Ewon® BY HMS NETWORKS

Arquitectura Talk2M – Documento Técnico

Talk2M y Ewon

Arquitectura para Acceso Remoto Industrial

descripción general v3.1

Proporcionando Acceso Remoto en el mundo de Automatización

La disponibilidad de acceso remoto a sistemas para fabricantes de máquinas y OEMS, está convirtiéndose en un estándar en las expectativas de los usuarios del universo de sistemas de automatización industrial. En un periodo de ocho años, acceso remoto por medio de la Internet, ha reemplazado las comunicaciones telefónicas como medio de conexión a un sistema. Al mismo tiempo conceptos tales como “Enrutador Industrial” y “VPN” se han hecho más y más populares entre proveedores de servicio.

Hay diferentes opciones de Acceso Remoto por medio de la Internet en el mercado. En el libro electrónico “Secure Remote Access for Industrial Machines For Dummies”, hablamos de los beneficios de una arquitectura de acceso remoto sobre la internet. Por supuesto, una arquitectura basada en la nube es perfecta para conectarse utilizando comunicación VPN; gestionada por usuarios por un lado con comunicación VPN y generada por dispositivos del otro lado.
Comunicación VPN es parte de la vida cotidiana de muchos hoy en día, como, por ejemplo, cuando la utilizamos para tener acceso privado al servidor central de nuestra oficina.

En este artículo, nuestro objetivo es describir de forma amplia el paradigma de una plataforma basada en nube que hemos creado en Ewon: Talk2M. Este documento no se trata de un manual de usuario, pero acaso lo necesite para nuestra nube Talk2M, sugerimos que acceda a la liga:

http://Ewon.biz/support/product/talk2m/talk2m

¿Que es VPN y tunelización?

VPN (virtual private network) y tunelización son técnicas que permiten, entre otros beneficios, encriptar enlaces de datos entre usted y otra computadora. Esa computadora puede pertenecer a su empresa, a una persona o empresa de su confianza, o a un servicio comercial de VPN. La tunelización encapsula segmentos de información dentro de un protocolo encriptado, haciendo todo el tráfico de información por medio del túnel ilegible a cualquiera, a lo largo de la ruta de transmisión. El uso de VPN u otra forma de tunelización, es una de las mejores formas de garantizar que los datos no sean comprensibles a personas que no sean de confianza. Otro beneficio importante es la técnica de autenticación de los dispositivos remotos.

¿Qué es Talk2M?

Talk2M propone un servicio de conectividad basado en internet entre máquinas de usuarios u otros sistemas de automatización industrial de una planta, a lo que llamaremos de “máquina” en ese documento. Los usuarios de ese servicio generalmente son Ingenieros de Automatización que necesitan acceder a equipos ubicados con diferentes clientes, muchas veces en diferentes partes del mundo.
En el lado del usuario remoto, es necesario instalar un software para sistema operativo Windows, que se llama eCatcher. Este software establece comunicación transparente entre la computadora y Talk2M, por medio de la internet. Hay la opción de utilizar un navegador web para conectarse al sistema remoto, sin la necesidad de eCatcher, pero esto trae límites a la finalidad.
En el lado de la máquina, se debe instalar un Gateway Industrial Ewon (Cosy o Flexy) conectado, generalmente, al corazón de la máquina, un PLC (Programmable Logic Controller), una Computadora Industrial, u otro dispositivo de automatización de una planta. El Ewon es conectado por medio de uno de los cuatro puertos Ethernet, USB o serial (RS-232/RS-485 o Siemens MPI).

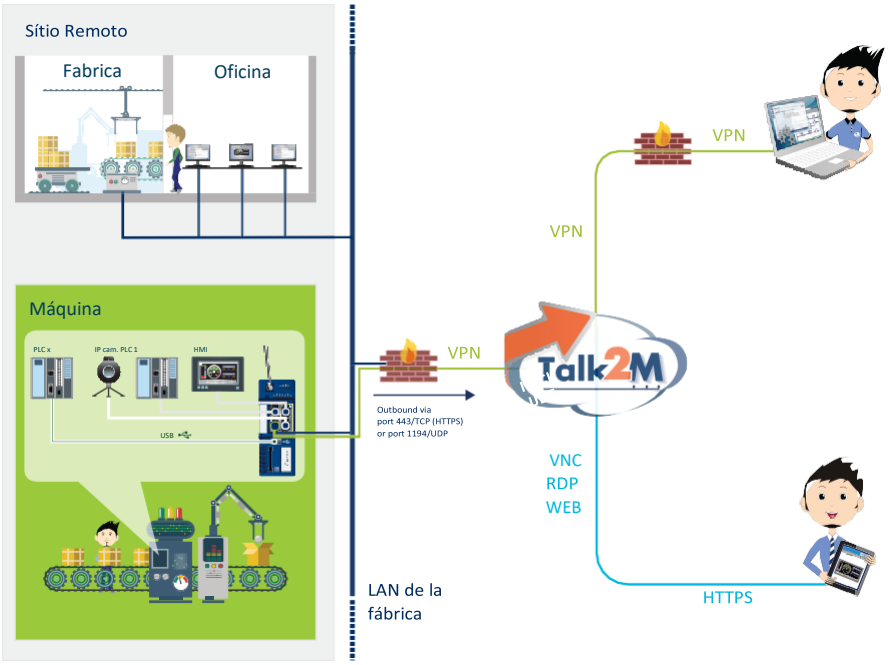


Figura 1: visión general de Talk2M

Entre el ruteador Ewon y el usuario, proveemos Talk2M, una infraestructura de comunicación basada en nube hecha de una serie de servidores, que permite comunicación originada por el usuario a los dispositivos remotos. El sistema opera una vez que los dos lados tengan acceso al Internet y alcancen a la nube Talk2M.

