ODVA
2014

Industry Conference
and 16th Annual Meeting

Contextually-Aware Access Controls

Nancy Cam-Winget
Cisco Systems

Technical Track

ICS Implications of the Internet Expansion

Increased Network Usage

More IP enabled devices

More device types

Increased use of mobile devices

Remote access

Different types of users

Increased Risks

Unauthorized devices

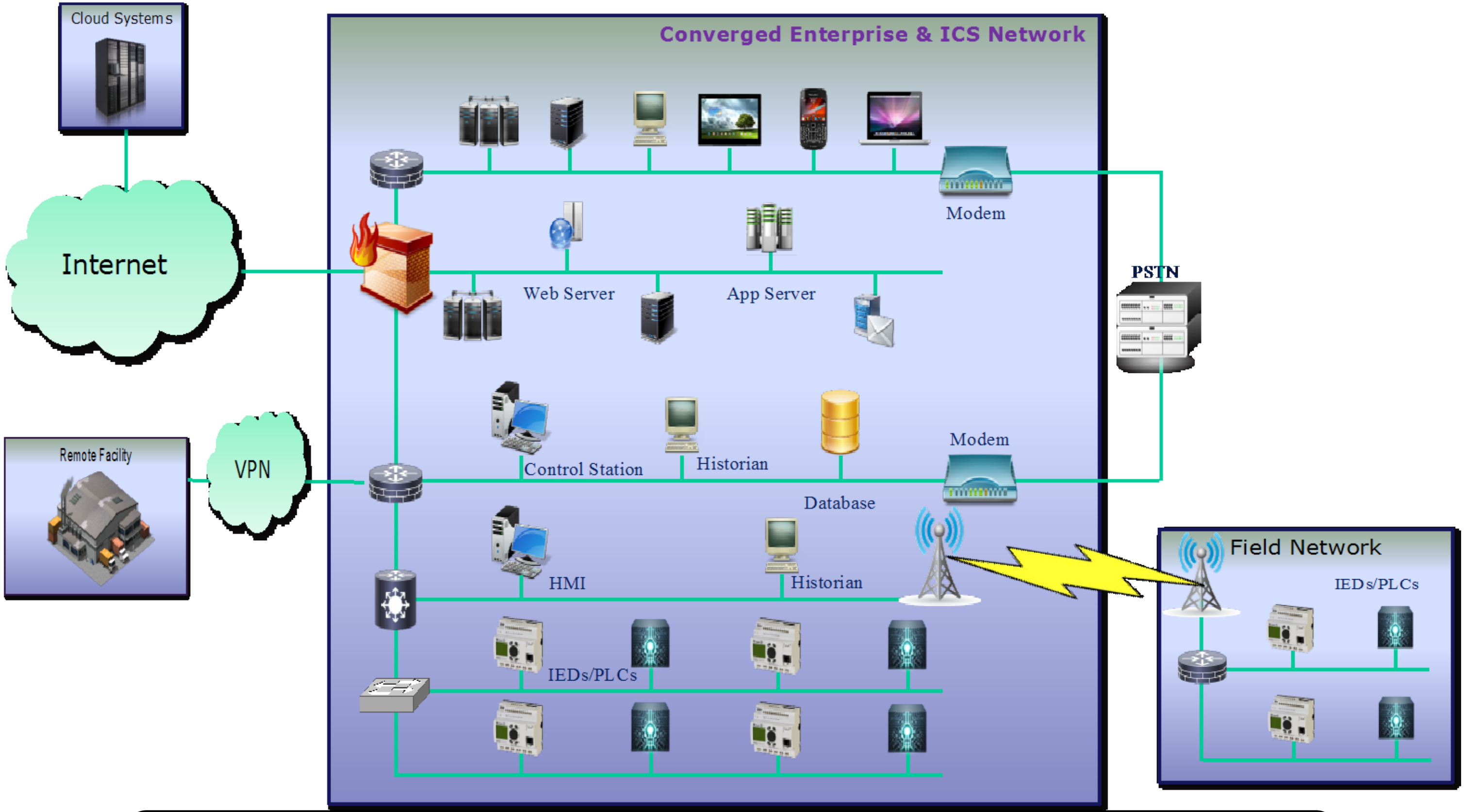
Unauthorized users

Infected Devices

Infected Users

Who’s on the network?

