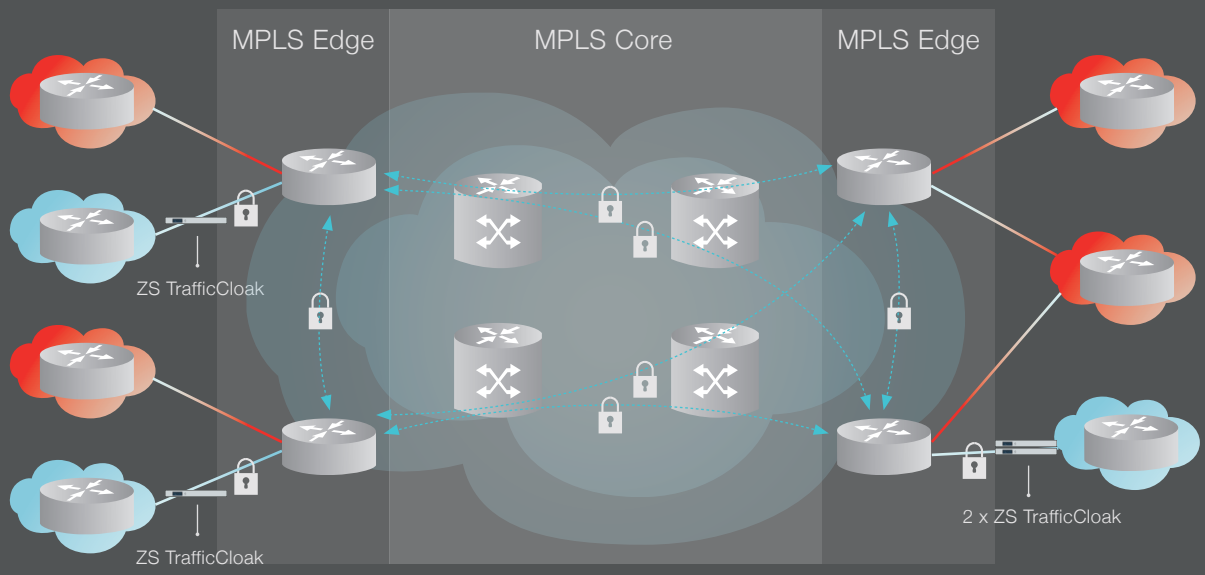
ZYBERSAFE



PRODUCT BRIEF

Zybersafe TrafficCloak – Securing MPLS

Layer 2 MPLS

MPLS has become a ubiquitous WAN service because it is protocol neutral, offers predictable services, and is extremely flexible. Layer 2 MPLS is based upon Layer 2 Ethernet switching, so there is no need to share routing tables with carriers. This typically result in much easier network deployment where the Layer 2 MPLS services simply “plug into” a campus LAN and extends the LAN to other geographical locations. Ease of use, performance, and cost advantages are driving continued demand for Layer 2 MPLS services.

What about encryption?

By itself, MPLS is not secure. Most carriers offers MPLS as a virtual end-to-end connection service, without encryption. Think of MPLS as a wide area analog to Virtual LANs (VLANs). MPLS separates IP packets or Ethernet frames, but does not protect information confidentiality or integrity with encryption on its own. Encryption may be implemented within carrier switches but as these switches reach capacity, cryptographic processing can restrain overall throughput, leading to performance bottlenecks and latency issues.

Key Features

- Strongest commercial encryption technology available (AES256)
- Full-Duplex real-time encryption
- Keys are not user manageable/accessible
- Automatic Key generation from True HW Random Number Generator
- Man-in-the-middle resistant
- Replay protection of transmitted data
- Authentication and data integrity secured
- Supports up to 100 G ethernet point-to-point links
- Encryption of unicast, multicast and broadcast traffic
- Network integration without any change of infrastructure (Pseudowire)
- No configuration steps required, simply plug-and-play
- Tamper protection mechanisms
- Designed to comply to FIPS 140-2 L3 and Common Criteria EAL4
- CE compliant

Encryption Key Management

Another issue, when using the carrier to deliver encryption services, is the management of the encryption keys. When the carrier manages the encryption in their equipment, the enterprise customer is not in control of the security management, thus relying on the carrier to handle the access to the encryption keys in a secure manner. This goes against the industry best practice of seperating the security management from the network management.

High-Performance Appliance

The only way to fully control the encryption is for the enterprise to manage the encryption themselves. By adding high-speed cryptographic appliances at network demarcation points of the carrier, the entreprise can seperate the security management from the network management of the carrier, and thereby address above mentioned security vulnerabilities, and meet regulatory compliance guidelines. Additionally, Zybersafe TrafficCloak have build-in automated key management eliminating the need for the enterprise to implement cumbersome security processes for handling the management of the encryption keys.

Zybersafe TrafficCloak in an MPLS environment

Zybersafe TrafficCloak is a purpose-built cryptographic appliance for Ethernet networks. This appliance is built for enterprise security needs by supporting AES-256 encryption with fully automated key management and flexible interfaces. The TrafficCloak ethernet encryption appliance offer a transparent, wire-speed encryption service on fiber or copper point-to-point links up to 100 Gbps.

Corporate Overview

Zybersafe is an innovative danish company specialized within building hardware encryption solutions.
We focus on building security products that ensure the highest level of protection for Data-in-Motion.