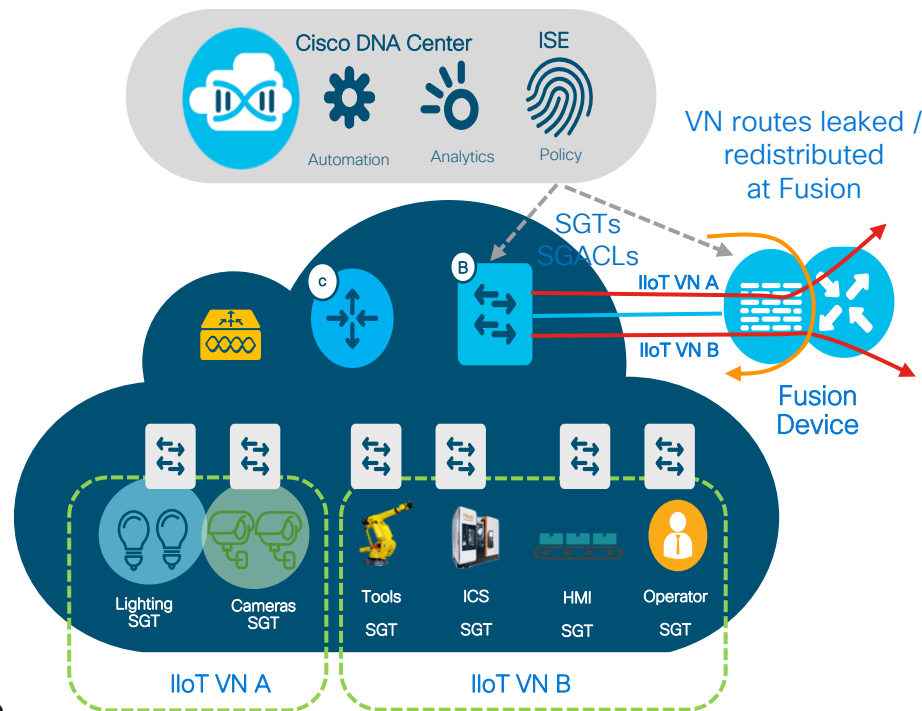
permit tcp dst eq 6970 log
permit tcp dst eq 6972 log
permit tcp dst eq 3804 log
permit tcp dst eq 8443 log
permit tcp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst range 30000 39999 log
permit udp dst range 5070 6070 log
deny ip log

```
- Default | Enabled | SGAZs - Permit P | Description - Default deny rule

Industrial IoT Secure Fabric Design

Policy Enforcement Point Consideration

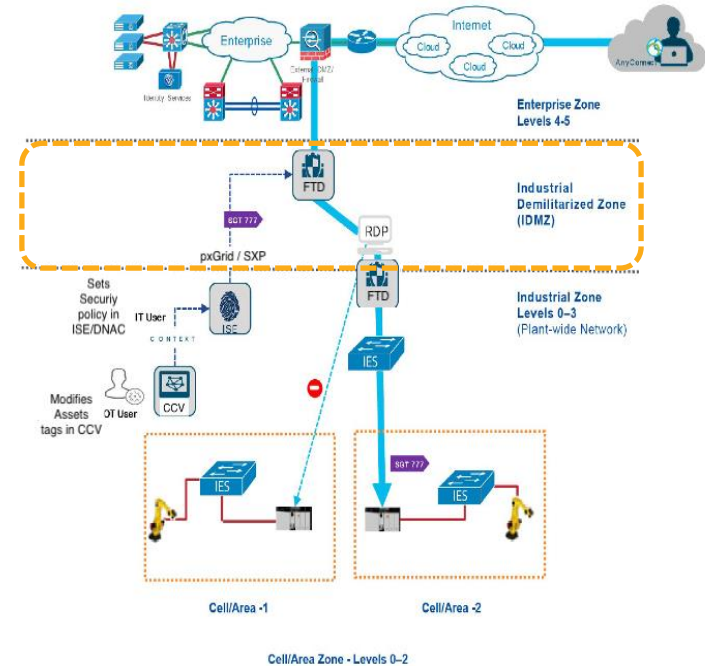
- **East-West Intra-VN** policies
 - Configured in DNA Center
 - Enforced on egress switches
- **East-West Inter-VN** policies
 - Configured and enforced on Firewall/Fusion*
- **North-South** policies
 - Configured and enforced on Firewall/Fusion*
 - SGT as source, destination or both



Industrial IoT Secure Fabric Design

Remote Vendor VPN Access

- VPN terminated into **iDMZ**
- VPN users can only access RDP VDI
- RDP VM can only access OT devices in host group 'Remote Access'
