Automating OT network segmentation to protect industrial operations

Cisco Secure Firewalls and Cyber Vision Working Together

Protecting industrial operations from cyberthreats goes beyond isolating the industrial network from the rest of the world. Using firewalls to build an Industrial Demilitarized Zone (IDMZ) is key to providing the first line of defense. But as more Operational Technology (OT) assets are connected, a more granular network segmentation approach is needed to contain the impact of a cybersecurity event.

In many cases, industrial organizations have isolated parts of their operational network using zone-based firewalls. While this greatly improves protection, it can be costly to deploy and cumbersome to manage. Worse, the rigid nature of such an architecture can hinder the ability to quickly adapt to the evolving requirements of modern industrial operations. Cisco® Secure Firewalls, together with Cisco Cyber Vision, offer an ideal solution to automate industrial network segmentation without having to modify network setups.

Benefits

- Safeguard production uptime by blocking common threats, known vulnerabilities, and zero-day exploits using a Machine Learning (ML)-based exploit detection engine.
- Protect industrial operations, thanks to the industry-leading Snort® intrusion detection and prevention system (IDS/IPS) with Cisco Talos® threat intelligence.
- Simplify OT network segmentation by eliminating the need for zone-based firewall appliances and complex physical setups.
- Enable collaboration between IT and OT teams to build the right access policies.
- Instantly adapt segmentation policies to industrial process changes with centralized management informed by OT visibility.
- Drive compliance with ISA/IEC 62443 by implementing industrial zones and conduits.

Cisco Cyber Vision

Cisco Cyber Vision is designed to help industrial organizations and critical infrastructures improve operational resilience by gaining comprehensive visibility into their industrial control networks and their OT security posture. It automatically builds a detailed inventory of all industrial assets, maps their communication activities, and provides insights into device vulnerabilities, network issues, malicious traffic, abnormal behaviors, and more.

Operations managers and control engineers can leverage the Cyber Vision map to group devices according to their role in the industrial process, creating logical zones within which communications are allowed. By doing so, they are documenting how the industrial network should be segmented and are building the foundation to drive compliance with the ISA/IEC 62443-3-3 industrial security standard.

Cisco Secure Firewall

The Cisco Secure Firewall portfolio delivers evolved network security backed by industry-leading Talos threat intelligence, protecting critical infrastructures against zero-day attacks in proprietary OT protocols as well as public malware campaigns and vulnerability exploits. In addition to traditional port and protocol segmentation, Cisco Secure Firewalls can decode OT protocols to define command-level filters and block legitimate but privileged commands to Industrial Control Systems (ICS), for instance.

Cyber Vision and Firewall Management Center allow OT segmentation groups defined by the OT team in Cyber Vision to be used for both east-west and north-south firewall enforcement. This level of automation helps reduce manual workloads, streamlines your security management process by enabling IT/OT collaboration, and helps ensure that your firewall policies remain in lockstep with your OT industrial processes.

How it works

- Cisco Cyber Vision inventories industrial assets and maps their communication activities.
- Operations managers leverage the Cyber Vision maps to group assets into industrial zones.
- Cisco Secure Firewall Management Center (FMC) pulls asset group information from Cyber Vision using the Cisco Secure Dynamic Attributes Connector (CSDAC).
- Each Cyber Vision group becomes a dynamic object in FMC, to which the IP addresses of the assets in the group are mapped in real time.
- IT and OT managers work together to define access policies to be applied to each dynamic object.
- Policies defined in FMC are enforced by Cisco Secure Firewalls.
- Any modification to Cyber Vision groups is reflected in FMC dynamic objects in real time and is automatically enforced by Cisco Secure Firewalls, without the need to redeploy policies.

Using the Cisco Secure Dynamic Attributes Connector (CSDAC), OT asset groups created in Cyber Vision are automatically made available to the Firewall Management Center as dynamic objects. IP addresses of OT assets are continuously imported and mapped to dynamic objects, helping ensure that objects are always aligned with the industrial processes defined by the OT team.

