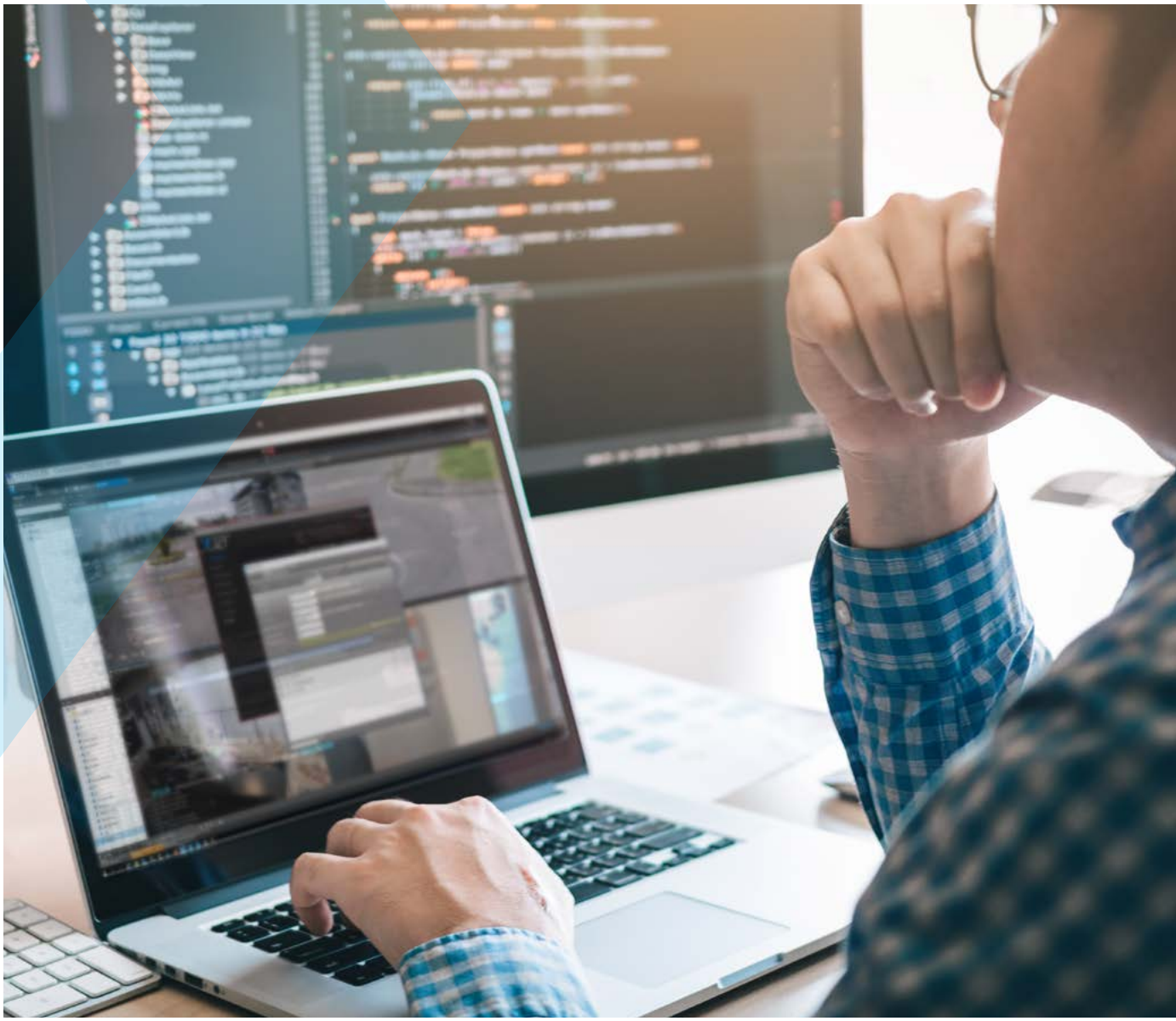

CONSEIL TECHNIQUE

Interconnexion des installations multi-sites et distantes de vidéosurveillance

MARCH networks

Introduction

Le déploiement d'un système de vidéosurveillance IP sur plusieurs sites distants peut être difficile. Sans une architecture de système adéquate, les performances peuvent se dégrader, les petites tâches peuvent prendre du temps et le coût de gestion du système peut augmenter.

