Permitirán Mis Clientes Conectarme?

Como aliviar las preocupaciones de seguridad con la conectividad remota

Muchos fabricantes de equipos originales (OEMs) están con la idea de conectar sus equipos en forma remota pero hay preocupación acerca de la complejidad en la manipulación de las conexiones, y sobre cómo administrar la seguridad entre los usuarios finales. El mayor inconveniente está en establecer una conexión VPN y lidiar con los problemas de firewalls y rutas de acceso. Afortunadamente, existe una mejor opción para las conexiones remotas VPN.

Los Pro y Contras de VPN

Una VPN (Virtual Private Network) esta diseñada para conectar a un usuario externo a la red. La VPN trabaja excelente para teletrabajos, pero no es la mejor opción para conectar equipos en forma remota. Por ejemplo, si se trabaja desde casa, se puede hacer una conexión remota VPN a la red de su compañía y accesar a todos los archivos y datos que se consultan normalmente en la oficina. Es totalmente comprensible que el grupo de usuarios finales del área de IT refuten en permitir que un usuario externo tenga los mismos accesos a la red. El área de IT puede limitar al usuario remoto para equipos específicos, pero esto significa que el personal de IT tiene que realizar labores adicionales de configuración que implican un mayor consumo de tiempo. Una VPN ha llegado a ser de alguna manera el factor estándar para las conexiones remotas de equipos de automatización, pero ciertamente no es la mejor solución.

Una Mejor Solución: Conectar Fuera, No Dentro

Las conexiones de entrada VPN requieren que los usuarios finales habiliten un Puerto de entrada, creando un espacio en su firewall. Una mejor solución es hacer que el equipo haga una conexión de salida hacia un servidor de almacenamiento en la nube. Muchos sitios permiten una conexión de salida, que a su vez permite a los usuarios accesar al internet por detrás de los firewalls, esto implica que no haya que realizar cambios en la configuración de los firewalls o en las políticas de seguridad requeridas. Una conexión hacia fuera dirigida a un servidor específico, confiable, ayuda a aliviar las preocupaciones que implica la conectividad a través de una red pública de internet.

RRAMAC
CONNECTED SYSTEMS

(844) 4RRAMAC • 763.544.6638
www.rramac.com • info@rramac.com

Porque usar una solución basada en la nube?

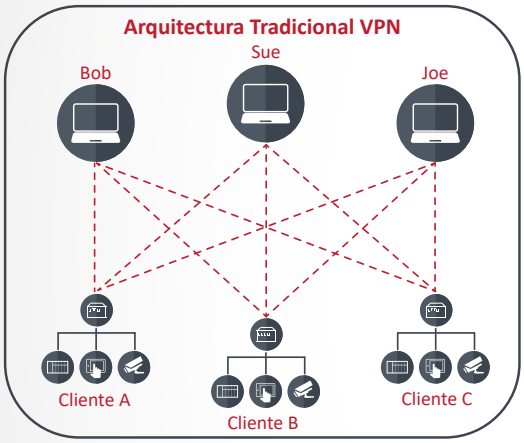
Por más de una década, RRAMAC ha estado implementando soluciones basadas en la nube. RRAMAC no solamente simplifica los aspectos de la conectividad remota (IIoT), sino que también cuenta con la experiencia en el soporte a los usuarios en cómo obtener los datos correctos de sus controladores, dispositivos, u otros equipos. La solución basada en la nube incluye mantenimiento preventivo, análisis de paras en la producción, registro de inventarios, y otros reportes personalizados. La información estaría disponible en un Sistema de Menús basados en la web, datos históricos, mensajes de texto, notificación a través de emails y aplicaciones personalizadas para dispositivos móviles.

Certificados de Encripción y Seguridad

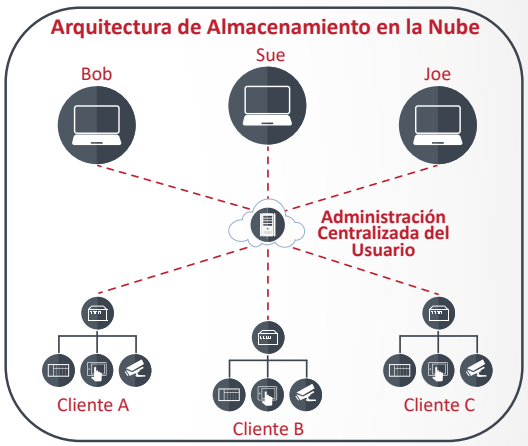
Cuando se establece una conexión de salida a un servidor de almacenamiento en la nube, la Encripción de datos es usada para prevenir accesos no autorizados a la información. Los certificados de seguridad son usados para asegurar que los datos van solamente al servidor especificado. Los certificados de Encripción y seguridad son usados por los bancos y compañías de tarjetas de crédito para transacciones a través de internet. Esta misma tecnología puede ser empleada para asegurar que la conexión de salida del equipo de un cliente puede ser establecida únicamente al servidor asignado en la nube. Cuando un usuario autorizado requiere accesar los datos, los certificados de Encripción y seguridad son empleados para validar la conexión del usuario al servidor en la nube.

Administración de la Cuenta del Usuario

La arquitectura de conectividad de un almacenamiento en la nube es mucho más segura y fácil de manejar con respecto a la conexión VPN, cuando se emplean cuentas de usuarios y claves. Suponga que un fabricante de equipo original (OEM) tiene 3 personas y necesita conectar a 3 clientes en lugares diferentes.



En este escenario Bob, Sue y Joe necesitarían nombre de usuario y claves para cada sitio del cliente remoto. Agregar y borrar usuarios de cada sitio en forma individual es tedioso, de manera que muchos OEMs terminan asignando un solo acceso para todos los usuarios. Esto podría significar que empleados que ya no están en la compañía aun tendrían las claves de entrada.



En este escenario, las cuentas de los usuarios son creadas y administradas desde un servidor en la nube. Por ejemplo, si Joe no labora más para la compañía, su acceso para todos los sitios pueden ser borrados con unos simples clicks del mouse.

Aislamiento de la Red y Conflictos IP

El otro problema asociado al uso de una VPN para la recolección de datos, es la dificultad de conectar simultáneamente a un múltiple número de sitios de los clientes. Debido a que la VPN esta diseñada para conectarse a una red remota, no es posible usar una simple VPN para conectar varios clientes simultáneamente. Una conexión simultánea de los clientes vía VPN crearía conflictos en el IP, lo que podría generar problemas en la seguridad. Aquí nuevamente, un servidor en la nube con certificados de seguridad es una mejor solución. Múltiples sitios pueden ser conectados simultáneamente dentro del mismo servidor en la nube, de la misma forma como muchos clientes de bancos pueden realizar sus transacciones en línea al mismo tiempo.

RRAMAC
CONNECTED SYSTEMS

15400 Medina Road
Plymouth, MN 55447

(844) 4RRAMAC • 763.544.6638
www.rramac.com • info@rramac.com