CERTES
CERTESNETWORKS.COM

WHITE PAPER |

THE TRUTH about MPLS SECURITY

MYTH: MPLS is private

"We use a private network" is often stated as the reason for not protecting data as it travels over 3rd party networks. But is MPLS really private? MPLS is technically a VPN or a Virtual Private Network, meaning it's not actually private - it only mimics privacy by logically separating data with labels. More importantly - even if MPLS were private, is privacy the equivalent of security? The answer is no.

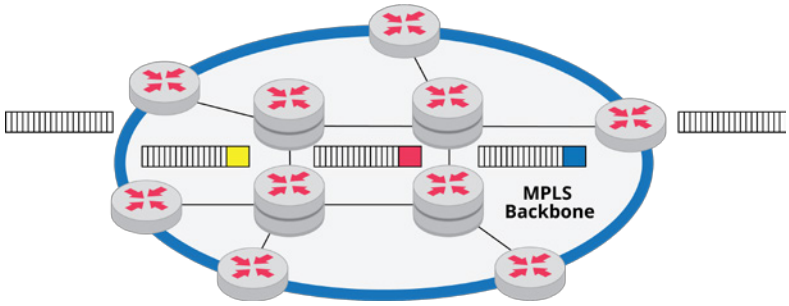
"It is important to understand that a service provider has the technical possibility to sniff VPN data, and VPN users can either choose to trust the service providers not to use their data inappropriately, or they can encrypt the traffic over the MPLS core." – Analyzing MPLS Security Michael H. Behringer and Monique Morrow.

FACT: MPLS is a shared service

MPLS is a shared network service - there is nothing private about it.

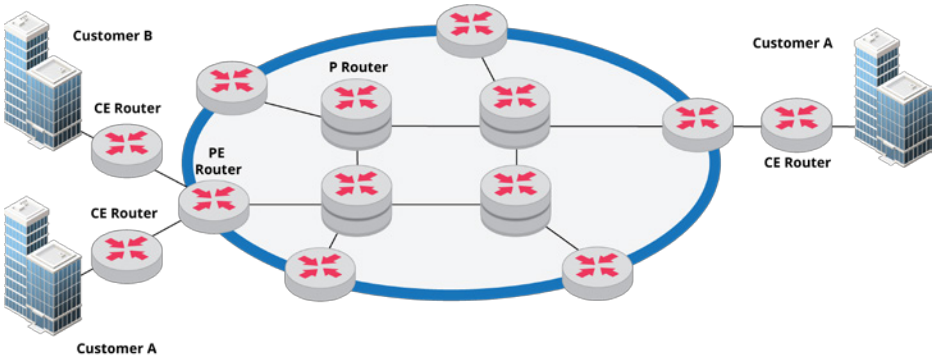
The labels generated by MPLS logically segment user traffic but they are used only for forwarding purposes. Traffic from thousands of different customers and users (including traffic from other carriers and the Internet) traverse a common set of backbone routers in rapid succession.

Each router in an MPLS network performs "label swapping". The new label is used by the next router for forwarding purposes. At any given moment traffic from competitors and other provider networks flows across a common infrastructure.



Data is shared almost immediately.

Customer Edge (CE) routers are assigned to individual customers, but Provider Edge (PE) and Provider backbone (P) routers are shared. In other words, only the router in your office is "private" - the very next router your traffic hits (and all the routers after it) are shared by multiple users.



MYTH: MPLS is secure

There is a common misconception that MPLS provides some level of security.

The truth is that MPLS offers:

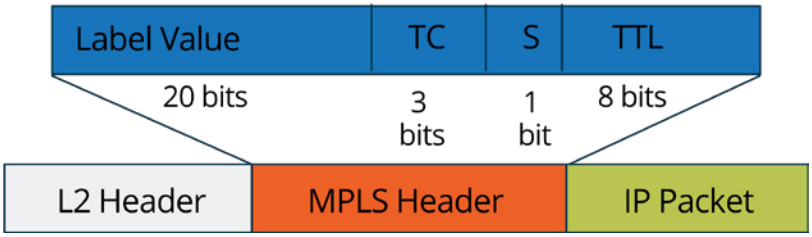
No protection against misconfigurations
Human and machine errors as well as OS bugs can result in MPLS traffic being misrouted.

