Encryption of network streams

AES 256 encryption key to protecting UNV Surveillance System

Protecting communication between UNV network video cameras, management software and clients

Securing all aspects of your security system communications, servers and data — is of increasing importance to businesses today. It's also driving the convergence of physical security and cybersecurity. Whether you are responsible for your organization's physical security or cybersecurity it is about continually identifying the assets and resources you need to protect. From this you can assess the most plausible threats to protect against and how to prevent, detect and remediate external and internal threats.

Few ways to encrypt network video streams

HTTPS

HTTPS is the standard protection used to encrypt traffic between clients and servers. TLS (Transport Layer Security) is used to create a secure channel where the HTTP traffic is tunneled. Video is typically transmitted using RTP (Real-time Protocol). For encrypted video the client needs to request the RTP stream over HTTPS. HTTPS (TLS) may use different types of ciphers. The cipher that is most commonly used is AES (Advanced Encryption Standard), which provides key lengths of either 128 or 256 bits.

Moving forward, businesses will need to consider incurring additional costs related to network protection as hackers continue to be more focused and persistent with attacks. IP devices and servers with AES 256 encryption greatly help to prevent intruders from reconfiguring devices or gaining unauthorized access to stored data.