March Networks® adopte une architecture centralisée lors de la gestion de plusieurs sites, et le logiciel Command™ Enterprise de March Networks (CES) est au cœur de la solution. Une fois qu'un enregistreur vidéo réseau (NVR) est enregistré auprès du CES, toutes les ressources liées à la vidéosurveillance sont stockées dans une base de données commune : CES est l'entité qui accorde aux utilisateurs authentifiés l'accès à ces ressources.

Voici un diagramme simplifié montrant le chemin des données pour un utilisateur qui lance une requête vidéo d'un enregistrement vidéo à partir d'un NVR sur site.

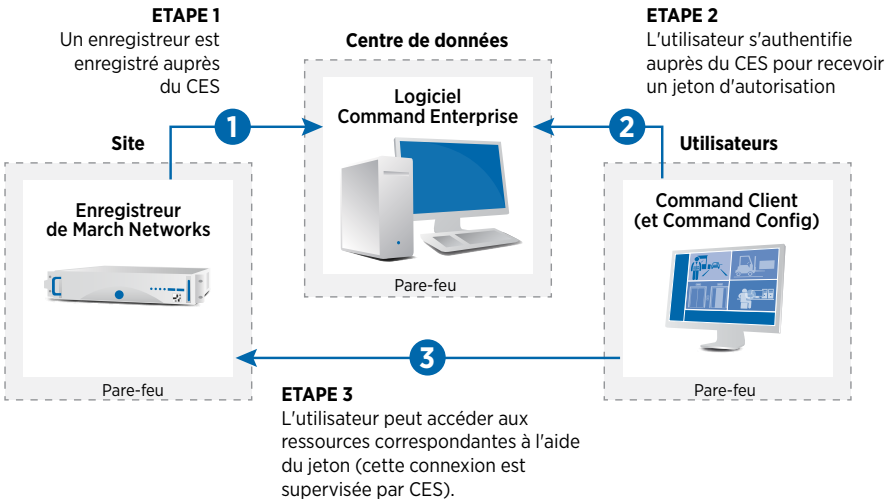

Figure 1 : Le logiciel Command Enterprise est au cœur de la solution March Networks. CES fournit des jetons d'accès aux utilisateurs authentifiés.

La création d'une installation de vidéosurveillance fonctionnelle et efficace à l'échelle géographique nécessite une conception et une configuration de réseau appropriées pour garantir que tout utilisateur puisse facilement accéder aux ressources requises avec une latence minimale.

Topologies réseau

Il est possible de connecter tous les composants du système de vidéosurveillance de différentes manières, mais chaque architecture système a un impact différent sur les performances. Certaines conceptions sont également plus complexes à configurer. Examinons les différentes options :

Option 1 : Redirection de port

La figure suivante illustre les ports requis devant être ouverts par un service informatique afin d'avoir une communication fonctionnelle entre les composants de l'appareil.

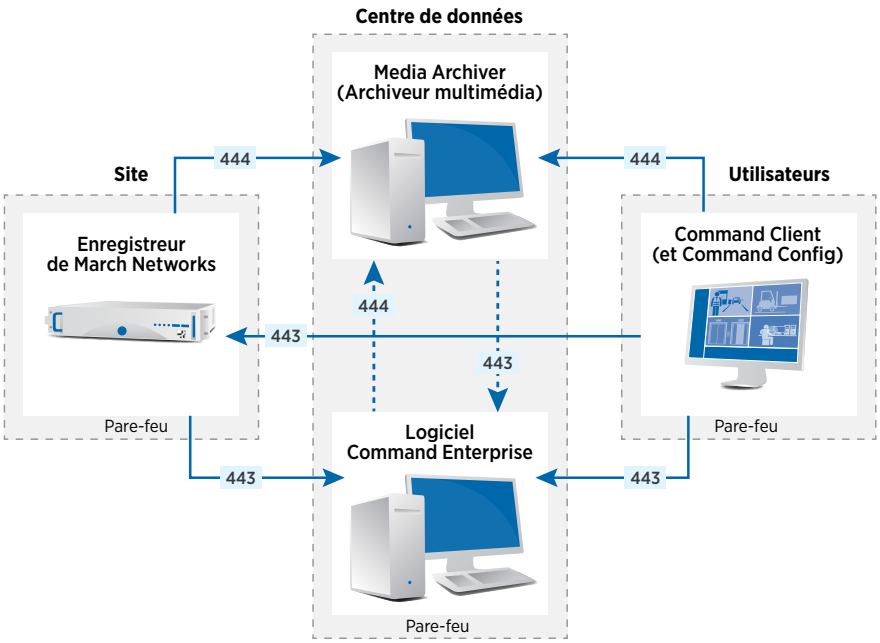

Figure 2 : Détails du port réseau pour chaque module composant la solution. S'applique à Command Solution 2.7 ou version ultérieure. Media Archiver de March Networks, qui fait partie de toute installation CES de March Networks, a été inclus dans le diagramme pour offrir une vue d'ensemble plus complète.