Empezaremos describiendo las posibilidades del lado del sistema de automatización industrial accediendo al internet, y como eso funciona.

¿Como conectar la máquina al Internet?

Tal como se ha mencionado anteriormente, el lado de la máquina necesita conectarse al internet para acceder a Talk2M. Hay distintas formas de hacerlo:

- La más común es usar una infraestructura física (por medio de cable) para acceder por medio de una LAN conectada al Internet.
- La segunda forma que se ve cada vez más comúnmente es por Wi-Fi. Muchos usuarios finales proporcionan acceso a una red inalámbrica, muchas veces hecha específicamente para uso de fabricantes de equipo original u otros proveedores de servicio remoto, aparte de la red corporativa de la planta.
- La tercera forma es, generalmente, una contingencia para cuando no hay LAN o Wi-Fi. La tecnología celular (3G, 4G) está disponible de forma global y proporciona una forma muy práctica de conectarse al Internet. En este caso, se necesita de una tarjeta SIM (chip) del proveedor de internet móvil, para permitir que nuestro ruteador celular se conecte al Internet.

De acuerdo con la tecnología utilizada por Ewon, la conexión a Internet es establecida por medio de una conexión WAN, a partir de una interfaz Ethernet (cable) o un modem embebido (celular, Wi-Fi, ADSL o PSTN). Es posible proveer más de una forma de acceso al Internet a un mismo dispositivo Ewon. Además de estas opciones, se pueden utilizar dispositivos externos para conectarse al Internet (modem celular, modem satelital, radio modem, etc).

Preferencia	Tipo de Conexión	Ventajas	Desventaja
1º	LAN	- No hay costo - Alto ancho de banda	Algunos usuarios no permiten uso de la LAN por política de seguridad
2º	Wi-Fi	- No hay costo - Alto ancho de banda	Disponibilidad creciente, pero es común al haber demasiados dispositivos
3º	Celular	- Acceso Global - Costo depende de la cantidad de datos en el plan seleccionado	Hay problemas de velocidad de conexión en diferentes partes. La tecnología cambia en cada país, y hay costo de acuerdo con el volumen de datos

Conectando la máquina a Talk2M

Una vez conectado al Internet, el Ewon se conectará a los servidores de Talk2M. La conexión es hecha en tres etapas:

1. Un proceso inicial donde el Ewon se conecta al servidor de acceso central (AS), se autentica por medio de una conexión HTTPS, y entonces va y busca los certificados. Esa operación es hecha una vez, pues el Ewon hace un respaldo de la clave de autenticación y de los certificados de seguridad. Hablaremos acerca de ese tema mas adelante.
2. Luego, toda vez que el Ewon necesite conectarse por medio de la VPN, lo hará por medio de una solicitud del nombre de host que debe usar del servidor VPN (VS), lo que puede cambiar en cada conexión. Esa solicitud es hecha por medio de una conexión HTTPS.
3. Finalmente, el Ewon establece un túnel VPN con el servidor más cercano disponible por Talk2M.

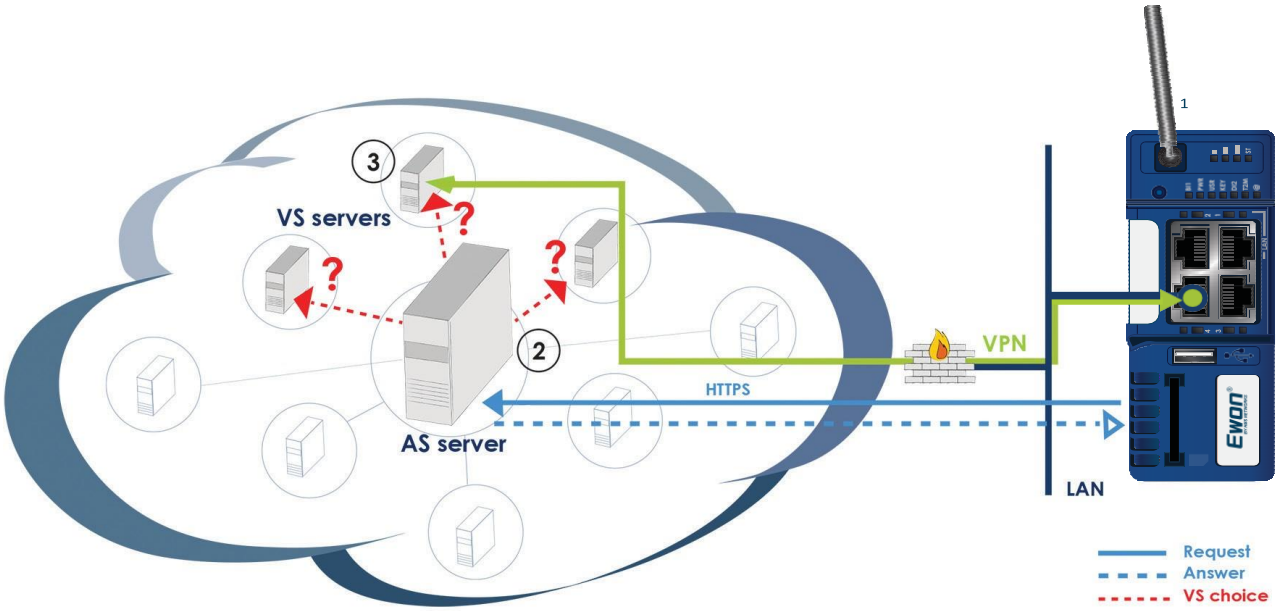


Figura 2: Visión general de comunicación de Talk2M

Conectando el usuario a Talk2M

De acuerdo con los pasos anteriores, todo se inicia por medio del software eCatcher en la computadora del usuario. Una vez inicializado, eCatcher necesitara la autenticación del usuario por medio de tres datos importantes:

