The EVPN Data Center
Line-rate encryption with Arista's TunnelSec

Introduction

The criticality of data confidentiality along with stricter compliance mandates has seen organizations including Governments, Service Providers and Enterprises take a more holistic approach to data security. In-transit encryption has become a major component within this drive to deliver end-to-end data integrity. The demand for in-transit encryption is further reinforced by the decentralization of services. Today, business critical data no longer remains within an organization's walls or crosses inherently secure private circuits, instead large volumes of information travel between private, shared and cloud facilities, flowing through third-party circuits and public networks, crossing national and continental boundaries.This ever expanding need for in-transit encryption, presents a major challenge in modern high performance networks where bandwidth trends continue on an upward trajectory. Moving high volume, media rich content across regions, countries and continents, within today's network infrastructure requires 100G and 400G speeds. With demand for 800G projected in the near future, alongside continuing security concerns for the data being moved, means in-transit encryption needs to keep pace with the bandwidth demands.

The traditional approach to providing data encryption across third party infrastructure has been through the deployment of dedicated IPsec platforms. While providing the required level of encryption to ensure data integrity, they are prohibitively expensive and lag behind the 100G and 400G bandwidth levels now required, consequently placing a major constraint on an organization's goal of delivering an end-to-end security strategy.

MACsec (802.1AE) has looked to address the throughput limitations of dedicated IPsec platforms, by providing encryption at the MAC layer, thereby providing 100G and 400G throughput speeds on cost-effective routing and switching platforms. This has seen MACsec successfully deployed within the campus and high performance data centers. However, MACsec is inherently a point-to-point, link-local technology and therefore not a direct replacement for all IPsec deployments. In a strict implementation, there is a need for each node in the path to be MACsec aware and under the control of the same organization, which is costly and places restrictions on the overall topology and the level

of resiliency a solution can provide. This means for MACsec to be deployed in the WAN, it's required to be transparently tunneled across an Layer 2 provider circuit; which involves additional complexity and puts the onus for resilience on the underlying circuit service, driving up costs. On the other hand, IPsec natively solves these limitations, by being agnostic to the underlying network, allowing it to be reroutable like any standard IP packet. However, for IPsec to continue to be the encryption model of choice for the WAN, it now needs to be delivered at the throughput and cost point equivalent to current MACsec platforms.

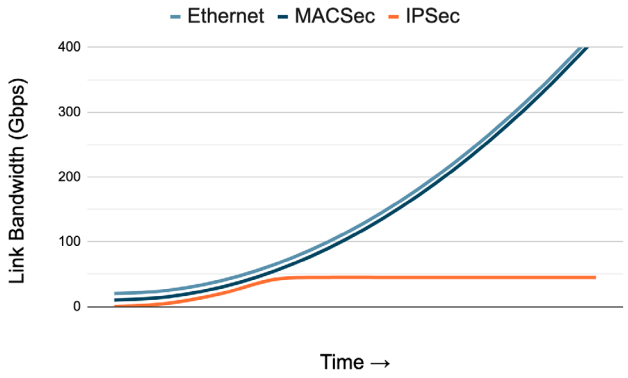

Figure 1: Link speed outpacing IPsec encryption

Alongside the need to provide cost effective 100G and 400G performance parity between MACsec and IPSec, the rollout of EVPN-VXLAN within and across data centers, has seen the evolution of new encryption requirements. While IPsec solves the challenges of end-to-end security, agnostic to the underlying IP topology, it does not natively meet one crucial data center requirement – the need to encrypt a mixture of Layer 2 and Layer 3 services over a shared IP infrastructure, this presents a new and evolving requirement for Data Center Interconnect (DCI) and co-location (colo) deployments.

TunnelSec

Arista's TunnelSec technology addresses each of these encryption use-cases by providing line-rate hardware based 10G to 400G encryption, embedded within the R3 series routing platforms with support for IPsec, MACsec and an innovative new VXLANsec™ solution. Providing TunnelSec encryption as an embedded component within the R3 series, delivers wire-speed encryption performance for all three protocols, removing the need for costly dedicated external encryption hardware and providing the flexibility to choose the appropriate encryption solution within a single platform, which can scale up to 21.6Tbps in a 7280R3A fixed system and up to 576 ports of 400G in the 7800R3 modular system.

