CLAROTY
Clarity for OT Networks

CLAROTY WHITEPAPER

Accelerating Network Segmentation Initiatives with Claroty Continuous Threat Detection

Table of Content

Introduction

Let's start at the top. We believe one of the most important actions industrial asset owners can take to protect their operational technology (OT) networks from cyberattacks is implement solid network segmentation. When we say "segmentation" we are referring not only to segmentation between the IT and OT networks, but also segmentation within the OT network environment (aka micro segmentation, zones, etc.). The former can make it harder for attackers to gain a foothold within the OT network and the latter can make it much more difficult for them to move laterally if they do happen to gain access. For example, if a piece of malware is introduced to the OT network from a connection to the IT network, segmentation can keep it contained, preventing it from propagating and causing widespread damage. The same goes for an attacker who gains direct access to the industrial environment. Network segmentation within this environment makes it much more difficult for attackers to do reconnaissance work or to access key targets.

After years of neglect, security requirements for OT environments are becoming more formalized and network segmentation is becoming a baseline requirement. Standards such as the ISA/IEC-62443 provide a reference for implementing secure network zones and segments within an ICS network – requiring that segmentation be put in place between control system networks and non-control system networks. Further validating this progression, the latest *Gartner Market Guide for Operational Technology Security* added a new product category referred to as OT Network Segmentation. This category includes the capabilities required to manage and secure data flow between defined networks, including firewalls and unidirectional gateways.

Obviously, network monitoring can provide early-warning of a possible attack regardless of whether you have segmented the network or not. The terms "monitoring" or "anomaly detection" that are applied to the category of tools like Claroty's Continuous Threat Detection (CTD) focuses on the product's ability to observe real-time changes and anomalies in an OT network that could impact industrial processes. This includes potential malicious behavior or critical changes that may or may not be malicious but should be reviewed. Logic says the sooner an attack is detected, the greater the chances of limiting its impact. But there are other benefits to this technology that may not be so obvious.

Based on our experience with hundreds of operational environments, network segmentation projects can require lengthy design and implementation periods, not only consuming significant staff time from both Network Ops and OT teams, but also requiring networks to be taken offline. Industrial enterprises are highly sensitive to any project that requires downtime in production plants and other operational processes, as this may have a direct revenue impact. Often the extended timelines come from the difficulty networking teams have in planning and designing segmentation schemes with limited or outdated information about how the industrial network is configured and operating in its current production state. This is where a network monitoring solution can play a pivotal role.

Network monitoring tools in general, and CTD in particular, provide several features that can help accelerate segmentation initiatives and improve your segmentation architecture – all the while proactively monitoring and protecting the industrial network.

How Claroty Can Help

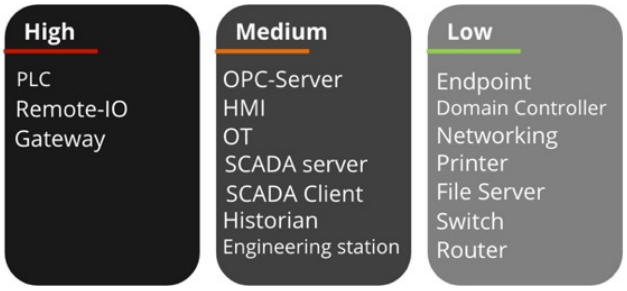
Claroty's Continuous Threat Detection provides network, operations and security teams with a deep, always-current, view of ICS network assets, communications, protocols and communication patterns. The system discovers all assets and asset configuration details across the entire industrial network – including application layer specific operational commands. Leveraging this detailed information, the system automatically generates a set of "virtual zones" – logical groups of assets communicating with each other under normal circumstances.

Consequently, and without deploying actual physical separation (VLANs) or logical isolation (firewalls), customers can implement a "virtual segmentation" scheme to highlight and further prioritize alerts that show potentially malicious communication between virtual network segments. Alternatively, customers can make use of virtual zones as the blueprint for designing and architecting logical or physical network segmentation projects and thus accelerate new or existing segmentation initiatives – let's take a closer look at how this is achieved.

Understanding Virtual Zones

By automatically profiling all the communication that occurs between assets in the network, the system generates high-fidelity baselines that portray communicating assets, used ports, protocols, and specific application-layer commands (e.g. ladder logic, configuration changes, and firmware updates). Armed with this information, and leveraging proprietary algorithms, Claroty's virtual zones functionality groups similar devices (e.g. PLCs), from like vendors (e.g. Rockwell Automation) sharing common communications characteristics into logical clusters (virtual zones).

Each virtual zone is then assigned a sensitivity level. For example, PLCs which have a direct impact on process integrity are automatically assigned a high sensitivity level. It should be noted that virtual zones are flexible and adaptable allowing the system to automatically assign newly discovered assets to the most appropriate virtual zone and consequent sensitivity level.



Alerting policies are defined based on the sensitivity of the generated virtual zone. For example, a newly discovered communication taking place between two virtual zones can be indicative of malicious traffic attempting to cross from one zone to another. Claroty's virtual zones enhance the contrast between legitimate communication and anomalous, potentially malicious, cross-zone communication. As seen in figure 1 on the following page, the system has automatically generated a virtual zones map – based on the identified asset types, vendor, and communication profile as exhibited in the ICS network.