- Nombre de Cuenta: una cuenta Talk2M se crea por medio de eCatcher. Cualquiera puede hacer esto de forma ilimitada. Cada cuenta incluye todos los usuarios que se pueden conectar a los Ewon dados de alta en esa cuenta especifica. Por ejemplo, el usuario A de la cuenta X nunca podrá conectarse a un dispositivo en la cuenta Y. Pero el usuario B de la cuenta Y lo puede hacer.
- Nombre de usuario: se recomienda no compartir cuentas, pero sí crear usuarios distintos por cada persona que necesita acceder a la cuenta Talk2M. No hay costo adicional para crear usuarios tanto en la cuenta Talk2MFree+ cuanto en la Talk2M Pro.
- Contraseña: cada usuario tiene su propia contraseña. El acceso al cambio de la contraseña puede ser del propio usuario o del administrador.

Una vez autenticado, el usuario tiene acceso al listado de dispositivos Ewon dados de alta en la cuenta Talk2M.

Ese paso es equivalente a las etapas 1 y 2 de la sección anterior, lo que significa que eCatcher almacenara la clave y lo certificado localmente, pero sí buscara el certificado después de cada autenticación. De hecho, eCatcher abre una sesión HTTPS en el servidor de acceso central (AS). El usuario puede realizar distintas acciones, como (por medio de los botones en el lado izquierdo de la pantalla):

1. Dar de alta un nuevo dispositivo Ewon en la cuenta. Daremos más detalles acerca de esa operación más adelante.
2. Cambiar/borrar información de dispositivos Ewon.
3. Añadir, modificar o borrar información de Usuários o Grupos de la cuenta Talk2M. Un Grupo es un conjunto de Usuários.
4. Añadir, modificar o borrar Pools, que son grupos de dispositivos Ewon.
5. Cambiar información de la cuenta.

Nota: El Punto 1 será explicado más Adelante en ese documento. Los puntos 2 a 5 pueden ser fácilmente ubicados en el la guía de usuario de Talk2M.

Cuando hacemos click sobre cualquier Ewon del listado (figura 3) y el dispositivo se encuentra en línea (lo que significa que una VPN con ese dispositivo es posible), eCatcher pide al AS abrir un túnel VPN. Así como en el párrafo anterior de la etapa 3, el AS indica al eCatcher cual servidor VPN (VS) se utilizará para establecer una conexión VPN. Pero en este caso es el propio Servidor VPN que ya se está utilizando por el dispositivo Ewon.

Entonces eCatcher inicializa el túnel VPN al VS que ya haya sido asignado por el AS. Las dos terminaciones VPN son automáticamente enlazadas por medio del mismo VS.

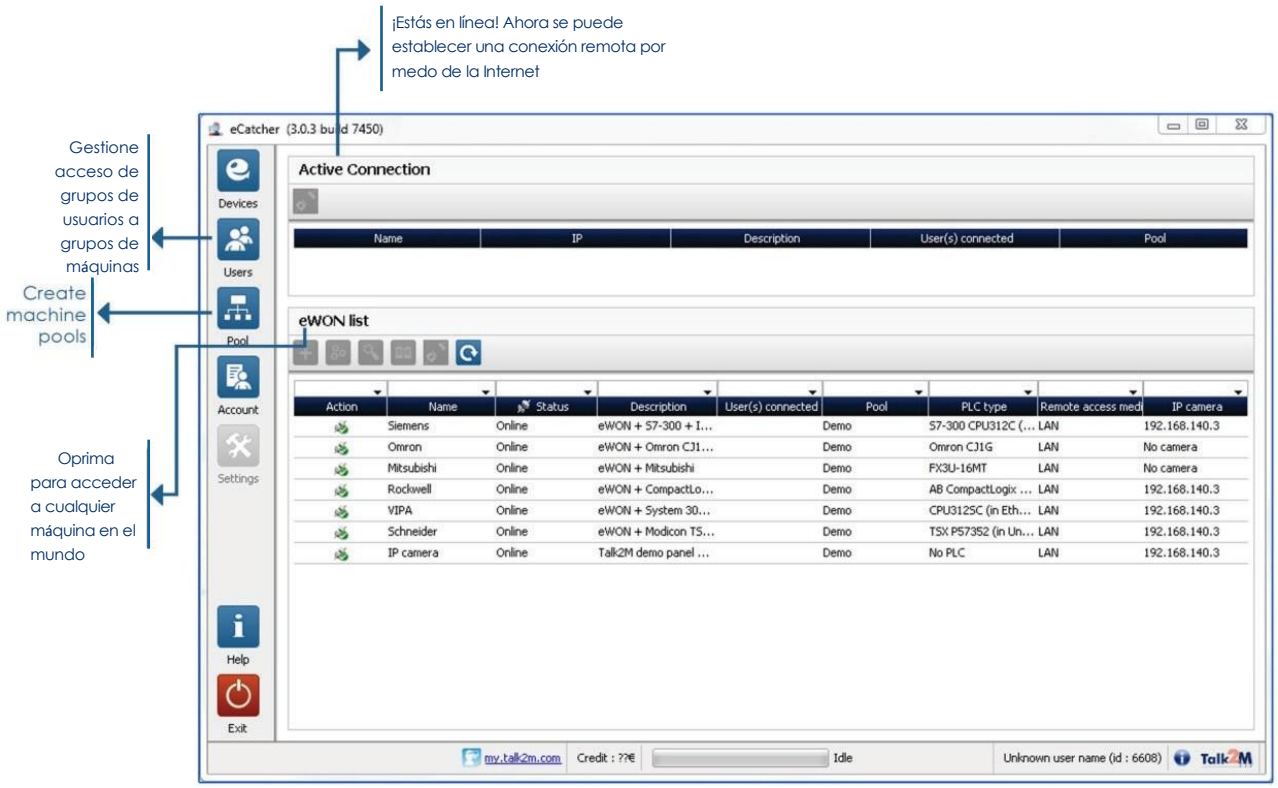


Figura 3: eCatcher y la lista de dispositivos conectados

Hablaremos más adelante de los dispositivos Ewon conectados de forma no permanente (fuera de linea)

