SENETAS
Security without compromise

CLOUD CONNECT ENCRYPTOR

LEARN ABOUT THE CLOUD CONNECT ENCRYPTOR CUSTOMER BETA PROGRAMME
(see back page for details)

CLOUD CONNECT ENCRYPTOR

High-speed encryption within the cloud; providing maximum data protection for cloud computing and storage. The Cloud Connect Encryptor from Senetas is a high-performance solution that enables the secure movement of data to, from and within cloud infrastructure. It delivers FIPS certified end-to-end encryption of data among enterprise premises and cloud computing and storage services and features seamless integration of Senetas hardware and software encryption appliances; creating a single, trusted platform for maximum data security.

A dedicated, mixed network encryption solution, the Cloud Connect Encryptor is designed to protect enterprise network links and cloud computing and storage services without compromising performance. Network independent encryption provides maximum security for all network types and topologies, without the performance penalties associated with IPsec and VPN, and without the vulnerabilities associated with dual-purpose network appliances, such as MACsec.

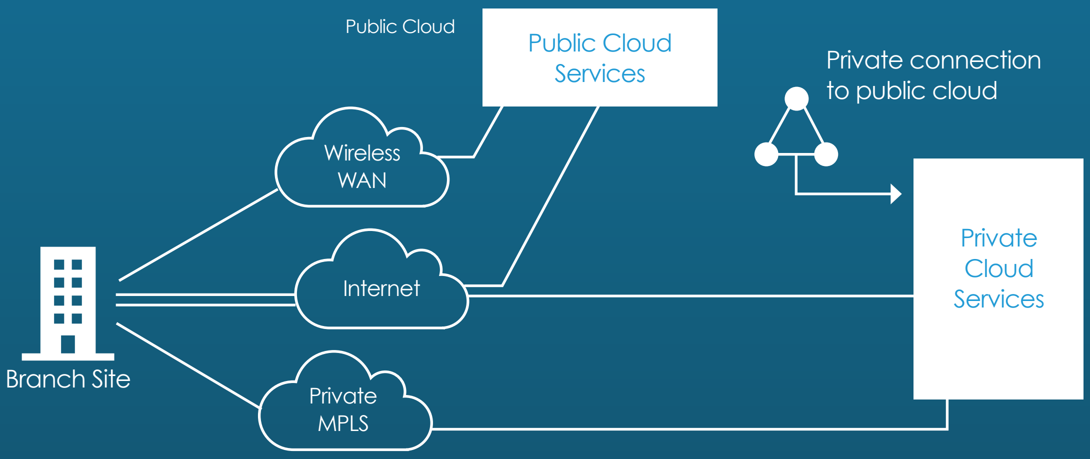
Customer Convenience

Customers already using Senetas CypherNET encryptors (Thales High Speed Encryptors distributed outside Australia and New Zealand) for on-premises applications, such as data centre interconnection, multi location data links and other network security needs, can easily add the Cloud Connect Encryptor. As simple as adding another encryptor, the Cloud Connect Encryptor will expand data protection to/within/from the cloud for secure cloud computing and storage.

Shared responsibility

The cloud shared responsibility model means that while cloud providers are responsible for infrastructure security, customers remain responsible for their own data security. Customers are responsible for the security of data both in the cloud and as it travels to/from the cloud.

With the Cloud Connect Encryptor, customers can leverage the industry leading high-speed encryption platform as a unified, cloud-native solution to protect data as it moves across critical infrastructure (to and from data centres, office locations and cloud computing and storage service providers) and bring Senetas's benefits of low-latency, tunnel free encryption to the cloud.

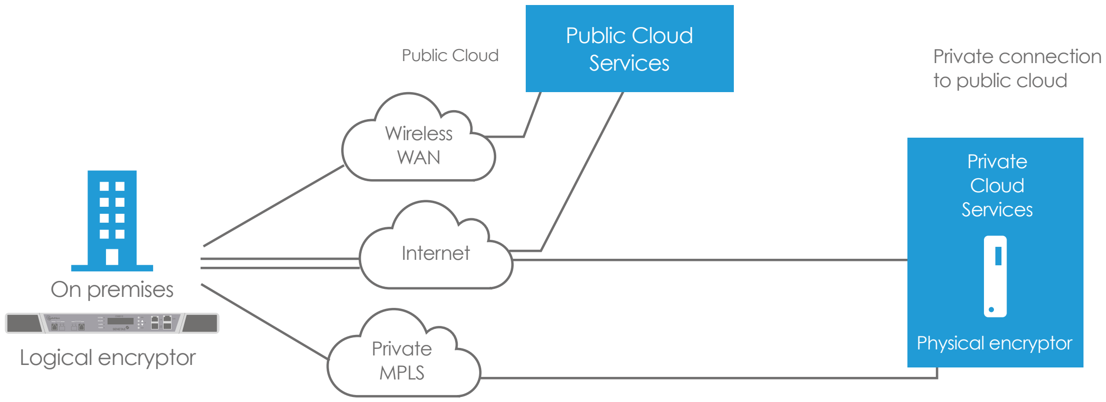


Most modern IT infrastructure comprises a complex mix of both public and private networks that are connected to both public and private cloud computing and storage environments. The challenge is to implement a solution that can meet the diverse security and compliance needs of these hybrid environments without compromising on performance or availability.

