Network Access Control and ICS:
A Practical Guide

GIAC (GICSP) Gold Certification

Author: Ronald Grohman, r.grohman@gmail.com
Advisor: Lenny Zeltser
Accepted: January 18, 2022

Abstract

Industrial Control Systems (ICS) are the lifeblood of the organizations that use them, often requiring one-hundred percent uptime. This requirement makes securing them and the networks they operate on extremely challenging, as increased security often increases the risk of interruption. Due to the nature of their function, Industrial Control Systems tend to be left untouched and in place until they physically break. Resulting in decades-old equipment operating on modern infrastructure with modern security risks. Those things combined with OT staff, who are often not trained in security or basic IT functions, means getting buy-in for anything that increases risk or changes their job function becomes near impossible. However, it is still possible to implement complex network access control systems safely and effectively and architect them in a way usable by plant engineers (OT staff) without the need for extensive security or IT training.

1. Introduction

Cybersecurity used to be simple. Install antivirus, turn on updates, install a firewall, and you are set –take a nap. Over the last few decades, the field and techniques have gradually evolved to unrecognizable levels, along with the complexity of implementing them.

Traditional conceptions of perimeter defense involve placing firewalls or an intrusion prevention system between the internal network and internet, creating trust zones and access policies. These methods are not effective anymore. A more robust system that evaluates the device's intent, not simply what it claims to be, is needed. That is the role of a modern network access control system.

The perimeter needs to be thought about differently to effectively understand and utilize a network access control system. In its most basic sense, the perimeter is where your network stops, and everything else begins. If we think about it this way, our perimeter becomes every switchport, wireless access point, firewall, IoT gateway, etc. Combining this new perspective with the concept of traditional perimeter defense, our "firewall" gets extended to every point of access, both internal and external.

When access is granted to an employee from the internet via VPN or a similar method, they have to identify themselves. A variety of ways to do so can be used, and once accomplished, the employee has access only to the resources needed. Applying the same process to the new perception of the network perimeter and the concepts of Network Access Control emerge.

In the case of ICS networks, accurately identifying and authorizing every device every time it connects can be especially difficult to do. The devices in these environments are IoT-style devices that have likely been in place for many years, long before modern network access control systems were developed. In addition, ICS networks are usually managed by the operational technology (OT) staff, not typical IT and security teams, making it more difficult to implement strong security controls.

The OT staff has good reason to be protective of the ICS network. Because of the age of the devices, criticality to business operation, and potential safety issues, ICS networks are extremely sensitive to interruption. In other types of networks, the inability of a single user or device to connect isn't a critical issue. However, that one device in an ICS network could be why an entire product run fails quality control, a factory worker is injured, or a failsafe doesn't work, causing an environmental disaster.

Despite all the challenges, network access control can still be implemented in ICS environments successfully. This research will analyze the required tools and techniques to implement network access control successfully in ICS environments, look at required configurations that differ from enterprise environments, tools needed to empower OT staff to securely onboard and manage devices, verify function, and some caveats requiring unique configurations.

2. Why Network Access Control is Needed

It is widely accepted that network access control is beneficial, if not necessary, in typical enterprise environments. However, there remains a good deal of confusion and reluctance to implement in ICS networks. There is a common misconception that ICS networks are protected due to traditional SCADA network designs. Even with old ICS equipment, modern business requirements often dictate departure from those traditional designs, forcing more interconnectivity and therefore opportunities for exposure. OT technicians need to interact with ICS devices, servers, and support systems that require updates and maintenance, which means traversal out of the protected environments. Machine vendors require a way to access and support their systems, on-site vendors need a way to configure and deploy new equipment, and the business requires data to report on a multitude of metrics. All of these things break the isolation of traditional ICS network designs, even if it is just a little bit, and all of those exceptions offer a way for unwanted or malicious traffic to make its way in.

3. What is Network Access Control

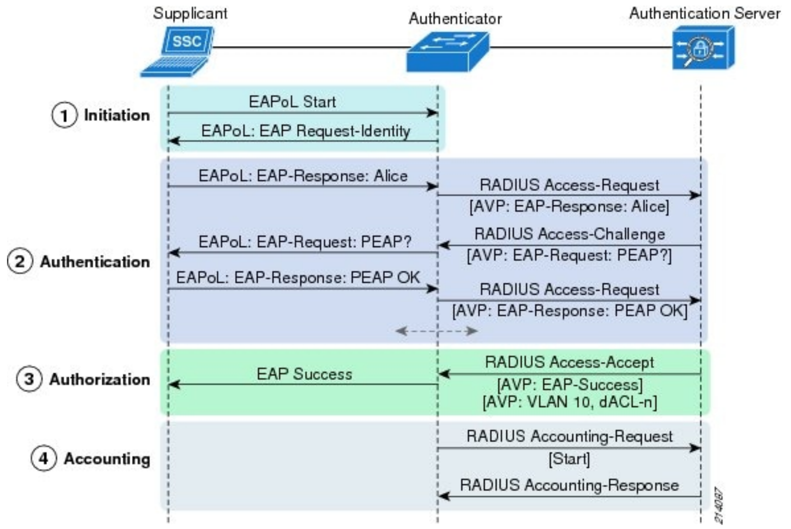
Network access control is a method to bolster the security, visibility, and access management of a proprietary network. It restricts the availability of network resources to endpoint devices and users that comply with a defined security policy. (Awati, 2021)

Modern network access control systems use several components to accomplish these tasks:

- Access control server – conducts the authentication, compliance policy checks, and pushes authorization policy to the point of network access
- Authenticator – the middleman that communicates with the endpoint and passes credentials to the access control server to verify
- Supplicant – software on the endpoint that communicates with the authenticator
- Endpoint – client or device trying to access the network

In addition to the components used in the process, the process itself needs to be understood. The following high-level diagram will help visualize the communication flow.

Figure 1 - Dot1x Process Flow



("Wired 802.1X deployment guide," 2011)

Depending on the specific NAC vendor chosen, there might be some variance in the process flow. However, generally, this is how a basic flow works. Your RADIUS server (access control server) may have different identity sources configured and relay the authentication request to Active Directory, a SAML server, and/or a token server for validation. In those scenarios, the RADIUS server acts as the central point and contains rules that specify which external identity source to use for each incoming authentication request.