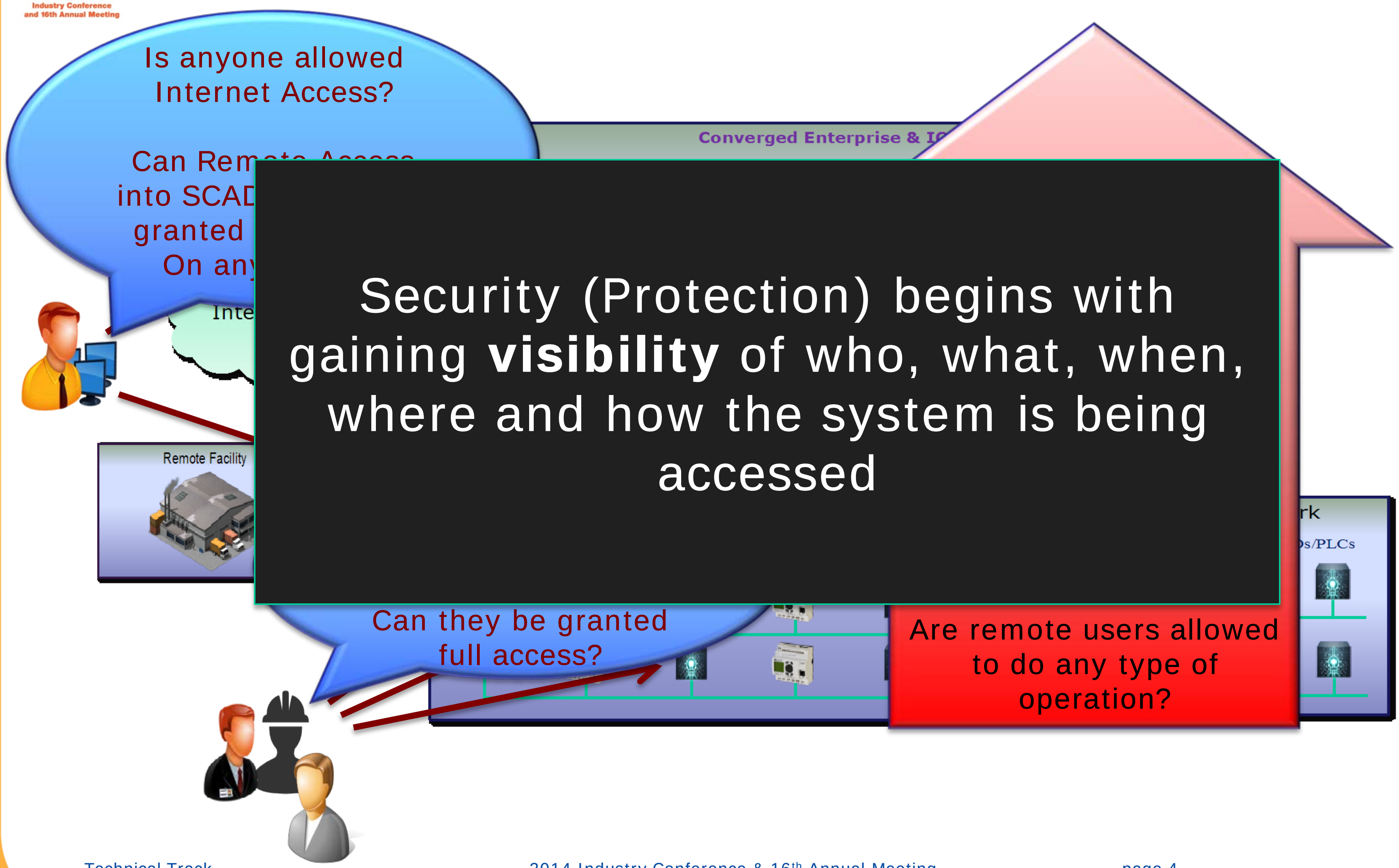
Network Security Trends



Internal threats from employees, vendors, contractors, infected devices
Behind firewall or "inside ICS" – inadequate protection

Increasingly, more attacks come from internal access

Why Contextual Access Control?



Is anyone allowed Internet Access?

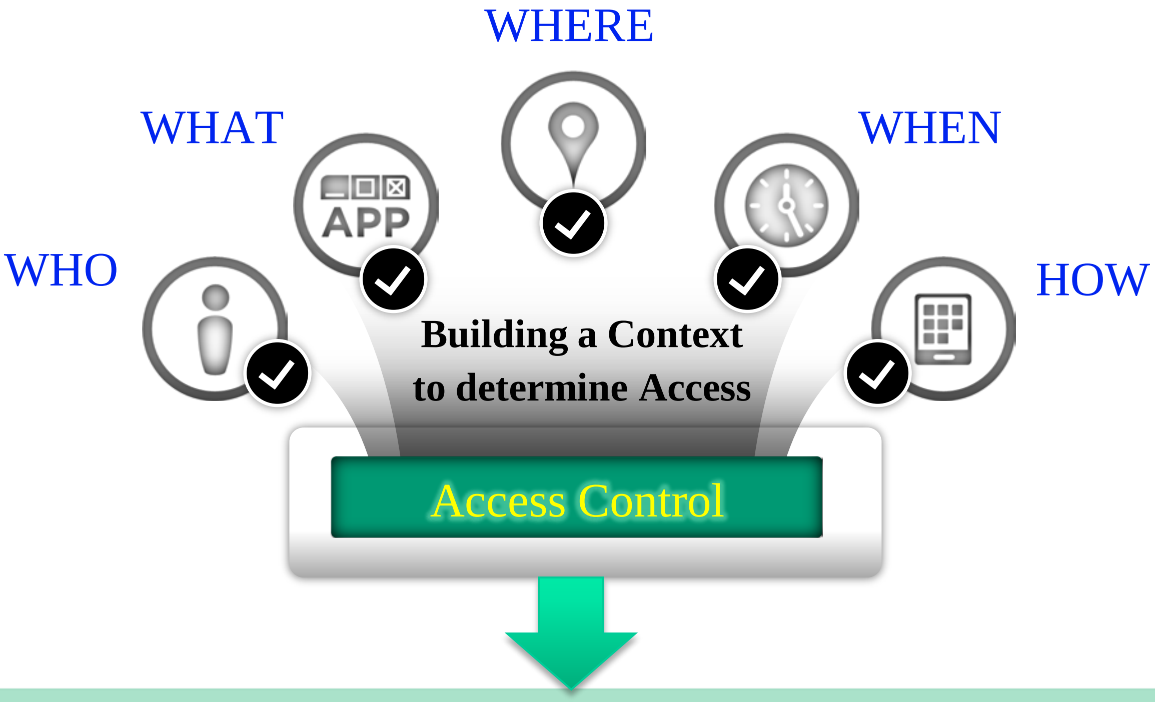
Can Remote Access into SCAD granted On any

Security (Protection) begins with gaining **visibility** of who, what, when, where and how the system is being accessed

Can they be granted full access?