Cette approche exige que chaque enregistreur fasse traduire le port local 443 en une adresse publiée à l'aide des paramètres de l'onglet Réseau dans Command Client de March Networks. Ce paramètre est disponible une fois que vous êtes connecté localement à l'enregistreur avec Command Client.

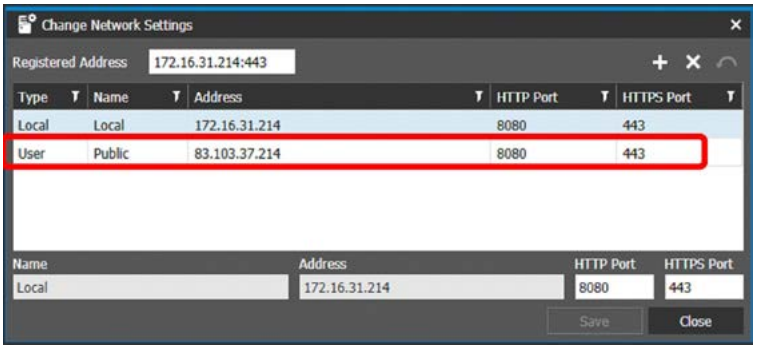

Figure 3 : Ajout de l'adresse publiée à chaque enregistreur à l'aide de la fonction "Modifier les paramètres réseau". À partir de Command Client version 2.7, le port HTTP est facultatif. Dans cet exemple, nous utilisons la valeur 443 d'origine, mais elle peut être modifiée pour correspondre aux exigences du réseau.

L'étape suivante consiste à ouvrir la console de gestion CES, à accéder à l'onglet Réseau et à ajouter la ou les adresses publiques du serveur CES :

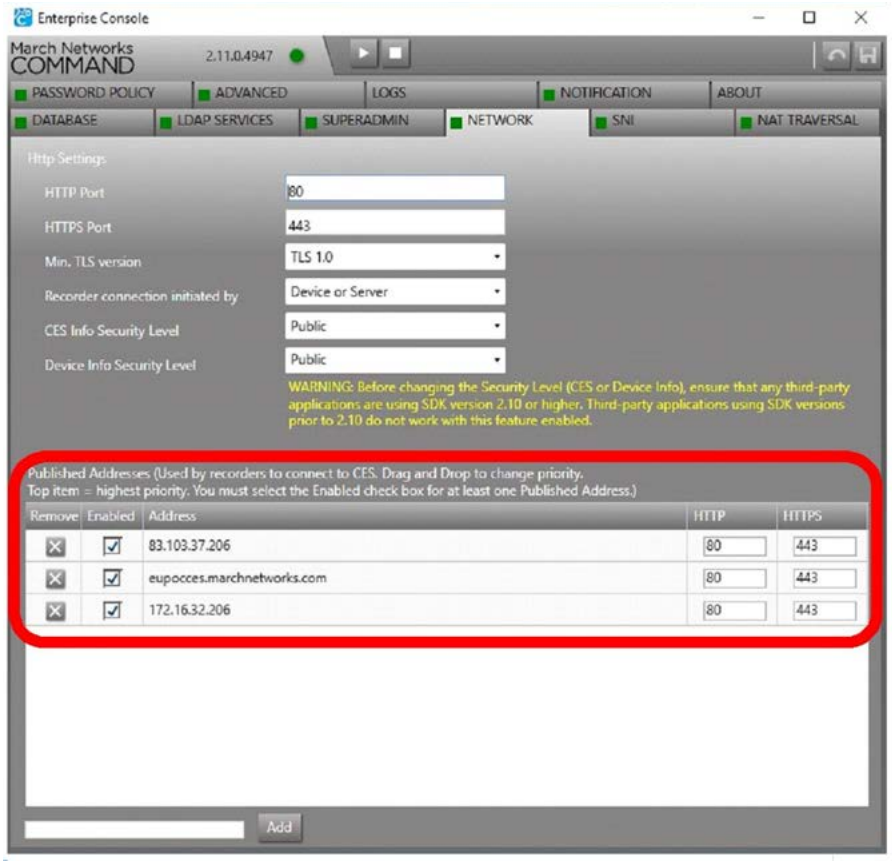

Figure 4 : Console de gestion CES. Ici, il est nécessaire d'ajouter l'adresse publique du serveur CES, en précisant la priorité. Ces valeurs sont transmises à chaque enregistreur pendant le processus d'enregistrement ou lors du redémarrage du CES / NVR (assurez-vous que "connexion de l'enregistreur initiée par" est réglé sur "périphérique ou serveur").

