Secure Industrial Automation
Remote Access Connectivity

Using eWON and Talk2M Pro solutions

www.ewon.us
Overview

eWON is a global provider of secure industrial remote access connectivity. By leveraging a combination of its cloud based, redundant infrastructure called Talk2M and its industrial eWON hardware devices, eWON created a first-to-market integrated approach to secure remote access to industrial control systems. Since its launch in 2006, eWON’s Talk2M has successfully hosted millions of encrypted VPN sessions allowing engineers to easily and securely remotely monitor and troubleshoot their machines.

Challenges

Remote access has posed numerous challenges for decades. Various solutions including modems, traditional VPNs, IT client software and IP Sec routers have failed to offer a repeatable and secure, reliable solution that is simple to configure, manage, deploy and use.

Customers have different network topologies, requirements and technical competencies. The biggest challenge remains being compatible with existing customer networks and industrial automation and control system (IACS) architecture.

Approach

Understanding the challenges associated with securely deploying and managing remote access within an IACS, eWON developed a solution compatible with industry accepted open standards that addresses the following key areas related to secure remote access in a defense-in-depth layered approach;

- Policies & procedures
- Network Infrastructure
- Management & Accountability
- Encryption
- Application
- eWON Hardware Devices

Benefits

The benefits of leveraging the eWON Solution include;

- Mitigating risks by improving uptime and equipment availability and efficiency with managed secure remote access, users and devices.
- Reduce onsite travel.
- Reducing mean-time-to-repair (MTTR).
- Lowering the total cost of ownership (TCO) of the IACS remote access approach.
- Professionally managed globally redundant cloud infrastructure.
- Compatible with industry standards (SSL and VPN).
The eWON Security Approach

Using a defense-in-depth approach based on guidelines set forth by ISO27002, IEC 62443-2-4 and NIST Cyber security Framework 1.0 in addition to numerous other publications, guidelines and industry best practices, eWON developed a managed, hybrid, layered cyber security approach to protect its devices, network and most importantly, its customers’ industrial control systems.

eWON, the global leader in secure industrial automation remote access, considers device and network security to be a core competency fully integrated at every level within the framework of our solution.
Security Vs Convenience and Acceptance
One of the key challenges with remote connections to industrial control systems is balancing the needs of an engineer or PLC technician with the mandate by the IT department to ensure network security, integrity and reliability. Finding a solution that is readily accepted by both business groups has been a challenge for many years and a source of frustration and inefficiency for all stakeholders. eWON understood that maintaining network security was essential for IT acceptance. At the same time, eWON realized users will never use solutions that are complex, difficult or interrupt productivity. By balancing both the security and ease of use, eWON has created a best-in-class Remote Access solution that works for both end users and IT managers.

The eWON Layered Security Approach
The integrated Talk2M and eWON remote access solution was designed with simplicity and security in mind. To make the eWON and the devices behind it remotely accessible, eWON routers make an outbound connection via UDP or HTTPS to the Talk2M infrastructure. Using our VPN Client software, eCatcher, authorized users are able to log into their Talk2M account and connect to their eWON devices anywhere in the world.

While ease of use is important, the security, integrity, and reliability of eWON's Talk2M cloud infrastructure and its customers' networks is eWON's first priority. Using a defense-in-depth approach based on guidelines set forth by ISO27002, IEC 62443-2-4 and NIST Cyber security Framework 1.0 and other publications, guidelines and industry best practices, eWON developed a managed, hybrid, layered cyber security approach to protect its devices, network and most importantly, its customers' industrial control systems.

eWON Hardware Devices
Network segregation, local device authentication, physical switch for enabling/disabling access.

eWON industrial routers are the physical hardware component of eWON’s remote access solution. The eWON units are typically installed in the machine control panel with the machine connected on one side (LAN) and the factory network on the other (WAN). When a connection needs to be established the eWON acts as the gateway through which all traffic passes. When the eWON is first configured for VPN access,
security settings on the device restrict traffic between its two network interfaces. This network segregation limits remote access to only those devices connected to the LAN of the eWON. Access to the rest of the network is prevented.

The eWONs themselves have user-level access rights separate from the Talk2M login. Only users with appropriate credentials and access rights can change the security settings on the eWON. Similarly, for the devices with data services, only authorized users can view or modify the data.

All of our hardware devices feature a digital input. A switch can be connected to this input and the state of the switch can enable or disable the WAN port. This allows the end user to keep full local control of whether or not the device is remotely accessible.