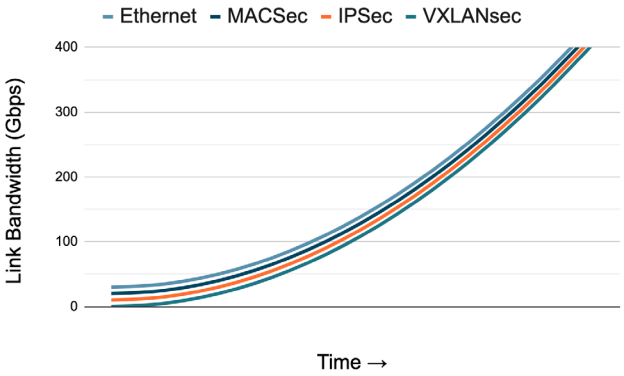

Figure 2: TunnelSec providing link speed alignment with encryption

TunnelSec provides the flexibility to select the type of encryption deployed for each network requirement. VXLANsec is ideal for EVPN DCI solutions, stretching layer 2 and 3 services between data centers, high speed IPsec enables the secure interconnection of branches and central offices while MACsec offers point-to-point encryption within the campus or the data center. The flexibility of Arista's TunnelSec solution ensures each of these can be addressed within a single R3 platform regardless of throughput or topology.

MACsec

Arista's TunnelSec platforms provide support for native 10G to 400G line-rate MACsec (802.1AE). MACsec is performed at the interface (MAC layer) level on the platform, where security keys are exchanged with the neighboring node of the link, resulting in all data beyond the initial Ethernet header being fully encrypted between the two nodes. This makes MACsec a suitable solution for high-speed point-to-point connections, or for end-to-end encryption when all nodes in the path are MACsec aware.

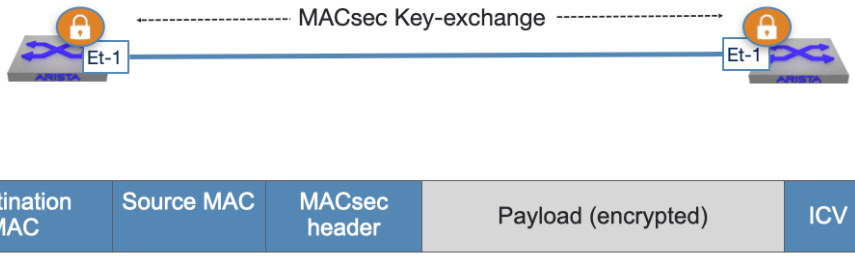

Figure 3: MACsec frame format and key exchange

By operating at the interface level, with the need for each node in the path to be MACsec aware, MACsec is an appropriate fit for providing data encryption on point-to-point links within the Campus risers or between the leaf spine links of a data Center fabric. It can also be deployed as a high-speed point-to-point DCI, when dedicated fiber or transparent circuits are deployed between sites.

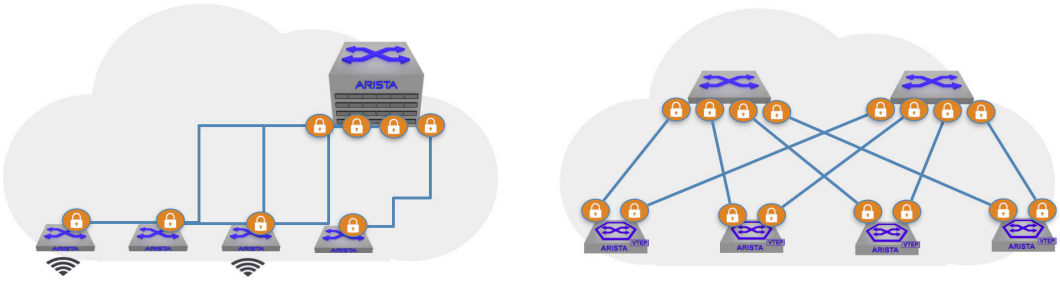

Figure 4: MACsec for Point-to-Point encryption in the Campus and the Data Center

IPsec

Arista's TunnelSec platforms provide support for standards based IPsec (RFC 4303) with 10G to 400G line-rate authentication and encryption using the AES-256-GCM block cipher. IPsec is an IP-in-IP tunneling technology, where the original IP payload is encrypted and encapsulated within a new IP packet (IPsec Tunnel node). This allows the encryption end-points of an IPsec solution to be interconnected via a routed infrastructure, rather than directly connected as is the case with MACsec.

