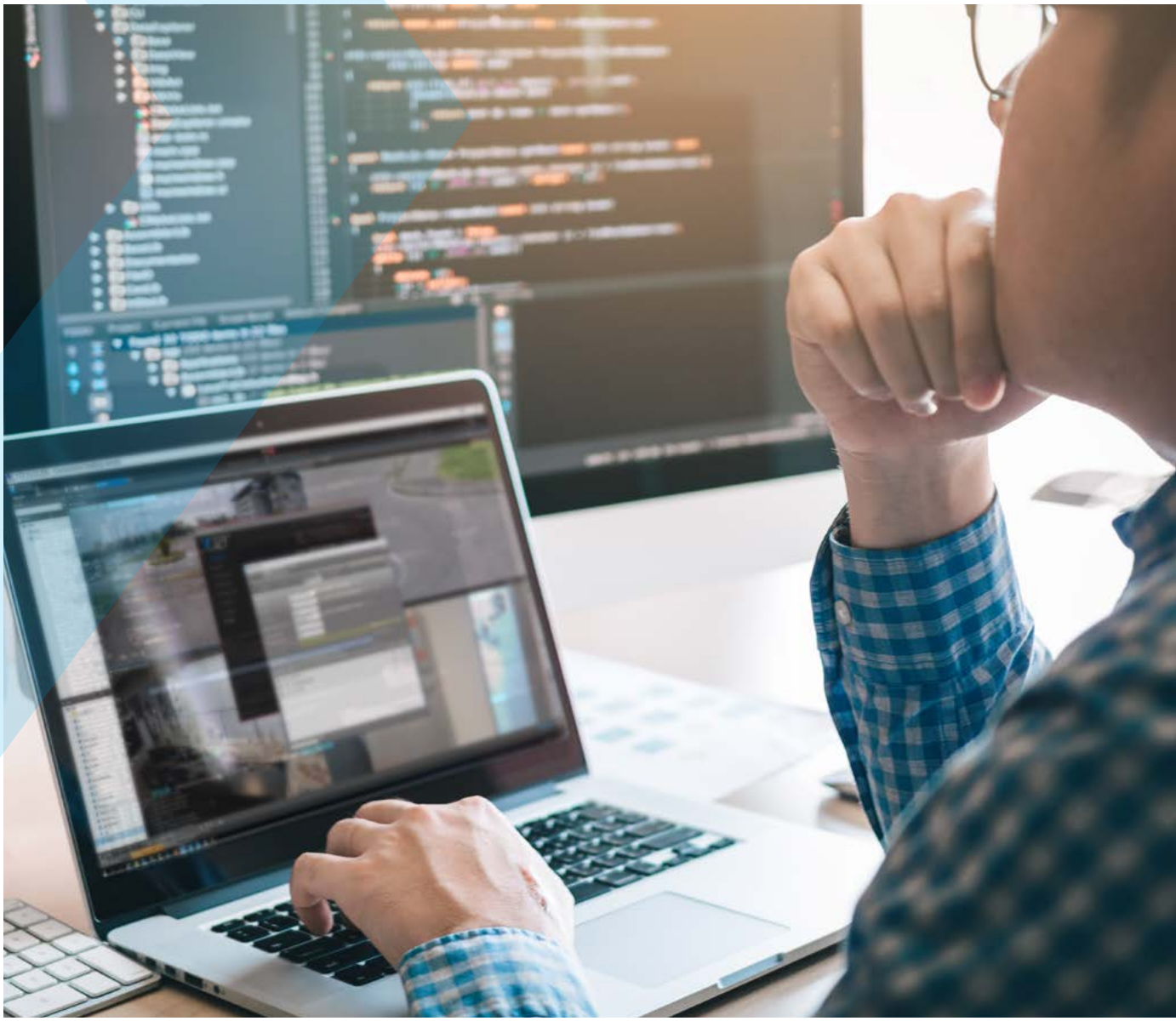

CONSIGLIO TECNICO

Collegamento di installazioni di videosorveglianza IP su scala geografica

MARCH networks

Introduzione

L'implementazione di un sistema di videosorveglianza IP in più sedi separate può rappresentare una sfida. Senza una progettazione adeguata del sistema, le prestazioni possono degradare, compiti semplici possono diventare dispendiosi in termini di tempo e i costi di gestione del sistema possono aumentare.