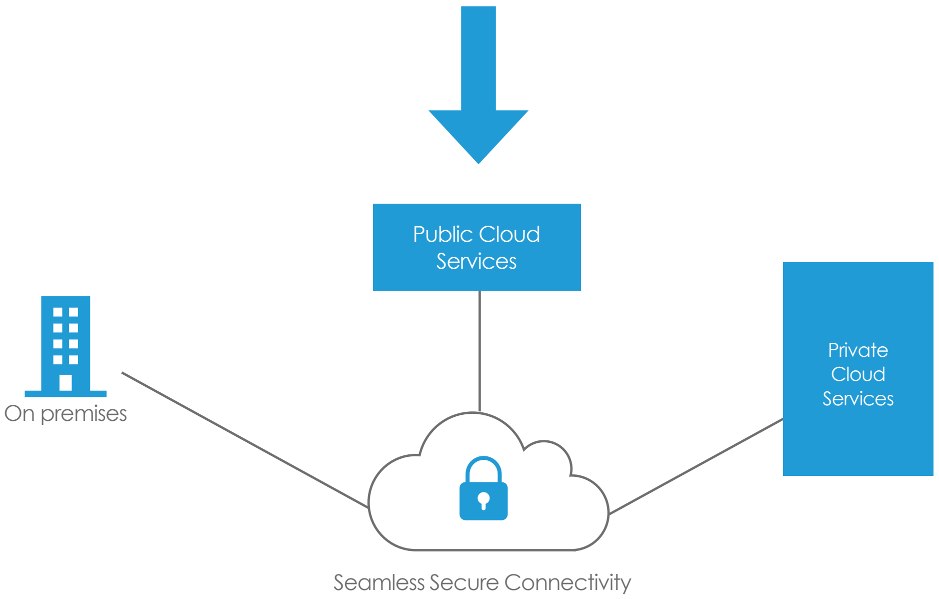
Cloud computing and Storage Services

Senetas Cloud Connect Encryptor supports Microsoft Azure and Amazon Web Services public cloud computing and storage.

Cloud Connect Encryptor's seamlessly integrated encryption platform is made up of dedicated physical and logical encryption. It enables multiple network layer security to/from, within and among multiple cloud computing and storage resources wherever they are located.



Unified infrastructure encryption



Senetas Cloud Connect Encryptor

With the introduction of the Cloud Connect Encryptor, customers have a single, unified solution that can secure all touchpoints:

- High-speed data centre interconnections
- Physical office to branch office connections
- Secure public cloud computing and storage access (single or multiple)

Key Features

The Cloud Connect Encryptor is a specific type of high-speed encryption (HSE) solution that is used to send encrypted traffic between a cloud solution provider and an office location over the public internet. It also enables encrypted traffic between Virtual Private Clouds (VPC) inside the cloud provider's network.

- Implemented as a cloud native Virtual Machine (VM)
- Supports Microsoft Azure and AWS (Amazon Web Services)
- Easy to deploy, scale and manage
- Ensures the authenticity, integrity and privacy of data transmitted:
    - to the cloud from on-premises
    - within a provider's cloud environment
    - between different cloud providers
- The Cloud Connect Encryptor authenticates and encrypts data in transit at one or more network layers. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted
- Encryption protects data if it is intercepted between site locations and the cloud provider or between cloud services
- Full interoperability with Senetas CypherNET CN Series physical and CV Series virtualised encryptors with HSE physical and virtual appliances

Technical Information

- FIPS certified
- Transport Independent Mode
    - Encrypts traffic at Layers 2, 3 and 4
    - Efficient tunnel-free encryption
- DPDK accelerated
- Software requires minimum 4 vCPUs and 2Gb RAM
- Supports AWS Gateway Load Balancer
    - Uses GENEVE encapsulation for high-performance connections to virtual encryptors in AWS
    - Allows greatly increased secure traffic volumes in/out of AWS
    - Allows horizontal elastic scaling and load balancing across a fleet of virtual encryptors
- Fully scriptable automatic deployment
- Layer 4 encryption

