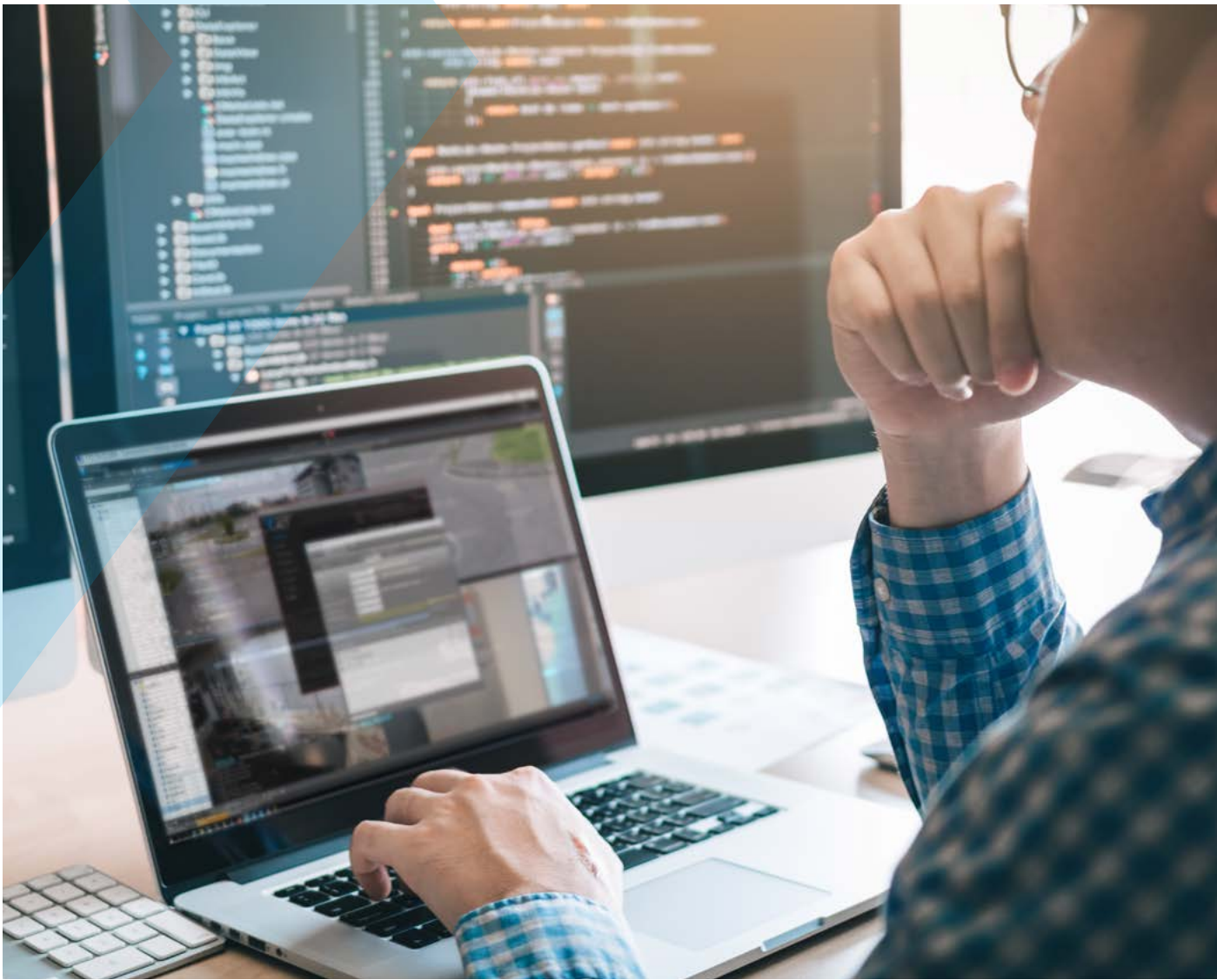




CONSEJO TÉCNICO

Conexión de instalaciones de videovigilancia IP en una amplia distribución geográfica.

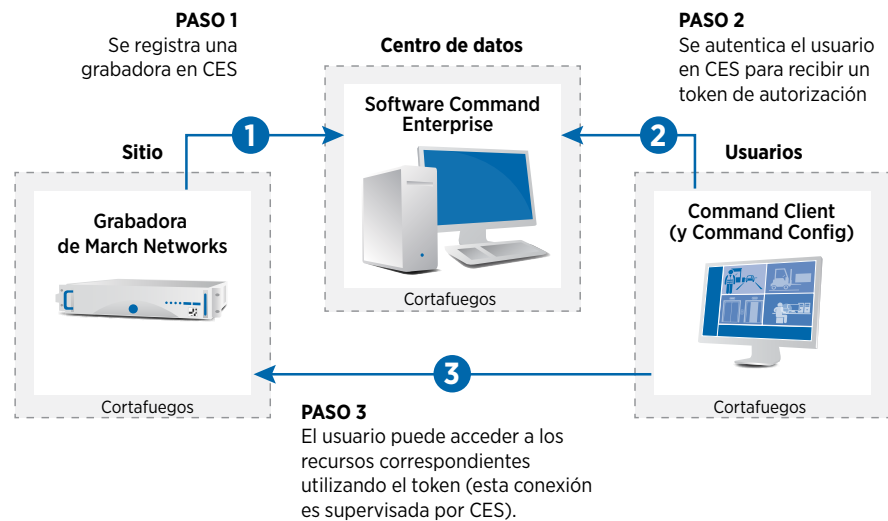
Introducción

El despliegue de un sistema de videovigilancia IP en múltiples ubicaciones dispersas puede ser todo un reto. Si no se cuenta con un diseño adecuado del sistema, el rendimiento puede degradarse, las tareas pequeñas convertirse en una pérdida de tiempo y el costo de gestión del sistema aumentar.

March Networks® adopta una arquitectura centralizada para la gestión de múltiples sitios y el software Command™ Enterprise (CES) de March Networks es el núcleo de la solución. Una vez que una grabadora de video en red (NVR) se registra en CES, todos los recursos relacionados con la videovigilancia se almacenan dentro de una base de datos común: CES es la entidad que otorga a los usuarios autenticados el acceso a dichos recursos.

Aquí se presenta un diagrama simplificado que muestra la ruta de datos de un usuario que inicia una investigación relacionada con el video grabado por una NVR local.

Figura 1: El software Command Enterprise es el núcleo de la solución de March Networks. CES proporciona el token de acceso a los usuarios autenticados.



La creación de una instalación de videovigilancia exitosa y eficiente con amplia distribución geográfica requiere un diseño y una configuración de red adecuados, para garantizar que cada usuario pueda acceder fácilmente a los recursos necesarios con una latencia mínima.



Topología de red

Hay varias maneras de conectar todos los componentes del sistema de videovigilancia, pero cada diseño del sistema tiene un impacto diferente en el rendimiento. También, algunos diseños son más complejos de configurar que otros. Veamos las diferentes opciones:

Opción 1: Redireccionamiento de puertos

La siguiente figura ilustra los puertos que se requieren abrir por el departamento de TI para que la comunicación entre los componentes del dispositivo sea satisfactoria.

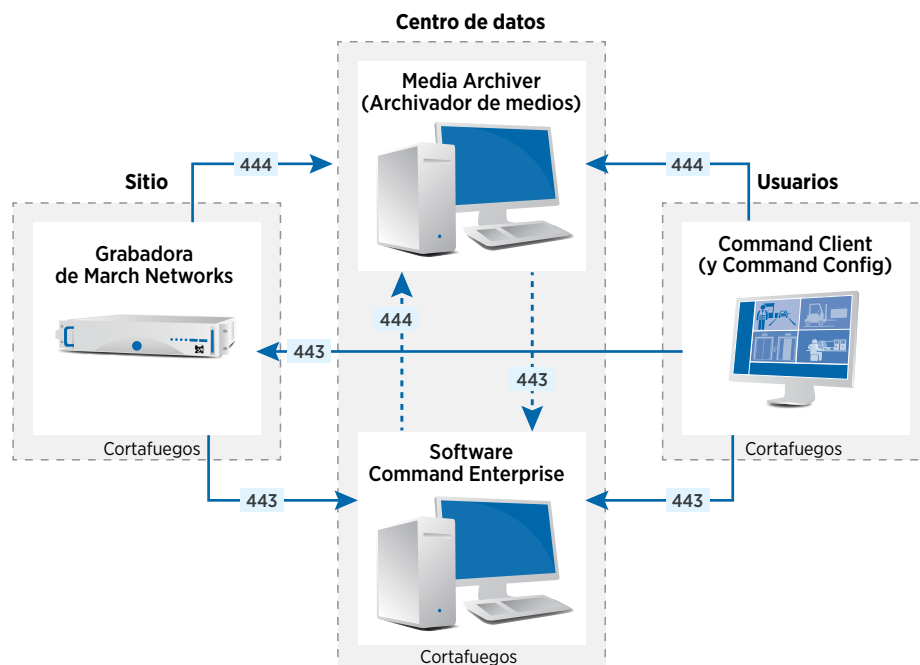
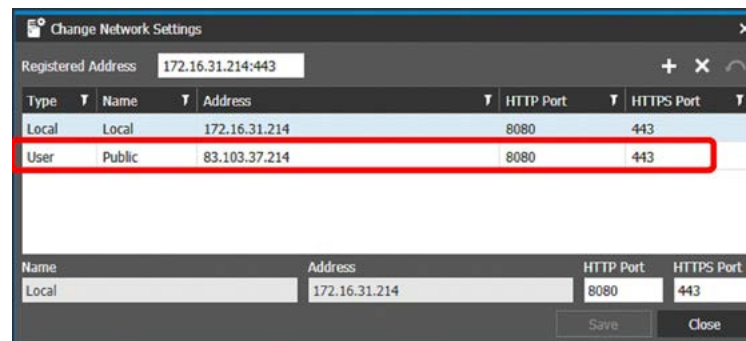


Figura 2: Detalles del puerto de red para cada módulo que compone la solución. Aplica a la solución Command versión 2.7 o superior. Media Archiver de March Networks, que es parte de cualquier instalación CES de March Networks, se ha incluido en el diagrama para ofrecer una visión más completa.

Este enfoque requerirá que cada grabadora tenga el puerto local 443 traducido a una dirección pública, usando la pestaña de Configuración de red en Command Client de March Networks. Esta configuración está disponible una vez que usted se conecta localmente a la grabadora con Command Client.

Figura 3: Agregar la dirección pública a cada grabadora utilizando la función “Cambiar configuración de red”. A partir de la versión 2.7 de Command Client el puerto HTTP es opcional. En este ejemplo, utilizamos el valor original 443, pero se puede cambiar para que coincida con los requisitos de la red.



CONSEJO TÉCNICO: Conexión de instalaciones de videovigilancia IP en una amplia distribución geográfica.

Figura 4: Consola de administración de CES. Es necesario añadir aquí la dirección pública del servidor CES y especificar la prioridad. Estos valores se transfieren a cada una de las grabadoras durante el proceso de registro o cuando se reinicia CES/NVR (asegúrese de que "Conexión de la grabadora iniciada por" está configurada para "dispositivo o servidor").

El siguiente paso es abrir la consola de administración de CES, ir a la pestaña "Red" y añadir la(s) dirección(es) pública(s) del servidor CES:

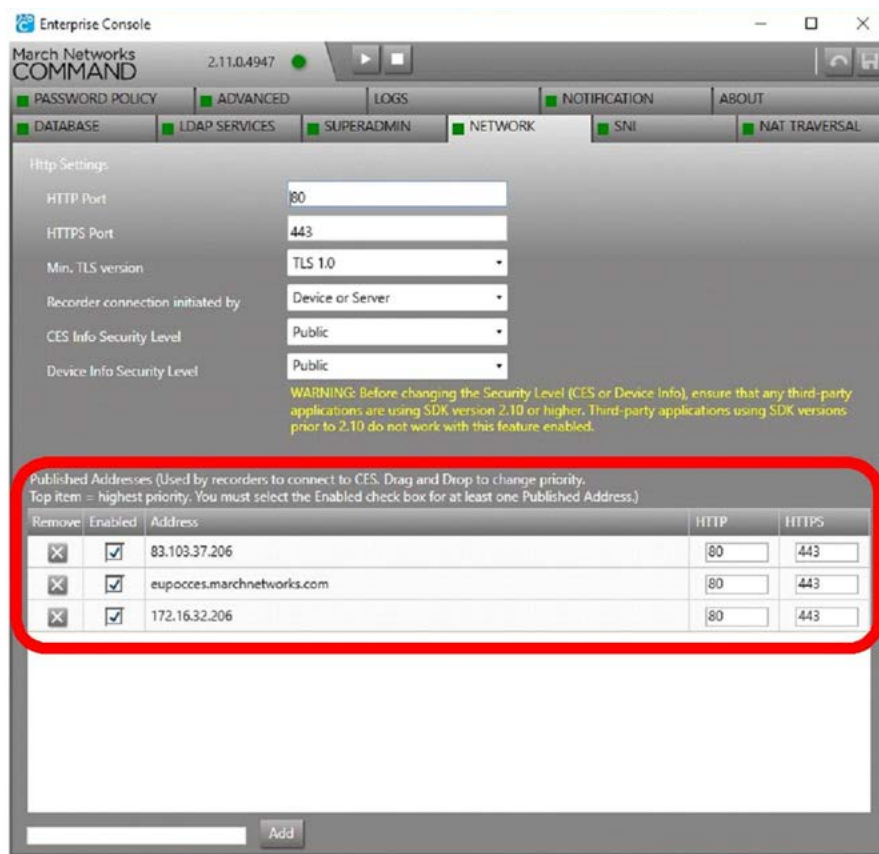


Figura 5: Si el “Nivel de seguridad de la información del dispositivo” está configurado como público en la consola de administración de CES, entonces se puede acceder a cada grabadora mediante http://NVR_IP/info para obtener detalles útiles sobre el estado de la NVR, incluida la lista completa de direcciones CES.

De esta manera, cada grabadora tendrá la lista completa de direcciones CES y tratará de conectarse a CES comenzando por la que tenga mayor prioridad. Se puede verificar que la lista de direcciones se haya pasado exitosamente a cada NVR, como se muestra en la siguiente imagen.

```
system.ready: true
system.ready.connected: true
system.ready.details: true
system.ready.registrationDetails: true
system.ready.ssl: true
system.ready.gateway.mobile: true
system.details.id: 344
system.details.manufacturer: 1
system.details.family: 257
system.details.model: 8
system.details.serial: AR1336P196
system.details.version: 5.19.0.0132
system.details.stationId: NVR-344
system.details.patchList: FPGA:23:2.3,EvidenceReviewerCD:
    050709.0126:5.7.9.0126
system.interface.1: Public
system.interface.1.address: 83.103.37.214
system.interface.1.httpPort: 8080
system.interface.1.httpsPort: 443
system.registration.enabled: true
system.registration.currentEndpoint: https://83.103.37.203:443
system.registration.endpoints: https://83.103.37.203:443,
    https://172.16.32.203:443, https://ces.marchnetworks.com:443,
    http://83.103.37.203:80, http://172.16.32.203:80,
    http://ces.marchnetworks.com:80
system.registration.server: 83.103.37.203:80
system.registration.addresses: 83.103.37.203:80, 172.16.32.203:80,
    ces.marchnetworks.com:80
system.registration.deviceId: 344
system.interface.httpPort: 8080
system.interface.httpsPort: 443
system.interface.streamPort: 8080
system.interface.secureStreamPort: 443
system.interface.version: 100.0.0.1385
system.interface.build: 2.11.0.1385
system.interface.api.version: 100.0.2.1385
system.productname:
agentmediaport: 8080
system.interface.wdport1: 80
system.interface.wdport2: 2804
_hash: nD52gzeBimUwJ+tV1CZGGUHu9Go=
```



Tabla 1: Suponiendo que dos IP públicas distintas están disponibles, es posible mapear el puerto 443 de LAN al puerto 443 de WAN tanto para CES como para la grabadora. En caso de que esto no sea posible, estos valores se pueden ajustar simplemente editando los paneles de las redes presentados.

Para completar la configuración será necesario implementar las reglas de redirección de puertos NAT para cada grabadora y servidor CES.

Dispositivo	IP LAN	Puerto LAN	IP WAN	Puerto WAN
CES	172.16.32.206	443	83.103.37.206	443
NVR	172.16.31.214	443	83.103.37.214	443

Este enfoque ofrece el mejor rendimiento en términos de latencia de video y capacidad de respuesta del sistema. No se necesitan recursos adicionales para conectar los distintos componentes del sistema. La principal desventaja es la necesidad de crear una regla NAT específica para cada dispositivo y esto puede ser problemático cuando se gestionan cientos o miles de grabadoras. Hay situaciones en las que este enfoque es imposible de implementar, para tales escenarios, es necesario explorar otras alternativas.

Opción 2: NAT traversal usando el servicio STUN/TURN

La utilización de un servidor STUN o TURN suprime la necesidad de crear reglas de redirección de puertos para cada grabadora. Esto simplifica en gran medida la configuración de la red, pero introduce un elemento adicional a la arquitectura, lo que causa una degradación significativa en el rendimiento y la latencia del sistema. Los servicios STUN o TURN se deben configurar en la consola de administración de Command Enterprise de March Networks:

Figura 6: La versión 2.7 o superior de Command Enterprise tiene la pestaña NAT TRAVERSAL para configurar los servicios STUN o TURN. Aquí se habilitan los servicios STUN locales o STUN/TURN de terceros.