Are remote users allowed to do any type of operation?

Contextual Based Access Control



Rule Name		Conditions		Access Control
Supervisor	if	Supervisor	then	SCADA and ICS
Employee	if	Employee, wired or wireless	then	ICS
Contractor	if	Contractor, 9am-5pm	then	ICS
ICS device	if	ICS Device, wired	then	ICS and SCADA
Default	If no matches, then	Deny Access		

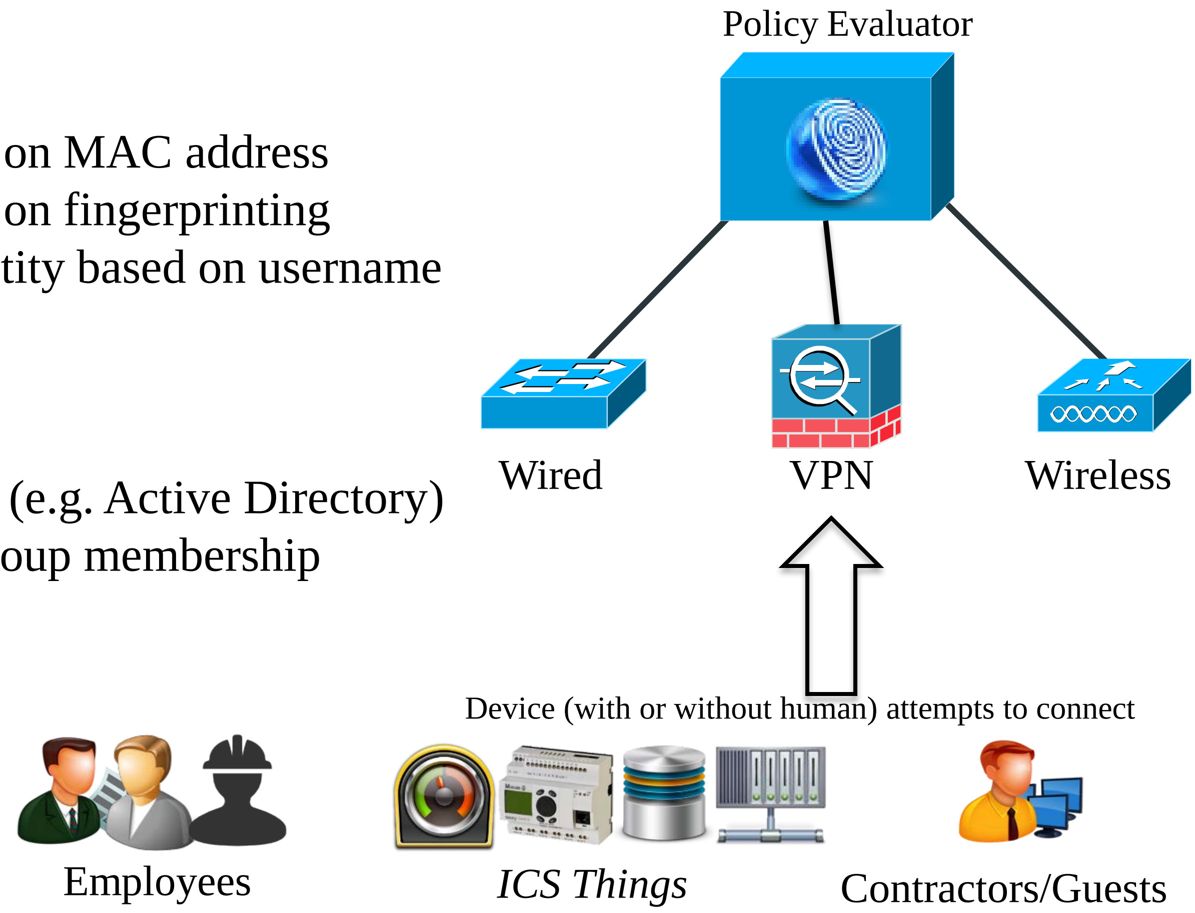
“Who” is connecting?

Who can be determined by:

- Device classification based on MAC address
- Device classification based on fingerprinting
- If a human is attached: identity based on username

Role can de determined by:

- Device classification
- Group membership defined (e.g. Active Directory)
- Combination of device + group membership

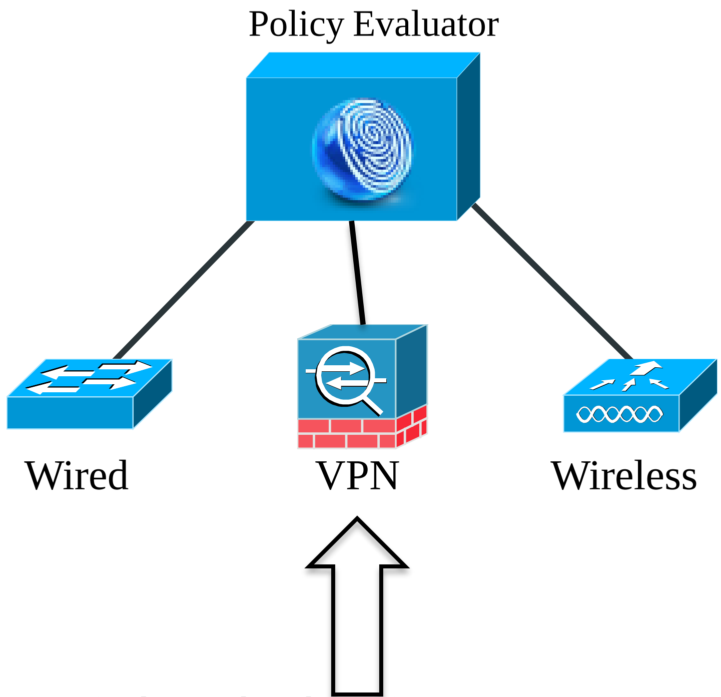


Connection Origin = “Where”

