HUGHES®
An EchoStar Company

SOLUTIONSHEET

OneWeb and Hughes Managed LEO Broadband Security

Hughes Managed LEO Service

Hughes offers low-latency broadband service for latency-sensitive applications and service in unconnected areas and hard-to-reach places. As a partner and distributor for OneWeb, the premier Low Earth Orbit (LEO) satellite communications company, Hughes can deploy LEO capacity as either a managed broadband service, multi-orbit mobility or enterprise solution, multi-transport Software-Defined Wide Area Network (SD-WAN), or a highly specialized military network.

Secure End-to-End Service

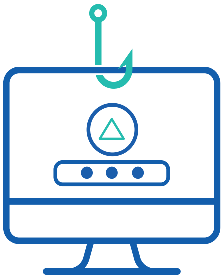
Hughes and OneWeb provide a secure transport layer and end-to-end encryption throughout the network. Each network segment performs its own unique encryption to secure its traffic leg. Broadband network security is critical due to interaction with the open Internet, untrusted endpoints, and many threats that occur.

Switched Networks Vulnerabilities

These networks, commonly called **Layer 2**, have the purpose of controlling how data is transferred between network nodes (e.g., Customer User Terminal (UT), OneWeb, Hughes, and Internet) and the means to detect and correct errors that occur at the physical layer, such as actual connection to equipment. Each layer interacts with one another; therefore, if one layer is compromised, then the preceding layers are also compromised.

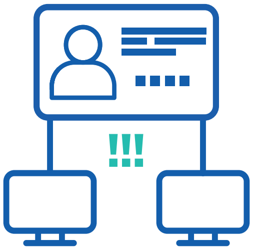
Common Layer 2 Attacks

MAC Address Flooding



DHCP Server Spoofing

Man-in-the-Middle

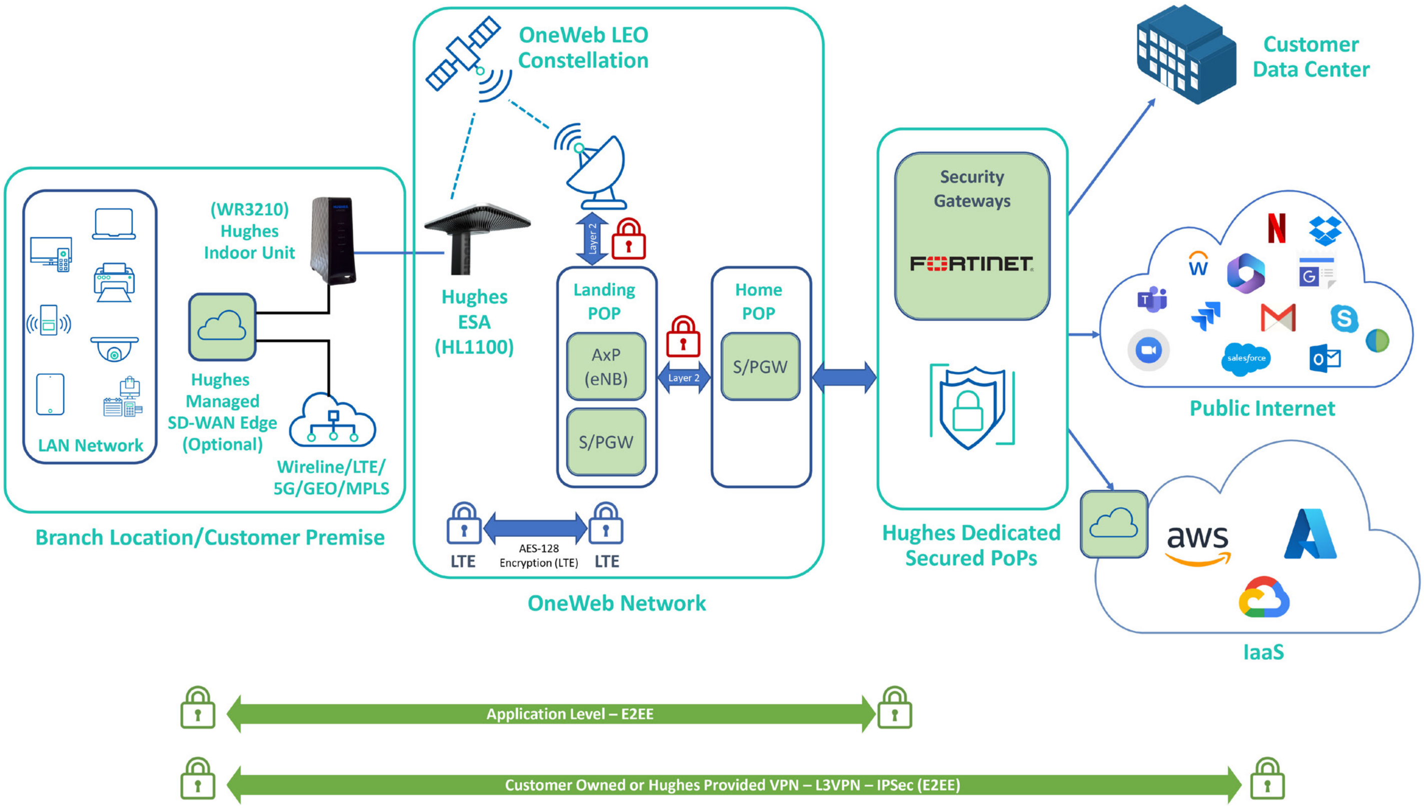


IP Host Spoofing

OneWeb Built-In Security

Our Managed LEO Service has end-to-end encryption (E2EE) and layered encryption at the transport layer security (TLS). The transport layer is an encryption protocol employed to deliver communication security over a network. End-to-end encryption is secure communication designed to prevent third parties from being able to access data while it is being transferred from one device, or end system, to another. It can also be used to secure data files, not only in transfer, but when they are at rest or being stored on servers or in the cloud as well.