- IT manages vendor VPN access accounts / MFA in ISE
- OT modifies asset group in Cyber Vision to grant / remove access to device on the shop floor



Solution Implementation



Solution Implementation

DNA Center & Network Device Onboarding

- **Software version** selection
- Enterprise CA certificates request
- Enterprise/Internet access **firewall policy** update
- DNA Center / ISE installation and integration
- Site hierarchy, network parameters, IP pool configuration
- Fusion & border **base config** build (VLAN/SVI/BGP/MTU/AAA)
- Discovery and provision fusion/border devices
- Underlay **LAN Automation** / PnP or discover with base config
- Code upgrade & use templates to deploy customized settings



Solution Implementation

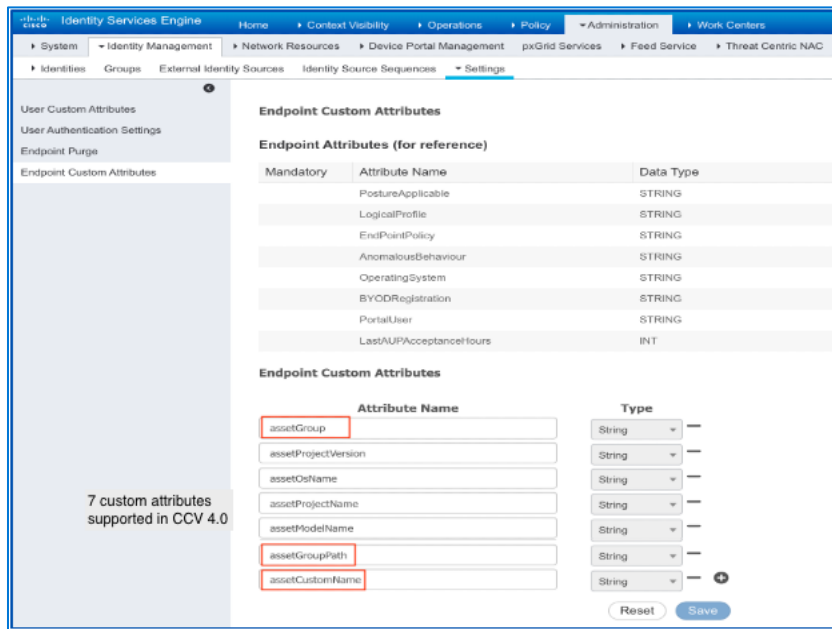
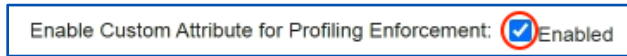
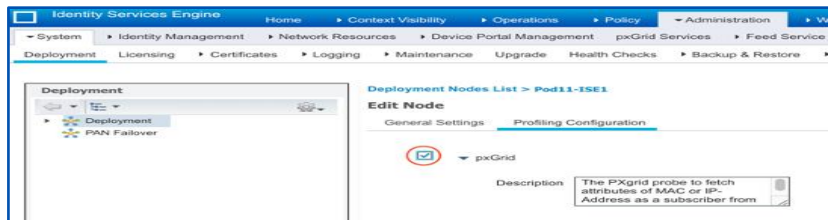
SDA Fabric Provisioning

- Create fabric site(s) and transit network