DPDK-AWS

- Three interfaces
- Cleartext ingress on Local Interface, Cyphertext ingress on Network Interface
- Layer 3 – Layer 4 encryption

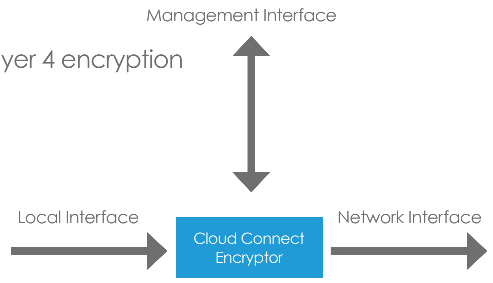


Figure 3 - Cloud Connect Encryptor for AWS

GWLB-AWS

- Two interfaces
- Cleartext/Cyphertext ingress/egress on Data Interface
- Supports GENEVE encapsulation
- Responds to AWS GWLB health checks

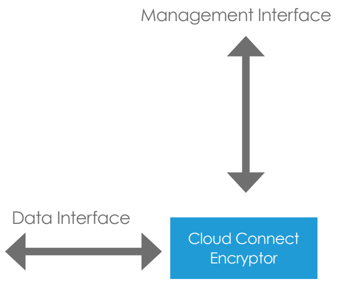
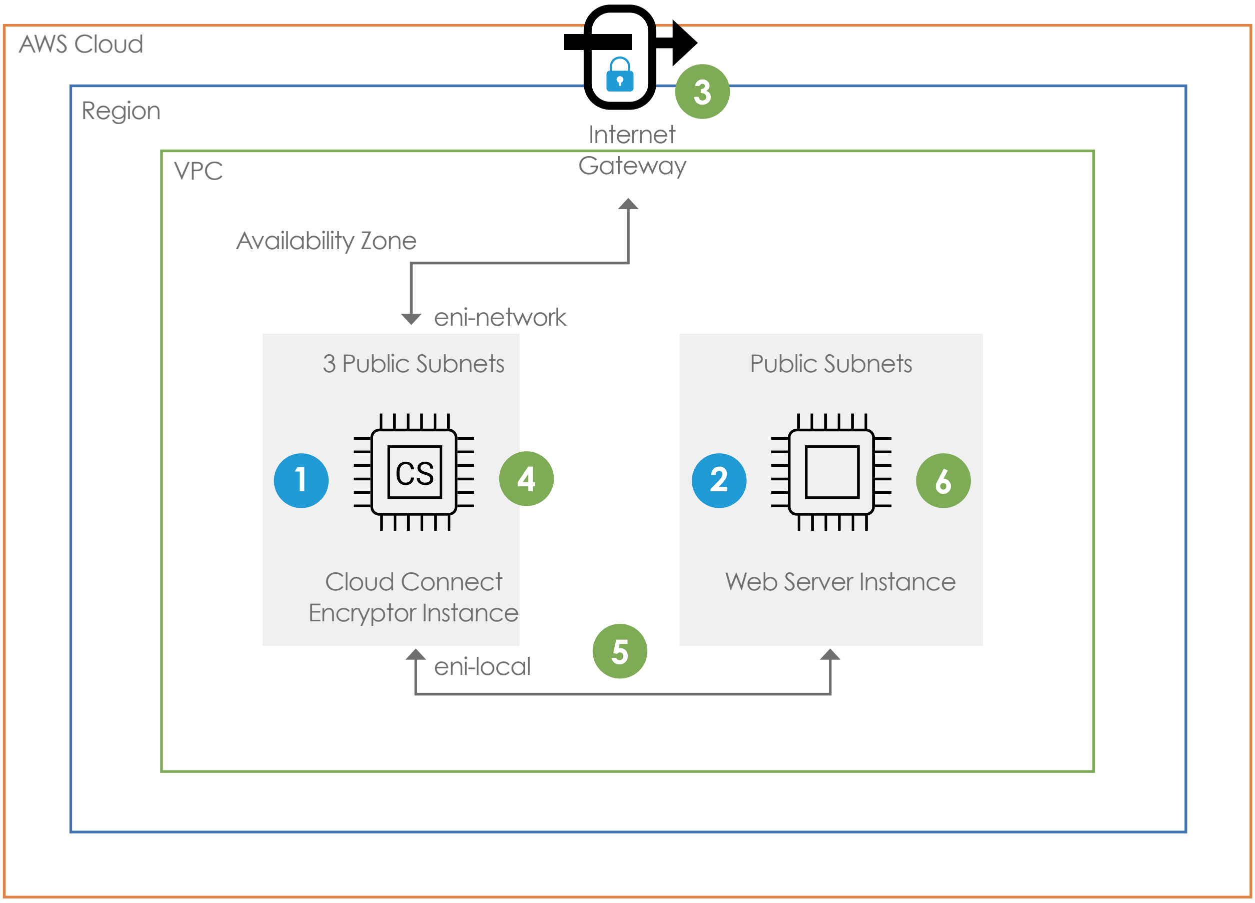