The dynamic nature of this integration eliminates the need for manual policy deployment each time there is a change to the Cyber Vision map. Adding an asset to a group in Cyber Vision or moving it to another group will automatically modify the corresponding object in FMC. The access policy configured for this object will apply to this asset in a matter of just a few seconds.

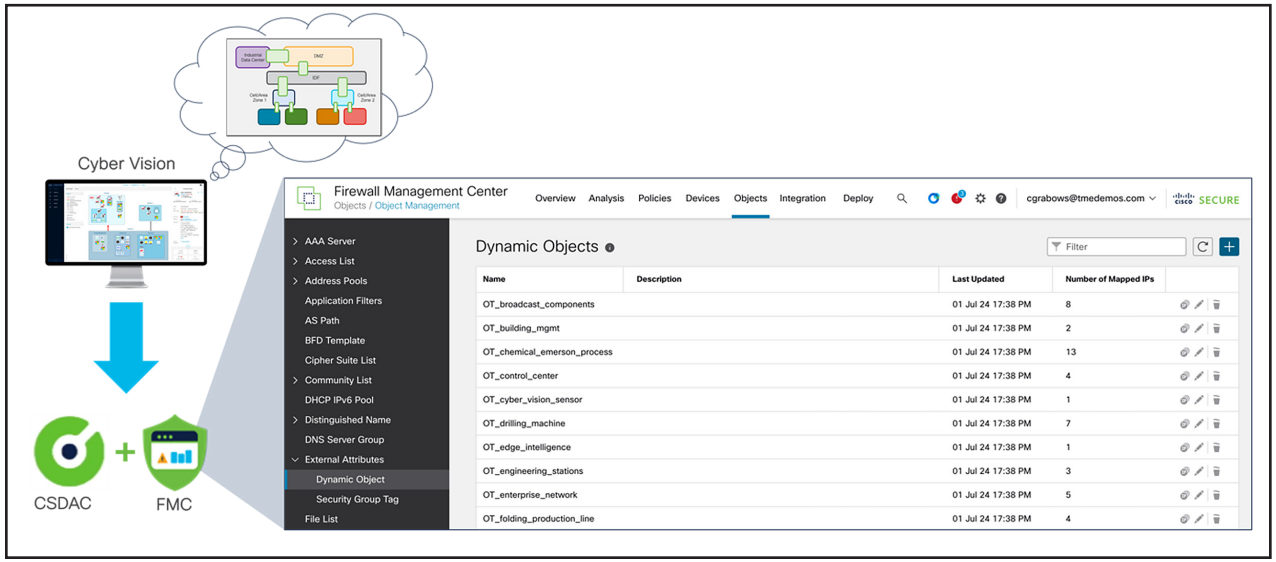

Figure 1. OT asset groups created in Cyber Vision are dynamic objects in FMC

Dynamic objects can easily be incorporated into access control policies to allow or deny communications between assets based on source/destination, ports, protocols, and even ICS commands using AppID. Cisco Secure Firewalls installed in the industrial distribution frame or Purdue level 3 will enforce these access policies, driving east-west and north-south segmentation without the need to deploy dedicated firewall appliances in each zone.

The Cisco advantage

For more than 20 years, Cisco has been helping industrial organizations around the globe digitize their operations, working with manufacturers, power and water utilities, energy companies, mines, ports, railways, roadways, and more. Today, Cisco offers a market-leading portfolio of industrial networking equipment plus a comprehensive suite of cybersecurity products, integrated tightly together with a deep understanding of OT requirements. It's a rare combination.

By designing, developing, and testing products together, Cisco enables IT and OT teams to achieve advanced outcomes while reducing the complexity, time, and gaps incurred by the need to make point products work together. Our solutions come with comprehensive design and implementation guides that will help you reduce risk, accelerate implementation, and make the most of your technology stack.

Streamline OT network segmentation today

Talk to a Cisco sales representative or channel partner and visit cisco.com/go/cybervision or cisco.com/go/fmc to learn more.

C22-4763071-00 11/24