- Create virtual networks (VRF) and assign to fabric sites
- Add IP pools and VLANs to fabric site/virtual networks
- Add border/control plane nodes and configure **layer-3/ layer-2** hand-offs
- Update fusion device with corresponding peering configuration (manual)
- Add edge nodes into fabric site
- Extended nodes (EN) and Policy EN onboarding
- **Selected port assignments** for devices do not support CTS authentication
- Network connectivity (E-W, Inter-VN, N-S, Internet) test

pxGrid Integration Implementation

ISE pxGrid Configuration

- Enable pxGrid service
- Enable pxGrid for **profiling config**
- Enable custom attribute for **profiling enforcement**
- Configure endpoint custom attributes
 - **assetSource** & **assetGroup**



pxGrid Integration Implementation

CyberVision 4.1 Attributes via pxGrid

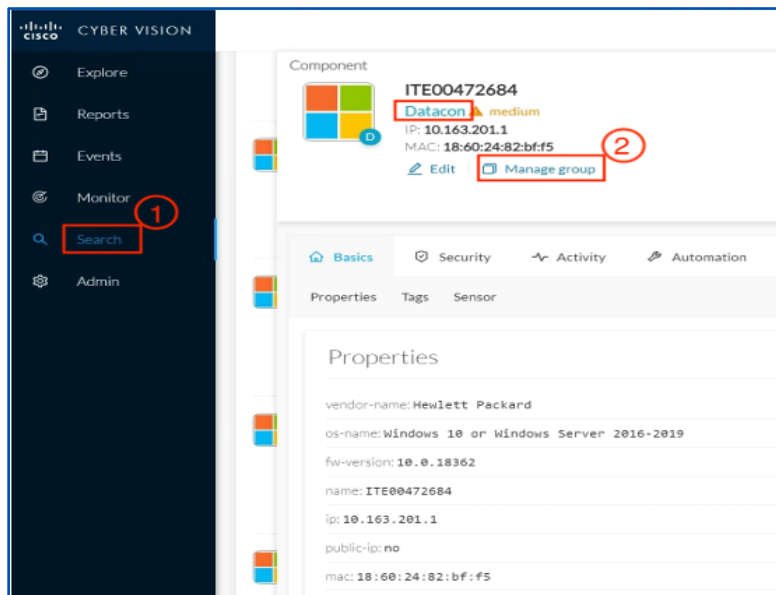
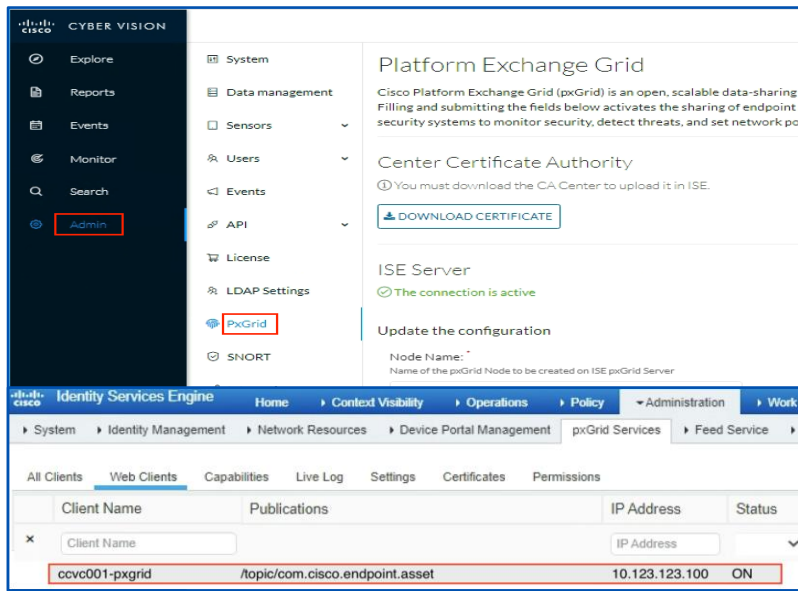


ISE Attribute	CV property	Description	ISE Cust. Attrib.
