SEC eDGE™
Digital Security to the Edge

SECeDGE SEC-VPN™

OVERVIEW

May 15, 2024 | Draft Version 1.0

1. TABLE OF CONTENTS

2. INTRODUCTION

The internet has evolved over the last few decades from being a means to deliver unlimited amount of information to human users, to a place for business/ecommerce activities and to a place to interact with peer human users belonging to social network organizations of all kinds and sizes (professional groups, large and small consumer groups, etc.) via fixed and mobile networks.

Connecting machines to this internet (IoT/Internet of Things) became another major area of growth with a total number of 'IoT' devices now exceeding the number of human users. However, this category of 'machine users' presents many new security and operational challenges to the traditional internet infrastructure. For example:

- 'machines' (IoT) do not login and access services as human users do… they operate on their own (e.g., smart meters, alarm systems, autonomous robots/machines), and thus present new security and trust problems.
- Human users access the internet to share and exchange large volumes of data (e.g., media data, enterprise data); IoT devices typically transmit or receive exceedingly small amounts of data.
- Machines never sleep and often perform critical operations and a disruption of service can cause considerable damage to society; a media service disruption has no critical consequences for the human user.

These examples show how reusing the old security and network technologies and approaches for machines/IoT have many limitations and weaknesses.

One of the major challenges is the enormous fragmentation of chip platforms: the Intel world is different from the Arm® world, and within the huge Armworld every semiconductor manufacturer has different security technologies in processors. As a result, the software solution built on top of the chip platform must be customized for each product, creating management hurdles, and potential security gaps.

The SecEdge approach is ground-up, resolving the chip fragmentation issue and delivering a state-of-the-art solution for IoT and Edge devices. SEC-VPN™ delivers a unique chip-to-cloud security solution, covering a large variety of chip platforms, addressing Edge and IoT security requirements, and supporting industry standards, regulations, and forums.

3. SEC-VPN™ OVERVIEW

3.1. SOLUTION OBJECTIVES

The SEC-VPN solution is an end-to-end approach, with three objectives:

+ **Device security and Trust:** Hardware, software and IT experts agree that the strongest security foundation at the edge resides at the silicon level with a unique and unalterable ID, also called a Root of Trust. The challenge is the implementation, management, and cost of the solution, given the diversity of devices and scale of IoT.

  SecEdge brings a revolutionary solution, enabling a hardware root-of-trust and a wide array of security features and functions in an Arm® TrustZone™ based silicon architecture. This solution simplifies the implementation of device security while lowering BOM cost and accelerating development. In addition, the same security technology can be enhanced for AI/ML model protection at the edge.

+ **Chip-to-cloud security:** data security and privacy are top requirements from customers and regulators in every market. As Edge and IoT deployments grow, the only method to guarantee the strongest encryption security is by anchoring it at the chip level (as explained above) with secure credential provisioning. SecEdge further enhances data security by delivering device data to backend server via IPSec tunnels, overcoming the limitations of conventional mTLS (designed originally for media and ecommerce applications). IPSec offers multiple security benefits (see Figure 1), is recommended by the National Institute of standards and Technology (NIST) for IoT and has been widely used by enterprise IT for VPNs. SecEdge provides a solution with cloud-based automation tools, KMS (Key management system) and a design suitable for both public cloud and on-premises environment.

Key Requirement	IPSEC VPN	Description	mTLS	Description
Separate control and data planes	✓	Separate tunnels for each	✗	One channel for all
Separate access for applications and users	✓	Separate tunnels for each	✗	One channel for all
Private Network Connection	✓	IP Address Hidden	✗	IP Address exposed
Scalable to unlimited devices, tenants and applications	✓	Automatic enforcement of rules, credentials, encryption and policy	✗	Rules, credentials, encryption and policy set up manually
Persistence (connection up as long as you need it)	✓	Connection-based (sessions are persistent)	✗	Session-based (connections are temporary)