Usando la conexión VPN

En los dos párrafos anteriores, describimos como conexiones desde un lado (usuario) a otro (máquina) son posibles.

Ambas conexiones VPN, cuando son establecidas, reciben una única dirección IP para VPN, proporcionada por el AS por medio del VS de la infraestructura de servidores. Mientras se pueda ver las direcciones VPN del lado del eCatcher y del lado del Ewon, no se podrá ver esas direcciones a partir del VS.

En eCatcher, la dirección VPN proporcionada es asignada a un adaptador TAP Win32. Ese adaptador provee la interfaz virtual que conecta la PC directamente al VS. La interfaz TAP es instalada automáticamente durante la instalación de la aplicación eCatcher.

Tener acceso al VS (por medio de la interfaz TAP) no es el objetivo final; de hecho, necesitamos alcanzar a la máquina remota o, en otras palabras, la LAN. Por otro lado, necesitamos indicar a la PC que todos los mensajes IP que contienen dirección de destino que pertenezca al rango de direcciones IP de la LAN del Ewon, deben ser encaminadas por medio de la interfaz TAP. Para que eso ocurra, una ruta debe ser automáticamente adicionada por eCatcher cuando la conexión VPN se establece. Esa ruta es borrada cuando la conexión VPN es cerrada o interrumpida. La dirección de destino de red es reconocida gracias a la información de configuración contenida en cada dispositivo Ewon, dado de alta en Talk2M. La dirección de la LAN es identificada cuando un Ewon se conecta a la cuenta Talk2M. En el caso que el usuario necesite conectarse a otro Ewon, la ruta anterior es borrada y se agregará una nueva ruta con la dirección del destino apropiado.

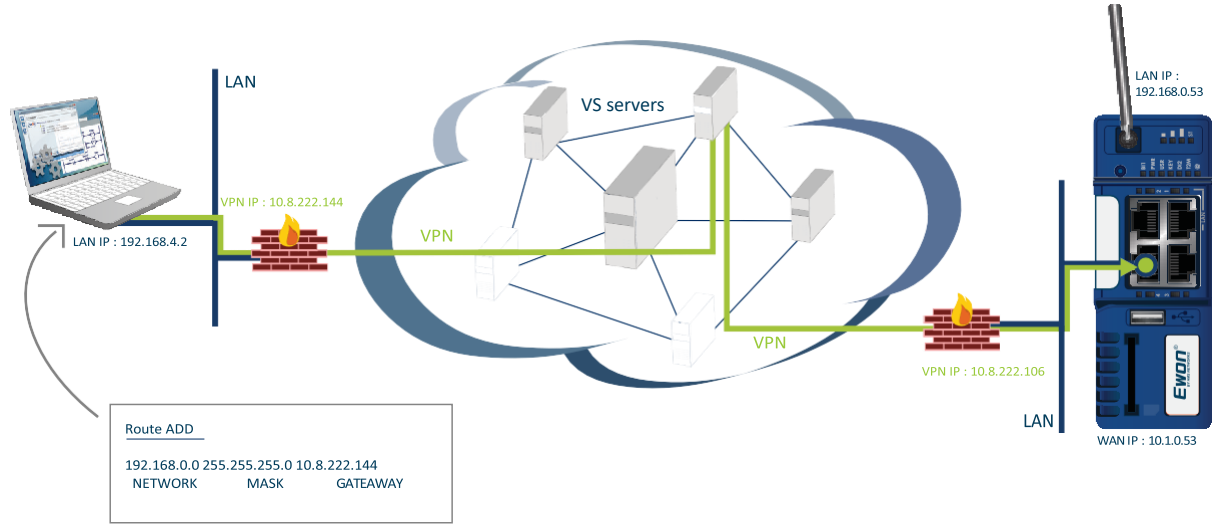


Figura 4: Conexión VPN de un lado a otro, con todas las direcciones IP involucradas

En el lado de la máquina, el tráfico IP que viene por medio de la VPN es enviado al lado LAN del Ewon de forma automática. Si un dispositivo en la red LAN necesita contestar a la PC, hay dos posibles estrategias:

- El recurso NAT (Network Address Translation) sobre LAN, también conocido como Plug'n Route, reemplaza la dirección IP del Ewon por la dirección IP de la PC. Esa es la configuración estándar del dispositivo Ewon. Vea figura 5 para una breve explicación.
- Todo dispositivo en el lado LAN debe tener al Ewon configurado como su gateway, lo que requiere la reconfiguración de la dirección IP en cada dispositivo de la red LAN. Esta es la estrategia menos preferida, pero puede ser necesaria en casos avanzados de configuración, acerca de ruteamiento de Internet.

