Encrypting network streams

An overview of why and how to encrypt network video

Genetec™ AXIS COMMUNICATIONS

Protecting communication between 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.

Purpose of this document

The aim of this guide is to provide an overview of how encryption keeps network streaming of video, audio and data secure.

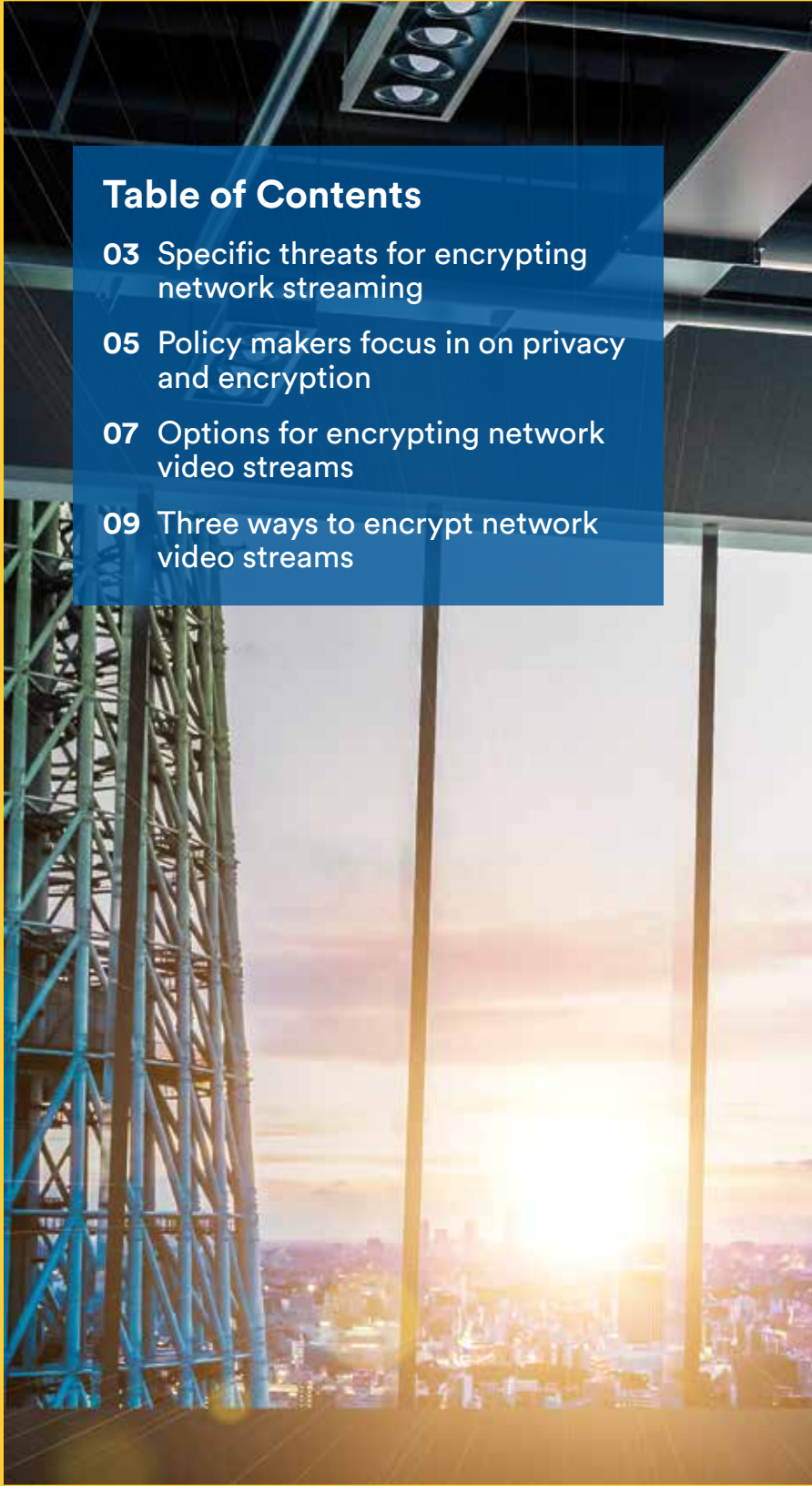


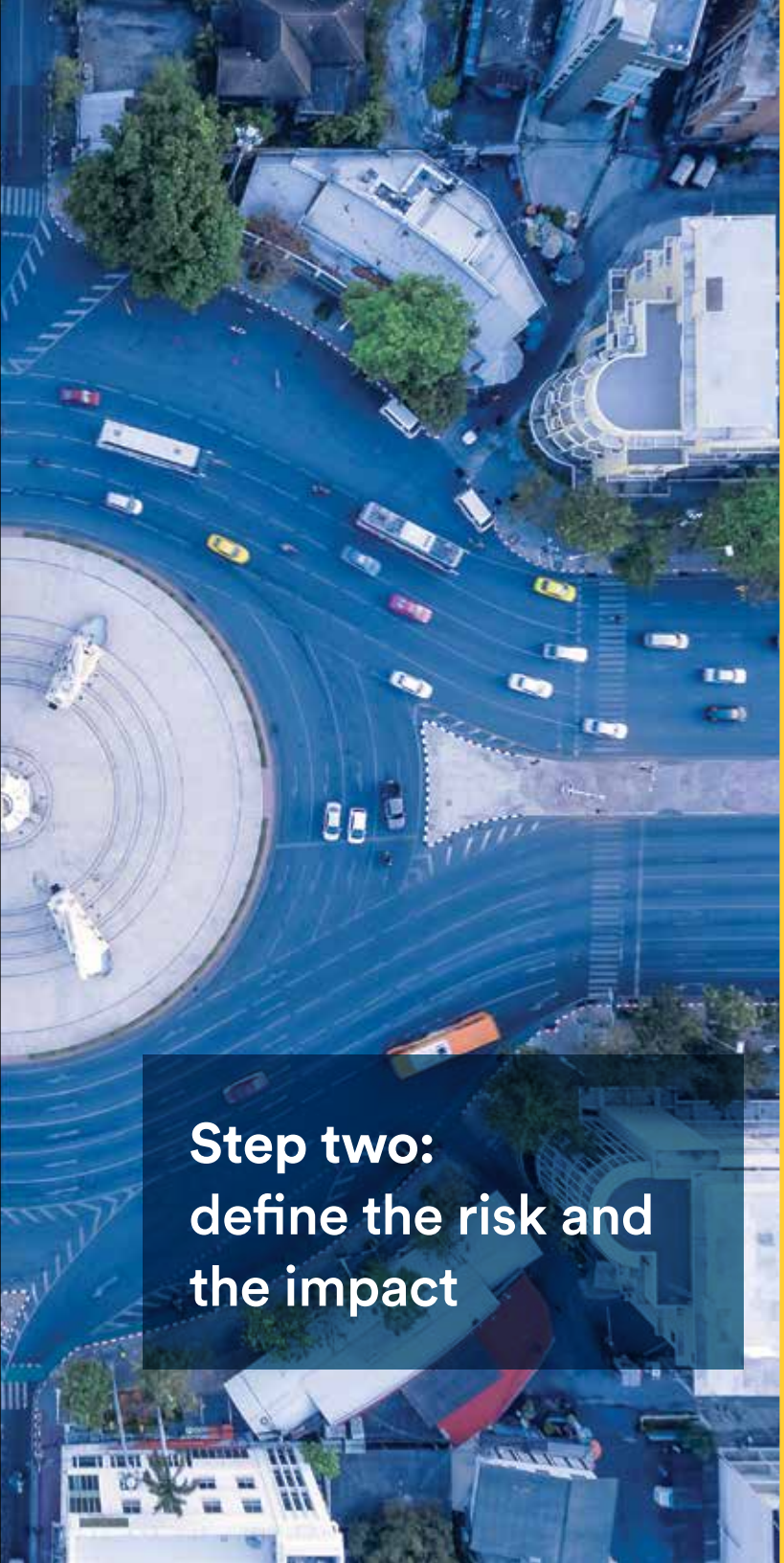
Table of Contents

Chapter 1

Specific threats for encrypting network streaming

As with anything that resides on a network, IP security software, systems and devices are susceptible to a variety of attacks. Understanding the threats implicit in network streaming is step one. The main external threats include:

- **Network sniffing (eavesdropping):** an adversary with access to the same network as two communicating devices can capture data packets. Any data — even sensitive and critical data — can be easily compromised if it is not protected.
- **Network spoofing (resource integrity):** a malicious computer can impersonate a network resources luring the other part to expose sensitive information or altering the data (integrity).
- **Man-in-the-middle (information integrity):** an adversary that is able redirect and intercept traffic has the ability to alter the communication between two parties.