March Networks® adotta un'architettura centralizzata per la gestione di più sedi, e il software Command™ Enterprise (CES) di March Networks è il nucleo della soluzione. Una volta che un videoregistratore di rete (NVR) viene registrato al CES, tutte le risorse relative alla videosorveglianza vengono memorizzate all'interno di un database comune: CES è l'entità che, previa autenticazione, garantisce all'utente l'accesso a tali risorse.

Ecco un diagramma semplificato che mostra il percorso dei dati per un utente che avvia un'indagine relativa a video catturati da un NVR installato sul campo.

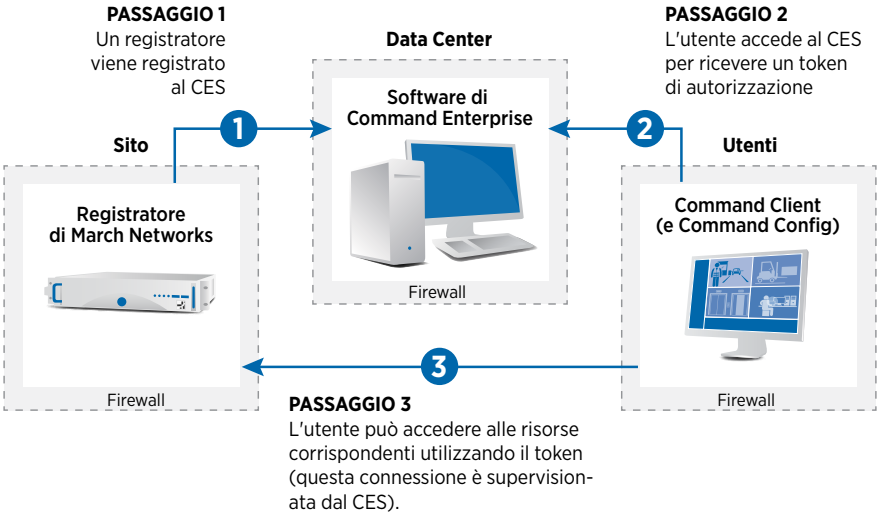

Figura 1: Il software Command Enterprise è il nucleo della soluzione di March Networks. Il CES fornisce i token di accesso agli utenti autenticati.

La creazione di un'installazione di videosorveglianza a livello geografico efficiente e di successo richiede un'adeguata progettazione e configurazione di rete per garantire che ogni utente possa accedere facilmente alle risorse richieste con latenza minima.

Topologie di rete

È possibile collegare tutti i componenti del sistema di videosorveglianza in modi diversi, ma ogni schema del sistema ha un impatto diverso sulle prestazioni. Alcuni schemi sono anche più complessi da configurare. Diamo un'occhiata alle varie opzioni:

Opzione 1: Inoltro porta

La figura seguente illustra le porte necessarie che devono essere aperte da un dipartimento IT per avere una comunicazione efficace tra i componenti del dispositivo.