The Authenticator plays a vital role. It has the instructions for how to request credentials from the endpoint, what to do if there is no reply, acceptable authentication methods, continually verifies the identity to ensure nothing has changed on the endpoint, and ultimately enforces the policy dictated by the access control server. For the purposes of this paper, we will focus specifically on the methods used by the authenticator to interrogate the endpoint. The two methods that will be examined concerning ICS networks are 802.1x and Mac Authentication Bypass (MAB).

Of the two authentication methods, 802.1x is the most reliable. It involves a supplicant that provides verifiable credentials to the authenticator. The credentials can take many forms – username and password, machine credentials, certificates, or any combination. The biggest issue with these types of credentials is the requirement for the supplicant. In the case of ICS networks, it is often not possible to install one, since most devices do not have an actual operating system for it to run on. This is where MAB steps in.

With MAB, the only thing inspected is the MAC address of the device as the credential passed to our policy server for verification. It might seem that this is acceptable because a MAC address is supposed to be globally unique and impossible to change once it is "burned in" on the device. However, it is easy to spoof MAC addresses, making the endpoint appear to be something it is not. If trust is based solely on the MAC, it provides a high degree of predictability but also a much higher risk of abuse.

When considering a highly sensitive and critical environment such as ICS networks, the tolerance for mistakes is extremely low. The sensitivity of these networks combined with the highly technical nature of network access control is where most of the OT resistance stems from. The OT side of the house is charged with the uptime of the control systems and without OT buy-in, there will be no chance of deploying a network access control system.

First, the OT team needs to understand what is happening. This can be addressed in many ways, but the primary concern is that a task that could have been completed entirely by OT staff for decades will now require IT intervention. In most cases, this will be a good enough reason to derail the implementation of a NAC system on its own. So, there must be a way to continue to do the OT tasks 24 hours a day without requiring IT intervention. Additionally, OT staff will still need the ability to troubleshoot issues in a way they will understand.

4. Profiling

Profiling uses information available, either directly provided by or gathered independently of the authentication process. Each of these additional bits of information are referred to as an attribute. When you have enough of them for an endpoint, the confidence in the endpoint's identity dramatically increases if it tries to authenticate subsequent times, thereby reducing the risk of using MAB as an authentication method. The challenge then becomes obtaining enough attributes to make an accurate determination and knowing which ones to trust more than others?

Generally speaking, attributes you get from more trusted sources are inherently more trustworthy. For example, Active Directory is an authoritative identity source. Both user and machine information needs to be added from a trusted administrator. Public Key Infrastructure (PKI) data also falls into this category because it is independently verified, and rules for issuing certificates are governed by trusted third parties. Other attributes that trusted individuals manually assign are also inherently more trustworthy. On the other hand, attributes gathered from sources like DHCP requests, ARP, DNS, and LLDP are less reliable. The main reason is that they are predicated on something that can be faked. DHCP is tied to a MAC address just like ARP. LLDP and CDP are dependent on the endpoint and are also easily forged. While attributes learned this way could be helpful to bolster a profile and provide additional depth, especially if we see changes in the attributes over time, they are not the best choice to solely base the degree of trust from.

When building a profile, the NAC system administrator should look at the combination of the attributes mentioned above. The more that match the defined profile, the more confident you are that a new endpoint is a particular type of endpoint on the network. For example, considering the MAC, DHCP, AD user account, and AD machine account can be sufficient to be sure that a newly seen laptop is a particular model used by a specific department. This is significant because we use these profiles to determine the degree of trust we have for an endpoint and, as a direct result, the level of access it is granted on the network.

5. Requirements for Success

Now that the groundwork has been laid to understand the necessary processes and components, they can be implemented. The first step is defining the goals for a successful implementation. Based on previous information, a list of requirements can be established to define a successful implementation:

1. An authentication method supported by typical ICS devices, including PLCs, safety relays, sensors, HMIs, and other I/O devices.
2. An authentication process that will not impact the uptime for devices or interfere with process operations.
3. Must be able to validate the assigned policies and access levels.
4. Use reliable sources of attributes for profiling of the ICS devices.
5. Provide a mechanism for OT staff to onboard ICS devices without IT intervention

The requirements themselves are not extraordinary. The only one that stands out differently from a regular enterprise network is the fifth one, providing the OT staff with a method to directly influence the onboarding process.

While it sounds like it should be something relatively straightforward, it is one of the more challenging to accomplish. Thinking about the goal of network access control - to securely grant access to devices based on a complicated measure of trust - allowing someone not trained in security or even traditional IT to manipulate the process poses a high degree of risk.

6. Lab Setup

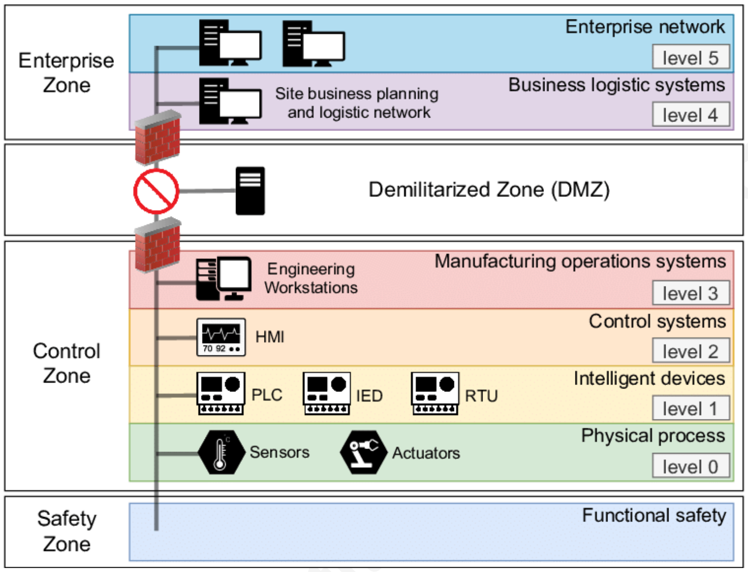
There are many options and combinations of tools that would accomplish these requirements. This research uses off-the-shelf tools representative of those accessible to most organizations.

- Access control server – Cisco Identity Services Engine (ISE). Cisco ISE is a highly robust and scalable platform that provides a wide array of tools and protocol support.
- Authenticator – Cisco industrial ethernet switches. This switching platform from cisco is the same as the Rockwell Stratix line of switches. They are hardened versions of the catalyst line and offer support for some specialized industrial protocols. However, all necessary configurations are the same on both product lines for our purposes.
- Supplicant – None. We will be testing more realistic industrial scenarios with older equipment that cannot use a supplicant.
- Endpoint – In the lab environment, two sample endpoints will be representative of real devices in a production deployment. A Rockwell Allen-Bradley controller (PLC) and a generic safety relay.
- OT software – Cisco Industrial Network Director (IND). Industrial Network Director is a tool designed to provide OT staff visibility and control of ICS environments.