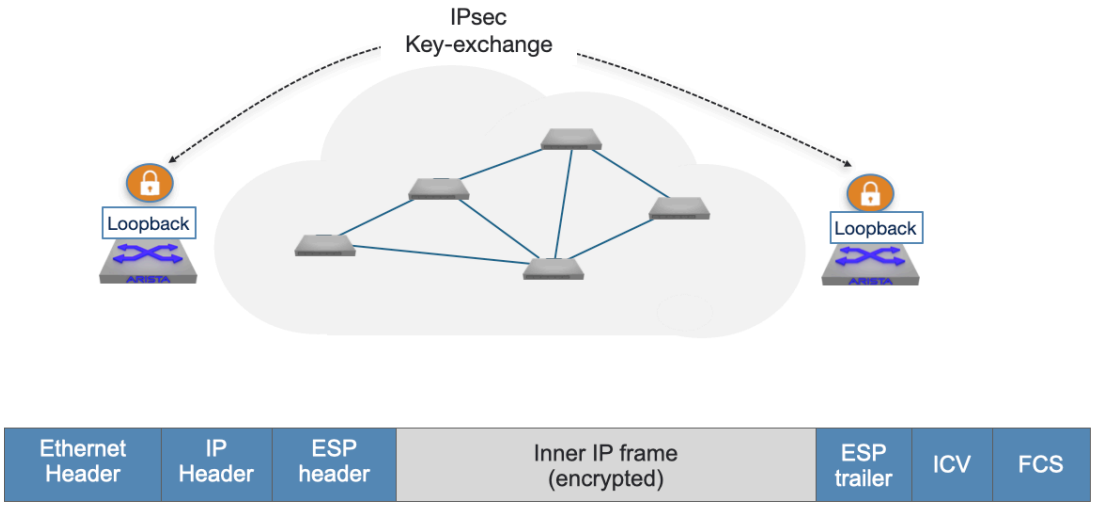

Figure 5: IPsec frame format and IPsec key-exchange

As an IP-in-IP tunneling technology, IPsec packets can also be transparently routed across an intermediate third-party infrastructure, with the ability to route around any failure at no additional cost to the solution. This is a cost effective approach when dedicated dark fiber between sites is cost-prohibitive for a MACsec solution. IPSec also offers the additional benefit over MACsec by natively supporting both point-to-point and point-to-multipoint encryption topologies. This allows the interconnection of multiple sites in both a full-mesh and a hub-and-spoke topology.

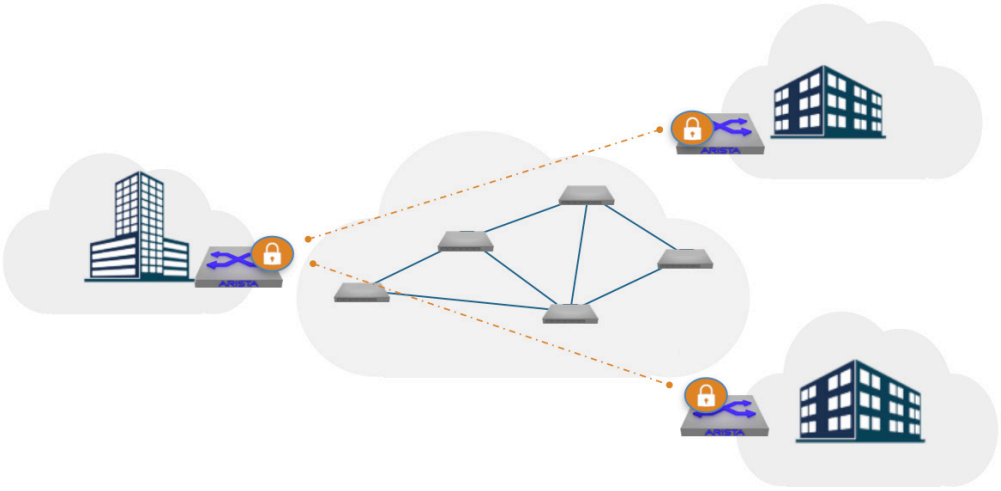

Figure 6: IPsec for Point-to-Point and Point-to-Multipoint encryption across an IP backbone

VXLANsec

Addressing the demands for high performance 100G and 400G encryption of VXLAN traffic when interconnecting EVPN-VXLAN domains within a colo or across sites as part of a Data Center Interconnect (DCI) solution, TunnelSec platforms also provide embedded support for Arista's innovative VXLANsec encryption technology.

VXLANsec provides the ability to encapsulate and encrypt VXLAN traffic for transparently forwarding layer 2 and 3 VPN traffic across an IP infrastructure. In a VXLANsec deployment Arista's TunnelSec platforms are standard EVPN-VXLAN VTEPs with the additional capability to encrypt the VXLAN header and inner payload, allowing both Layer 2 and 3 traffic to be encrypted and transported between associated VTEPs. As illustrated below, VXLANsec utilizes a standard IPsec UDP-ESP frame format to encapsulate and encrypt the original VXLAN header and payload.