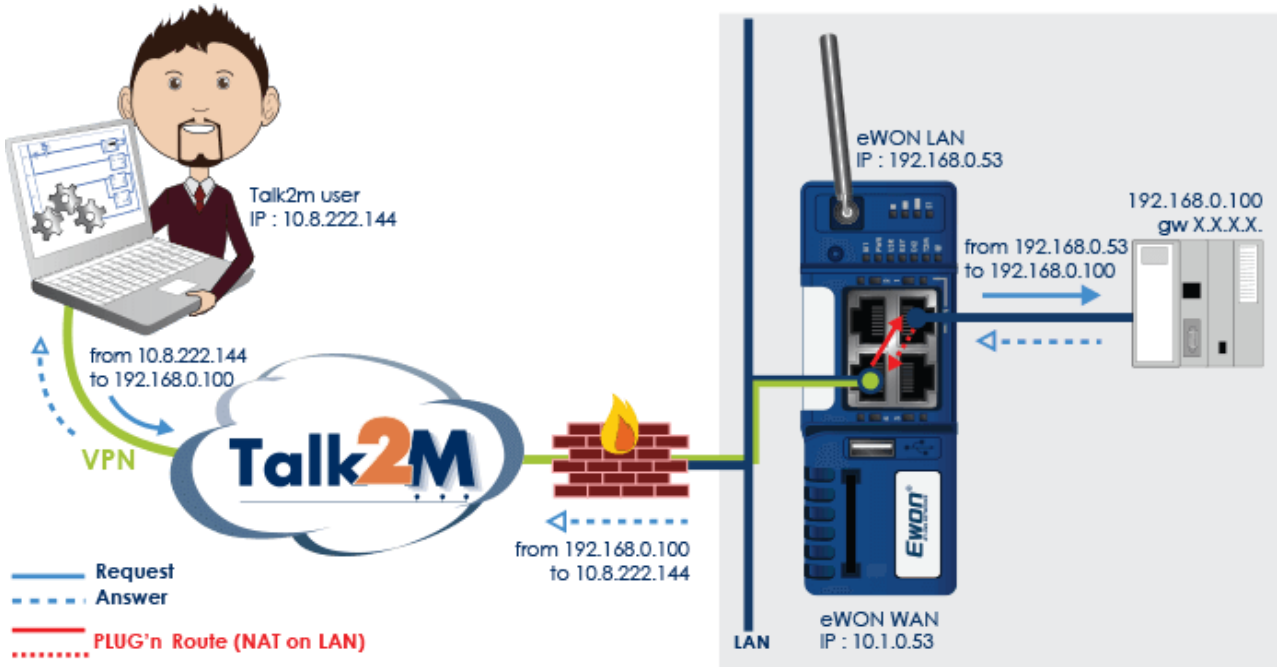


Figura 5: Plug'n Route (NAT on LAN)

Tecnología VPN utilizada

Los protocolos VPN de Talk2M son basados en Open SSL y Open VPN. OpenVPN está destinado a usar UDP por el Puerto 1194 por estándar, pero también usamos TCP 443 (HTTPS). Un beneficio del uso de TCP 443 por la LAN, es la posibilidad de hacer el paso de proxies HTTP. Eso requiere configurar la autenticación de proxy en ambos los lados (usuario y Ewon).

Los formatos de proxy soportados son:

- Proxy sin autenticación
- Proxy con autenticación de usuario y contraseña
- Proxy de autorización NTLM

Dando de alta un Ruteador Ewon en una cuenta Talk2M

Dar de alta un dispositivo Ewon en una cuenta Talk2M requiere dos etapas:

1. Adicionar un dispositivo Ewon en la cuenta, por uno de los tres métodos disponibles.
2. Correr el asistente de conexión Talk2M dentro del dispositivo Ewon, lo que lo conecta a Talk2M por primera vez, y completa el proceso. Este paso también se puede realizar durante la puesta en marcha del dispositivo Ewon en el sitio del usuario final, de forma completa o parcial (en el caso de que el dispositivo ya haya sido incluido en la cuenta de fabrica, solo faltaría revisar la conexión al Internet).

Los tres métodos para dar de alta un Ewon en la cuenta son:

- Por medio de la clave de activación: se trata de la forma más común de hacerlo. Talk2M genera una clave única que se usara en la etapa de configuración dentro del dispositivo Ewon.
- Por medio de un nombre para el dispositivo Ewon: es una contingencia para dar de alta a un Ewon cuando el mismo ya se encuentra en sitio y aún no ha sido dado de alta.
- Por medio de SMS: el mensaje SMS contiene la clave de activación, lo que hace ese método similar al primero. nSe trata de un último recurso, utiliado cuando hay un problema critico como pérdida de comunicación. Cuando el Ewon recibe el SMS, automáticamente corre el asistente y se reconfigura para conectarse a los servidores Talk2M.

Durante el proceso del asistente, la primera etapa es la requisición del certificado para el AS. Trae la clave privada y los certificados necesarios para los algoritmos de encriptación.

El proceso de alta de un Ewon también relaciona el numero serial del dispositivo Ewon a cada certificado. Como no se puede dar de alta dos Ewons con el mismo número serial (en ese caso, el nuevo registro borra el anterior), el sistema permite duplicar la configuración de un Ewon a otro, en caso de reemplazo de equipo. En ese caso, Talk2M solo verifica los certificados.

Usuario final mantiene control del lado de la máquina

Usar una conexión LAN generalmente significa que el dispositivo Ewon estará permanentemente conectado al servidor Talk2M. Hay casos en el que el cliente final no desea mantener el Ewon conectado permanentemente, especialmente cuando el uso de acceso remoto es esporádico, o mismo cuando el cliente final desea tener total control del acceso remoto.