No protection from attacks within the core
MPLS is vulnerable to all the traditional WAN attack vectors.

No protection or detection of sniffing/snooping
It is impossible to detect if someone is siphoning or replicating data - there is no "alarm" that goes off if data is being stolen.

No Data Security
The data is left in the clear and can be accessed, replicated, or used by anyone who gains access to it.

FACT: MPLS has no inherent security



The illustration above shows the components of an MPLS header. Note the absence of any security measures within the header itself.

- The Label Value provides forwarding information used by the routers.
- Traffic Class (TC) bits are used to provide services such as traffic prioritization.
- The Stacking bit (S) allows multiple labels to be used.
- TTL is a "time to live" marker to allow packets to expire.

None of these mechanisms provide security.

Also note that the original IP packet is unchanged, which means:
With MPLS – your data traverses a shared network in the clear.

MYTH: Providers position MPLS accurately

In a podcast dated April 2009, a Product Director from a major service provider said security was "built in" to MPLS based on the following:

- Traffic streams are kept separate.
- There are controls around provisioning and management.
- There are gateways between the Public Internet and the MPLS.
- Netflow and J-Flow are used to identify "malicious" activity.
- Nearly every MPLS service provider makes similar claims.

Service providers can make these claims because they bear no responsibility for the integrity of your data - SLAs are built around reliable delivery, not data integrity or security.

FACT: Providers continue to market MPLS as a secure service

Hackers and Data Thieves know better!

There are papers and video tutorials readily available on the Internet that provide a "cook book" approach to sniffing and redirecting MPLS traffic. Here's what Black Hat had to say about MPLS security claims:

PROVIDERS SAY: Traffic streams are kept separate.

HACKERS KNOW: The mechanism used to separate traffic can also be used to identify targets of interest!

PROVIDERS SAY: There are controls around provisioning and management.

HACKERS KNOW: Provisioning and management are to data security what traffic lights are to bank robbers - they do not prevent data theft!

PROVIDERS SAY: There are gateways between the Internet and the MPLS network.

HACKERS KNOW: Traffic is not accidentally leaking out to the Internet, it is being stolen right off the MPLS backbone!

PROVIDERS SAY: They use Netflow / J-Flow to identify "malicious activity".

HACKERS KNOW: Post-event notification is not a substitute for prevention.

MYTH: Encryption breaks MPLS

IPsec VPNs are typically used to protect data on MPLS networks.

While they do provide excellent security, they also mask many of the features service providers offer, including:

• Class of Service • Netflow / J-Flow • Network Address Translation (NAT) • Policy based routing

Other traditional issues with IPsec tunnels include:

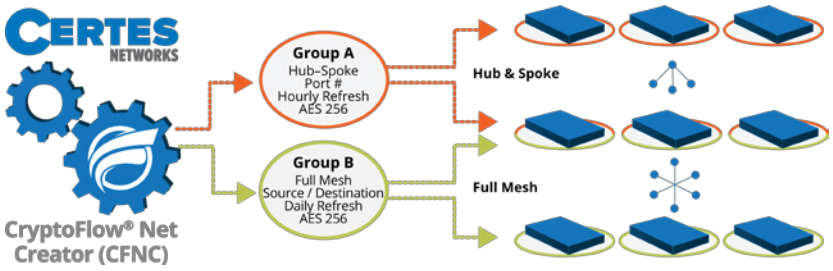
- Forces any-to-any networks to become point-to-point connections
- Requires complex configurations, which are expensive to operate and manage
- Is not VoIP or Video compatible (due to increased latency)
- Slows / breaks Multicast
- Breaks load balancing
- Often requires router / OS upgrades
- Hides application information required for troubleshooting

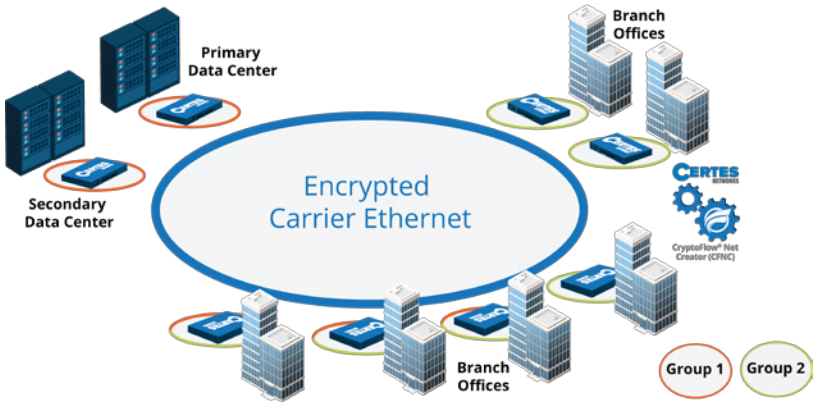
FACT: Group Encryption is transparent to MPLS

Group Encryption allows security administrators to create encryption policies that match the existing network topology and application flows - without creating tunnels.