assetId	ID	Cyber Vision Component ID	No
assetName	Name	Component name	No
assetIpAddress	IP	Component IP address	No
assetMacAddress	Mac	Component MAC address	No
assetVendor	Vendor-name	Component manufacturer (IEEE OUI)	No
assetProductId	Model-ref	Manufacturer product ID	No
assetSerialNumber	Serial-number	Manufacturer serial number	No
assetSwRevision	Fw-version	Component firmware version	No
assetHwRevision	Hw-version	Component hardware version	No
assetProtocol	Protocols	All Protocols concatenated in one string	No
assetModelName	Model-name	Manufacturer model name	Yes
assetOsName	OS-name	Operating system name	Yes
assetProjectName	Project-name	Project name (from PLC program)	Yes
assetProjectVersion	Project-version	Project version (from PLC program)	Yes
assetGroup	Group	Component group in Cyber Vision	Yes
assetGroupPath	Group Path	Component group path in CV (Nested Groups)	Yes
assetCustomName	Custom Name	Custom Name assigned to component by user	Yes

pxGrid Integration Implementation

Assign Host Group to Device in Cyber Vision

- Enable pxGrid integration in Cyber Vision
- Find device based on MAC or IP
Update host group setting



pxGrid Integration Implementation

Endpoint Custom Attributes and Profiler Policy in ISE

CCV Parent Profiler Policy

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, and Policy. The left sidebar shows Endpoints, Users, Network Devices, and Application. The main content area displays the configuration for an endpoint with MAC address 18:60:24:82:BF:F5. The 'Attributes' tab is selected, showing 'General Attributes' and 'Custom Attributes'. The 'Custom Attributes' section is highlighted with a blue box and the text 'Custom Attributes' in blue. A table lists custom attributes with their strings and values:

Attribute String	Attribute Value
assetGroup	Datacon
assetProjectVersion	
assetSource	CCV
assetOsName	Windows 10 or Windows Server 2016-2019
assetGroupPath	Datacon
assetCustomName	
assetProjectName	
assetModelName	

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Profiler Policy. The top navigation bar includes Home, Context Visibility, Operations, and Policy. The left sidebar shows Endpoints, Users, Network Devices, and Application. The main content area displays the configuration for a Profiler Policy named 'CCV_LearnedAsset'. The 'Policy Enabled' checkbox is checked. The 'Minimum Certainty Factor' is set to 10. The 'Exception Action' and 'Network Scan (NMAP) Action' are both set to 'NONE'. The 'Create an Identity Group for the policy' radio button is set to 'No, use existing Identity Group hierarchy'. The 'Parent Policy' is set to '***NONE***'. The 'Associated CoA Type' is set to 'Global Settings'. The 'System Type' is 'Administrator Created'. The 'Rules' section shows a condition: 'If Condition CUSTOMATTRIBUTE_assetSource_EQUA...'. A red box highlights the 'Conditions Details' section, showing the expression: 'CUSTOMATTRIBUTE:assetSource EQUALS CCV'.