En esos casos, recomendamos la instalación de una llave selectora en el tablero. Esa llave puede ser conectada eléctricamente al dispositivo Ewon. En el dispositivo Cosy, la entrada discreta que permite esta funcionalidad, cuando en nivel bajo (0 volt), deshabilita la conexión VPN. En otros modelos de dispositivos Ewon (Flexy, CD), la misma funcionalidad existe, pero se puede configurar su funcionamiento. Los dispositivos incluyen también una salida discreta para indicar el estado de la conexión a la nube Talk2M (nivel alto indica conectado).

Hay otros tipos de conexión que requieren recursos adicionales para inicializar el enlace. Cuando se utiliza conexión celular, no es necesario mantener la conexión VPN permanentemente en funcionamiento. Mantener el túnel abierto requiere el envío regular de mensajes “keep alive”, lo que incrementa el consumo de la conexión (de 1 a 2 MB por día).

Durante la primera fase de alta de un dispositivo, el usuario puede declarar que tipo de conexión al internet se utilizará. En el caso de celular, un número de teléfono debe ser declarado en la configuración. Ese número telefónico puede enviar mensajes SMS al Ewon. Una vez recibido el mensaje, el Ewon se conectará al proveedor de servicio móvil y, consecuentemente, a los servicios de conectividad Talk2M para inicializar el túnel VPN.

Seguridad del sistema y arquitectura Talk2M

Seguridad es probablemente el punto más importante de la arquitectura Talk2M. Hemos elaborado una filosofía de seguridad basada en DPA (Defense in Depth Approach – figura 6). DPA es coordinado por múltiples medidas en diferentes capas de control de seguridad. El propósito es garantizar la seguridad, confidencialidad, disponibilidad e integridad de la plataforma Talk2M.

Figura 6. Defense-in-Depth (DPA)

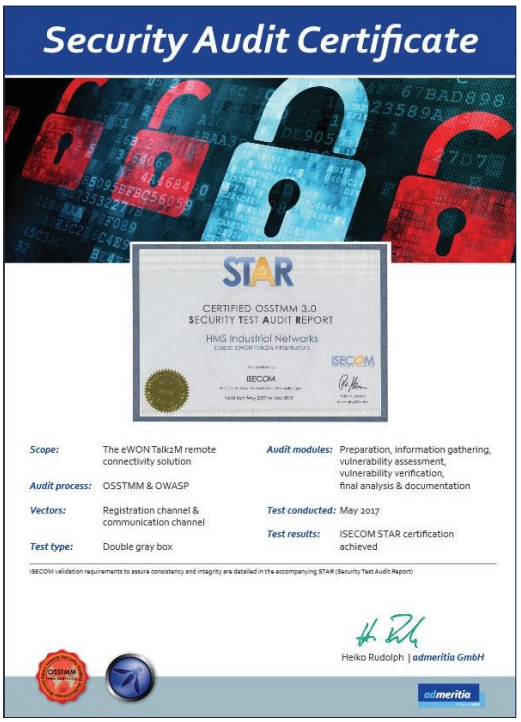
Todo es basado en pautas definidas por los estándares más importantes de seguridad, como ISO27001, IEC 62443-2-4 y NIST Cyber Security Framework 1.0, además de una serie de publicaciones y buenas prácticas de la industria.

A continuación, una descripción de las diferentes capas empezando por la más interna hasta las externas y los respectivos detalles de seguridad de cada una.

Capa	Nombre	Seguridad implementada
1	Dispositivo Ewon	1. Configuración Ewon: usuarios deben de pasar por la autenticación de seguridad Ewon, requiriendo por lo menos derechos de administrador de Ewon. 2. Segregación de red: el tráfico de datos en el lado de la máquina/LAN es aislado del lado WAN (NAT 1:1). Usuarios solo pueden acceder a los dispositivos autorizados del lado de la LAN. 3. El dispositivo se autentica a la plataforma Talk2M. 4. Selector físico para controlar el acceso a internet.
2	Firewall	Filtering/Firewalling: hasta 4 niveles de filtro son posibles, lo que permite filtrar el acceso del usuario a cualquier dispositivo Ethernet, cualquier dispositivo USB/serial, o mismo a servicios internos del Ewon. El filtro es gestionado y aplicado en la plataforma de conectividad Talk2M, y no en el dispositivo Ewon.
3	Encriptación de tráfico	Los usuarios y ruteadores Ewon son autenticados por el AS utilizando TLS para autenticación de sesión HTTPS, y encriptación de datos. Mientras se establece la conexión VPN al VS, el Ewon usa los mismos protocolos y mecanismos TLS para la seguridad del túnel de transporte. Solo cifrados seguros son utilizados.