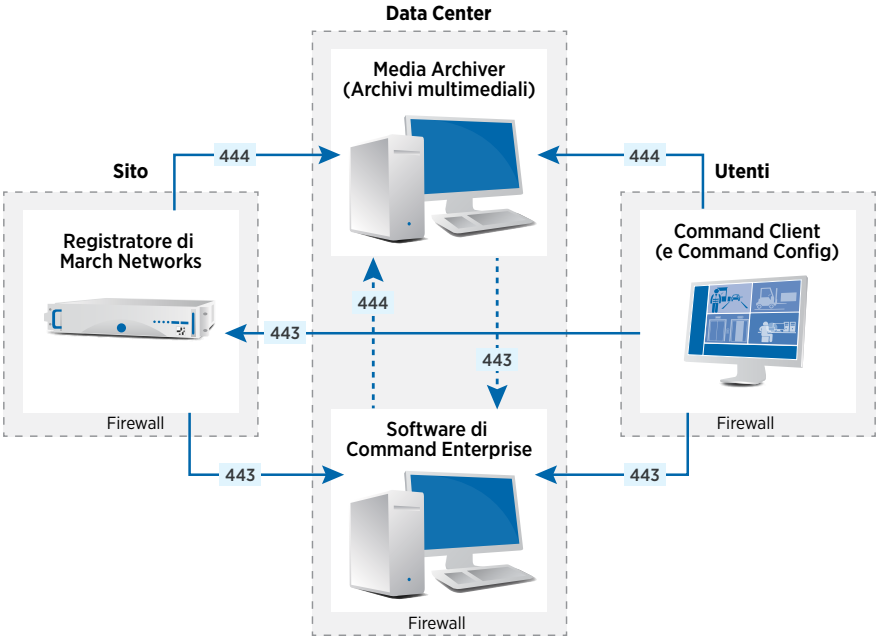

Figura 2: Dettagli della porta di rete per ciascun modulo che compone la soluzione. Si applica alla soluzione di Command 2.7 o superiore. Essendo Media Archiver di March Networks componente di qualsiasi installazione CES di March Networks, è stato incluso nel diagramma, per offrire una panoramica più completa.

Questo approccio richiederà che ogni registratore abbia la porta locale 443 mappata in un indirizzo pubblicato utilizzando le impostazioni della scheda Rete del Command Client di March Networks. Questa impostazione è disponibile quando si è connessi localmente al registratore con Command Client.

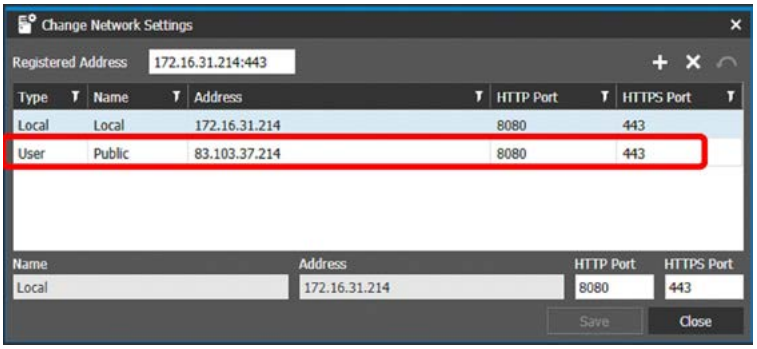

Figura 3: Aggiunta a ciascun registratore dell'indirizzo pubblicato, utilizzando la funzione "Modifica impostazioni di rete". Dalla versione 2.7 di Command Client la porta HTTP è facoltativa. In questo esempio viene utilizzato il valore 443 originale, ma può essere modificato per soddisfare i requisiti di rete.

Il passo successivo consiste nell'aprire la consolle di gestione di CES, navigare alla scheda Rete e aggiungere l'indirizzo, o gli indirizzi, pubblico del server CES:

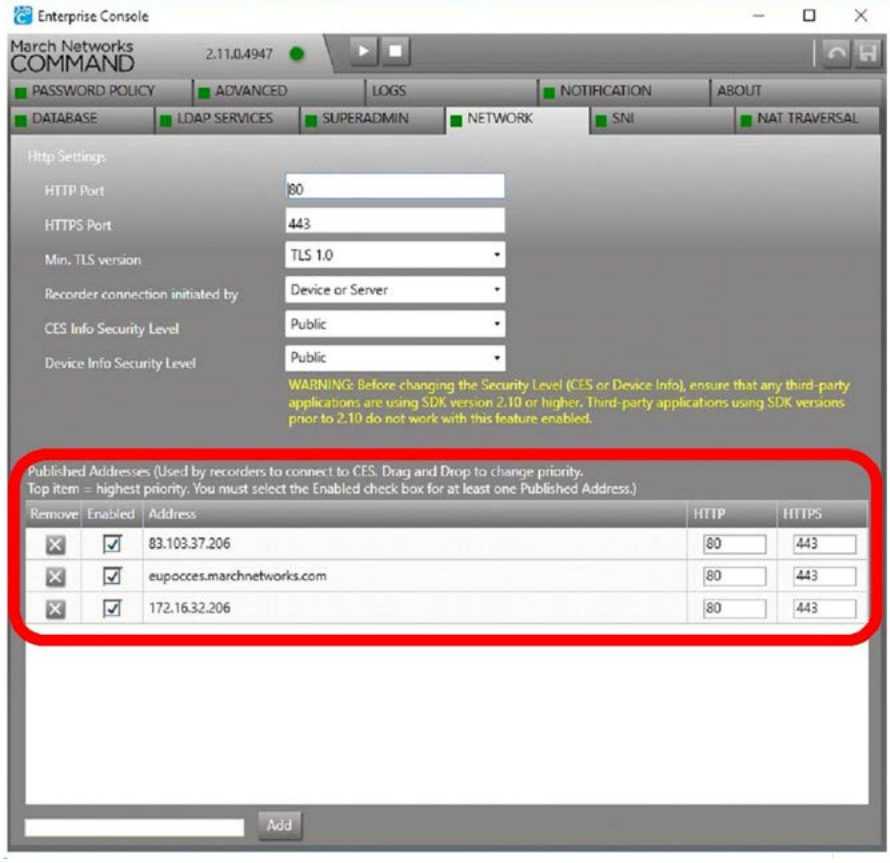

Figura 4: Consolle di gestione CES. Qui è necessario aggiungere l'indirizzo pubblico del server CES, specificandone la priorità. Questi valori vengono trasmessi a ciascun registratore durante il processo di registrazione o al riavvio di CES/ NVR (assicurarsi che "Connessione del registratore avviata da" sia impostata su "Dispositivo o Server").

In questo modo, ogni registratore conserverà l'elenco completo degli indirizzi CES e proverà a connettersi al CES partendo da quello con priorità più elevata. È possibile verificare che l'elenco indirizzi sia stato trasmesso correttamente a ogni NVR, come mostrato nell'immagine seguente.

```
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=
```

Figura 5: Se "Informazioni sul livello di sicurezza del dispositivo" è impostato su Pubblico nella consolle di gestione CES, è possibile interrogare ciascun registratore utilizzando http://NVR_IP/info per raccogliere dettagli utili sullo stato del NVR, incluso l'elenco completo degli indirizzi CES.

Per completare la configurazione, sarà necessario implementare regole di inoltro porta NAT per ciascun registratore e server CES.

Tabella 1: Supponendo che siano disponibili due IP pubblici separati, è possibile mappare la porta LAN 443 sulla porta WAN 443 sia per il CES che per il registratore. Nel caso in cui ciò non fosse possibile, tali valori possono essere regolati semplicemente modificando i pannelli delle reti evidenziati.

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

Questo approccio offre le migliori prestazioni in termini di latenza video e reattività del sistema. Non sono necessarie risorse aggiuntive per collegare i vari componenti del sistema. Lo svantaggio principale è la necessità di creare una regola NAT specifica per ogni dispositivo e questo può essere problematico quando si gestiscono centinaia o migliaia di registratori. Ci sono situazioni in cui questo approccio è impossibile da implementare quindi, per tali scenari, è necessario esplorare delle alternative.