pxGrid Integration Implementation

ISE Host Group Profiler Policy Configuration

CCV Host Group Profiler Policy

- Parent Policy selected
- Create an identity group
- Rule: **assetGroup** equals <CCV Host Group Name>
- One policy per Cyber Vision host group
- More conditional rules can be added

The screenshot displays the Cisco Identity Services Engine (ISE) Profiler Policy configuration interface. The page title is "Profiler Policy List > CCV_AssetGroup_PLCs". The "Profiler Policy" section shows the following configuration:

- * Name: CCV AssetGroup PLCs
- Description: (empty)
- Policy Enabled: ☒
- * Minimum Certainty Factor: 10 (Valid Range 1 to 65535)
- * Exception Action: NONE
- * Network Scan (NMAP) Action: NONE
- Create an Identity Group for the policy: ☒ Yes, create matching Identity Group
- * Parent Policy: CCV_LearnedAssets
- * Associated CoA Type: Global Settings
- System Type: Administrator Created

The "Rules" section shows a rule configuration:

- If Condition: CUSTOMATTRIBUTE_assetGroup_EQUALS
- Then: Certainty Factor Increases
- Value: 20

A red box highlights the rule configuration area, showing the "Condition Name" and "Expression" fields. The expression is: CUSTOMATTRIB... EQUALS PLCs. Below the expression, the text reads: CUSTOMATTRIBUTE assetGroup EQUALS <CCV Component Group Name>.

pxGrid Integration Implementation

ISE AuthZ Policy Configuration

- Condition: Identity Group Name equals EIG generated by profiler policy
- More conditions can be included for added security
- Result: Assign VLAN and SGT

Status	Rule Name	Conditions	Results	
			Profiles	Security Groups
✓	IoT_CCV_Group_PLCs	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:CCV_AssetGroup_PLCs Wired_MAB	* AuthorP_OVPool1-Campus_VN1 +	IoT_PLCs x +
✓	IoT_CCV_Group_FLCcell	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:CCV_AssetGroup_FLCcell Wired_MAB	* AuthorP_OVPool1-Campus_VN1 +	FLCcell_SGT x +
✓	IoT_CCV_Group_HVLCcell	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:CCV_AssetGroup_HVLCcell Wired_MAB	* AuthorP_OVPool1-Campus_VN1 +	HVLCcell_SGT x +
✓	IoT_CCV_Group_Datacon	AND IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:CCV_AssetGroup_Datacon Wired_MAB	* AuthorP_OVPool1-Campus_VN1 +	Datacon_SGT x +

pxGrid Integration Implementation

FMC/FTD Group-based Policy Configuration

Firepower Management Center
Policies / Access Control / Firewall Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy

New **FTD** SGT AP

Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (0)

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
Mandatory - New FTD SGT AP (1-79)													
												BaseFile BasePAC BasePAC	Allow

Analysis → User Activity for IP-SGT Mapping Information

Firepower Management Center
Analysis / Users / User Activity

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy

Bookmark This Page | Report Designer | Dashboard | View Bookmarks | Search

Predefined Searches

2021-08-31 15:33:00 - 2021-09-01 16:31:16 Expanding

No Search Constraints (Edit Search)

Table View of Events Users

	Time	Event	Username	Realm	Discovery Application	Authentication Type	IP Address	Security Group Tag	Endpoint Profile	Endpoint Location	Device