De cette façon, chaque enregistreur conservera la liste complète des adresses CES et essaiera de se connecter au CES en commençant par celle qui a la priorité la plus élevée. Il est possible de vérifier que la liste d'adresses a bien été transmise à chaque NVR, comme illustré dans l'image suivante.

```
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=
```

Figure 5 : Si "information sur le niveau de sécurité de l'appareil" est défini sur Public dans la console de gestion CES, il est possible d'interroger chaque enregistreur à l'aide de http://NVR_IP/info pour obtenir des détails utiles sur l'état du NVR, y compris la liste complète des adresses CES.

Pour terminer la configuration, il sera nécessaire d'implémenter des règles de transfert de port NAT pour chaque enregistreur et serveur CES.

APPAREIL	IP LAN	Port LAN	IP WAN	Port WAN
CES	172.16.32.206	443	83.103.37.206	443
NVR	172.16.31.214	443	83.103.37.214	443

Tableau 1 : En supposant que deux adresses IP publiques distinctes sont disponibles, il est possible de mapper le port LAN 443 au port WAN 443 pour le CES et l'enregistreur. Si cela n'est pas possible, ces valeurs peuvent être ajustées simplement en éditant les panneaux de réseaux présentés.

Cette approche offre les meilleures performances en termes de latence vidéo et de réactivité du système. Aucune ressource supplémentaire n'est requise pour connecter les différents composants du système. Le principal inconvénient est la nécessité de créer une règle NAT spécifique pour chaque appareil, ce qui peut être problématique lorsque l'on gère des centaines ou des milliers d'enregistreurs. Il existe des situations où cette approche est impossible à mettre en œuvre, et dans ce cas il est nécessaire de rechercher des alternatives.

Option 2 : Traversée NAT à l'aide du service STUN / TURN

L'introduction d'un serveur STUN ou TURN supprime la nécessité de créer des règles de redirection de port pour chaque enregistreur. Cela simplifie grandement la configuration du réseau, mais introduit un élément supplémentaire dans l'architecture, ce qui entraîne une dégradation significative en termes de performances du système et de latence. Les services STUN ou TURN doivent être configurés dans la console de gestion d'entreprise de Command de March Networks :