7. Topology

The topology for the lab setup will mimic, at a reduced scale, the best practice Perdue model for ICS network design pictured in Figure 2.

Figure 2 - Purdue Model ICS Network Architecture



("Fig. 1: ICS Purdue model architecture," 2021)

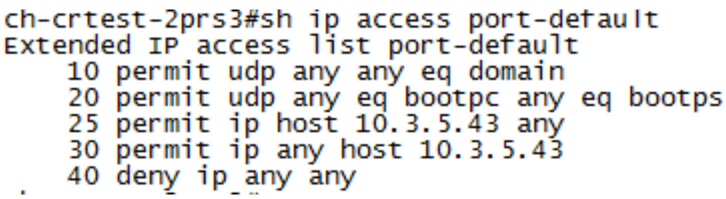
The ISE server will be placed in the enterprise zone while the switch is dedicated for only ICS traffic and the endpoints are in separate VLANs (levels), pictured above, for PLCs and sensors. Industrial Network Director resides in the Manufacturing operations zone and is accessed via HTTPS, over a VPN connection from the enterprise zone to the control zone.

8. Configuration

The majority of the configuration is the same for ICS and non-ICS deployments. The focus will be on the key differences and understanding why these changes were made, beginning with the authenticator.

First and foremost is the access control list in place before the endpoint completes the authentication process. Certain functions are required to be in place, regardless of the trust state of the endpoint, because they are used in profiling. In addition to those, we have to make accommodations for the server the OT staff will use to assist in onboarding endpoints, which is the first significant departure from a standard non-ICS deployment.

Figure 3 - Default Port Access List



```
ch-crtest-2prs3#sh ip access port-default
Extended IP access list port-default
    10 permit udp any any eq domain
    20 permit udp any eq bootpc any eq bootps
    25 permit ip host 10.3.5.43 any
    30 permit ip any host 10.3.5.43
    40 deny ip any any
```

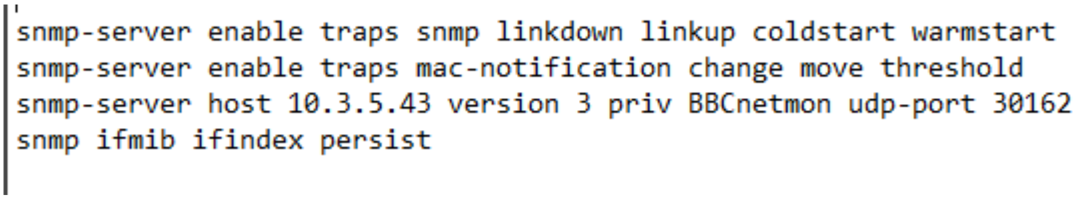
This config shows that DNS, DHCP, and IP access to our IND server are permitted pre-auth for all endpoints. DNS and DHCP are required for several things:

- If the endpoint is unknown, it needs to be forwarded to a guest process
- DHCP is captured and sent to ISE to assist in profiling
- DHCP and DNS are needed so IND can interrogate the endpoint so OT staff can positively identify for onboarding
- DHCP is also required for the authorization process. The IP address is recorded in a switch database and used to fill in any policy pushed to the port by ISE

It is important to remember that even though there is no established trust yet, a degree of access with minimal risk is needed to generate the attributes we will use to positively identify the device and establish the degree of trust.

In addition, SNMP traps have been configured to be sent to the IND server as well. Note that only the configuration specific to this process is shown in Figure 4.

Figure 4 - SMNP Lab Setup

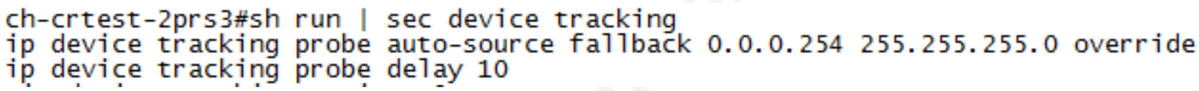


```
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.3.5.43 version 3 priv BBCnetmon udp-port 30162
snmp ifmib ifindex persist
```

Based on this config, when a device moves interfaces or gets plugged in, it sends a trap to the IND server. When this happens, the IND server begins its interrogation process of the endpoint.

Another feature used in non-ICS networks and is required for successful network access control deployment must be tweaked for an ICS environment. Device tracking is a feature that sends a gratuitous ARP to the port to find and record what is on that interface. This is not a problem in most environments and can easily be dealt with by any modern endpoint. Unfortunately, ICS networks, in some cases, are made up of decades-old endpoints that are not always able to handle these requests. To accommodate these older endpoints, we have to change the way the request is sent:

Figure 5 - IP Deice Tracking

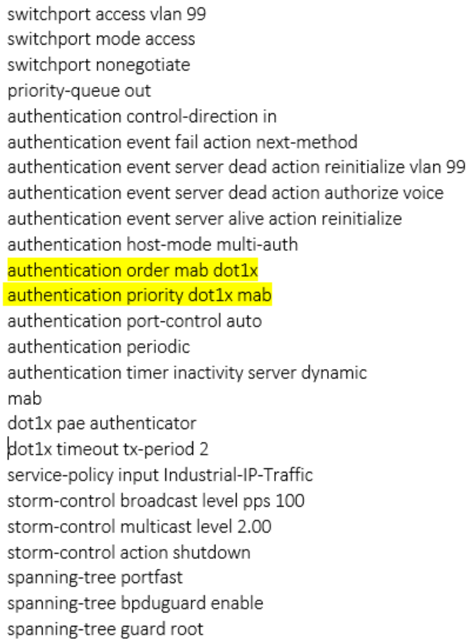


```
ch-crtest-2prs3#sh run | sec device tracking
ip device tracking probe auto-source fallback 0.0.0.254 255.255.255.0 override
ip device tracking probe delay 10
```

Figure 5 shows the commands needed to modify the default behavior of the device tracking feature to use a valid source address instead of the default source address of 0.0.0.0 and delay the process long enough for the endpoint to fully connect to the network. Without these modifications, older endpoints will think there are duplicate addresses on the network, effectively taking them offline.