The eWON needs the same type of settings as a PC connected to the same network (IP address, subnet mask and gateway, plus any optional proxy settings). Since the eWON can act as a DHCP client, it can be configured to receive those settings automatically. However, the eWON also can be set up to use a static IP address that is assigned and controlled by the IT department if preferred.

**Application**

IP, port, and protocol filtering/firewalling available. Restricted access based on user, group, site for all or single devices or specific port.

Within the eCatcher application, Talk2M account administrators can set filtering and firewalling rules about which devices behind the eWON are remotely accessible and even over which ports and with which protocols they are accessible. When combined with Talk2M’s user rights management discussed below, Talk2M administrators have the ability to tailor the remote access rights to fit their organizational structure.

**Encryption**

VPN sessions are end-to-end encrypted using SSL/TLS for session authentication and IP SEC ESP protocol for tunnel transport over UDP and TCP/IP.

Communications between the remote user and the eWON are fully encrypted. All users and eWON units are authenticated using SSL/TLS for HTTPS session authentication and the IPsec ESP protocol for secure transport over UDP. Talk2M supports the X509 PKI for session authentication, TLS for key exchange, the cipher-independent EVP interface for encrypting tunnel data, and the HMAC-SHA1 algorithm for authenticating tunnel data.

**Management & Accountability**

Unique user logins, configurable user rights to different devices, connection traceability.

A Talk2M account may have an unlimited number of users. Administrators can create unique logins for every user who needs to access equipment remotely. These unique logins makes it easy to grant and revoke access privileges as needed. In addition, Talk2M account administrators can restrict which remote eWONs particular users can access, which devices behind those eWON are accessible and even the ports on those devices and the communication protocols used. For instance, an administrator might permit remote users to reach the web services in a particular
device for monitoring purposes but limit the ports used for making programming changes to only specific engineers.

Every remote connection is documented on the Talk2M Connection report. The Talk2M Connection report is a powerful IT auditing tool which allows account administrators to monitor which users are connected to which eWON and when and for how long they were connected.

**Network Infrastructure**
Globally redundant Tier 1 hosting partners, 24/7 monitoring, SOC 1/SSAE 16/ISAE 3402 Data Centers, ISO270001, CSA, SOC2.

The Talk2M infrastructure is a critical integrated element in our remote access solution. It is a fully redundant network of distributed access servers, VPN servers, and other services that act as the secure meeting place for eWONs and users. To increase reliability, redundancy and reduce latency, eWON works with multiple industry leading Tier 1, 2 and 3 hosting partners throughout the world to ensure best in class service. Talk2M is hosted in SOC 1/SSAE 16/ISAE 3402 and ISO 27001 certified data centers. The network of servers is monitored 24/7 to ensure maximum availability and security using intrusion detection systems (IDS), host intrusion prevention systems (HIPS) in addition to an array of alerting mechanisms.

**Policies & Procedures**
The eWON/Talk2M solution enhances and is compatible with existing corporate security policies, firewall rules, and proxy servers.

eWON understands that its customer designed their corporate security policies carefully. The Talk2M remote access solution is designed to be compatible with customers’ existing security policies. By using outbound connections over commonly open ports (TCP:443 and UDP:1194) and by being compatible to most proxy servers, the eWON is designed to be minimally intrusive on the network and work within the existing firewall rules. Within eCatcher, Talk2M account administrators can customize the password policies to force compliance to corporate password policies and can restrict which users can access which devices remotely. Talk2M account administrators can also view the Talk2M Connection report to see which users are connecting to which eWON devices and when. This report can be a valuable tool to ensure that your corporate remote access policies are being followed.
Summary
A combination of unique hardware and globally redundant cloud infrastructure creates a robust, secure and convenient method to enable encrypted remote access to machines, panels and other industrial automation devices.

The key added-value of Talk2M is the full integration of IT security standards by allowing an Internet communication tunnel between the user and the remote machine while still following the existing firewall rules and security policies of each network. This means little or no IT changes required and gives organizations the ultimate solution to manage their Remote Access needs with maximum control, visibility and security.

Technical Contact Information
In the U.S. contact;
eWON Inc.
Tel: (412) 586-5901 Fax: (412) 586-5920
Web: www.ewon.us Email: info@ewon.us
2345 Murray Ave, Suite 305, Pittsburgh, PA 15217

More information is available on our website at www.ewon.us or visit our support site at: http://support.ewon.biz

Worldwide Offices:
United States Belgium Japan