Where is determined by connection type:

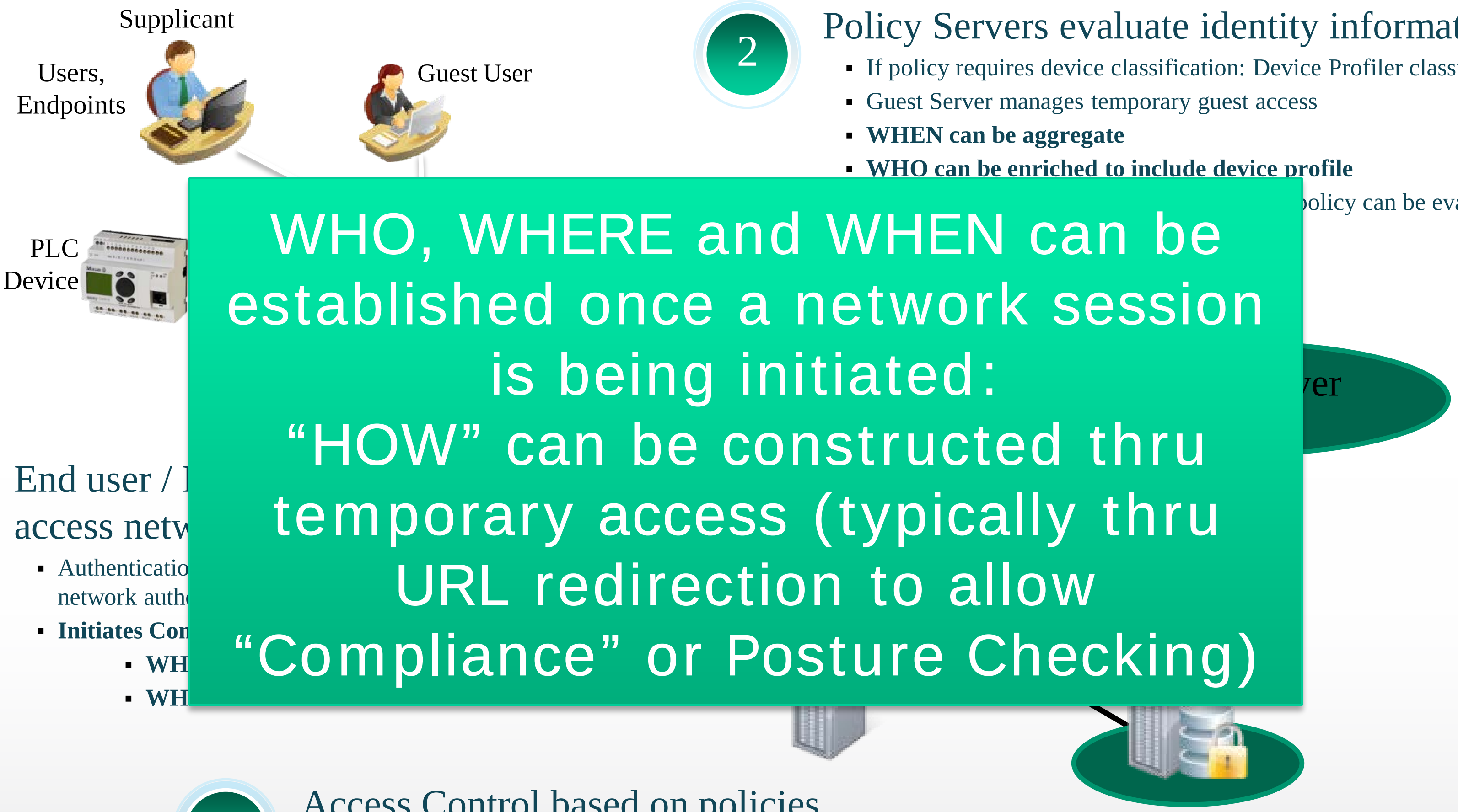
- Wired
- Wireless
- Remote Access

Where is determined by the access edge device (e.g. Switch, Access Point, VPN server)



Device (with or without human) attempts to connect

Building Context in action



2

Policy Servers evaluate identity information

- If policy requires device classification: Device Profiler classifies device type
- Guest Server manages temporary guest access
- **WHEN can be aggregate**
- **WHO can be enriched to include device profile**
- policy can be evaluated and

WHO, WHERE and WHEN can be established once a network session is being initiated:
"HOW" can be constructed thru temporary access (typically thru URL redirection to allow "Compliance" or Posture Checking)