Capa	Nombre	Seguridad implementada
4	Administración de usuarios y acceso	1. Usuarios y control de acceso: el propósito es definir cuales usuarios pueden tener acceso a cuáles máquinas. Eso funciona de acuerdo con las reglas (asignaciones) que se pueden atribuir a los Grupos de Usuários y Grupos de Equipos para permitir diferentes niveles de acceso. 2. Credenciales de acceso únicas con (opcional): a. Políticas adicionales de contraseña, requiriendo longitud mínima, letras, números y caracteres especiales, período de vencimiento, y listado de contraseñas antiguas. b. Autenticación de dos factores: además del tradicional registro de usuario y contraseña, una segunda ventana se abre para ingresar una clave enviada por SMS. 3. Pista de auditoria de conexiones (quien, cuando y por cuanto tiempo). 4. Bloqueo de usuario por cuenta de demasiados intentos de conexión, para adivinar la contraseña. 5. Uso de la selectora física para mantener control local.
5	Infraestructura de red Talk2M	Nuestra compañía regularmente evalúa la arquitectura Talk2M como parte del requisito de gestión de riesgos. Controles apropiados son incrementados para cumplimiento y efectividad. Enumeramos las diferentes partes y metas de esa evaluación: a. Política de seguridad: para proveer al equipo dedicado a Talk2M soporte acerca de las prácticas y leyes relevantes sobre seguridad de datos. b. Organización de seguridad de datos: para proveer referencias para implementación, monitoreo y control del sistema de administración de seguridad de Talk2M. c. Seguridad de recursos humanos: para garantizar que todos los empleados comprendan sus responsabilidades, y sean los adecuados para sus funciones, reduciendo el riesgo del mal uso del sistema Talk2M. d. Gestión de activos (servidores e infraestructura de internet), Seguridad Física y Ambiental: para esa parte, Ewon sigue firmando contractos con diferentes compañías de host. Para la parte crítica, Ewon confía en la compañia Rackspace, por cuenta de las certificaciones ISO27001, SSAE16 type II SOC1, SOC2 (Security and Availability Only) y SOC3, que es la más reciente acerca de certificación de hosting. La SSAE16 se trata de una versión más avanzada de la SAS 70. Estamos hablando de un estándar de auditoria diseñado para habilitar un auditor independiente que emite su opinión acerca de los controles de una organización de servicios. El reporte de auditoria de la SSAE16 trae la opinión del auditor, una descripción de los mecanismos de control implementados, y en el caso de una auditoria tipo II, una descripción de las pruebas utilizadas para revisar la efectividad de estos controles. e. Pista de Auditoria Permanente: todos los servidores son auditados por medio de grabación de toda información operacional. Ewon también implementa ingreso (logging) continuo.
6	Cumplimiento de política	La solución de acceso remoto Talk2M fue diseñada para ser compatible con las políticas de seguridad existentes en nuestros clientes. Por medio del uso de conexiones a través de puertos de salida, generalmente abiertas (443 y 1194) y la compatibilidad con la mayoría de los servidores proxy, el Ewon fue diseñado para ser mínimamente intrusivo en la red y funcionar con las reglas existentes del firewall. Consecuentemente, no hay necesidad de cambiar las configuraciones de seguridad de su red. En eCatcher, los administradores de la cuenta Talk2M pueden customizar el sistema para exigir el cumplimiento de las políticas de contraseña corporativas y restringir cuales usuarios pueden acceder a cuáles dispositivos remotamente. Los administradores también pueden revisar el reporte de conexiones de Talk2M para saber cuáles usuarios se están conectándose a cuáles equipos y cuando. Ese reporte es una herramienta muy valiosa para garantizar que las políticas corporativas del acceso remoto estén siendo enforzadas.

Nuestros sistemas de Talk2M son evaluados regularmente por compañías independientes de seguridad cibernética, para garantizar que mantengamos una postura de seguridad adecuada, y proporcionemos el más alto nivel de protección a nuestros clientes.
Por esa razón, recibimos, en Mayo de 2017, nuestro primer certificado de seguridad cibernética, STAR (Security Test Audit Report), que es el resultado de la evaluación de Talk2M hecha por la compañía admeritia GmbH.
¡Tener una buena postura de seguridad es para nosotros sumamente importante, sin embargo, para mantenerla, es necesario un buen sistema de gestión, enfocado en riesgos, mejora continua y definición de procesos!
Esa es la responsabilidad de nuestro gerente de seguridad, que lo hace basado en el estándar ISO27001. HMS tiene su sistema Talk2M certificado por ISO27001 desde septiembre 2017.



Disponibilidad de los servidores Talk2M

Después de los aspectos de seguridad, la segunda prioridad más importante de la arquitectura Talk2M, es proveer la máxima continuidad posible de los servicios de conectividad. Dos tipos de servicio son ofrecidos a los clientes:

- Talk2M Pro, servicio pagado de misión crítica con acuerdo de nivel de servicio (SLA), o
- Talk2M Free+, servicio gratis de conectividad

El servicio de misión crítica ha sido diseñado para proveer continuidad a más de 99.6% del tiempo durante el período de un año, con interrupción máxima de 4 horas continuas del AS para todos los clientes Talk2M, y en el VS para los clientes Talk2M Pro. Para ofrecer estos dos niveles de servicio, la arquitectura Talk2M es reforzada por múltiples características y objetivos de control, tales como:

1. Proveedores de Hosting SLA: Ewon tiene acuerdos con diferentes proveedores. Dependiendo de los servicios Talk2M, Ewon puede utilizar diferentes compañías:
    a. Servicios Talk2M Pro de misión crítica son hospedados por nuestro partner Rackspace, que nos ofrece acceso a Internet con SLA de garantía de acceso de 99.99% 24/7/365, con máximo tiempo de interrupción de 1h.

    b. Para los servicios Talk2M Free, confiamos en diferentes proveedores de hospedaje que proponen SLA de 99% o más, con tiempo máximo de interrupción un poco más largo.

2. Monitoreo del Sistema: nosotros monitoreamos los indicadores del desempeño de todos los servidores. Tenemos un sistema de registro de alarmas que envía mensajes de SMS y correo electrónico a nuestro equipo de servicio para atención inmediata, 24h al día, los 365 días del año.
3. Transferencia de Servidores: con tres diferentes proveedores, en caso de un problema grave en algún servidor, podemos rápidamente transferir las conexiones VPN de un VS a otro.
4. Equipo de monitoreo continuo: Los servicios Talk2M son monitoreados por un equipo específico de ingenieros de acuerdo con un calendario de programación.