Lastly, configurations on the switchports must be modified. Shown in Figure 6 is the entire switchport configuration required for NAC deployment with ISE and conforming to best practices for a higher security environment.

Figure 6 - NAC Switchport Configuration

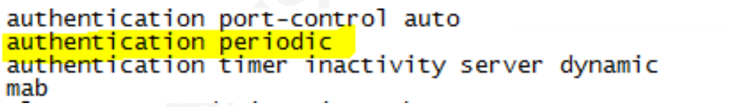


```
switchport access vlan 99
switchport mode access
switchport nonegotiate
priority-queue out
authentication control-direction in
authentication event fail action next-method
authentication event server dead action reinitialize vlan 99
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer inactivity server dynamic
mab
dot1x pae authenticator
dot1x timeout tx-period 2
service-policy input Industrial-IP-Traffic
storm-control broadcast level pps 100
storm-control multicast level 2.00
storm-control action shutdown
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree guard root
```

Lines worth noting here are highlighted. Acknowledging the sensitivity of these types of endpoints and that they are likely not able to participate in 802.1x, the first authentication method tested is MAB. However, if the endpoint is newer and can use 802.1x, it is likely also able to handle a change in the authorization. For that reason, we prioritize the authentication result received from 802.1x if it is successful.

There is one other key difference between enterprise and ICS deployments. In an enterprise deployment, the authenticator should periodically test the endpoint to ensure it is still the same and there have been no changes. However, this process can briefly interrupt the communication in an ICS environment until the reauthentication completes. The following configuration line should be omitted to avoid this from happening, which makes reauthentication happen only when the port state changes for up to down and back up.

Figure 7 - ICS Port Configuration Modification



```
authentication port-control auto
authentication periodic
authentication timer inactivity server dynamic
mab
```

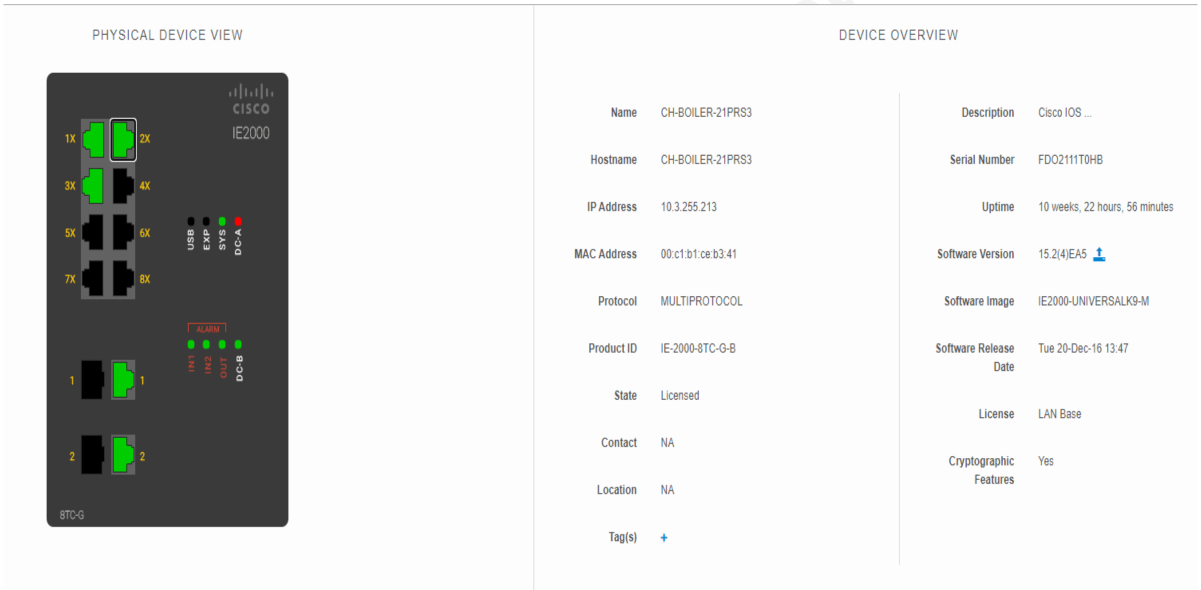
9. Onboarding for OT

To this point in the deployment, the authenticator has been set up and configured for the devices to make a connection. Next, the profiling and onboarding processes that will enable the OT staff to continue functioning normally will be examined. Those two processes, profiling and OT onboarding, will be instrumental in verifying the devices, allowing them to be appropriately authorized for network access.

Both of those processes will be facilitated by Cisco's Industrial Network Director. Industrial Network Director is a tool specifically designed to scan and aid in the management of industrial networks. It provides role-based access and uses numerous industrial protocols to directly communicate with sensitive ICS devices without interfering with their operation.

Software that provides this type of capability is key to implementing complex, modern controls in an ICS environment, including a network access control system. The following is a sample taken from the lab setup:

Figure 8 - IND Lab Sample Switch Details



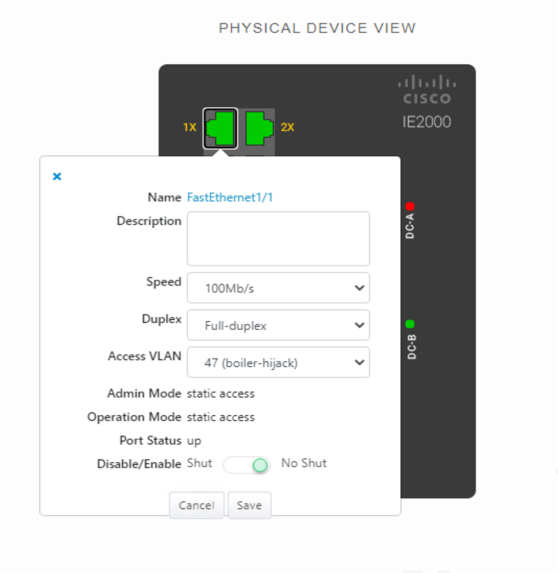
PHYSICAL DEVICE VIEW

DEVICE OVERVIEW

Name	CH-BOILER-21PRS3	Description	Cisco IOS ...
Hostname	CH-BOILER-21PRS3	Serial Number	FDO2111T0HB
IP Address	10.3.255.213	Uptime	10 weeks, 22 hours, 56 minutes
MAC Address	00:c1:b1:ce:b3:41	Software Version	15.2(4)EA5
Protocol	MULTIPROTOCOL	Software Image	IE2000-UNIVERSALK9-M
Product ID	IE-2000-8TC-G-B	Software Release Date	Tue 20-Dec-16 13:47
State	Licensed	License	LAN Base
Contact	NA	Cryptographic Features	Yes
Location	NA		
Tag(s)	+		

As shown in Figure 8, IND provides abundant information to the OT staff using it. Figure 9 shows a sample of a port's current configuration. Clicking on the port gives more options, including changing basic settings.