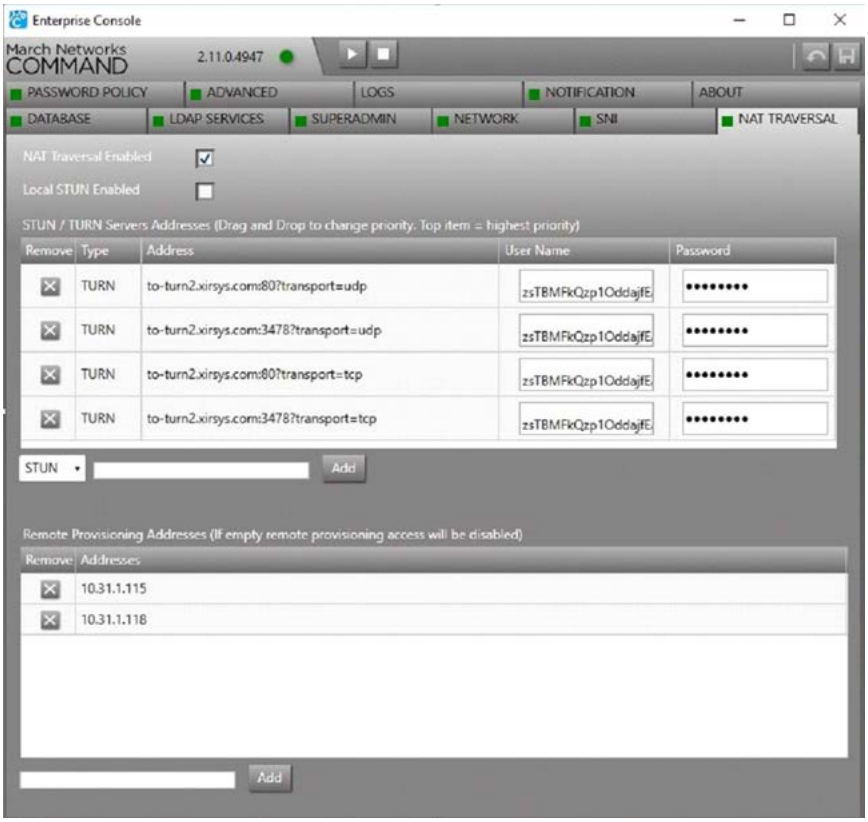

Figure 6 : Command Enterprise version 2.7 ou supérieure dispose de l'onglet TRAVERSEE NAT pour configurer les services STUN ou TURN. Ici, il est possible d'activer les services STUN locaux ou les services STUN / TURN tiers.

Le fonctionnement des services STUN et TURN est assez différent :

Le service STUN agit comme un opérateur qui relie les connexions entre les périphériques, établissant une communication bidirectionnelle peer-to-peer. Le protocole STUN s'appuie sur des paquets UDP pour établir la connexion. Cela doit être pris en compte en choisissant cette solution avec le service informatique, pour garantir qu'aucune règle active n'empêche ce type de protocole de se propager à l'intérieur du réseau. Les ressources STUN sont généralement gratuites et CES propose un service STUN intégré qui peut être activé dans la console de gestion d'entreprise (le trafic UDP est acheminé par défaut sur le port 3478). De plus, il est possible d'utiliser les services Google STUN, ce qui réduit encore les règles à mettre en place.

Le service TURN fait office de "relais" entre Command Client et les enregistreurs. Ce type de service est proposé par plusieurs sociétés tierces moyennant un abonnement mensuel et nécessite l'ouverture de ports personnalisés, en fonction de l'opérateur sélectionné.

Le schéma suivant offre un aperçu des ressources réseau à prendre en compte lors de l'introduction des services STUN / TURN :

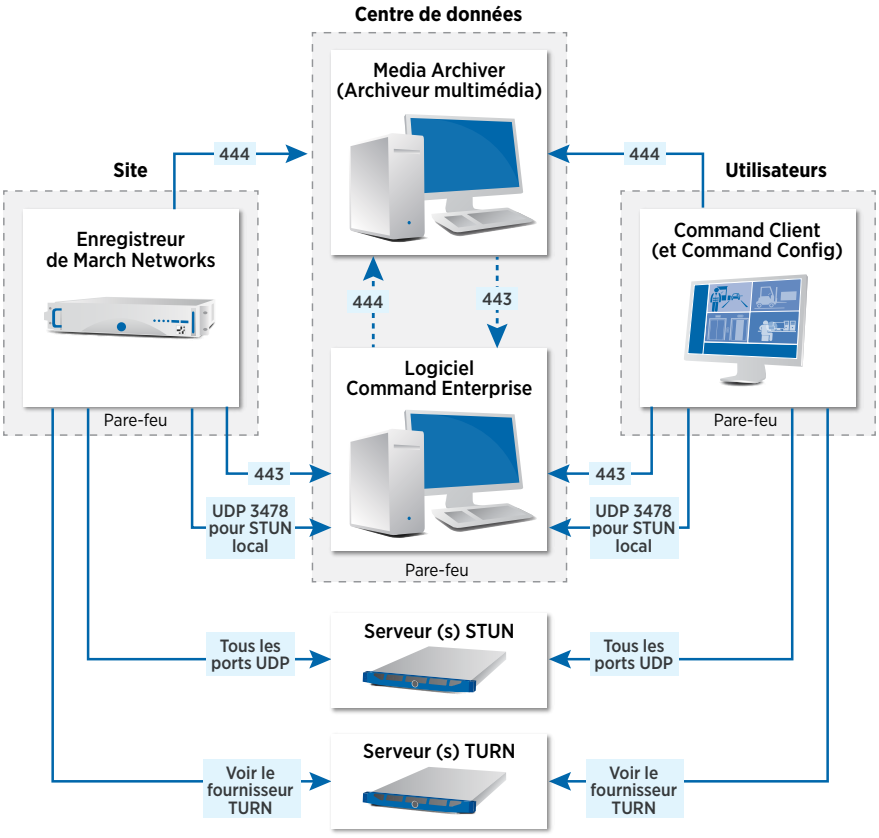

Figure 7 : Architecture réseau lors de l'introduction des services STUN ou TURN. Le serveur CES doit toujours être publié / accessible à partir du PC client, mais aucune connexion directe entre le client et l'enregistreur n'est nécessaire. Tout le trafic lié à la vidéo est géré par le serveur STUN / TURN .

