ENET VPN Gateway

Virtual Private Network Gateway for Enterprise and Telco Cloud

The ENET VPN Gateway, an FPGA-based security appliance, features Ethernity's rich networking technology packaged with open source security software to deliver a complete, ready-to-deploy solution. The ENET VPN Gateway enables site-to-site secured connectivity or aggregation of multiple virtual private networks (VPNs) in a single low-power appliance equipped with a fully programmable SmartNIC.

The ENET VPN Gateway integrates open source Libreswan security management software with Ethernity's ACE-NIC FPGA SmartNIC solution, avoiding vendor lock-in and offering programmability in both control and data plane functions, which ensures future readiness for new security protocols and crypto algorithms.

Ethernity offers accelerated IPSec performance with inline cryptographic functions leveraging ENET's carrier-grade pipeline. The ENET VPN Gateway can support the full Libreswan feature set, accelerating the primary crypto functionality.

Beyond that, Ethernity's new Host Bypass feature isolates traffic exclusively to the FPGA, protecting the user from breaches, which are more common when crypto and packet editing are performed in the CPU.

The solution is available as either a ready-to-use network appliance or as a kit that includes Ethernity software and the ACE-NIC FPGA smart network adapter (SmartNIC).

Product Highlights

- Ideal VPN security solution for next-gen networks at the edge, in the cloud, or for enterprise data centers
- Offers complete programmability of control plane (handled in CPU) and data plane (handled in FPGA)
- Ideal for virtual environments with built-in slicing support
- Combines security and packet processing data plane in a single programmable low-power FPGA
- Easy to customize with new crypto protocols, overlay methods, or capturing capabilities
- Improves security by reducing opportunities to breach the CPU
- Uses open source Libreswan control stack

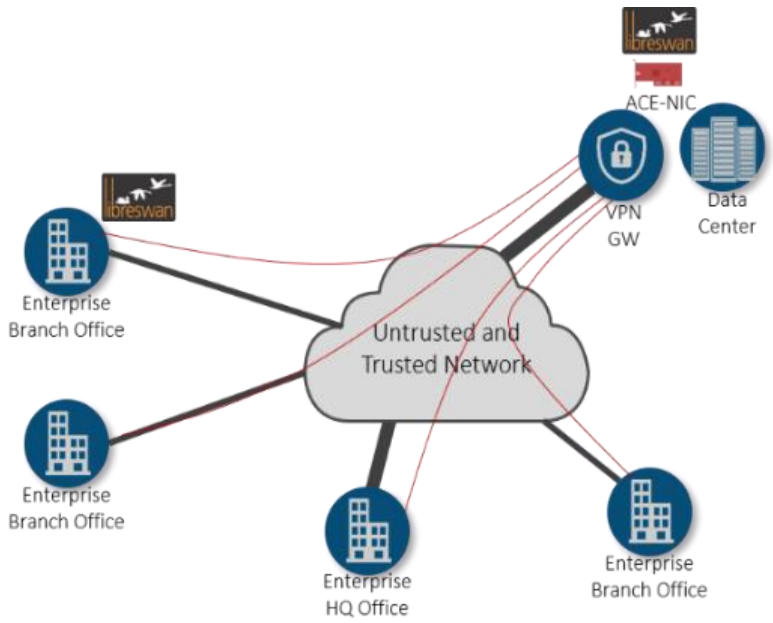

Figure 1: ENET VPN Gateway deployment scenario

Target Applications

Control and Data Path

Security control in the ENET VPN Gateway is handled by the open source Libreswan package, which runs the container environment and is integrated with the Ethernity acceleration plugin. As a result, the product combines both IPSec control of IKE, native Linux IP stack, and ENET Flow Processor data plane running on FPGA.

High Performance Security Offloads

The Ethernity ENET VPN Gateway offers IPSec offload and inline processing with no CPU intervention, with additional support for advanced features such as packet classification and flow aggregation with encapsulation. The product maintains support for traditional offloads, such as inner and outer transport with end-to-end packet encryption. Checksum offload is also available upon request.

Overlay Networks Offload

A cornerstone of 5GPPP requirements in a multi-tenant cloud and enterprise infrastructure is isolation within the shared network. Overlay networks carry traffic from each VNF encapsulated in formats such as VxLAN, NVGRE, and GTP as well as many others, such as L2/L3 VPNs. Ethernity's ENET VPN Gateway is not only capable of supporting these overlays and tunnels, but also provides high determinism upon data forwarding, filtering, and replication.

Ethernity's solution is differentiated from the competition by its ability to handle multiple offloads along with different overlay techniques within both fixed and mobile networks.

Switching and Routing

The ENET VPN Gateway solution enables extended functionality that provides high performance L3 packet forwarding, routing, and NAT with integrated access control and flow control support. The gateway can further provide replication functions that can be associated with different services, security associations, tunnels, and users.

Slicing and VNO Model Support

Upon request, the ENET VPN Gateway solution enables crypto resources to be separated between different services or VNOs, enabling the same engines to be reused with no risk of attack because of clear virtual isolation between the various virtual tables.

Quality of Service (QoS)

Ethernity's ENET VPN Gateway enables extended functionality that offers high precision network scheduling and prioritization of traffic based on H-QoS, packet coloring, congestion notification, and priority- and weight-based scheduling. The solution supports hierarchical traffic management with hundreds of virtual interfaces that can be associated with different services, IPSec security associations, tunnels, and users, each running different queues with either SP or WFQ methods to manage and shape traffic, as well as per queue policer (2r3c) and WRED.

Features and Specifications

SmartNIC Interface Options (depends on product model)

- PCIe Gen3 x16 (x8 + x8 bifurcation)
- PCIe Gen3 x8
- PCIe Gen2 x8

Crypto Algorithms (Libreswan)

- AES 128/256
- SHA1/SHA2
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512

Ethernet

- IEEE 802.2ba (40/100GbE)
- IEEE 802.3ae (10GbE)
- IEEE 802.3z (1GbE)
- IEEE 802.1p Priority
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1BR Bridge Port Extension
- IEEE 802.3x Flow Control
- IEEE 802.3ad Load Balancing
- Ethernet II and 802.3 encapsulated frames
- Multiple MAC addresses per interface
- Jumbo frames up to 9.6KB

The following additional options are available upon request:

Forwarding Offload

- L3 forwarding
- VRF support

Stateless Offloads

- TCP/UDP IPv4/6 checksum offload
- TSO, LSO, and GSO for IPv4 and IPv6
- Up to 1M filters with line rate packet editing and attack protection
- Packet tracing, sniffing, mirroring
- VxLAN, NVGRE, L2TP

H-QoS

- 256 virtual interfaces with 8 queues each
- Shaper per egress traffic
- Policer 2r3c per port / per queue

Ordering Options

Product Name	Product Number	Product Description
ENET VPN Gateway	ENS-1044-S20	4 x 10G interface with 17MPPS data path and router
	ENS-2080-S40	2 x 40G (1 + 1) interface with 25-42MPPS data path
	ENS-2050-S50	2 x 25G @ 30MPPS data path