Servidores Talk2M distribuidos globalmente

Otro beneficio es la distribución geográfica de nuestros hosts. Para reducir la latencia de los paquetes IP, hemos implementado nuestra infraestructura en diferentes partes del mundo, como Europa, EE.UU. y otros países/zonas (vea la figura 8 – VS implementados hasta 1ro de Julio de 2015). Seguimos expandiendo esta estructura a otras partes. Se trata de un requisito importante de algunos protocolos de comunicación de controladores industriales que han sido diseñados para intercambiar paquetes TCP/IP pequeños: en el caso de conectividad lenta de internet, adicionalmente a largas distancias entre el usuario y la máquina, estis protocolos de red son muy más sensibles a la ocurrencia de fallas de comunicación (timeouts).

Figura 8: Los VS disponibles en la red Talk2M

Consecuentemente tenemos la capacidad de migrar en cualquier momento una conexión VPN de un ruteador Ewon al VS geográficamente más cercano. El Ewon entonces se reconectará al nuevo VS inmediatamente.

Advertencia: El nombre del servidor Talk2M debe ser declarado en el Proxy/FW del usuário final: mantenga siempre abierto *.talk2m.com. Nombres de host o direcciones IP individuales no pueden ser utilizadas una vez que los escenarios de conmutación por error no son soportados.

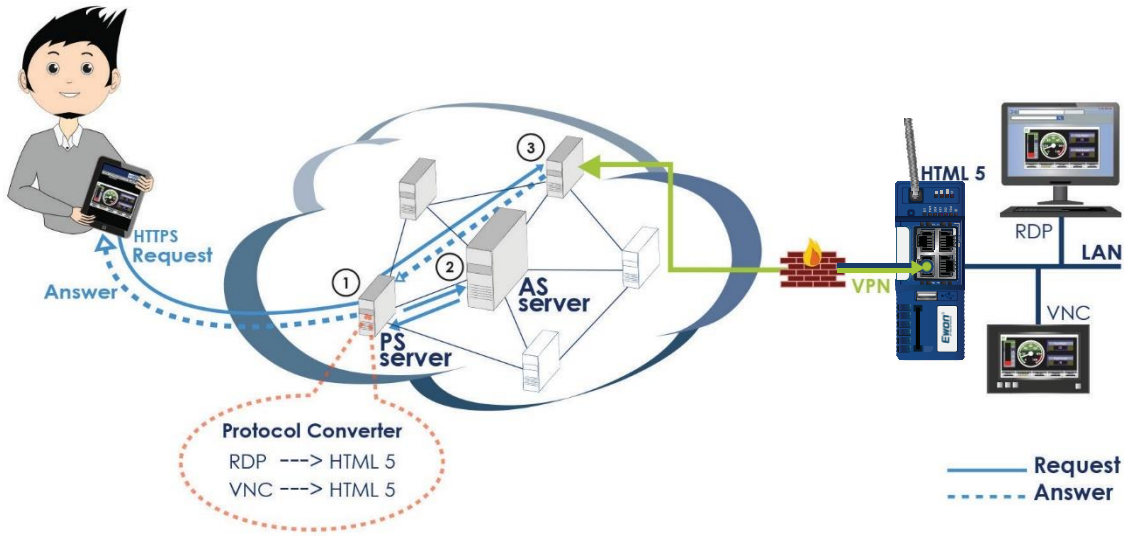
Para permitir rápida conexión entre los diferentes servidores, todos los servidores VS son interconectados al AS por medio de túnel VPN IPsec.

M2Web, el cliente Talk2M para monitoreo remoto de HMI

En vez de utilizar eCatcher, usuarios tienen la opción de conectarse por medio de nuestro portal M2Web, utilizando un navegador web. Esto permite que usuarios se conecten a Talk2M empleando conexión HTTPS, sin la necesidad de instalar un software específico. Con ese servicio, es posible acceder a la maquina por medio del navegador como cliente por el portal https://m2web.talk2m.com. En ese portal, el tráfico HTTPS es redireccionado a la maquina apropiada por la VPN de la máquina, para finalmente alcanzar al ruteador Ewon.
Una vez que los ruteadores Ewon hayan sido diseñados para conectarse remotamente con dispositivos de automatización industrial, la propuesta de M2Web es permitir conexión a los dispositivos HMIs (Human Machine Interface) de las máquinas, como paneles, PCs, o cualquier otro dispositivo que traiga un servidor HTML5.0.
M2Web también incluye conversores de los protocolos VNC (Virtual Network Computing) y RDP (Remote Desktop Protocol) a HTML5.0. El protocolo VNC es ampliamente utilizado en HMIs en formato panel y RDP se encuentra disponible en plataformas basadas en sistema operativo Microsoft Windows

La conexión a una máquina por medio de un navegador web en HTTPs es ejecutada en 3 etapas (figura 9):

1. El usuario accede al link de la página web del portal M2WEB. El web proxy contesta con una ventana de autenticación.
2. Una vez autenticado, el AS indica al web proxy cual servidor VS es utilizado por el túnel VPN de la máquina.
3. Todas las solicitudes HTTP inicializadas por el navegador, pasan por el web proxy y son redireccionadas por medio del túnel de la VPN de la máquina y finalmente alcanzan el Ewon o los dispositivos del lado de la LAN que soporten los protocolos HTML5.0, VNC o RDP. Eso es posible dentro del Ewon habilitando la funcionalidad de port forwarding (llamada de Proxy).



La figura 9 presenta la cadena completa de una conexión M2Web

Servidores adicionales: SMTP relay, SMS gateway

TalK2M también ofrece servicios adicionales al acceso remoto, como SMTP relay y SMS gateway servers. Ambos son utilizados para extender el mecanismo de notificación del sistema de alarmas disponible en un ruteador Ewon. Cualquiera información recolectada de un PLC o dispositivo industrial por el Ewon, puede ser usada para generar mensajes de alarma enviadas por el túnel VPN. A la salida del túnel, son reenvidas por medio del Internet como correo electrónico o SMS.