1

End user / I access netw

- Authenticatio network authe
- **Initiates Con**
  - **WH**
  - **WH**

3

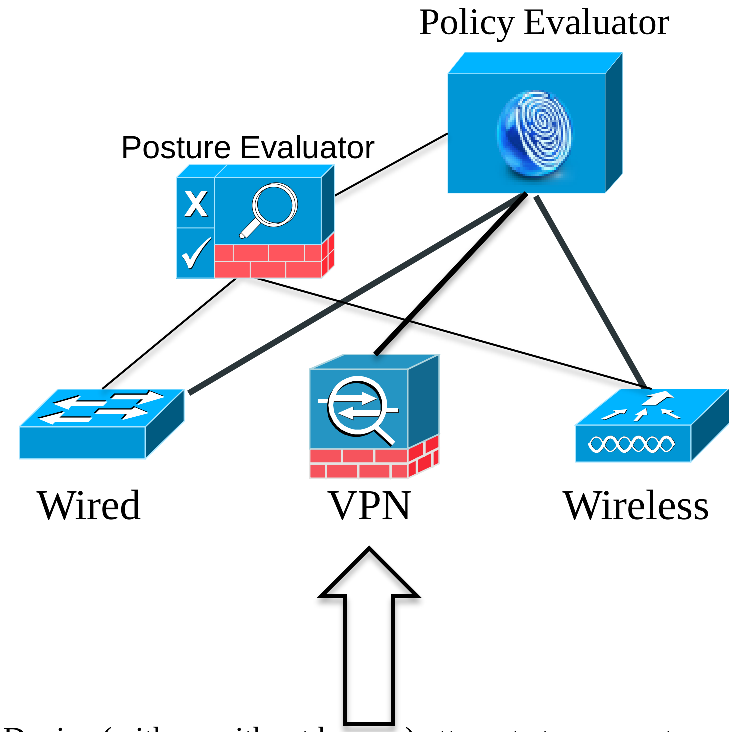
Access Control based on policies

- Switch enforces access control based on policy (VLAN Assignment, dACL, RBACL)

“How” are they connecting?

How can be determined by:

- A combination of the device classification and “Posture” check
- Posture check is the means to determine if the device is installed with the right OS, patches and applications



Device (with or without human) attempts to connect

Posture Policy Profiles

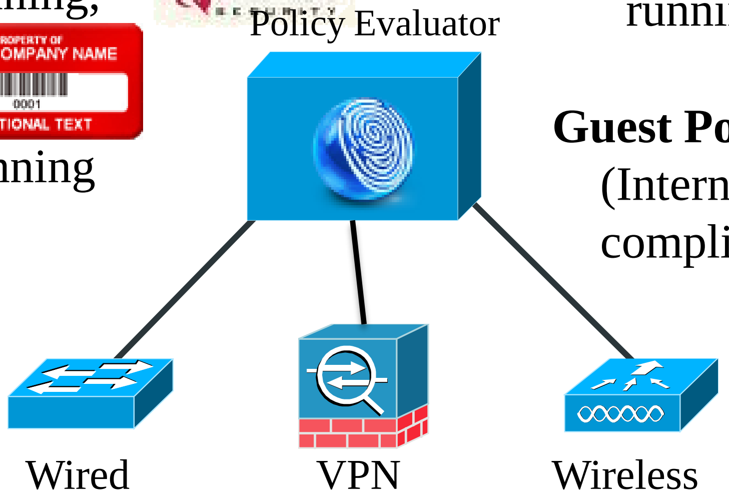
Corporate PC/HMI Policy:

- Microsoft patches updated
- McAfee AV installed, running, and current
- Corp asset checks
- Enterprise application running

Contractor Policy:

- Any AV installed, running, and current

Guest Policy: Accept Authentication (Internet Access Only- no compliance check done)