Step two: define the risk and the impact

Impact and risk levels

A series of specification standards for an information security management system, ISO 27000 classifies data and services as restricted, private or public. Each risk classification is based on its potential impact. For example, one video system can classify assets as:

- Live video classified as public, which refers to both the general public as well as the public within an organization. If the live video is exposed to the public, the harm is limited.
- Recorded video may be classified as private, only accessible to a specific organizational unit, because some recorded incidents may be sensitive.
- System configurations, accounts and passwords are classified as restricted, only accessible to selected individuals within the organization.

Two steps in setting your policy

Axis and Genetec recommend creating security policies associated with every network technology deployed within an enterprise. It should define which data in your network is sensitive so that it can be properly protected when in transit.

Chapter 2

Policy makers focus in on privacy and encryption

Compliance to changes in governmental legislation as well as industry-specific standards or norms. Demands to meet the latest requirements that will stem from the General Data Protection Regulation or to protect sensitive personal data. New outline threats. Desires to unify security, operational and administrative systems. All these factors constantly impact the need to protect personal data and video streams.

Privacy, integrity and origin important issues today

Surveillance video also encompasses the need to consider protection of sensitive personal data and privacy, as the General Data Protection Regulation (GDPR) reminds us. Its aim is to strengthen the rights of data subjects within the European Union (EU) and European Economic Area (EEA) with regard to how their personal data is used and how it's protected. To most, the term 'personal data' means any information that relates to an identified or identifiable natural person. This includes video.

So when it comes to video footage, the ability to restrict activity and access is extremely important. Access to recorded or streamed video must also be highly secure and protected to ensure privacy. Three aspects are important independent of which solution is used:

Privacy: protects personal identity information and keeps identities secret

Integrity: proves that the video has not been tampered with

Source origin: proves that the video came from the correct source

Ensuring data integrity, confidentiality and source origin is typically managed via Hyper Text Transfer Protocol Secure (HTTPS) and Transport Layer Security (TLS).

Chapter 3

Options for encrypting network video streams

Compliance to industry standards is one of the main drivers for network security and managing transmission of network video. However, a common recommendation today is for all security data in transit over a network to be encrypted — and all resources should be authenticated.

Securing network streaming requires implementing security for both the camera component, video management system and the network infrastructure that those communication streams traverse. There are different levels of security when it comes to securing video being sent over IP networks. Hardening the network involves establishing and maintaining authenticated communication streams, digitally signing configuration files and encrypting data and video streams and signaling between all the various components. All of these security features are not required for every network, but they provide options for increasing levels of security.

Of course, each form of protection has a cost associated with it and typically requires various workflow routines. Often, more advanced routines are associated with more advanced forms of protection, leading to escalating costs.

Unicast versus multicast

Unicast and multicast transmissions are two methods in which video is commonly streamed over a network, from the camera to its destination. Each video transmission method comes with its own pros and cons, and every installation's functional requirements will dictate which transmission is best. In general:

- **Unicast streaming** is the most common way to stream network video. Each client requests one media stream. This transmission ensures that all network packets are delivered to the client.
- **Multicast streaming** broadcasts packets and allows multiple clients to view the same video stream. This is a more effective scheme when multiple clients view the same video stream. Multicast does not ensure that all clients will get all the packets due to network disruption. For video streams the impact may be very limited, often unnoticeable.

The network infrastructure and system usage dictate which scheme to use.