Figure 9 - IND Port Configuration

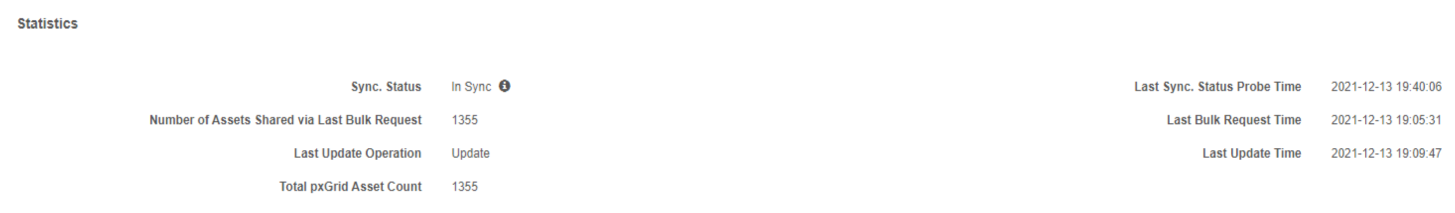


Name FastEthernet1/1
Description
Speed 100Mb/s
Duplex Full-duplex
Access VLAN 47 (boiler-hijack)
Admin Mode static access
Operation Mode static access
Port Status up
Disable/Enable Shut ● No Shut

Being able to change simple things like this safely increases OT comfort level with any modernization. Providing visibility to the environment and essential troubleshooting functions.

In addition to that, IND has tight integration with our policy server, ISE. Every bit of information gathered about the endpoints it sees is shared with ISE to enrich the endpoint profile to provide a higher level of confidence and, in turn, more granular access authorization. As shown in Figure 10, there is an overview of the sharing status and amount of data being shared with ISE.

Figure 10 - Shared Asset Summary in IND

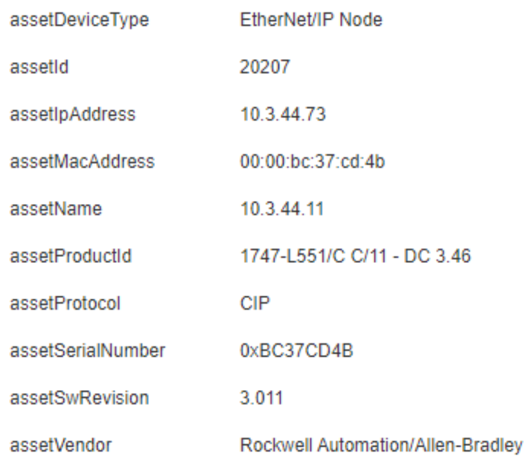

Statistics

Sync. Status	In Sync	Last Sync. Status Probe Time	2021-12-13 19:40:06
Number of Assets Shared via Last Bulk Request	1355	Last Bulk Request Time	2021-12-13 19:05:31
Last Update Operation	Update	Last Update Time	2021-12-13 19:09:47
Total pxGrid Asset Count	1355		

The shared data can be grouped into two categories. Learned and manually set. Learned data is gathered about the device when it is discovered. As described before, this is done automatically when the device is connected to the network. The SNMP link trap sent by the switch, which we configured previously, initiates a process of discovery in which the device is probed with different industrial protocols. Common industrial protocol (CIP) is one of those used.

Figure 11shows what is discovered about the test device and shared with ISE during this process:

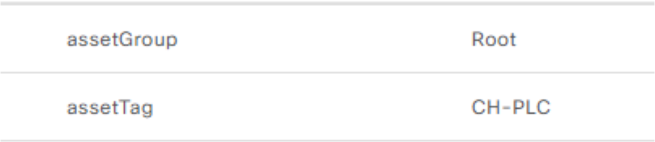
Figure 11 - IND Shared Attributes



assetDeviceType	EtherNet/IP Node
assetId	20207
assetIpAddress	10.3.44.73
assetMacAddress	00:00:bc:37:cd:4b
assetName	10.3.44.11
assetProductId	1747-L551/C C/11 - DC 3.46
assetProtocol	CIP
assetSerialNumber	0xBC37CD4B
assetSwRevision	3.011
assetVendor	Rockwell Automation/Allen-Bradley

In addition to these types of attributes, there are manually entered attributes. As seen in Figure 12, IND offers a method of adding tags to devices and placing them in groups. The groups can be defined logically, where they all belong to a process or physically, based on placement in the plants.

Figure 12 - Custom Shared Attributes



assetGroup	Root
assetTag	CH-PLC

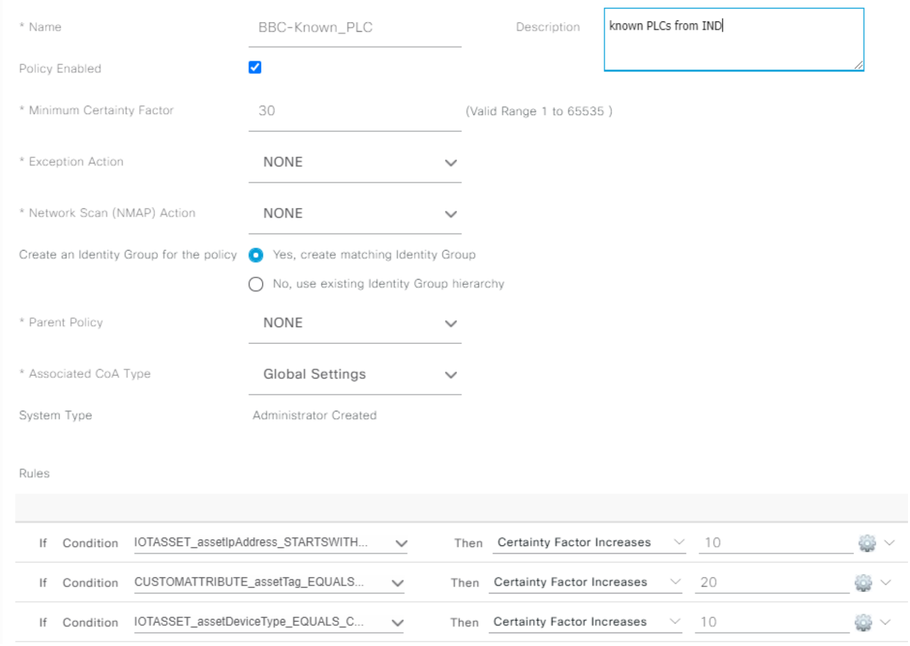
The process of assigning these tags to an asset causes an immediate update from IND to ISE. If they cause the endpoint to match a new profile, ISE will send a new set of access rules, called an authorization policy, to the authenticator.