Opzione 2: Attraversamento NAT con servizio STUN/ TURN

L'introduzione di un server STUN o TURN elimina la necessità di creare regole di inoltro porta per ogni registratore. Ciò semplifica notevolmente la configurazione della rete, ma introduce un elemento aggiuntivo nell'architettura, che provoca un significativo degrado in termini di prestazioni e latenza del sistema. I servizi STUN o TURN devono essere configurati all'interno della consolle di Command Enterprise:

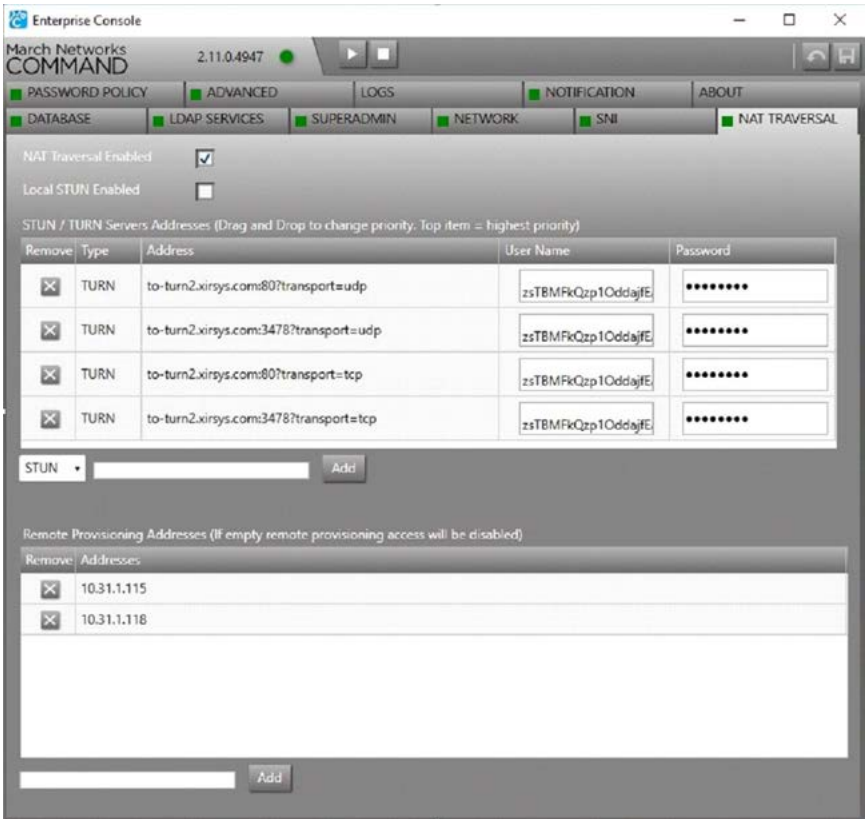

Figura 6: La versione 2.7 di Command Enterprise, o successive, ha la scheda ATTRAVERSAMENTO NAT per configurare i servizi STUN o TURN. Qui è possibile abilitare servizi STUN locali o servizi STUN/ TURN di terze parti.

La modalità di funzionamento dei servizi STUN e TURN è abbastanza diversa:

Il servizio STUN agisce da operatore che collega le connessioni tra i dispositivi, stabilendo una comunicazione bidirezionale peer-to-peer. Il protocollo STUN si basa su pacchetti UDP per stabilire la connessione, quindi questo deve essere preso in considerazione quando si discute la soluzione con il dipartimento IT, per garantire che nessuna regola impedisca a questo tipo di protocollo di propagarsi all'interno della rete. Le risorse STUN sono di solito gratuite e il CES stesso offre un servizio STUN integrato che può essere abilitato all'interno della consolle di gestione d'impresa (il traffico UDP viene instradato di default sulla porta 3478). Inoltre, è possibile utilizzare i servizi STUN di Google, riducendo ulteriormente le regole da mettere in atto.

