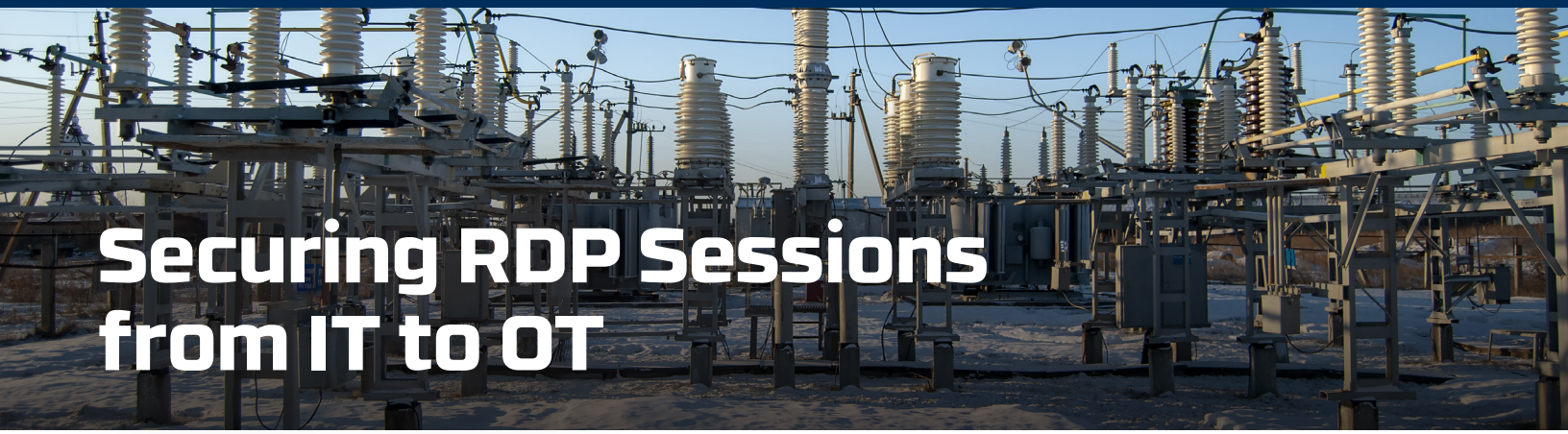
OWL Cyber Defense

USE CASE



Securing RDP Sessions from IT to OT

Use Case Summary

INDUSTRY

Critical Infrastructure

CHALLENGES

Need for secure, remote access into an OT network from an IT network to adjust configurations, change settings, apply software patches, and perform routine maintenance and support

SOLUTION

ReCon, Owl's bidirectional data diode with two, independent, one-way paths and a single, locked down port

BENEFITS

Customers do not need to physically access the OT network to perform updates and can easily and remotely access the network when necessary, from IT, to perform routine updates and maintenance as quickly as possible.

Cybersecurity Challenge

The explosion of employees working from home has created a new set of security challenges. Critical infrastructure operational technology (OT) networks consist of a variety of industrial control systems that need to be updated and maintained. In many cases, critical infrastructure organizations utilize the Remote Desktop Protocol (RDP) to update OT systems remotely or from within their information technology (IT) network. To secure this two-way communication, critical infrastructure organizations typically deploy a firewall between an IT and OT network, however firewalls rely on software configuration and are susceptible to zero-day attacks. The Department of Homeland Security (DHS) states, "If bi-directional communication is necessary, then use a single open port over a restricted network path". Designed to meet DHS guidance for securing bi-directional communications, ReCon secures RDP sessions with hardware-enforced data diode level security, providing more security than traditional firewalls.

ReCon Use Case

ReCon enables highly restricted bi-directional RDP communications between IT or remote locations and OT networks. It consists of two, individually isolated, one-way paths, all within a single 1U hardware appliance. ReCon restricts the use of TCP/IP ports and each side of Recon must be configured and managed separately. The TCP/IP connection can only be initiated from the source side of ReCon. Operators outside of the OT network can use ReCon to remote into OT to adjust configurations, change settings, apply software patches, and perform routine maintenance and support. Client authentication ensures that only authorized users can access ReCon securing the integrity of the device and data being transferred. ReCon can be turned on, only when an RDP session is required, and turned off once the session is complete.

USE CASE REQUIREMENTS

- A secure, two-way connection for remote RDP access from an IT network or a remote location into an OT network to perform updates
- Maintain an air-gapped OT architecture

Solution

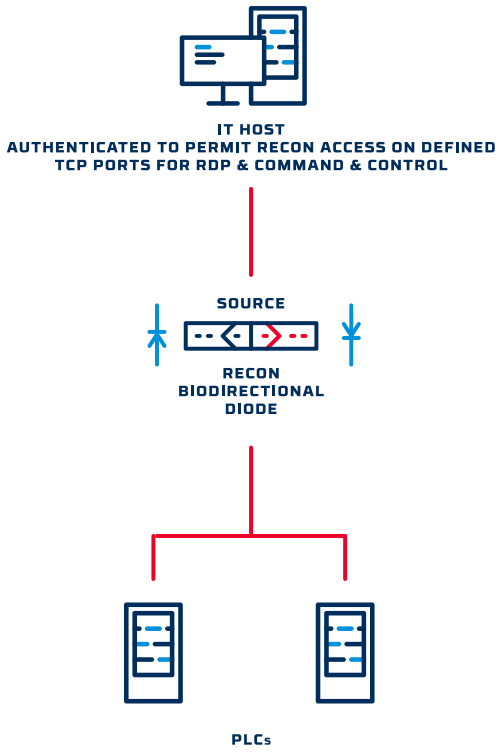
RECON
Hardware-enforced data diode, built for secure, round trip, bidirectional communications with secure remote access capabilities.

Secure RDP Access through ReCon

The urgent need to move employees from onsite to remote has transformed the way customers access OT assets. Considered insecure for OT access, RDP sessions have become more common as organizations are forced to consider alternative ways to ensure business continuity. The challenge is how to secure RDP sessions.

For example, a technician, working from home or from an IT network, requires OT access to modify settings on two PLCs. A ReCon appliance is installed at the OT boundary. A certificate authority on the ReCon device generates authentication credentials delivered "out-of-band" to the remote technician. A client application is installed on the remote client computer, authenticating the user to the Recon device, over a secure VPN connection. Once authenticated, the technician can securely access the PLC.

ReCon is comprised of two unidirectional data diodes over independent one-way paths. A TCP/IP protocol break prevents steganography and ensures that no routable information is passed between networks. The TCP connection can only be initiated from the source side, from a single whitelisted source IP address connected to a fixed destination IP address. Dual Administration (source/destination) provides highly segmented management control and port mapping, allowing the administrator to control the destination address for the connection, ensuring that no entity outside the destination network knows anything about that network.



OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense
203-894-9342 | Info@owlcyberdefense.com