ENTROPYA

VIRTUAL DISSIMULATED ENCRYPTED SERVER (VDES)

Overview

The Virtual Dissimulated Encrypted Server (VDES) is a platform designed for maximum concealment. It hides the real endpoint IP address and infrastructure. The VDES acts as a traffic redirector by accepting connections from end-user devices. It generates an encrypted tunnel, employing the Post-Quantum Cryptography (PQC) gold standard, FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) over a private IP, and redirects the traffic through an internal encrypted tunnel to a non-routable IP server. This infrastructure is built and configured according to the highest security standards, incorporating multiple layers of protection, including an Intrusion Detection System (IDS) and Disaster Recovery. Unlike other providers, the VDES can be optionally configured to provide highly secure direct access to historical and live logs and records through a unique SSH key, ensuring complete oversight and compliance for the most sensitive Zero Trust needs.

Key Features

Traffic Obfuscation 1

- VDES serves as a traffic redirector, concealing the real endpoint IP address of landing servers.
- Operates web servers on masked ports, blending seamlessly with cyberspace noise.
- Reveals only two open ports during external cyber scans for enhanced external security.

Decoy Obfuscation Tool (DOT)

- Creates a symbolic link for the PQC certificate connection, rendering destination servers non-routable.
- Conceals the IP address of destination servers from the outside cyber world.

Post-Quantum VPN Technology

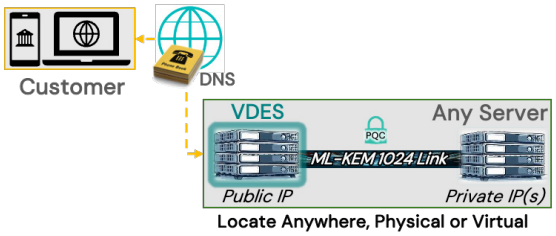
- Features a proprietary VPN server with ML-KEM, National Institutes of Standards and Technology (NIST) Security Level 5 technology, as ML-KEM 1024.
- Generates a single PQC certificate with no DNS resolution for added obfuscation.
- Exported certificate is hard-coded onto destination servers, ensuring a singular coupling.

Multi-Layered Security Configuration

- The PQC-KEM VDES is armored with multiple security layers, enhancing overall protection.
- Conveys no unique digital signatures, further contributing to its cyber stealth.

Benefits

- **Maximum Security**: The PQC-KEM protected VDES offers robust security layers, Post-Quantum Cryptography, and decoy obfuscation, ensuring your digital assets remain safeguarded from persistent and advanced cyber threats.
- **Stealth Operation**: The solution operates discreetly, concealing proprietary digital signatures and 99.999% reduction to the vulnerable attack surface.
- **User-Friendly Integration**: With a user-centric approach, the VDES seamlessly integrates into your existing infrastructure, providing a secure and transparent experience for end-users.



Locate Anywhere, Physical or Virtual

Applications

- Ideal for securing unique servers and services such as blockchain, web, VOIP, Citrix, and database access.
- Suitable for environments where IP obfuscation and protection against advanced cyber threats are paramount.

User Experience

- Device requests an HTTPS session that directs it through automatic DNS routing to the VDES.
- The VDES relays through an ML-KEM tunnel to the protected server to complete the request and authentication.

Contact: office@entropya.com