Figure 1 IPSec communication vs conventional mTLS

- **Ease of deployment and scale:** SecEdge minimizes the friction encountered by the customers at various levels and makes customers' IoT projects easy to deploy and manage:
- **Device Level:** MicroEdge™ software works with Linux OS, a widely adopted OS in the IoT/Edge and Computing space and can be integrated by any developer. It is designed to work with several Root of Trust options for devices equipped with an ARM processor (discrete TPM, Secure Element, etc.), or with SecEdge Device security solutions (EmSPARK™ or SEC-TPM™). MicroEdge does not add any constraint or limitation to the device application. With MicroEdge, device data is always encrypted by default and a chain of Trust is established automatically.
- **Cloud or Data Center:** CloudEdge™, the data termination point, installed in a standard VM in a server backend or cloud. One single CloudEdge instance can support 30K devices, thus enabling medium to large size deployments easily by adding more CloudEdge instances if the total number of devices require it.
- **Management Services:** ControlEdge™ allows administrators to control their devices through their own dashboard and apply/enforce the security policies over all their devices. ControlEdge™ can be delivered: a) via APIs, for integration with management software, or b) as software running on-premises in a Kubernetes environment.
    - **Resiliency Built-in:** the architecture is designed for scale with management tools providing capabilities to enforce security policies, with automated methods to change and update credentials. ControlEdge (the central software performing the heavy lifting security services) can have multiple CloudEdges in a group and shift the devices if one of them fails.

3.2. USE CASES

MicroEdge can work with a broad range of processors. The minimal requirement is Linux OS as shown below:

PROCESSOR	TPM	OS	COMMENTS
ARM	Discrete Chip	Linux	Chip to cloud security supported

PROCESSOR	TPM	OS	COMMENTS
ARM with TEE	EmSPARK/ SEC-TPM	Linux	Chip to cloud security supported
Intel/AMD	Discrete chip	Linux	Chip to cloud security supported
ARM/Intel/AMD	No TPM chip	Linux	Device to cloud security only (no hardware RoT)*
Any processor	With/without TPM	Windows, or RTOS	NOT supported

(*) this scenario may be suitable for non-critical application without Root of Trust

Note: MicroEdge supports multiple IPSec tunnels from the edge device (multi-tenant IPSec tunnels), even with hardware equipped with small processors and limited resources.

3.3. SEC-VPN™ PLATFORM ARCHITECTURE

Figure 2 below illustrates the architecture of the SEC-VPN platform with its three major software components: MicroEdge, CloudEdge and ControlEdge.

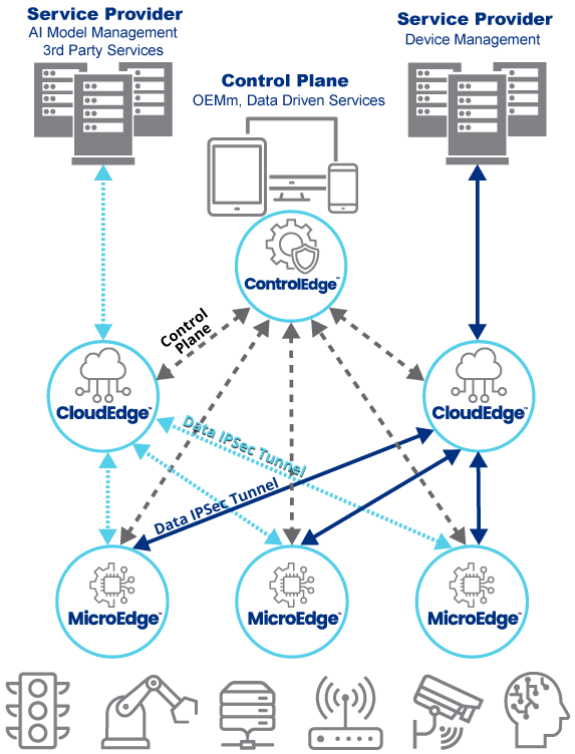

Figure 2 SecEdge Service Platform Architecture

+ MicroEdge™ is a middleware component which provides zero-touch security provisioning, secure end-to-end data in motion and at rest for Internet of Things. The solution can be deployed to a variety of devices. It is installed on devices equipped with Linux OS. A single MicroEdge instance on a device enables multi-tunnel connectivity to different CloudEdge servers enabling more secure services and/or new monetization options for the owners of the IoT/Edge devices.