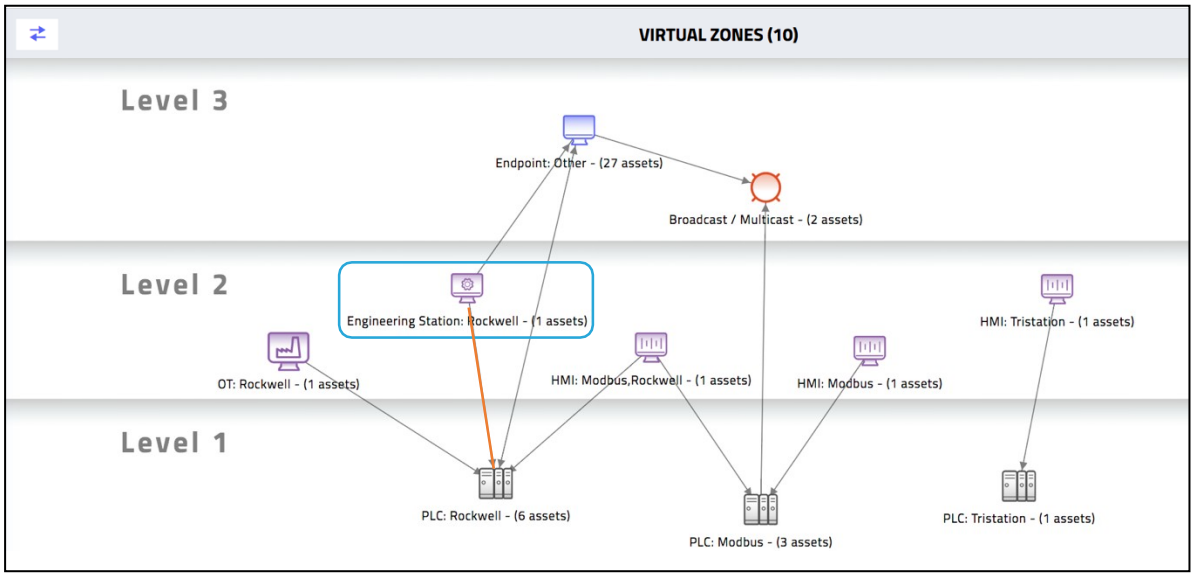


Figure 1 – Automatically generated virtual zones example

In this scenario, 10 virtual zones were created – with each zone containing a description and number of similarly grouped assets. We can see a Rockwell engineering station found in level 2 performing write operations to 6 Rockwell PLC's found in level 1. The downward pointing arrow (marked in orange) determines the direction of the performed operation (write from level 2 -> level 1).

Manually Altering Virtual Zones

While the system automatically generates a model based on existing ICS network assets and communication patterns, users have the option to manually change the location of a specific asset (e.g. in the respective Purdue Model layer) and alter its original virtual zone association. For example, as seen in figure 2 on the following page, an asset (originally in level 3) is manually assigned to a virtual zone in level 1. As a precaution, the system immediately alerts on this anomaly, displaying a warning icon and message that the asset has been assigned to a Purdue level to which it did not originally belong. Manually assigning an endpoint to a different virtual zone, as in this example, also automatically changes its default sensitivity level and overall alert triggering policy.