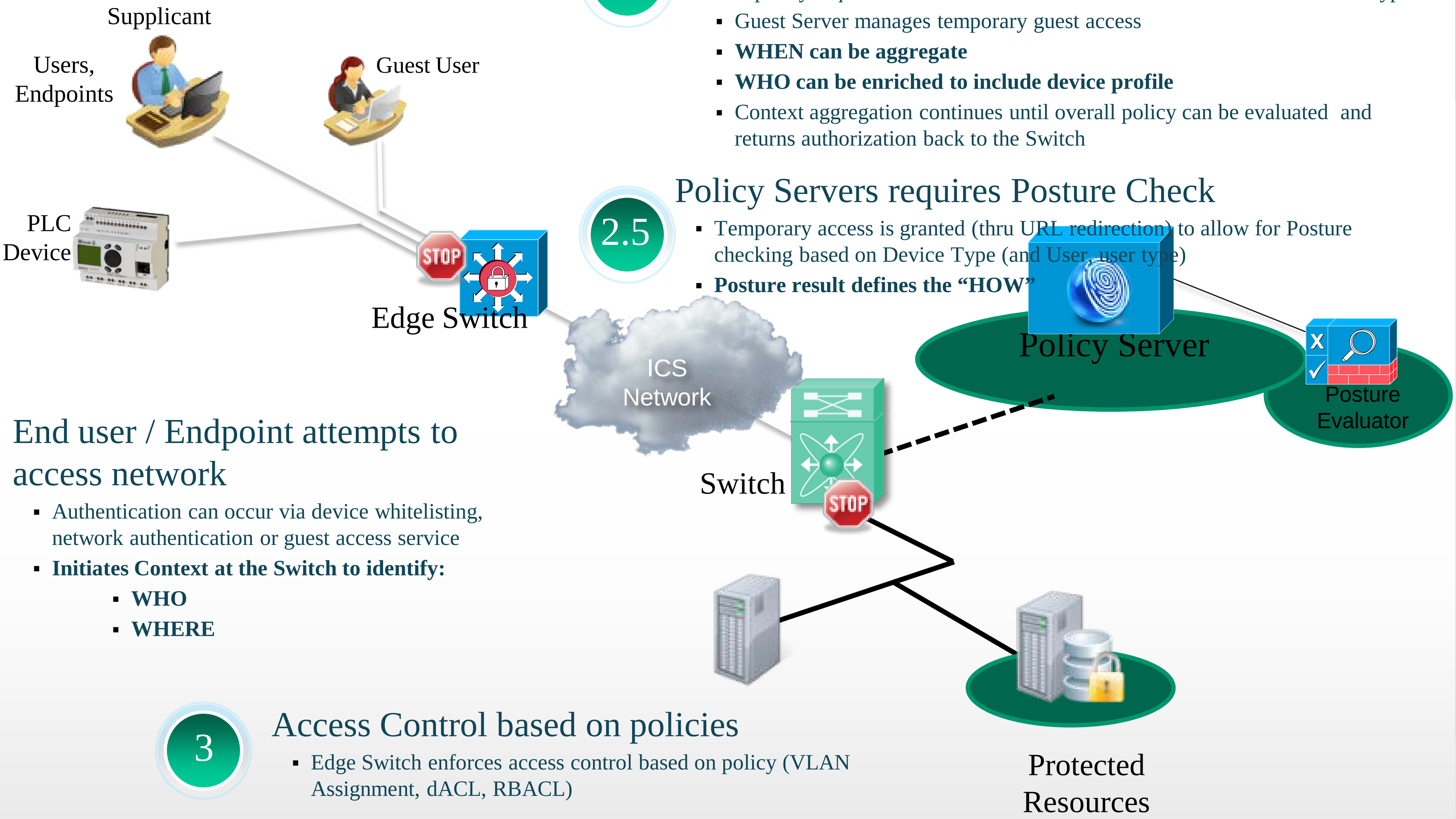


ICS Policy:

- Configuration verification
- Version updates
- Asset checks

Device (with or without human) attempts to connect

Building Context in action



2 Policy Servers evaluate identity information

- If policy requires device classification: Device Profiler classifies device type
- Guest Server manages temporary guest access
- **WHEN can be aggregate**
- **WHO can be enriched to include device profile**
- Context aggregation continues until overall policy can be evaluated and returns authorization back to the Switch

2.5 Policy Servers requires Posture Check

- Temporary access is granted (thru URL redirection) to allow for Posture checking based on Device Type (and User, user type)
- **Posture result defines the "HOW"**

1 End user / Endpoint attempts to access network

- Authentication can occur via device whitelisting, network authentication or guest access service
- **Initiates Context at the Switch to identify:**
  - **WHO**
  - **WHERE**

3 Access Control based on policies

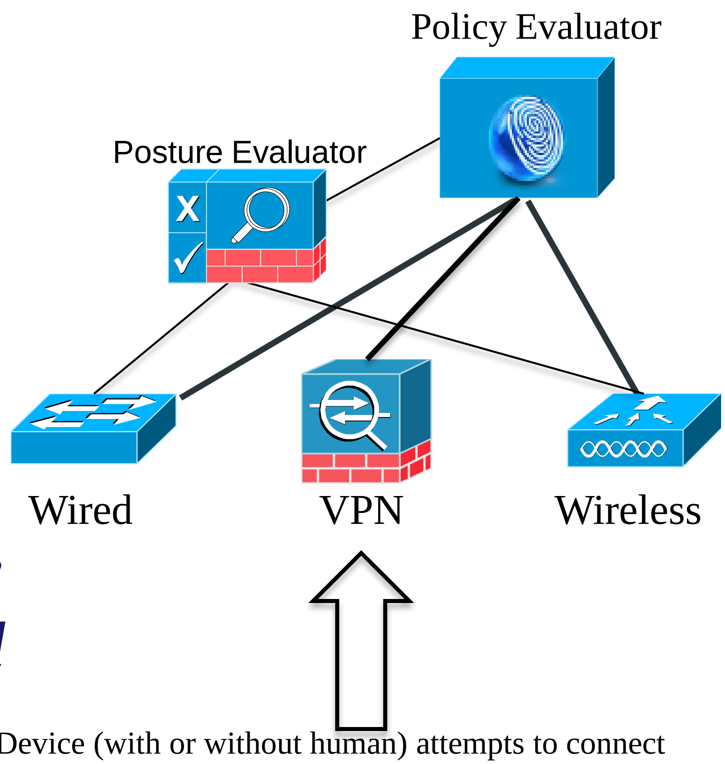
- Edge Switch enforces access control based on policy (VLAN Assignment, dACL, RBACL)

“What” is being accessed?