2021-09-01 15:34:01	User Logoff	00		LDAP	Passive Authentication	10.12.34.56	BasePACFile	CCV_BasePACFile	172.16.10.68	embfwicmc001.entds.ngisn.com	
2021-09-01 15:34:01	User Logoff	00		LDAP	Passive Authentication	fe80::9bd:9618:3683:d415	BasePACFile	CCV_BasePACFile	172.16.10.69	embfwicmc001.entds.ngisn.com	

Solution Implementation

Stealthwatch

- Apply NetFlow config onto all host ports in fabric edges
- Host group configuration or import
- Flow record review and report
- Host group-based aggregated flow report for policy implementation



hostGroups	srcPort	peer.hostGroups	dstPort	Protocol	FTD/DNAC
ICS_PAC_Svr	-1	PAC_Dev	-1	ICMP	FTD
ICS_PAC_Svr	55263	PAC_Dev	502	TCP	FTD
ICS_PAC_Svr	55278	PAC_Dev	3389	TCP	FTD
ICS_PAC_Svr	55258	PAC_Dev	5000	TCP	FTD
ICS_PAC_Svr	55260	PAC_Dev	5555	TCP	FTD
PAC_Dev	3834	PAC_Dev	445	TCP	DNAC
PAC_Dev	5353	Multicast	5353	UDP	DNAC

Device Onboarding Workflow

OT/IT Collaboration

- OT/IT team **joint planning** on network req., new host groups
- Configure new **profiling and authorization policies** in ISE
- New devices connect onto fabric
- Assign **host group** for the new devices in Cyber Vision
- Review NetFlow data in Stealthwatch for group-based policy creation
- For E-W flow, configure SGACLs in DNAC and deploy to switches
- For N-S flow, configure SGT based policies in FMC, push to FTD

Challenges and Solutions



Challenges & Solutions

- **Harsh** environment deployment
 - IE switches deployed as Extended Node (EN) / Policy EN
- 3rd party **built-in switches**
 - Disable STP bpduguard, authentication still can apply (access mode)
- **Duplicated IPs** / NAT support
 - NAT devices can be inserted between IoT device and edge switch
- Same subnet both inside and outside fabric or **firewall as device gateway**
 - Layer 2 hand-offs
- **Silent hosts**
 - Layer 2 flooding / Directed broadcast / Wake-on-LAN or DHCP with reservation

Industrial IoT SD-Access Use Case

How We Meet the Requirements

- Automate deployment and expansion
- Simplify operation support with improved **visibility**
- Identity-based access control and group-based segmentation
- Flexible and secure vendor remote access VPN
- Secure, resilient, scalable with industrial protocols support
- Support Industry 4.0 digitalization initiatives

Success Factors

- Stake holders and executive sponsorship
- Build an IT / OT / Security **cross-functional** team
- **Document** use case requirements
- Enterprise-wide **architectural design**
- Start with a **pilot** or limited production deployment
- **Training** for engineering and support teams
- Follow Cisco design & implementation **best practice**
- Start your OT network transformation journey with Cisco CX

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

Pay for Learning with
Cisco Learning Credits

(CLCs) are prepaid training
vouchers redeemed directly
with Cisco.



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

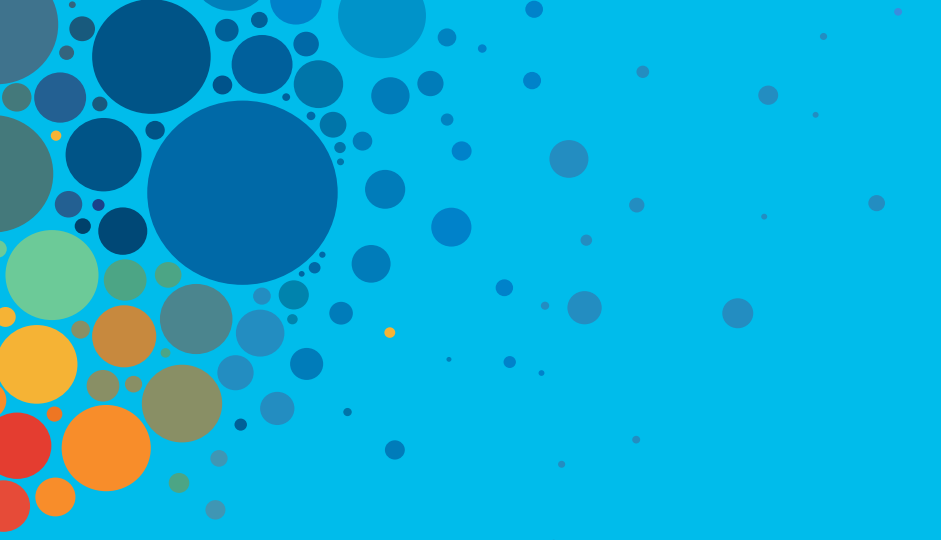
Cisco Guided Study Groups

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 related demos
- 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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive