Ensemble
A Division of ADVA Optical Networking

ConnectGuard™ Cloud

Software encryption for multi-cloud applications

Multi-cloud environments provide enterprises the ability to mix and match private clouds with multiple public clouds. The “multi” in multi-cloud raises the importance of connectivity between and among those clouds, and of securing that connectivity. The “cloud” aspect makes achieving that security more complex. You can’t march into a data center owned by AWS, Azure or IBM and demand to install your encryption appliance to protect your links. A different approach is needed.

Securing data in motion

For encrypted data in motion using internet connections, the current best practices are insufficient. One option is to use IPSec encryption in the cloud infrastructure, but IPSec is inefficient with respect to compute resources. IPSec incurs the further penalty of using up more bandwidth due to IPSec tunnel mode and GRE encapsulation, especially for bridged traffic, as well as increased cloud compute usage for IPSec itself.

Relying solely on application-level security is another option, but it puts the onus on developers to adhere to security standards. Furthermore, these developers may not be security experts, the security is not easily testable, and it may not be controlled by your IT team.

Now, there’s a new approach: ConnectGuard™ Cloud from the Ensemble division of ADVA.

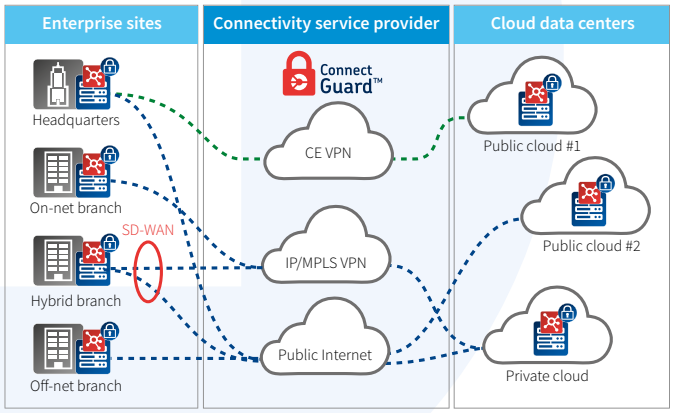
Introducing ConnectGuard™ Cloud

ConnectGuard™ Cloud is the industry’s first transport-layer-independent cloud security solution implemented completely in software. Based on Senetas’ FIPS-certified CN series of encryptors, ConnectGuard™ Cloud delivers robust, low-cost, software-based network protection on a simple subscription or perpetual license basis. Enterprise, government and service provider customers can now leverage fully secured cloud access with none of the performance issues of IPSec and with the ability to address Layer 2, 3, and 4 connectivity.

ConnectGuard™ Cloud

- Cloud-native software encryption can be hosted on uCPE or in the cloud
- End-to-end encryption in multi-cloud environments – prevents man-in-the-middle attack vectors
- Encryption at Layer 2, 3 or 4 as needed – match the encryption to the application
- Based on FIPS-compliant technology from Senetas
- Compute efficiency minimizes cost of hosting server – no need for hardware appliances
- Bandwidth efficiency means greatly improved throughput, overhead and latency versus IPSec
- Encrypted connections can be shared by multiple applications – no need to rely on SD-WAN or firewall encryption
- Automated key management for operational simplicity – no need for an externally managed IKE or PKI system

ConnectGuard™ Cloud removes the need to rely on VNF application encryption solutions or security VNFs, simplifying service chaining, avoiding vendor lock-in, and giving operators complete control.



Built on field-proven Ensemble Connector

ConnectGuard™ Cloud is implemented in Ensemble Connector as the Connector Encryption feature. Ensemble Connector is a universal CPE (uCPE) network OS that can be placed on a commercial off-the-shelf (COTS) platform or bare metal server in a cloud environment. Connector allows for complete flexibility connecting the encrypted stream to hybrid cloud providers, SOCs, or security hubs such as IBM's secure network.

ConnectGuard™ Cloud comes with two key management options. First, the encryption can operate with any KMIP-based external key server or special protocol such as the Gemalto's SafeNet™ KeySecure™ NAE-XML interface.

The second option is a truly revolutionary technology known as Transport Independent Mode (TIM). TIM provides for transport-agnostic encryption independent of the network topology, providing flexible encryption policy and concurrent encryption at OSI Layers 2, 3 and 4. TIM requires no control plane connectivity between encryptors, and operates in point-to-point, point-to-multipoint and multipoint-to-multipoint topologies. In addition, TIM provides flexibility to concurrently encrypt the data plane at a mix of L2, L3 and L4 payloads in accordance with configured policy. TIM provides a scalable key management model that allows thousands of ConnectGuard™ Cloud nodes to securely and reliably exchange encrypted traffic, making the solution ideal for cloud deployments. ConnectGuard™ Cloud provides high-performance, low-latency encryption that replaces the slower encryption typically found in VNFs and firewalls. Based on a NIST-recommended key derivation function, this encryption delivers military-grade protection.

ConnectGuard™ Cloud harnesses the power of NFV to extend networking, simplify operations and maximize choice. It extends encryption into the cloud and small branches by leveraging low-cost uCPE platforms. It provides a cloud-native virtualized solution for encrypting WAN connections from 10Mbit/s on low-end platforms up to 10Gbit/s.

Applications in your network

- AES-256 CTR or GCM encryption
- L2 encryption + L2 VPN
- L3/L4 encryption + L3 VPN
- 10Mbit/s to 10Gbit/s throughput, depending on platform
- Automated root certificate and key generation from Ensemble Director
- Zero touch provisioning

> "... the industry's first transport-layer-independent cloud security solution implemented completely in software ..."

Applications in your network

- Replacement for hardware encryption appliances in point-to-point applications
- Securing data center access for hybrid cloud and multi-cloud applications
- Transport-independent encryption for uCPE applications, including SD-WAN

For more information please visit us at www.dvaoptical.com

Product specifications are subject to change without notice or obligation.

ADVA™ Optical Networking