# SECURITY IN A POINT TO MULTI-POINT OPERATIONS ENVIRONMENT


## ABSTRACT

Implementing a secure OT environment presents new challenges. Meeting these challenges requires new security tool capabilities that are not being serviced adequately by today's offerings. This paper discusses the key requirements that network management should be reviewing as part of their tool selection process.



cuculan LLC

Most practitioners will agree that OT environments have historically been neglected as a critical network component from a security perspective. In the past, the IT community were not involved in managing the OT network with the engineering community looking at OT as being their domain to manage while the IT guys managed the "business systems" network. This has all changed with the increasing convergence of OT and IT and the security vulnerabilities that this exposes to a business. The exposure dramatically changes the role of the CISO and expands their role in managing the security vulnerabilities of the total network.

OT networks are no longer just confined to a single network. As operational environments become regional, national, and global OT information becomes a critical resource enabling businesses to competitively provide products and services.

**What does that mean for existing security capabilities and what additional capabilities do we need to ensure security in these environments?**

Today we have several security solutions which are all effective solutions in particular use cases. However, they also present challenges in terms of their management and breadth of capability to provide full security for an OT environment.

- Firewalls which are general-purpose solution designed to address a wide array of requirements. They are used to protect individual resources and require a Firewall in-line with each resource to support east/west protection in an OT environment. Moreover, they require sophisticated networking management knowledge with both filtering and encryption required to fully secure a resource
- Remote access VPN typically used for temporary remote access to a network
- Site-to-site VPN used for connecting two or more networks. In an OT environment network connectivity is not sufficient. Individual resource to resource protection is required within each connected network as well as between network segments. To implement resource to resource security would require individual site-to-site VPN's for each connection along with associated management complexity and cost

**So, what do we need to provide full protection of OT resources from a communications perspective?**

We need a security capability whose goal is management simplicity but delivers to the full security requirements of an OT point to multi-point OT resource network. The solution needs to segment and isolate resources from other resources on the network.

This means:

- All security management is self-contained within the security device without the need for reaching into the cloud for management or installing agents on protected resources. Each additional node in the security network itself is another attack surface so minimizing the attack surface is critical
- The solution should be a purpose designed device to address point-to-point and point-to-multipoint security. The device should be designed specifically for this purpose and not provide general purpose networking solutions flexibility such as a Firewall
- Communication from a source to a destination are proactively authorized in advance of communication with the destination
- The destination resource proactively verifies that each communication is from an authorized source prior to acceptance
- Communication between resources is encapsulated, encrypted, and tunneled end to end
- The solution can support micro-segmentation to an individual resource in the network
- Each resource-to-resource connection uses a unique key set established using industry standard TLS 1.3 protocol. Keys are periodically automatically refreshed without interrupting communications
- Security devices have automatic failover capability
- Packet replay protection is provided
- A single pane of glass for deploying and remotely managing all security capabilities in the network

Cuculan offers a solution that meets the above requirements for your consideration.

https://cuculan.com/product