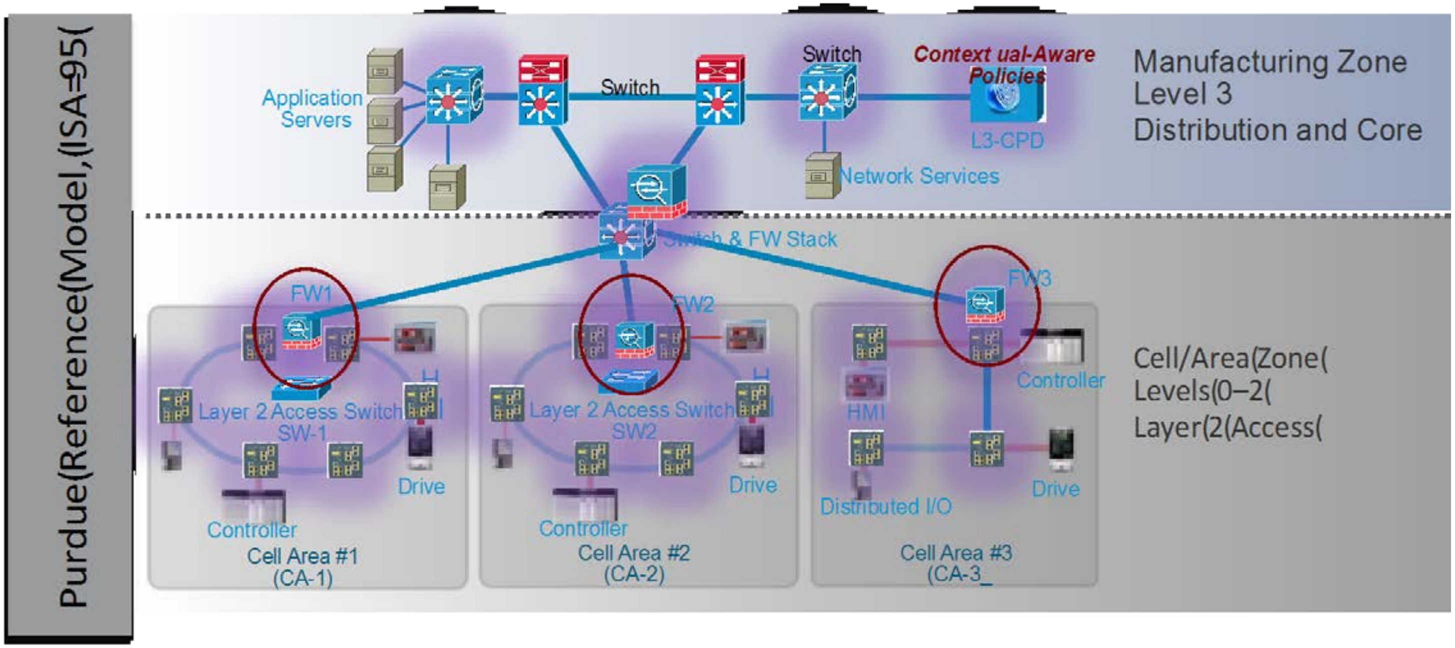
What can be determined by:
A Deep Packet Inspection probe to discover

- Application type
- Protocol type
- Operations within application and/or protocol

“WHAT” further helps define policies to detect whether Users and Devices are communicating to the right sources and with correct privileges

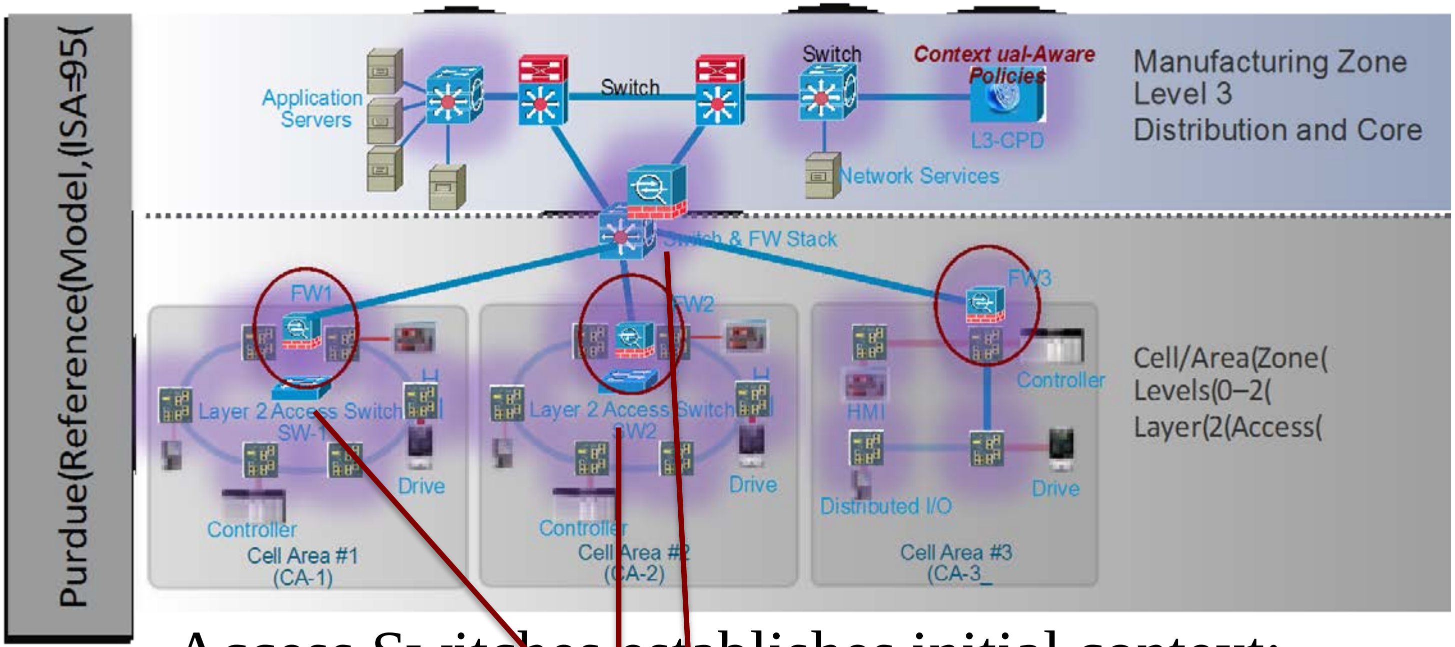


ICS Policies = more Context



Rule Name		Conditions		Access Control
Supervisor	if	Supervisor	then	SCADA and ICS
Employee	if	Employee, wired or wireless	then	ICS
Contractor	if	Contractor, 9am-5pm	then	ICS
ICS device	if	ICS Device, wired	then	ICS and SCADA
No Updates	if	***Active Device in Cell Area***	then	***Block Update commands***
Default	If no matches, then	Deny Access		

