

HIGH-ASSURANCE ENCRYPTION FOR LAW ENFORCEMENT NETWORK DATA IN MOTION

CASE STUDY

Application of certified high-assurance network encryption	
Sector:	Local Law Enforcement
Use Case:	WAN encryption for CJIS compliance
Solution:	CN6000 Series encryptors protect data in motion across high-speed, point-to-point Ethernet network

Local Law Enforcement Office deploys Senetas certified high-assurance encryptors to meet CJIS-SP compliance obligations.

OVERVIEW

With a Criminal Justice Information Services Security Policy audit looming, a US county sheriff's department was required to upgrade the security of its core Ethernet network infrastructure.

To meet its compliance obligations, the Law Enforcement Office needed to protect data in motion across its high-speed, point-to-point Ethernet network. However, in order to meet its business needs, the certified encryption solution must not adversely impact on network or application performance.

BUSINESS NEED

In a densely populated area, a County Sheriff's office provides police services to more than a million residents, across several towns and cities.

The Law Enforcement office oversees the county jail system and inmate transport. In addition, it provides security at the local courthouse, hospitals and the nearby international airport.

The County Sheriff employs almost 10,000 officers, support staff and volunteers. For them to perform their duties effectively, they require continuous access to sensitive, personally identifiable data.

CHALLENGE

A core component of this data network is access to the United States' Criminal Justice Information Services (CJIS) database; owned and operated by the FBI. A recently mandated condition of use is that data transmitted to and from the CJIS database is encrypted; and that the encryption solution be FIPS certified.

Given the sensitive nature of the information contained within the CJIS database, the Sheriff's Office needed to meet the obligation to encrypt. However, it also needed to ensure that data protection did not come at the expense of network or application performance.

EVALUATION

The Sheriff's Office has previously assumed that access to the CJIS database via Virtual Private Network (VPN) constituted "secure" access. However, a recently introduced mandate required all data in motion be encrypted.

This reflects the understanding that VPNs and dedicated fibre optic networks are not secure.

Layer 2 (Ethernet) and Layer 3 (IPSec) encryption solutions were considered. However, IPSec was quickly ruled out because of the detrimental impact it would have on performance, plus the complexity and latency it would have added to the network.



SOLUTION

The Sheriff's Office chose to protect its network data with Senetas CN6000 Series certified, high-assurance encryptors. When it came to choosing the right solution, the Sheriff's Office considered several key factors; including centralized management, ease of deployment, scalability and zero impact on network performance, applications and other network devices.

The CN6000 Series encryptors are rack-mounted, carrier-grade devices, providing full-line rate encryption of voice, video and data at speeds of up to 10Gbps. Flexibility and scalability are built-in, with the CN6000 Series providing support for metro and wide-area Ethernet networks of all topologies; from point-to-point to hub and spoke or fully meshed.

All Senetas CN Series encryptors offer peace of mind, thanks to three core principles: High-Assurance, Multi-Certified and Crypto-Agile.

The Senetas CN6000 Series is certified as suitable for government and defence use by FIPS, Common Criteria and NATO. Crypto-agility means support for custom curves and algorithms, BYO entropy and Quantum Key Distribution (QKD), ensuring long-term protection for data in a post quantum-computing world.

To offer high-assurance encryption, any solution must feature secure, dedicated, tamper-proof hardware. It should also feature state-of-the-art, zero-touch key management and end-to-end, authenticated encryption. Finally, it should support to use of standards-based encryption algorithms, such as AES 256.

BENEFITS

Senetas encryptors' vendor agnostic, bump-in-the-wire simplicity meant the Sheriff's office was able to rapidly implement the solution; without the need for a proof of concept and in time for the impending security audit.

By deploying Senetas certified high-assurance encryptors, the Sheriff's Office obtained maximum network security and network throughput, with near-zero latency.

Most importantly, with all data in motion between its facilities encrypted, the Sheriff's office may now securely share highly confidential data across the wide-area network. Safe in the knowledge that should a data breach occur, the data would be useless in the hands of an unauthorised user.

The flexibility and high-bandwidth performance of the CN6000 Series easily copes with peaks in workloads; allowing thousands of users to access the system simultaneously, without impacting on network or application performance.

Scalable, rate-limited options and flexible licensing models enable the Sheriff's office to rapidly expand the system to cope with future bandwidth requirements; helping to contribute to an industry-leading ROI and lower total cost of ownership.



SENETAS CORPORATION LIMITED

E info@senetas.com

www.senetas.com



Senetas designs, develops and deploys high-assurance network data encryption solutions. Designed for today's core Metro Area and Carrier Ethernet WAN infrastructures, Senetas solutions support all Layer 2 protocols and topologies.

Our multi-certified CN Series hardware encryptors have crypto-agility built in and are used by some of the world's most secure organisations; including governments and defence forces, commercial and industrial enterprises, Cloud, data centre and telecommunications service providers in more than 35 countries.

gemalto

www.gemalto.com

Senetas CN Series certified high-assurance network encryptors and CV Series virtual encryptors are distributed and supported internationally by Gemalto (North America, Europe, Asia, Middle East and Africa) as SafeNet Ethernet Encryptors.

INTERNATIONAL SUPPORT AND DISTRIBUTION

Senetas CN Series High-Assurance Encryptors and CV Series Virtual Encryptors are distributed and supported by Gemalto, the world's largest data security company, as SafeNet Ethernet Encryptors.

Gemalto also provides pre-sales technical support to hundreds of accredited partners around the world; including systems integrators, data network providers, Cloud and data centre service providers, telecommunications companies and network security specialists.

TALK TO SENETAS OR OUR PARTNERS

Senetas and Gemalto also work with customers' own data network service providers, systems integrators and information security specialists to specify the optimal encryption solution for their needs.

Wherever you are, simply contact Senetas or Gemalto directly to discuss your needs. Or, if you prefer, your service provider may contact us on your behalf.

ENCRYPTION SECURITY WITHOUT COMPROMISE

Whatever your Layer 2 Ethernet network security needs, Senetas has an encryption solution to suit. They support data network links from modest 10Mbps and 100Mbps bandwidths to high speed 1Gbps, 10Gbps and even ultra-fast 100Gbps networks.

LAWENF-CS0917