Il servizio TURN funge da "Relè" tra il Command Client e i registratori. Questo tipo di servizio viene offerto da diverse società terze a pagamento mensile e richiede l'apertura di porte personalizzate, a seconda dell'operatore selezionato.

Il seguente diagramma offre una panoramica delle risorse di rete da considerare quando si introducono i servizi STUN/TURN:

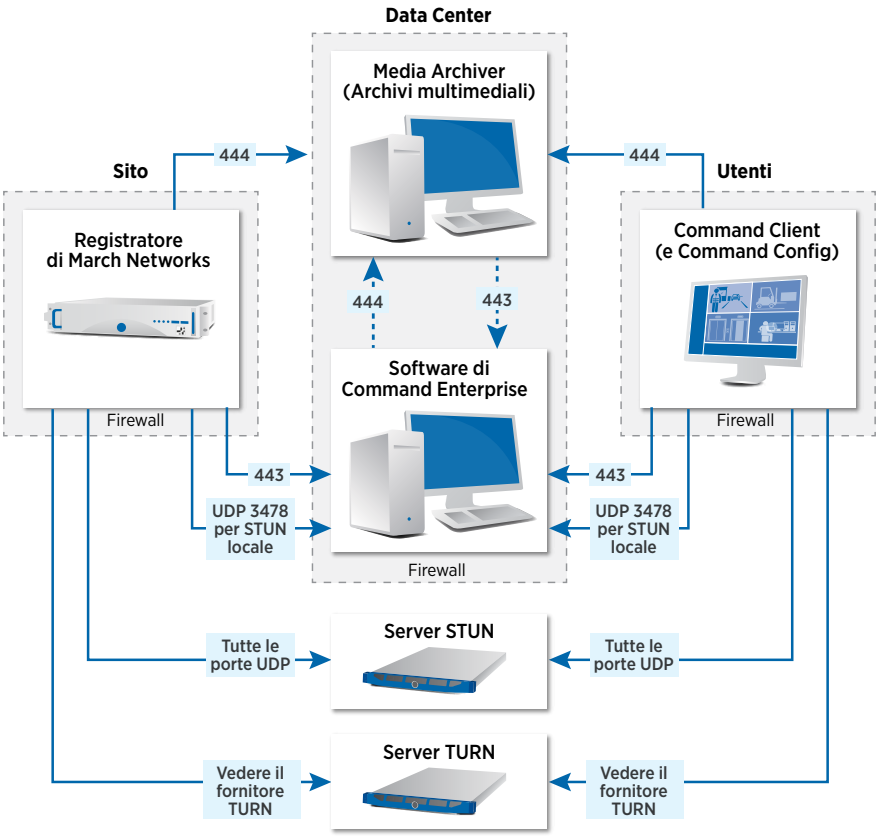

Figura 7: Architettura di rete quando si introducono servizi STUN o TURN. Il server CES deve ancora essere pubblicato/accessibile dal PC client, ma non è necessaria alcuna connessione diretta tra client e registratore. Tutto il traffico relativo ai video è gestito dal server STUN/TURN.

Un paio di note riassuntive:

1. Se abilitate l'attraversamento NAT ma lasciate le "regole di inoltro porta" vigenti sul firewall per il registratore, il client continuerà a utilizzare il metodo "connessione diretta". Il client potrà fare affidamento su una connessione di attraversamento NAT solo quando non sarà in grado di raggiungere il registratore tramite la connessione diretta.

2. I requisiti di larghezza di banda possono essere enormi nel trasferimento di contenuti video, soprattutto quando più telecamere vengono esaminate in parallelo. Ciò può saturare rapidamente le risorse disponibili, quindi questo approccio non è raccomandato per le sale di controllo che richiedono disponibilità video 24 ore su 24, 7 giorni su 7. L'inoltro porta è ancora l'opzione migliore per questo tipo di applicazione. Tuttavia, supponendo che l'utente abbia solo sporadiche richieste video, l'approccio attraversamento NAT può potenzialmente offrire una maggiore protezione contro gli attacchi informatici, poiché non è necessario aprire una porta permanente per nessuno dei registratori.