+ CloudEdge™ is the cloud termination endpoint for MicroEdge device tunnels. Endpoint devices can be anchored to one or more peer endpoints on an external network residing on the same administrative span of control as the MicroEdge endpoint. Customers deploy one or several instances of CloudEdge in their backend to connect securely all IoT/Edge devices to their backend application server.

+ ControlEdge™ administers all edges (IoT devices equipped with MicroEdge and CloudEdge) within the SecEdge ecosystem. ControlEdge performs all the heavy lifting functions to set, configure and manage the security of the entire deployment. All this connectivity and provisioning is managed by ControlEdge services which allow for the deployment of IPSec tunnels facilitating secure communications between instances.

Note: SecEdge delivers and supports the cloud/data center software (ControlEdge, CloudEdge). The Cloud hosting services is performed by the customer in the cloud environment of their choice: public cloud (Azure, AWS, GCP) or on-premises.

4. SECeDGE STUDIO™

SecEdge Studio™ available on Google Marketplace, accelerates the integration and deployment of SEC-VPN, a multi-tenant, chip-to-cloud, scalable IPSECec Solution, providing secure connectivity to edge devices, applications, and users.

SecEdge Studio enables development and test end-to-end the SEC-VPN solution in Google Cloud Platform (GCP) cloud environment without hardware. Shown in Figure 3 below, SecEdge Studio uses ControlEdge in GCP supported, by SEC-VPN and deploys virtual machines (VMs) in the GCP customer's account.

ControlEdge in GCP

- Orchestrates security services between MicroEdge (in VM1) and CloudEdge (in VM2).
- Users have full control to test end-to-end the various security features via SecEdge Studio dashboard.

VMs in Customer's GCP Account

- Device VM: Emulates edge device and its applications connectivity via an IPSec tunnel with MicroEdge.
- One or more IPSec tunnel(s) can be implemented from the emulated device (Device VM) and tested easily (with one CloudEdge per tunnel).
- CloudEdge VM: receives encrypted data from the emulated device and delivers it to customer's backend application.

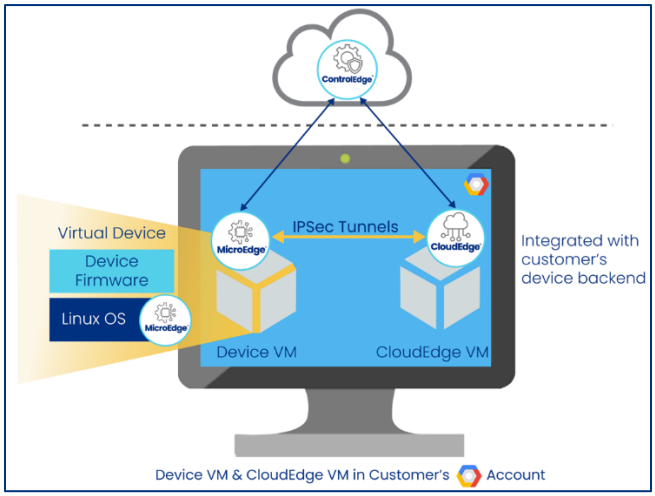

Figure 3 SecEdge Studio

5. SEC-VPN™ DOCUMENTATION

Detailed documentation on SEC-VPN is available upon request under NDA.

+ MicroEdge installation guide
+ CloudEdge installation guide:
+ ControlEdge APIs

SecEdge Studio documents can be downloaded from SecEdge website:

+ Get Started: https://www.secedge.com/?sdm_process_download=1&download_id=8934
+ Tutorial: https://www.secedge.com/?sdm_process_download=1&download_id=8937
+ User Guide: https://www.secedge.com/?sdm_process_download=1&download_id=8935