10. Access Control Server

Our access control server (ISE) now has enough information to correctly identify the endpoints and assign an access policy. Let us take a closer look at putting the pieces we have so far together.

The first step in assigning policy is building a custom profile to positively identify our MAB authenticated devices using the attributes shared by IND. Figure 13 shows a screenshot of the profiling policy in the test lab:

Figure 13 - ISE Profile Policy



* Name	BBC-Known_PLC	Description	known PLCs from IND
Policy Enabled	☑		
* Minimum Certainty Factor	30	(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 ○ No, use existing Identity Group hierarchy		
* Parent Policy	NONE		
* Associated CoA Type	Global Settings		
System Type	Administrator Created		

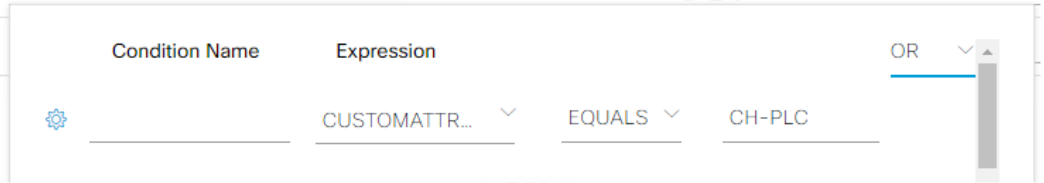
Rules

If	Condition	IOTASSET_assetIpAddress_STARTSWITH...	Then	Certainty Factor Increases	10
If	Condition	CUSTOMATTRIBUTE_assetTag_EQUALS...	Then	Certainty Factor Increases	20
If	Condition	IOTASSET_assetDeviceType_EQUALS_C...	Then	Certainty Factor Increases	10

There are a few things of significance here. First, the policy creates a matching identity group for the endpoints. This is significant later and while it isn't necessary for most types of endpoints being profiled, using it here will aid in faster authorization for more sensitive endpoints found in ICS environments.

The policy itself works off of a certainty level. Endpoint attributes match based on the conditions at the bottom. Conditions can have higher degrees of certainty depending on how reliable the attribute is. For example, in the lab, some common attributes like IP address are used to help locate the endpoint in our environment, associating a subnet with a site location. However, an IP address doesn't mean the endpoint is trustworthy on its own. Next comes the manually set attributes from IND that were discussed earlier. As shown in Figures 14 and 15, the asset tag assigned by OT staff during the onboarding process can be seen. Because each device is individually verified and tagged by the OT staff, it is more trustworthy, and we can assign this a high certainty level.

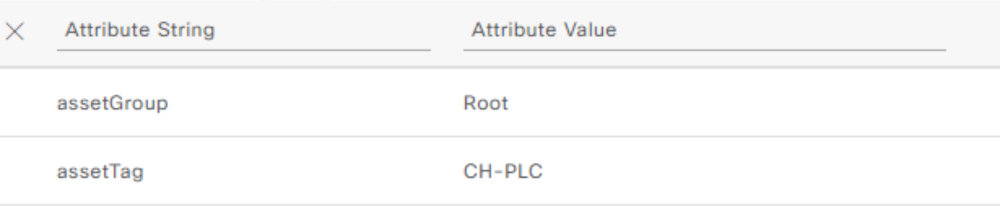
Figure 14 - ISE Profile Policy Condition



Condition Name	Expression			OR
	CUSTOMATTR...	EQUALS	CH-PLC	

This corresponds to the attribute shared by IND, shown in Figure 15, in the ISE the endpoint database:

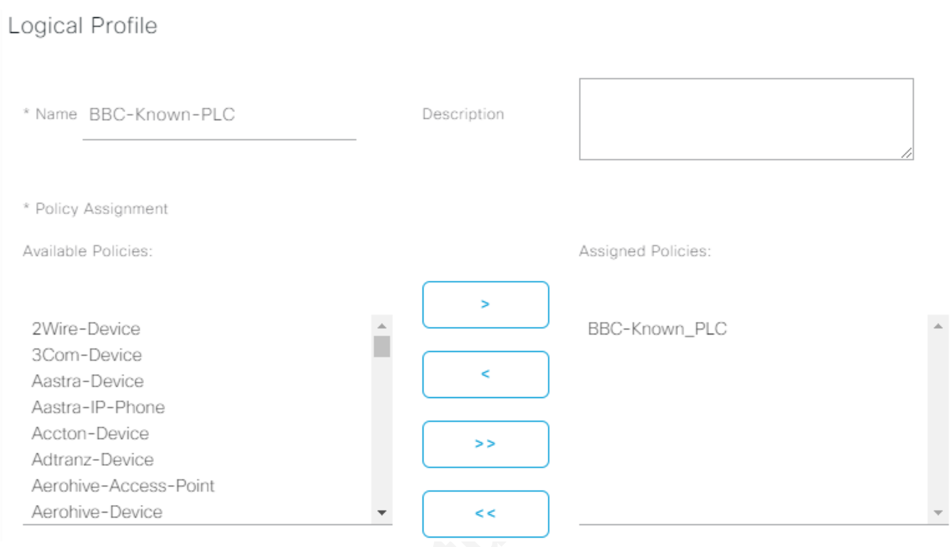
Figure 15 - Endpoint Custom Attributes from IND



Attribute String	Attribute Value
assetGroup	Root
assetTag	CH-PLC

From here, a logical profile is created that groups together similar profile policies and applies the custom profile label to the endpoint.