Figure 4 -Cloud Connect Encryptor for AWS Gateway Load Balancer



1	CCE Interface	IP Address
	Management	172.31.1.254/24
	Elastic IP address	18.133.145.83
	Local (eni-local)	172.31.2.254/24
	Network (eni-network)	172.31.3.254/24
2	Server Interface	IP Address
	Web Server	172.31.2.250/24
	Elastic IP address	18.133.48.91
3	Destination	IGW Target
	172.31.0.0/16	Local
	172.31.2.0/24	eni-network
4	Destination	Network Subnet Target
	172.31.0.0/16	Local
	0.0.0.0/0	igw-id
5	Destination	Management Subnet Target
	172.31.0.0/16	Local
	0.0.0.0/0	igw-id
6	Destination	Local Subnet Target
	172.31.0.0/16	Local
	0.0.0.0/0	eni-local

GLOBAL SUPPORT

Senetas encryption solutions are distributed and supported internationally (outside Australia and New Zealand) by Thales and within government & defence sectors by Thales Defense & Security Inc.

Thales is the world leader in digital security and defence, servicing over 30,000 customers across 180 countries. Senetas products are sold by Thales under its SafeNet brand.

THALES

ANZ PARTNER COMMUNITY

Senetas works directly with customers and their service providers across Australia and New Zealand. We provide technical consultancy and support to data networks providers, systems integrators and cloud service providers. For a current list, visit our **ANZ Partner Community Page**.

CLOUD CONNECT
ENCRYPTOR - CUSTOMER
BETA PROGRAMME

Customers and partners are welcome to participate in the Cloud Connect beta programme.

The programme includes Senetas technical support; your environment and technical requirements, deployment and beta performance assistance.

Click below to enquire about how to join the programme and arrange a technical discussion.

Click Here

© SENETAS CORPORATION LIMITED

www.senetas.com

Senetas is a leading developer of end-to-end encryption security solutions; trusted to protect enterprise, government, defence, Cloud and service provider network data in over 40 countries.

From certified high-assurance hardware and virtualised encryption, to secure file sharing and collaboration with data sovereignty control, all are based on the same crypto-agile platform and deliver security without compromise.

Regional Contacts:

Asia	**T:** +65 8307 3540	**E:** infoasia@senetas.com
Australia & New Zealand	**T:** +61(03) 9868 4555	**E:** info@senetas.com
Europe, Middle East & Africa	**T:** +44 (0)1256 345 599	**E:** infoemea@senetas.com
The Americas	**T:** +1 949 436 0509	**E:** infousa@senetas.com

GET IN TOUCH

Are you looking for a service provider to help you select and implement a network data encryption or secure file sharing and collaboration solution? Contact Senetas and we'll help you find the right one.

Senetas works with IT infrastructure service providers and systems integrators across the globe, to help specify the optimal cybersecurity solution for their customers' needs.

Customers may contact Senetas directly to discuss their requirements; or ask their service provider to speak to us on their behalf.

NETWORK DATA SECURITY WITHOUT COMPROMISE

Whatever your network security needs, Senetas has a network independent encryption solution to suit. Our multi-certified high-assurance encryptors protect data across networks operating at speeds from modest 100Mbps to ultra-fast 100Gbps and support all network topologies.

Our virtualised encryption solution, for virtual CPE and virtualised WAN, supports bandwidths of up to 15Gbps. It provides policy-based, end-to-end encryption across multi-Layer networks.

Senetas encryptors are recognised globally for delivering maximum data security and crypto-agility, without compromising network or application performance.

They are trusted to protect much of the world's most sensitive government, defence and commercial data.

SECURE COLLABORATION

SureDrop offers all the flexibility of a drop-box style solution, with the added benefit of best-in-class encryption security and 100% control over data sovereignty.

For customers seeking additional layers of content security, SureDrop is also available with the Votiro Secure File Gateway extension.

DISARM MALICIOUS CONTENT

Votiro Secure File Gateway leverages patented Content Disarm & Reconstruction (CDR) technology to protect your files from the most advanced, persistent cyber-attacks. It sanitises incoming files, eliminating the risks associated with zero-day or undisclosed attacks, whilst preserving 100% file functionality.

SENETAS