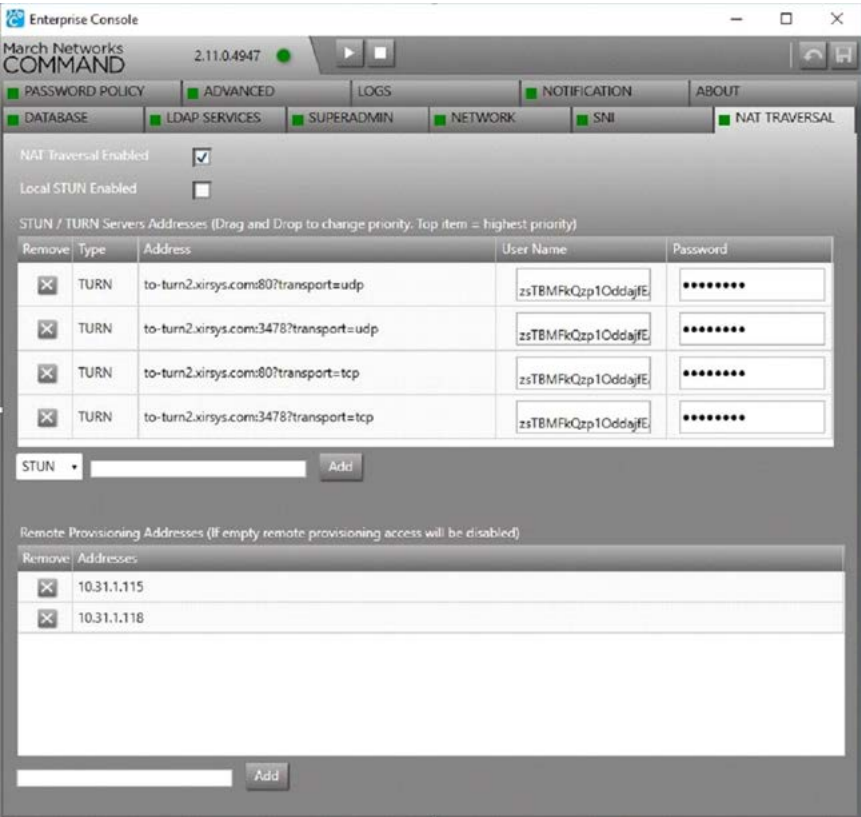


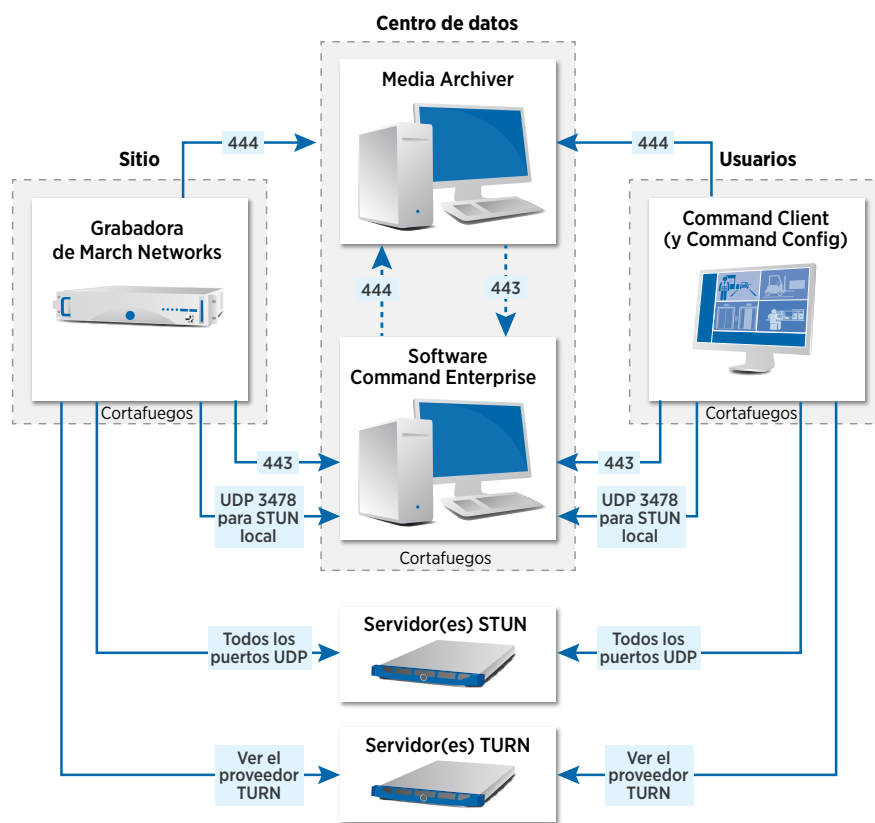
Figura 7: Arquitectura de red al considerar los servicios STUN o TURN. El servidor CES tienen que seguir siendo público/accesible desde la PC del cliente, pero no se necesita una conexión directa entre el cliente y la grabadora. Todo el tráfico relacionado con el video lo gestiona el servidor STUN/TURN.

La forma en que los servicios STUN y TURN funcionan es bastante diferente:

El servicio STUN actúa como un operador que enlaza las conexiones entre dispositivos, estableciendo una comunicación bidireccional peer-to-peer. El protocolo STUN se basa en paquetes UDP para establecer la conexión. Esto se debe tomar en cuenta a la hora de discutir la solución con el departamento de TI, para asegurarse de que no hay reglas que impidan la propagación de este tipo de protocolo dentro de la red. Los recursos de STUN suelen ser gratuitos y el mismo CES ofrece un servicio STUN integrado que se puede habilitar vía la consola de administración (el tráfico UDP se dirige por defecto al puerto 3478). Además, también se pueden utilizar los servicios STUN de Google, lo que reduce aún más las reglas que hay que establecer.

El servicio TURN actúa como “retransmisor” entre Command Client y las grabadoras. Este tipo de servicio lo ofrecen varias compañías por una cuota mensual y requiere la apertura de puertos personalizados, dependiendo del operador que se elija.

El siguiente diagrama ofrece una visión general de los recursos de red que se deben tomar en cuenta al considerar los servicios STUN/TURN:



En resumen:

1. Si habilita la función NAT traversal, pero deja las “reglas de redirección de puertos” en el cortafuegos de la grabadora, el cliente seguirá usando el método de “conexión directa”. El cliente solo volverá a una conexión NAT traversal, cuando no pueda llegar a la grabadora a través de la conexión directa.