Quelques notes de synthèse :

1. Si vous activez la traversée NAT mais laissez les "règles de transfert de port" en place sur le pare-feu de l'enregistreur, le client continuera à utiliser la méthode de "connexion directe". Le client ne reviendra à une connexion par traversée NAT que lorsqu'il est impossible d'atteindre l'enregistreur via la connexion directe.

2. Les besoins en bande passante peuvent être énormes lors du transfert de contenu vidéo, en particulier lorsque plusieurs caméras sont examinées en parallèle. Cela peut rapidement saturer les ressources disponibles. Cette approche n'est donc pas recommandée pour les salles de contrôle nécessitant une disponibilité vidéo 24h / 24 et 7j / 7. Le transfert de port reste la meilleure option pour ce genre d'utilisation. Cependant, si l'utilisateur n'a que des demandes vidéo occasionnelles, l'approche par traversée NAT peut potentiellement offrir plus de protection contre les cyber-attaques car aucun port permanent n'a besoin d'être ouvert pour aucun des enregistreurs.

Option 3 : Création d'un tunnel VPN entre le NVR, le CES et les clients

La création d'un VPN pour connecter toutes les ressources de vidéosurveillance éliminerait la nécessité de publier des adresses ou d'adopter des serveurs STUN / TURN. Cette option est laissée au choix du service informatique de l'utilisateur final pour sa mise en œuvre et, pour cette raison, n'est pas traitée dans ce document. Cette solution représente une alternative valable pour les installations de transit où du LTE ou du Wi-Fi est utilisé pour connecter des équipements mobiles avec des serveurs centraux, puisque la couche de cryptage introduite par le VPN augmente la sécurité contre les cyber-attaques.

En termes de performances, l'architecture VPN devrait offrir des performances satisfaisantes, mais elle est légèrement dégradée par rapport à la redirection de port, en raison de la couche supplémentaire introduite par les protocoles VPN.

Conclusions

Différentes méthodes ont été présentées pour mettre en place l'interconnexion des installations multi-sites et distantes de vidéosurveillance. Lorsque cela est possible, la redirection de port standard offre les meilleures performances et une latence réduite. C'est donc la solution à privilégier, sauf si votre service informatique ne peut pas mettre en place la redirection de port. Dans ce cas, la traversée NAT ou un VPN peuvent offrir d'autres moyens d'établir la connectivité entre les composants de l'appareil. Mais ces solutions présentent certains inconvénients qu'il faut prendre en compte, à la fois en termes de performances réduites (STUN / TURN), de coût (TURN / VPN) et de complexité (VPN).

Présentation de l'entreprise

March Networks® aide les organisations à transformer la vidéo en intelligence commerciale grâce à l'intégration de la vidéosurveillance, d'analyses et de données provenant de systèmes d'entreprise et d'appareils IoT. Des entreprises du monde entier utilisent nos solutions logicielles pour améliorer l'efficacité et la conformité, réduire les pertes et les risques, améliorer le service client, et être plus compétitives. Avec une présence établie dans la sécurité vidéo et la mise en réseau, March Networks est également reconnu comme le leader des superviseurs vidéo et des services hébergés évolutifs pour le monde de l'entreprise. Nous sommes fiers de travailler avec de nombreuses institutions financières parmi les plus importantes au monde, des marques de vente au détail, des exploitants de cannabis et des régies de transports en commun. Nous diffusons nos logiciels et nos systèmes à travers un vaste réseau de distribution et de partenaires dans plus de 70 pays. Fondée en 2000, March Networks est basée à Ottawa, Ontario, Canada. Pour plus d'informations, veuillez visiter **www.marchnetworks.com**.

Veuillez contacter l'équipe d'ingénierie commerciale de March Networks pour plus de détails. Elle travaillera avec vous pour identifier la meilleure solution pour les besoins spécifiques de votre entreprise.

Service client et assistance

Amérique du Nord, Amérique du Sud et Australie

Direct : 1.613.591.1441

Appel gratuit (US & Canada) : 1.800.472.0116

E-mail : techsupport@marchnetworks.com

Europe, Moyen-Orient et Afrique (EMEA)

Direct : +39 0362 17935 ex. 3 (HNEC)

E-mail : emeatechsupport@marchnetworks.com

Moyen-Orient et Afrique

Direct : +00 971(0)52 818 8483

E-mail : supportmea@marchnetworks.com