OneWeb's transport layer is built upon 4G/LTE technology (3GPP LTE), with the inherent ability to utilize Advanced Encryption Standard 128 (AES-128) encryption algorithm. Their Evolved Node B (eNB), a base station that provides coverage and converts data between the satellite network and core in the Point-of-Prescence (POP), performs initial encryption, while IPsec tunneling between the eNB and S/PGW (Landing and Home POP) is used to offer Quality of Service (QoS) to manage security centrally.



Our Security Deliverables

End-to-End Encryption Application

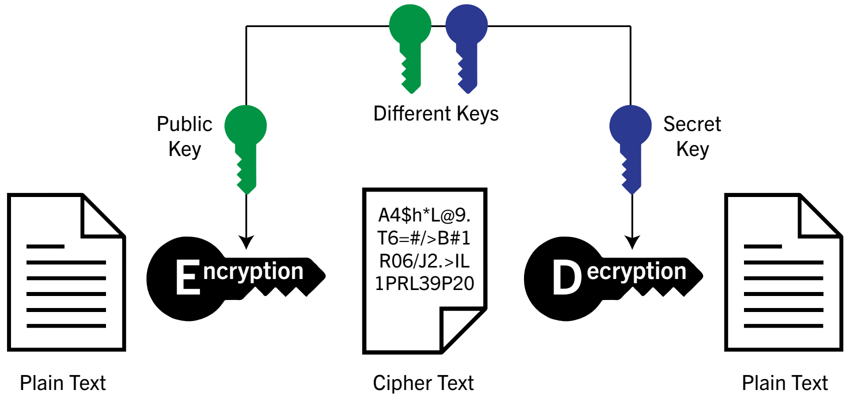
Symmetric or asymmetric encryption is utilized between the user and host application, and the encryption strength is chosen per the application's design.

Hughes POP Encryption: Fortinet

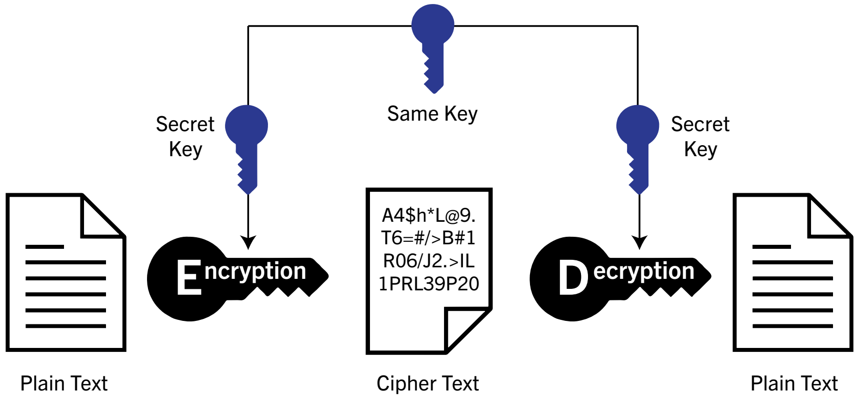
Fortinet's FortiGuard AI-Powered Security consistently detects and responds to protect application content, web traffic, devices, and users within the network. It continuously assesses risks and automatically responds to/counters known and unknown threats anywhere across the distributed network. Its coordinated and consistent real-time services defend against the latest attacks and can be deployed close to protected assets to ensure rapid, real-time detection and response.

Below are Layer 2 security mechanisms that counter previously listed attacks:

- Dynamic Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- 802.1X Authentication (Port-based, MAC-based, and Mac Authentication Bypass (MAB))
- Access Control List (ACL) Ingress, Multistage, and Scheduled



Asymmetric Encryption



Symmetric Encryption

User Terminal to OneWeb Landing POP (AES 128): LTE

Encryption between the UT and the Landing POP is secured with AES-128 and aligns with 3GPP standards for the "air interface" within LTE networks.

"Site-to-Site" or "Link-to-Link" (AES 256): OneWeb Layer 2

OneWeb manages the encryption keys, which are the link-to-link standard IEEE 802.1AE (also called MAC Sec or MAC Layer Security). AES-256 is a virtually impenetrable symmetric encryption algorithm that uses a 256-bit key to convert your plain text or data into a cipher.

Securing Your Broadband Connectivity

OneWeb and Hughes ensure data privacy and security by using the latest encryption standards within a rigid Layer 2 network between POPs, E2EE, TLS, and 3GPP LTE. These building blocks help create a stronger, stable, and secure network for all your networking needs.

For more information about Hughes Managed LEO, visit www.hughes.com/LEO

HUGHES
An EchoStar Company
11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com