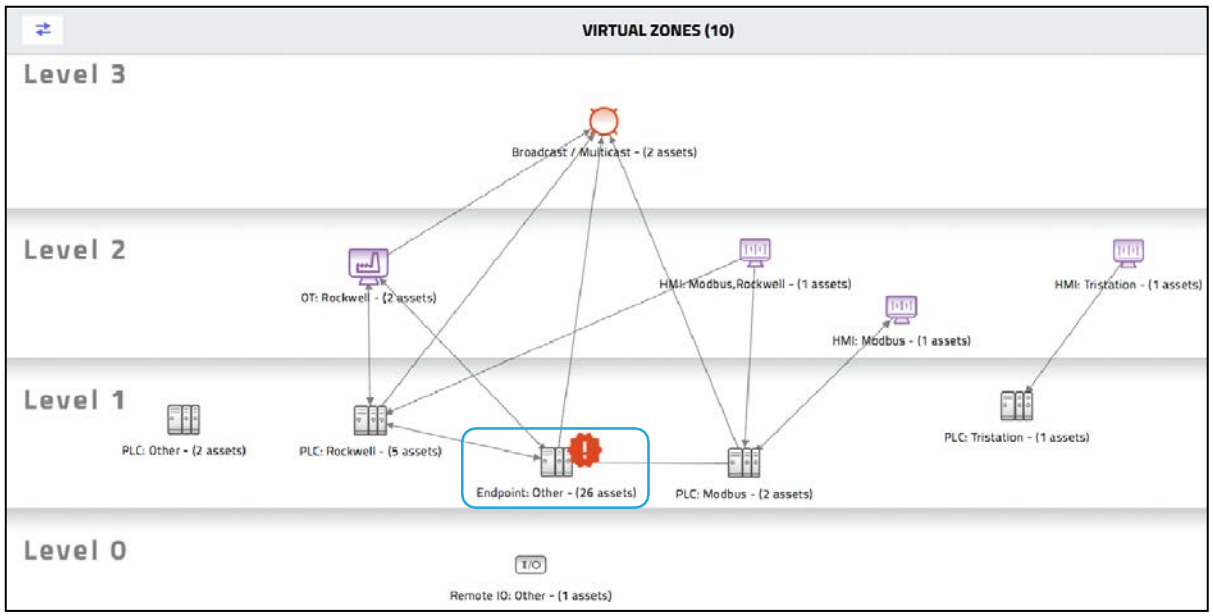


Figure 2 –Customized virtual zones example

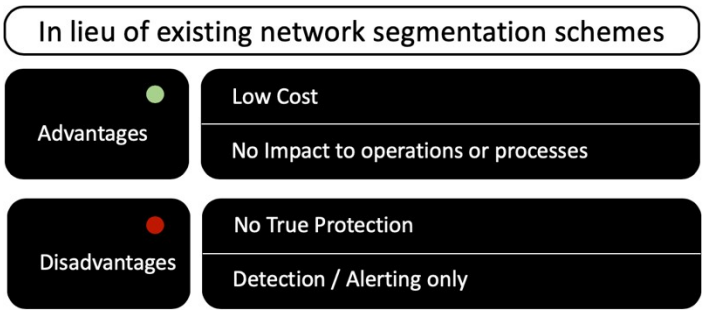
Virtual Zones & Network Segmentation Options

Claroty's advanced virtual zones can be used to either kick-start new network segmentation initiatives or implement an alert-based "virtual segmentation" scheme to improve security without having to perform physical ICS network segmentation. Let's take a closer look at how this can be achieved along with the advantages and disadvantages of each approach.

Using Virtual Segmentation In Lieu of Actual Segmentation

Many ICS networks are originally designed as "flat", meaning all assets are in a single segment. In these situations where no current physical or logical separation exists, and implementing physical segmentation would be too costly, prolonged or impractical, "virtual segmentation" can significantly reduce risk to the network with comparatively little time, cost or effort.

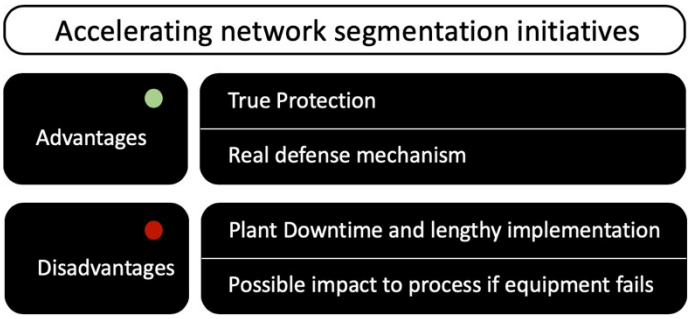
Without actual physical separation (VLANs) or logical isolation (firewalls), CTD groups devices into logical clusters (virtual zones) and creates virtual segments, based on communication characteristics observed under normal operating circumstances (as previously described). The system is then able to prioritize alerts dealing with anomalous activity that communicates across zones. This improved level of detection and alert prioritization can be achieved at a relatively low cost, without impacting existing processes and without requiring network downtime for implementation.



Accelerate Network Segmentation Initiatives

While CTD provides virtual segmentation, it can also help accelerate real network segmentation initiatives -- such as those leveraging VLANs or firewalls. These types of physical and logical network separation schemes help to actively prevent any interconnecting traffic from occurring between zones – preventing attackers from moving across the network if they do get access.

On the upside, actual segmentation provides a real proactive defense mechanism. On the downside, if implemented incorrectly, it has the potential for blocking legitimate ICS network traffic and consequently impacting physical process or the OT team's ability to monitor operations. Again, we believe starting with a detailed map of the network can greatly reduce these risks.



Claroty's virtual zones feature helps network administrators better understand which assets are required to continue communicating with each other to execute legitimate automation processes, and consequently, which assets need to belong to each network segment. In addition, the system provides comprehensive information about exactly how assets are communicating – including application level conversations – providing the necessary details beyond just port and protocols as required by security teams when creating new or updating existing firewall rules.

Conclusion

Many large ICS environments are susceptible to today's sophisticated attacks due to a focus on perimeter security – leaving internal networks "flat" and difficult to defend even from known (and well-documented) exploits. Attacks on poorly segmented industrial networks are often the result of malware (or a live attacker) finding the path of least resistance into the network, and moving to penetrate more valuable assets.

The first step to securing these environments is having an effective methodology for complete network visibility, mapping, and monitoring of changes in real-time. As a consequent step, it is critical to build, test and validate segmentation policies to proactively restrict access to critical assets. Irrespective of whether you are looking to accelerate network segmentation initiatives or implement a virtual segmentation scheme – Claroty's advanced virtual zones feature within Continuous Threat Detection, can help you implement these important projects.