2. Los requisitos de ancho de banda pueden ser enormes cuando se transfiere contenido de video, especialmente cuando se investigan varias cámaras en paralelo. Esto puede saturar rápidamente los recursos disponibles, así que este enfoque no se recomienda para las salas de control que requieren la disponibilidad de video las 24 horas los 7 días de la semana. La redirección de puertos sigue siendo la mejor opción para este tipo de aplicaciones. Sin embargo, suponiendo que el usuario tiene solicitudes esporádicas de video, el enfoque de NAT traversal puede ofrecer potencialmente mayor protección contra los ciberataques, ya que ningún puerto necesita estar abierto permanentemente para ninguna grabadora.

Opción 3: Creación de un túnel VPN entre la NVR, CES y los clientes

La creación de una VPN para conectar todos los recursos de videovigilancia eliminaría la necesidad de publicar las direcciones o adoptar servidores STUN/TURN. Implementar esta opción queda a la discreción del departamento de TI del usuario final y, por esta razón, no se cubre en este documento. Esta solución es una alternativa válida para las instalaciones de tránsito donde LTE o Wi-Fi se utilizan para conectar los equipos móviles con los servidores centrales, ya que la capa de cifrado añadida por la VPN aumenta la seguridad contra los ciberataques.

En términos de rendimiento, la arquitectura VPN debería ofrecer un rendimiento adecuado, pero se degrada ligeramente en comparación con la de redirección de puertos debido a la capa adicional añadida por los protocolos VPN.

Conclusión

Se han presentado diferentes métodos para implementar la conectividad de una instalación de videovigilancia en una amplia distribución geográfica. Cuando sea posible, la redirección de puertos estándar ofrece el mejor rendimiento y una latencia reducida. Por lo tanto, debería ser el camino a seguir, a menos que el departamento de TI no pueda implementar las reglas de redirección de puertos. En este caso, NAT traversal o VPN pueden ofrecer otros medios para establecer la conectividad entre los componentes del dispositivo, pero esto tiene algunos inconvenientes que hay que considerar, tanto en términos de rendimiento reducido (STUN/TURN), como de costo (TURN/VPN) y complejidad (VPN).



Para más detalles, por favor póngase en contacto con el equipo de ingenieros de ventas de March Networks. Ellos trabajarán con usted para identificar la mejor opción para las necesidades específicas de su negocio.

Atención y soporte al cliente

Norteamérica, Sudamérica, y Australia

Directo: 1.613.591.1441

Número gratuito (EE.UU. y Canadá):

1.800.472.0116

Correo electrónico:

techsupport@marchnetworks.com

Europa, Medio Oriente y África (EMEA)

Directo: +39 0362 17935 ext. 3 (HCE)

Correo electrónico:

emeatechsupport@marchnetworks.com

Medio Oriente y África

Directo: +00 971(0)52 818 8483

Correo electrónico:

supportmea@marchnetworks.com

Generalidades de la compañía

March Networks® ayuda a las organizaciones a transformar el video en inteligencia de negocios a través de la integración de la videovigilancia, las analíticas, los datos de los sistemas de información del negocio y los dispositivos IoT. Las empresas de todo el mundo utilizan nuestras soluciones de software para mejorar la eficiencia y el cumplimiento normativo, reducir las pérdidas y los riesgos, mejorar el servicio al cliente y ser más competitivas. Con una presencia consolidada en la seguridad por video y redes, March Networks también es reconocida como líder en gestión de video escalable de clase empresarial y servicios alojados. Estamos orgullosos de trabajar con muchas de las instituciones financieras, comercios, operadores de cannabis y autoridades de transporte más grandes del mundo. Ofrecemos nuestro software y sistemas a través de una extensa red de distribuidores y socios en más de 70 países. Fundada en el 2000, March Networks tiene sus oficinas centrales en Ottawa, Ontario, Canadá. Para más información, por favor visite www.marchnetworks.com.



Norteamérica	1.800.563.5564
Latinoamérica	+5255 5259 9511
Europa	+39 0362 17935
Asia	+65 6818 0963
Australia y Nueva Zelanda	+61 1300 089 419
Oriente Medio y África	+971 4 399 5525

© 2021 March Networks. All rights reserved. Information in this document is subject to change without notice. MARCH NETWORKS, March Networks, Command, March Networks Searchlight, March Networks RideSafe, and the MARCH NETWORKS logo are trademarks of March Networks Corporation. All other trademarks are the property of their respective owners. 060-3447-SP-A