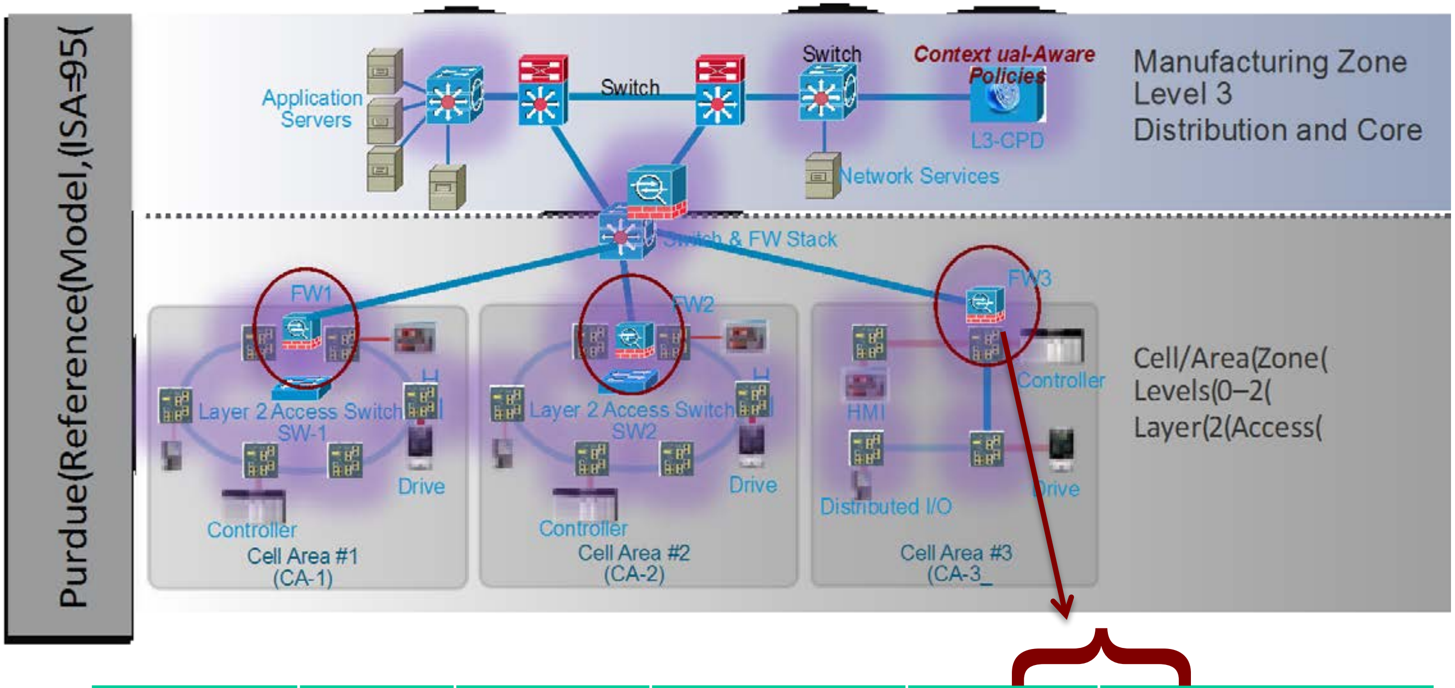
Context post-Edge Access



Access Switches establishes initial context:

Who	What	Where	When
HMI	Web, CIP	wired	7:00am PST
I/O	CIP	wired	7:00am PST
Controller	CIP	wired	7:00am PST
Drive	CIP	wired	7:00am PST

Context updates with DPI probing



Who	What	Where	When	Group	State
HMI	Web, CIP	wired	7:00am PST	CA-3	Active
I/O	CIP	wired	7:00am PST	CA-3	Inactive
Controller	CIP	wired	7:00am PST	CA-3	Inactive
Drive	CIP	wired	7:00am PST	CA-3	Inactive

Dynamic Context updates = Dynamic policy enforcement

Who	What	Where	When	Group	State
HMI	Web, CIP	wired	7:00am PST	CA-3	Active
I/O	CIP	wired	7:00am PST	CA-3	Inactive
Controller	CIP	wired	7:00am PST	CA-3	Inactive
Drive	CIP	wired	7:00am PST	CA-3	Inactive

Context created at Edge Access

Context Aggregated by FW's

Policies evaluated at Edge Access

Rule Name		Conditions		Access Control
Supervisor	if	Supervisor	then	SCADA and ICS
Employee	if	Employee, wired or wireless	then	ICS
Contractor	if	Contractor, 9am-5pm	then	ICS
ICS device	if	ICS Device, wired	then	ICS and SCADA
No Updates	if	Active Device in Cell Area	then	Block Update commands
Default	If no matches, then		Deny Access	

Continuous evaluation enables Stateful (dynamic) policies