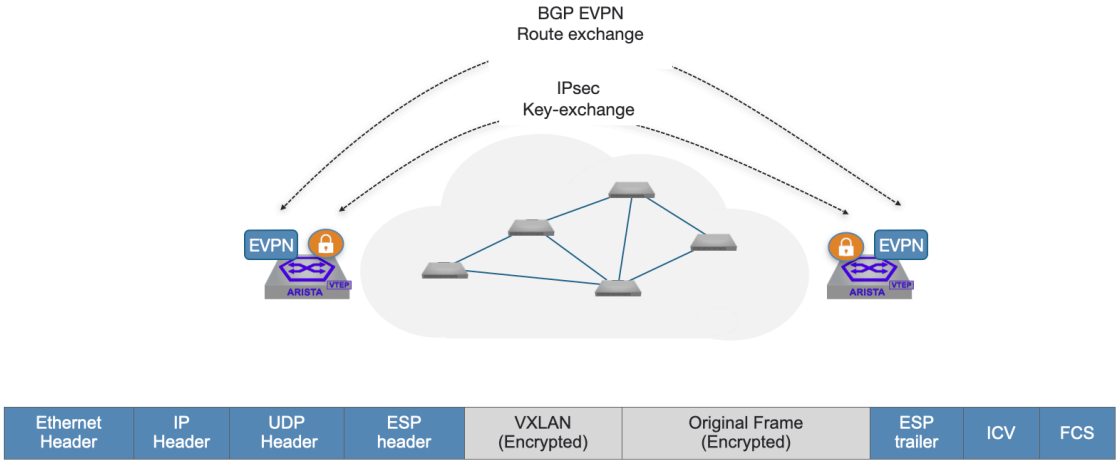

Figure 7: VXLANsec frame format, key-exchange and BGP-EVPN peering

VXLANsec is also fully integrated with the EVPN control-plane and an EVPN GW for hierarchical multi-domain topologies. The solution can be used within a colo site for securely interconnecting EVPN domains across third-party circuits, ensuring all VXLAN encapsulated traffic (layer 2 or 3) traversing the circuit is fully encrypted.. With support for encryption within both point-to-point and point-to-multipoint topologies VXLANsec can also be deployed as a high-speed DCI solution for interconnecting multiple DC locations across a shared IP infrastructure, where any VXLAN traffic traversing between sites would be fully encrypted.

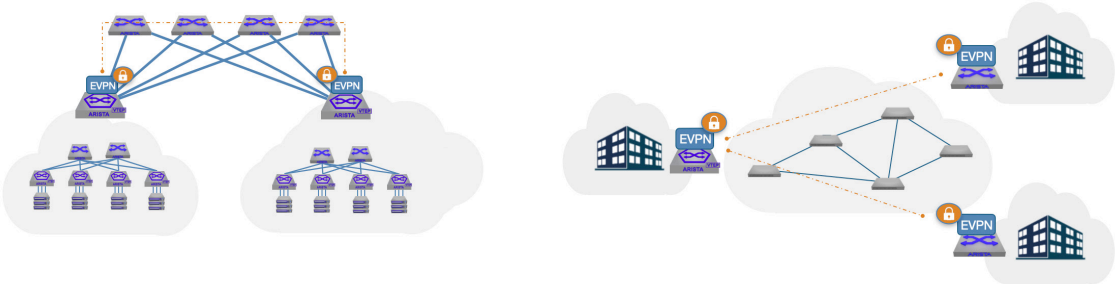

Figure 8: VXLANsec, for encrypted EVPN multi-domain and Data Center Interconnect (DCI)

VXLANsec is also suitable for leaf-spine topologies where there is a requirement to encrypt all communication between VTEPs. This approach ensures encryption occurs between the leaf nodes of the topology and is transparently IP forwarded by the spine, removing the need for any additional functionality at the spine layer.

Summary

Arista's TunnelSec technology, embedded in the R3 Series, provides high speed in-line strong encryption at line-rate from 10G to 400G. With a choice of standards based IPsec, MACsec or Arista's innovative VXLANsec solution, TunnelSec provides all the tools necessary for Service Providers, Enterprises and other security conscious organizations to provide ubiquitous encryption. Delivered as embedded functionality, TunnelSec eliminates the performance bottleneck, cost and complexity of legacy encryption deployments, while augmenting the rich routing feature set of the R3 series. Arista TunnelSec provides the ability to collapse routing and encryption functionality into a single platform for dramatically improved total cost of ownership (TCO).

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062