Figure 16 - ISE Logical Profile



Logical Profile

* Name BBC-Known-PLC

Description

* Policy Assignment

Available Policies:

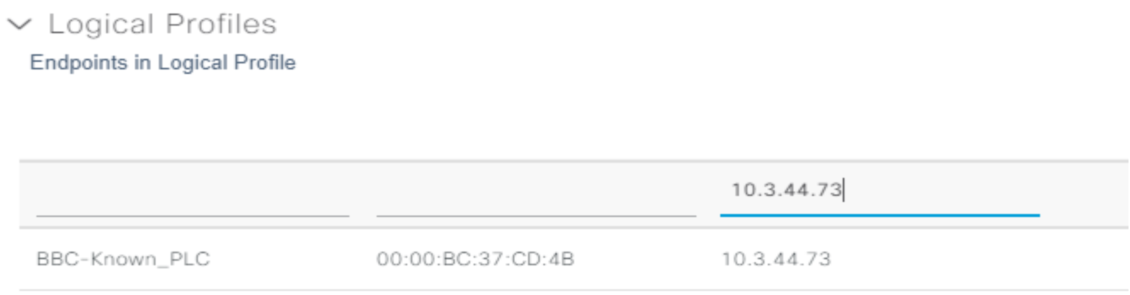
- 2Wire-Device
- 3Com-Device
- Aastra-Device
- Aastra-IP-Phone
- Accton-Device
- Adtranz-Device
- Aerohive-Access-Point
- Aerohive-Device

Assigned Policies:

- BBC-Known_PLC

This step allows us to group several profile policies so you can assign granular device profiles with common access permissions. It is best practice to use this method to provide scalability, even if you only have a single policy to start with. An example of when you would benefit from this model is if there are multiple manufacturers of I/O devices on the same production line. We would create a profile for each manufacturer but logically group them for the same access permissions. When creating the logical profile, it is visible in real-time what endpoints are being caught and labeled by the policy.

Figure 17 - Dynamic Endpoint Grouping



Logical Profiles

Endpoints in Logical Profile

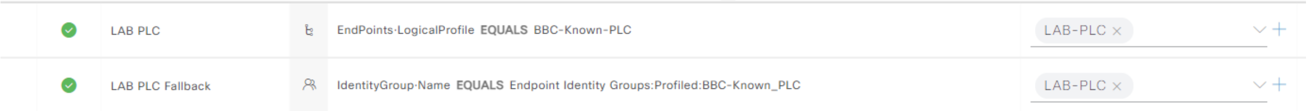
		10.3.44.73
BBC-Known_PLC	00:00:BC:37:CD:4B	10.3.44.73

Up to this point, the endpoint has been successfully tagged in IND, the tag and other attributes shared with ISE, built a profiling policy, and assigned a logical profile. The next step is to build an authorization policy to assign access permissions on the network.

11. Authorization Policy

When building the authorization policy, it is always best to be as specific as possible, ensuring only the intended endpoints are given access. As shown in Figure 18, 2 rules are present for the test ICS endpoints:

Figure 18 - Authorization Rules



✓	LAB PLC	EndPoints·LogicalProfile **EQUALS** BBC-Known-PLC	LAB-PLC ×
✓	LAB PLC Fallback	IdentityGroup·Name **EQUALS** Endpoint Identity Groups:Profiled:BBC-Known_PLC	LAB-PLC ×

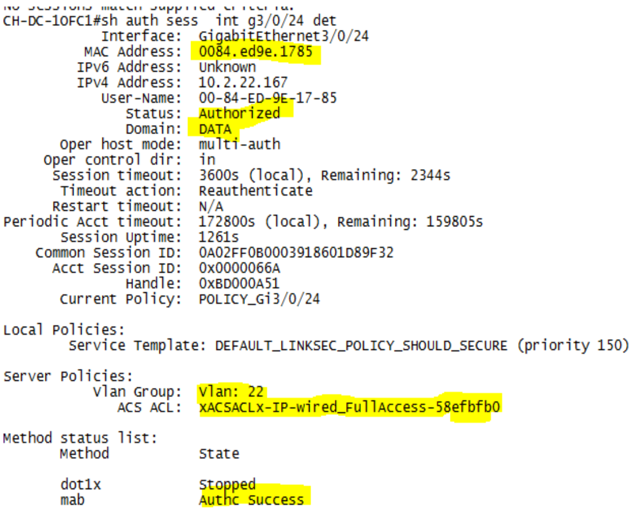
The first rule has a condition set that if the endpoint matches the profile created earlier, it gets an authorization policy called “LAB-PLC”. In that authorization policy can be many things; however, in this instance, it is only used to grant network access to its VLAN.

The second uses the endpoint group that was created earlier. Being second on the list, it will be used rarely. Its only purpose is a failsafe for endpoints that were previously profiled and, for some reason, disconnected. Upon reconnecting, if the profiling process takes too long, the endpoints will temporarily be given the same access as previously until the profiling finishes and the assigned policy updates. While this will still be a quick process from our perception, without this failsafe, it can cause a temporary issue with the device should profiling take too long or complete incorrectly on its initial attempt. This method can be considered risky, but it outweighs the risk of the process failing and causing a denial of service in the ICS environment.

12. Verification

Verifying the policy is being applied correctly can be done in a few ways. Of course, the NAC system will have its internal logs, and initial troubleshooting can be done here to ensure it matches the policy you believe it is. However, the best way is on the network access device itself, the switch. The switch is where the policy is ultimately applied, regardless of what is set in the NAC server, and therefore the best place to see what is happening. Looking at Figure 19, several points of interest are highlighted:

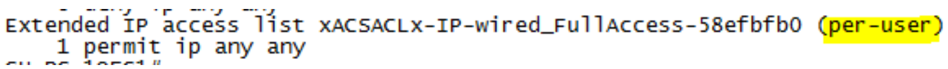
Figure 19 - Switch Authentication Details



```
CH-DC-1OFC1#sh auth sess  int g3/0/24 det
            Interface:  GigabitEthernet3/0/24
          MAC Address:  0084.ed9e.1785
         IPv6 Address:  Unknown
         IPv4 Address:  10.2.22.167
            User-Name:  00-84-ED-9E-17-85
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  in
      Session timeout:  3600s (local), Remaining: 2344s
       Timeout action:  Reauthenticate
      Restart timeout:  N/A
Periodic Acct timeout:  172800s (local), Remaining: 159805s
       Session Uptime:  1261s
    Common Session ID:  0A02FF0B0003918601D89F32
      Acct Session ID:  0x0000066A
               Handle:  0xBD000A51
       Current Policy:  POLICY_Gi3/0/24

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 22
              ACS ACL:  xACSACLx-IP-wired_FullAccess-58efbfb0

Method status list:
       Method           State

       dot1x            Stopped
       mab              Authc Success
```

The highlighted items show the detected MAC address, and the endpoint was authorized for data access. These three lines are helpful to confirm the device is what was expected and that it fully passed the NAC process. Moving on to the VLAN assignment and access-list name in the "Server Policies" section. Server Policies refers to settings sent to the switch to be enforced from the NAC server. Based on the output in Figure 19, the test endpoint matched a profile for a device that should be on VLAN 22, and the port default of 99 was successfully changed, placing it in the appropriate VLAN. Additionally, the access control list was applied and can be viewed to verify it.

