Case Study

SE*link*™

Ensuring video surveillance network segmentation and segregation with Zero Trust Secure Virtual Networking

Background

IP video surveillance network infrastructure is challenged to find the balance between efficiency, cost, bandwidth and security to guarantee performance. Video surveillance networks are growing in complexity with the exponential increase in number of devices and network traffic, thus resulting in laggy networks. To conduct efficient communications, private connections, network segmentation and segregation, are a common practice. Segmentation and private networking are achieved through subnets, VLANs data flows isolation, while segregation is usually done through dedicated telco links and/or air-gap, firewall(s), bridge gateways or data diodes. These practices however are often no longer sustainable or exceedingly difficult to implement. A fine-grained network segmentation and data segregation solution, broadly applicable, efficient and secure is mandatory.

Challenge

Network segmentation and private connectivity are well-established best practice, but expensive and exceedingly difficult to implement. The manual configuration of subnets, VLANs, access control lists (ACLs), and firewalls makes it difficult to keep pace with a dynamic network. Although traditional segregation techniques ensure physical network separation without a return channel, they do not meet today's requirements for bandwidth, reliability, implementation speed or bi-directional protocols. Most solutions only work at network layer with unidirectional protocols, with no acknowledgment of receipt which may lead to data loss. Due to protocol implementation, data transfer speed and reliability are also impacted, resulting in a bad QoS. Moreover, private networking requires costly dedicated contracts. The high cost of acquisition and maintenance, specialised knowledge and skills required represent a further challenge.

Industry

Surveillance Camera & Visual Analytics

Challenge

- Remove the complexities from network segmentation
- Guarantee isolation of each data stream at application level
- Support two-way communications without compromising security

Goals

- Enforcing unidirectional simultaneous data flows at each network component
- Obtain maximum network performance, stability and availability
- Apply technology at more than just the network layer
- Seamless integration for easy setup, deployment
- Fast-track compliance

Solution

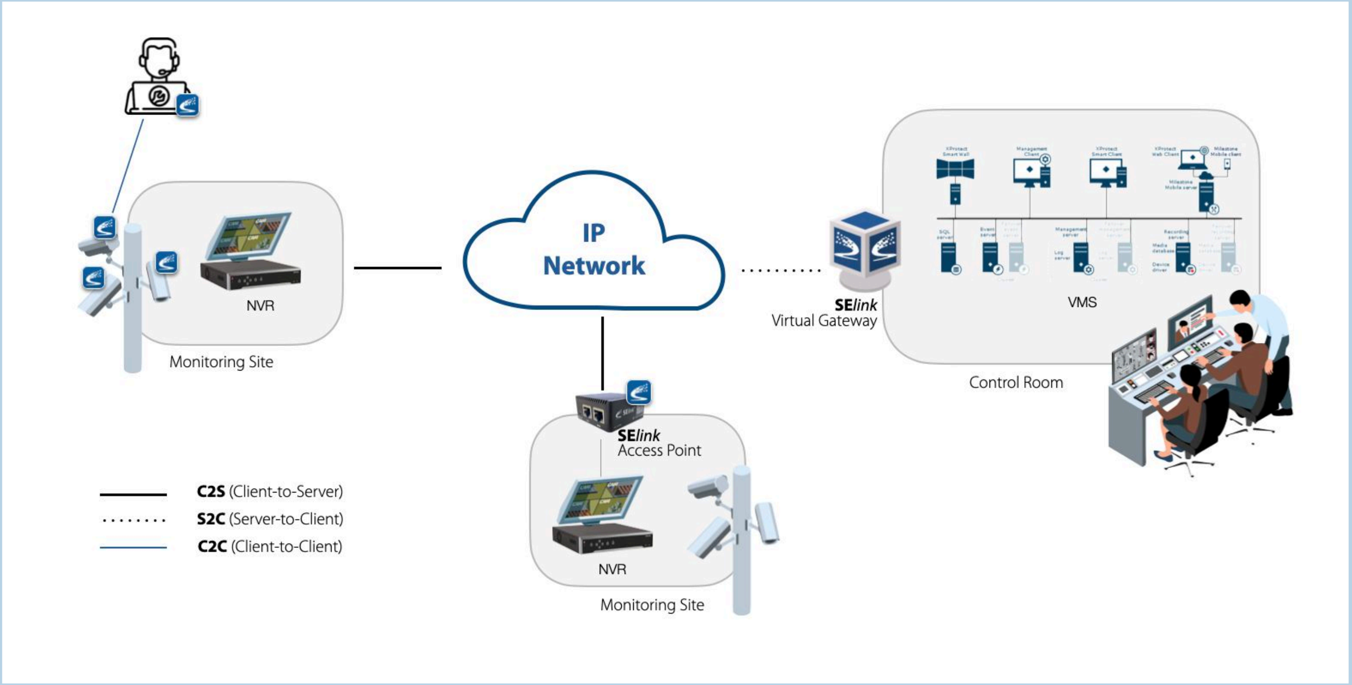
SE*link*™ provides a zero trust security model combined with Service-level software defined network segmentation, granular privileged access management and network diode. Delivering efficiency, security and control to Devices and Networks in a single solution.