Chapter 4

Three ways to encrypt network video streams

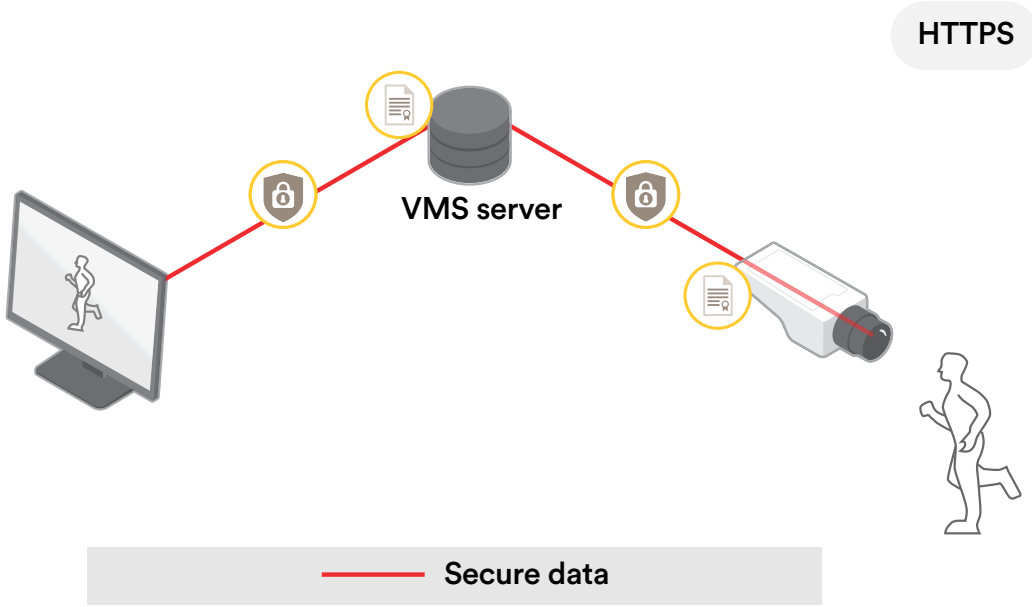
HTTPS

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. If the server has a Certificate Authority (CA)-signed certificate the client will be able to validate that it is accessing a legitimate server and not a malicious computer impersonating the camera.

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.

Axis cameras come preloaded with a self-signed certificate and HTTPS enabled. This is sufficient for a client to access the camera with HTTPS out-of-the-box. If there is a threat of spoofing, the certificate needs to be replaced with a CA-signed certificate.

This task is typically time consuming and difficult to manage in enterprise level systems that deploy large quantities of edge-based IP cameras. AXIS Device Manager (ADM) software can act as a CA for cameras, making a trust point for the VMS. Using AXIS Device Manager to deploy and renew CA-signed certificates enables efficient management of up to a couple thousand Axis cameras on one site — or several thousand on a multiple sites — in batches. This provides significant time savings when compared to manually managing one camera at a time through its web interface.