Figure 20 - Dynamic Access Control List



```
Extended IP access list xACSACLx-IP-wired_FullAccess-58efbfb0 (per-user)
    1 permit ip any any
```

As shown in Figure 20, the access list has been dynamically placed in the switch configuration. It has the designation of "per-user", indicating that this is being applied to a specific user, in our case device, session. Even though our lab permits traffic to any destination, you can restrict the traffic based on the Perdue model architecture or your adaptation of it.

13. Caveats

The lab testing has shown what it looks like to have an entirely successful scenario. However, there are plenty of ways that things can go wrong. The normal NAC process has been heavily customized, added steps and components not typically involved. With each of them, there can be challenges. Here are a few of the more significant ones.

The biggest challenge is the consistency of design, referring to the actual connectivity of the PLCs and endpoints. The typical PLC backplane design is made up of a few parts:

- Processor – The brain that runs the ladder logic.
- I/O cards – Cards of this type are used to either direct connect devices or for some older style (non-ethernet) communications.
- Comm cards – Ethernet communication cards used in more modern designs.

The older, preferred way for machine designers to deploy these devices is by using two ethernet cards. The first one provides the OT staff with a management point, and the second branches off to a wholly unmanaged and isolated network. While complete visibility to the private network would be available via IND, no policy or any form of NAC can be applied without modifications.

Two ways to overcome this limitation would be to either create management connections to the isolated switches behind the second comm card and make further configuration customizations to force their use for all the NAC functions or convince the OT staff to abandon this design and instead make full use of the Perdue model shown in Figure 2. That approach would entail every endpoint being directly on the IP network and segregated by using VLANs and NAC policy.

Another thing to be on the lookout for is the age of the devices. It is critical to have a complete understanding of the endpoints you are dealing with before attempting to use any of the configurations mentioned. In addition, a lab setup like the one used to test should be considered a requirement. This is important because of something mentioned earlier – some devices are not able to handle a change in the authorization. If you look at the port configuration shown in Figure 6, it starts in access VLAN 99 when the endpoint connects. This is essentially a dummy VLAN and not capable of communication to other production network segments. During the course of authorization, the NAC server assigns it a new VLAN to use when the endpoint is properly identified. This process is called a change of authorization, and older devices cannot handle this change after the first initialization of the network card. Not knowing which endpoints fall into this category before deployment can cause significant outages.

To account for that type of issue, you will have to first identify them in a lab or a slow, controlled rollout of NAC. Once you have the list, we will take a calculated risk and not use the temporary access VLAN at the start. You would put the final intended VLAN as the default access VLAN on those interfaces. The NAC process will still function as it should, and our initial access control list will prevent unauthorized levels of access to devices before they are fully identified and authorized. The default VLAN of 99 is an added layer of security and should be used when the endpoints support the dynamic change. Having a production plan in place initially will not compromise the security of our systems (beyond a potential attacker knowing the IP scheme you use) since the NAC prevents all communications beyond DNS, DHCP, and IND probes.

Lastly, while the addition of IND to the NAC process is vital for the OT staff to continue to control and troubleshoot the environment, it can also be a risk. Remember that the tags applied in IND are key to assigning profiles and, ultimately, access policy. Accidental changes in those tags can cause devices to be reevaluated and potentially cause devices to lose access completely. It also added another step in the process and must be treated as a critical system itself, for purposes of controlling access to the software and ensuring the integrity of the systems it runs on.

14. Conclusion

Looking back at the requirements stated before we started, our goals were to:

1. Provide authentication method supported by common ICS devices
2. Not impact uptime or reliability of connection for devices
3. Must be able to verify the process, end-to-end

4. Be easily scalable
5. Use reliable sources of attributes for profiling
6. Provide a mechanism for OT staff to onboard endpoints and troubleshoot

Throughout the paper and testing in the lab, we have illustrated that all of these are possible in an ICS environment with proper planning. As with any NAC deployment, planning remains the most crucial element. We discussed the process of discovering device types, their specific requirements, and potential challenges with outdated equipment. Highlighted unique configurations needed to ensure success in a highly sensitive ICS environment and how to verify the correct policy is being applied.

Providing a method for OT staff to onboard and troubleshoot endpoints was vital in the success of the deployment, not just a method to gain acceptance. It offered a way to validate the devices before granting network access, gave OT staff tools to perform basic network tasks, and was vital in providing highly reliable endpoint attributes needed for profiling.

Even though this process was successful, it is not without its risks. Our lab was set up under ideal conditions, with very few devices and no additional load on the NAC servers beyond our tests. The caveats, risks, and deployment complexity suggest that a NAC deployment in such highly sensitive environments should be done in slow, staged rollouts to minimize potential interruption.

For these reasons, I conclude that NAC deployment in ICS environments is not only possible but achievable in real-world environments. However, such a deployment must not be taken lightly. It will require extensive planning, testing, and validation in a controlled environment before implementing it on production systems.

References

Awati, R. (2021, July 26). What is network access control (NAC) and how does it work? Retrieved from https://www.techtarget.com/searchnetworking/definition/network-access-control

Cisco Identity Services Engine Installation Guide, Release 3.0. (2021, December). Retrieved from https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/install_guide/b_ise_InstallationGuide30.pdf

Fig. 1: ICS Purdue model architecture. (2021, February 13). Retrieved from https://www.researchgate.net/figure/ICS-Purdue-Model-architecture_fig1_349195440

Installation guide for Cisco industrial network director, release 1.11.x. (2021, December). Retrieved January 17, 2022, from https://www.cisco.com/c/en/us/td/docs/switches/ind/install/ind_1-11_install.html

Wired 802.1X deployment guide. (2011, September). Retrieved from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html