Opzione 3: Creazione di tunnel VPN tra NVR, CES e i clienti

La creazione di una VPN per collegare tutte le risorse di videosorveglianza eliminerebbe la necessità di pubblicare indirizzi o adottare server STUN/TURN. L'implementazione di questa opzione è a discrezione del dipartimento IT dell'utente finale e per questo motivo non è trattata in questo documento. Questa soluzione rappresenta una valida alternativa per le installazioni di transito in cui vengono utilizzati LTE o Wi-Fi per collegare apparecchiature mobili con server centrali, poiché il livello di crittografia introdotto dalla VPN aumenta la sicurezza contro gli attacchi informatici.

In termini di prestazioni, l'architettura VPN dovrebbe offrire prestazioni adeguate, ma è leggermente degradata rispetto all'inoltro porta, a causa del livello aggiuntivo introdotto dai protocolli VPN.

Conclusioni

Sono stati presentati diversi metodi per implementare la connettività di un'installazione di videosorveglianza su scala geografica. Quando possibile, l'inoltro porta standard offre le migliori prestazioni e una latenza ridotta, quindi questa dovrebbe essere la strada da percorrere, a meno che il vostro dipartimento IT sia impossibilitato a implementare le regole di inoltro porta. In questo scenario, l'attraversamento NAT o la VPN possono offrire modi alternativi per stabilire la connettività tra i componenti del dispositivo, ma questo ha alcuni svantaggi da considerare, sia in termini di prestazioni ridotte (STUN/TURN), sia di costi (TURN/VPN) e di complessità (VPN).

Presentazione dell'azienda

March Networks® aiuta le organizzazioni a trasformare il video in business intelligence attraverso l'integrazione di video di sorveglianza, analytics e dati di sistemi aziendali e dispositivi IoT. Le aziende di tutto il mondo utilizzano le nostre soluzioni software per migliorare l'efficienza e la conformità, ridurre le perdite e i rischi, migliorare il servizio clienti e competere con maggiore successo. Con radici profonde nella videosicurezza e nel networking, March Networks è anche riconosciuta come leader nella gestione video scalabile e a livello aziendale, e nei servizi ospitati. Siamo orgogliosi di lavorare con molte delle più grandi istituzioni finanziarie, marchi al dettaglio, operatori di cannabis e autorità di transito del mondo, e di fornire i nostri software e sistemi attraverso una vasta rete di distribuzione e partner in più di 70 paesi. Fondata nel 2000, March Networks ha sede a Ottawa, Ontario, Canada. Per ulteriori informazioni, visitate: **www.marchnetworks.com**.

Vi preghiamo di contattare il team tecnico di vendita di March Networks per ulteriori dettagli. Lavoreranno insieme a voi per identificare l'opzione migliore per le vostre esigenze aziendali specifiche.

Supporto e servizio clienti

Nord America, Sud America e Australia

Diretto: 1.613.591.1441

Numero verde (Stati Uniti e Canada): 1.800.472.0116

E-mail : techsupport@marchnetworks.com

Europa, Medio Oriente, Africa (EMEA)

Diretto: +39 0362 17935 int. 3 (OCE)

E-mail : emeatechsupport@marchnetworks.com

Medio Oriente e Africa

Diretto : +00 971(0)52 818 8483

E-mail : supportmea@marchnetworks.com

© 2021 March Networks. Tutti i diritti riservati. Le informazioni contenute in questo documento sono soggette a cambiamenti. MARCH NETWORKS, March Networks Command, March Networks Searchlight, March Networks RideSafe e il logo MARCH NETWORKS sono marchi registrati di March Networks Corporation. Tutti gli altri marchi registrati sono di proprietà dei rispettivi titolari. 060-3447-IT-A