Solution

SE*link*™ introduces Virtualisation, Isolation and Encryption for IP Video Surveillance networks, while ensuring a logical separation of network domains. Each host and network is segmented and segregated from the data link layer, up to and including the application layer. Identification, authentication and authorisation of hosts to access services is based on least-privilege principles, increasing the overall security posture of the environment. SElink™ is more than a data diode or traditional network-based segmentation through subnets. **SE*link*™ is a Zero Trust service-oriented, secure, virtual networking solution to protect end-points, to segregate services and to create private networks.** SE*link*™ replicates heterogenous clients and server behaviours in a seamless way, as in a private LAN. The SE*link*™ Gateway performs endpoint device "virtualisation", even showing to the server the original IP for each endpoint device. The advantages are overwhelming. SE*link*™ protects both the data channel and the access to the communication channel, which can only be used by authorised processes. This ensures that the server is protected even if the endpoint device is compromised, avoiding infection propagation through the network, with major service disruptions and significant impact on business continuity. **Implementing SE*link*™, devices no longer need public static IP addresses, resulting is significant reductions of the attack surface and positive reflections in terms of efficiency and operational costs.** Lightweight protocols and zero encryption overhead make band availability and integration of security no longer a limit. Easy integration in any third-party devices (i.e. VMS components, both client and server side) and environment, over any protocol, portable, multi-device for a fast deployment of new devices at accident sites without requiring experts to travel to the site. SE*link*™ is ready to use the Post-Quantum algorithms shortlisted by NIST. Crypto agility allows SE*link*™ to migrate to new symmetrical algorithms in a centralised way without any effort. A centralised deployment and management security system guarantees control across a large-scale network.

Benefits

1. **Zero Trust Network Access and Assumed Breach model** strategies
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices and **Zero Encryption Overhead** compared to TLS/SSL
3. **Low-bandwidth strategies coupled with smart mechanisms** to improve QoS and availability of service
4. **Private networking** with no need for costly dedicated connectivity contracts
5. **No need for costly dedicated data diode appliances** for one way flow segmentations
6. **Enhanced system longevity and resilience** to quantum attacks and **Seamless encryption updates, redesign-free** through Crypto Agility



NVR
Monitoring Site
IP Network
SElink
Virtual Gateway
XProtect Smart Wall
Management Client
XProtect Smart Client
XProtect Web Client
Milestone Mobile client
Milestone Mobile server
SQL server
Event server
Failover event server
Management server
Log server
Failover management server
Recording server
Media database
Device driver
Failover recording server
Cluster
VMS
Control Room
SElink
Access Point
NVR
Monitoring Site
C2S (Client-to-Server)
S2C (Server-to-Client)
C2C (Client-to-Client)