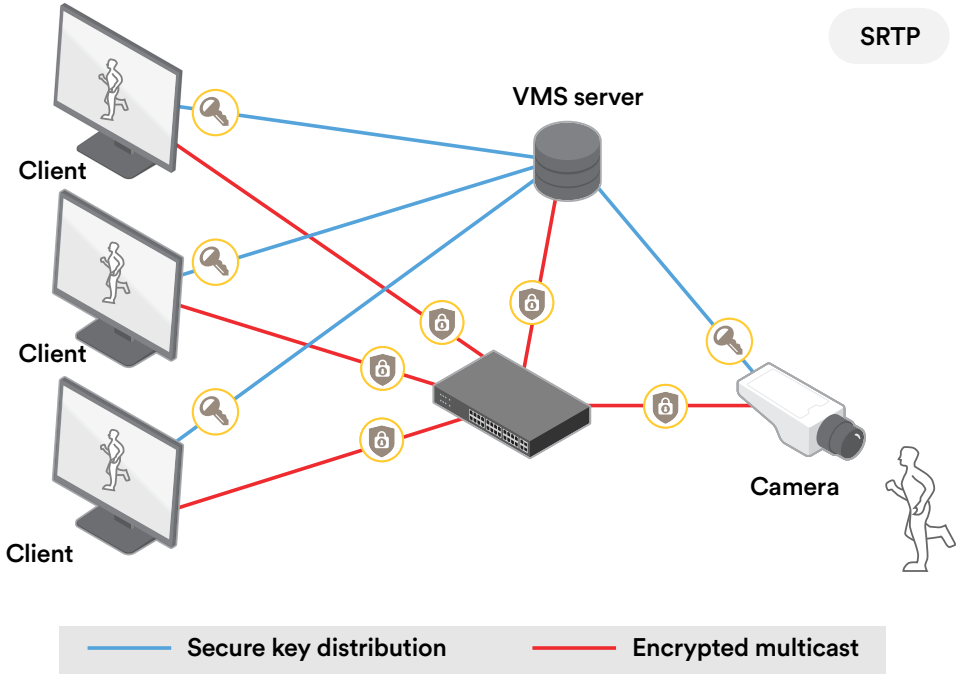


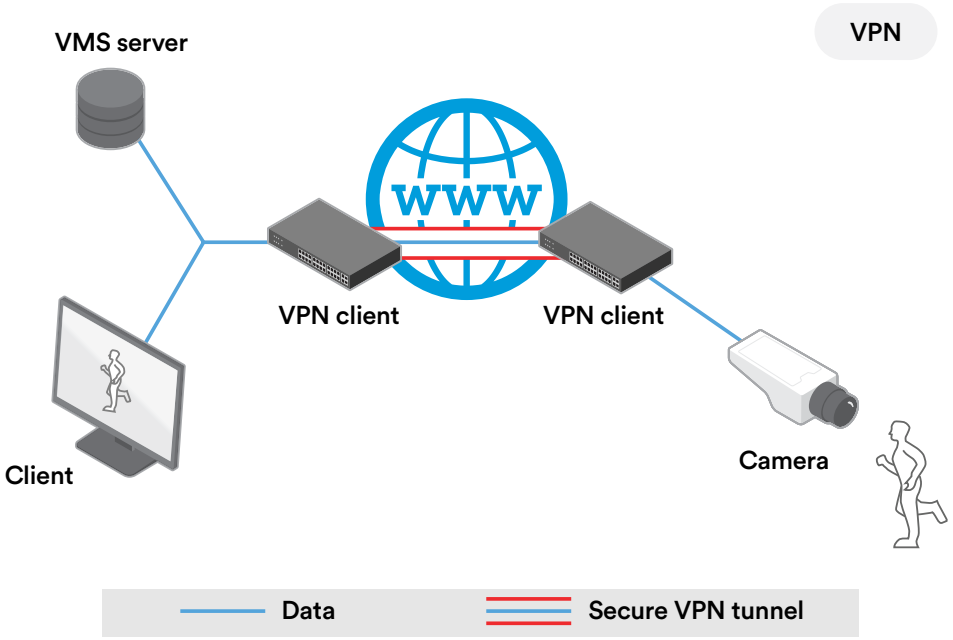
Secure Real-time Protocol (SRTP)

SRTP is an extension to Real-time Transport Protocol (RTP). It is used for both point-to-point and multipoint for data transmissions.

While HTTPS creates a tunnel between the client and server, SRTP encrypts each RTP packet. This means that SRTP can only be used for encrypting streaming media. If the client needs to do administrative tasks to the camera, such as changing some configuration, HTTPS needs to be used.

SRTP uses the same ciphers as HTTPS, typically AES with 128 bit key length.
As AES uses a symmetric key, both the video producer and video consumer need to know the key. The Genetec and Axis SRTP solution provides a way to distribute the keys to clients and cameras in a secure way. The keys are renewed every minute and the solution secures that keys are synchronized between all clients and cameras.





Virtual Private Network (VPN)

VPN provides a secure tunnel and is often used to link two remote networks (sites) in a secure way. VPN can be implemented in different ways and using different protocols, such as Point-to-Point Tunnelling Protocol, Internet Protocol security or OpenVPN.

VPN is typically used to secure connection to remote cameras in a network video system. That could be a camera placed on Internet, a city network or connected over mobile 4G. HTTPS could be used for the same purpose. The primary difference is that HTTPS exposes the camera's public IP address for different types of attacks. A VPN solution provides a local IP address to the camera and thus reduces the public exposure while encrypting the traffic.

Partnering for effective cybersecurity protection

Genetec and Axis are committed to helping its customers and communities excel in the security of security. One of the ways we do this is by finding effective solutions to harden our respective devices, software and systems. For example, our respective hardening guides offer clear means to apply security controls. Moreover, our close collaboration means you can automatically implement a range of the recommendations to secure Axis cameras contained in the Axis hardening guide directly in the Genetec Security Center.

Knowledge sharing is another way Genetec and Axis work together to support the security of your security devices and system. Here we outline two steps in creating security policies for network video technology and three options we offer you for using encryption to protect communication between security systems, networks and communications.

Contact us

Genetec Inc.

genetec.com/trust
info@genetec.com
@genetec

AXIS Communications

Axis Communications AB (Sweden)
Tel: +46 46 272 18 00
Axis Live Support Chat: www.axis.com/support/chat