By maintaining the original headers, Group Encryption allows you to retain all of the benefits (including Layer 4 services) of MPLS, while providing the highest level of data protection.

With Group Encryption you can decouple security from the infrastructure and maintain application performance, while protecting data and complying with privacy regulations.





MYTH: Encryption kills performance

Latency has traditionally been one of the major drawbacks of encryption.

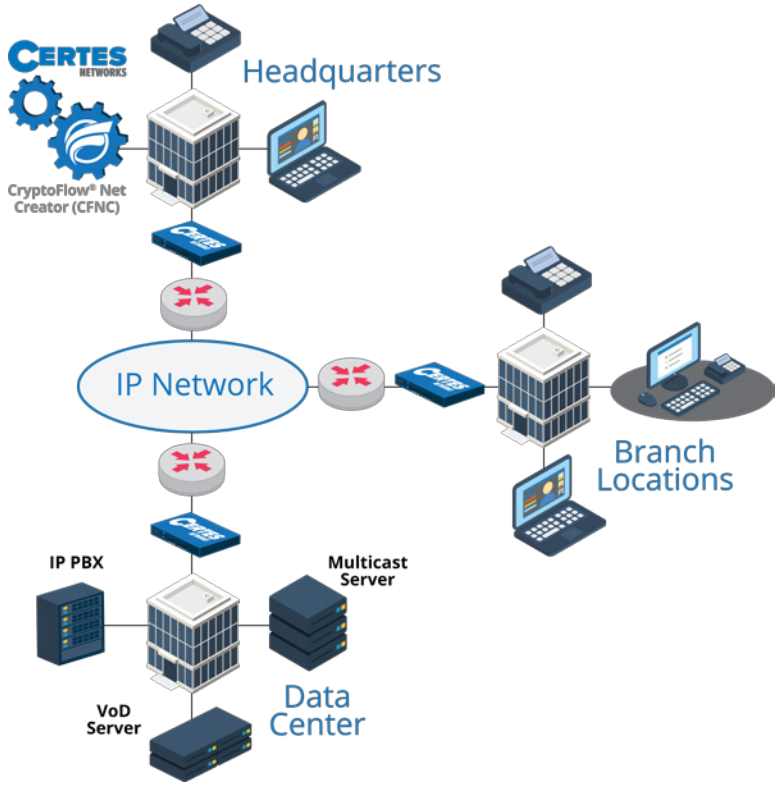
Even with an accelerator card in place there can be as much as an 80% drop in performance on a WAN link while encrypting.

No amount of cryptographic acceleration can help because encryption is not the only cause of latency.

Other contributors are massive policy maps and the associated look-ups that get created when an any-to-any network is relegated into point-to-point relationships.

Latency can also be caused by the repeated passing of packets through the router backplane.

FACT: You can encrypt MPLS without impacting quality or performance



Group Encryption does not impact network performance.

Because Group Encryption does not impact the underlying infrastructure or impose point-to-point connections, any topology can be secured without modifications.

- Full mesh networks can be encrypted while preserving Layer-4 services.
- VoIP can be encrypted without impacting call quality.
- Dual carrier networks can be secured without impacting SLAs.
- Load balanced networks can be secured without impacting high availability.
- Encrypt latency sensitive application such as Voice and Video.

Because the complexity of tunnels and the latency inducing policy look-ups are avoided, voice and video can be secured without hampering quality.

Additional Facts

Certes Networks released the industry's first Group Encryption solution in 2006.

Certes Networks has partnered with premier service providers to provide MPLS compatible encryption as a managed service.

Certes Networks offers the industry's only Layer 4 compatible encryption solution.

Certes Networks offers tunnel-less Group Encryption at Layer 2, Layer 3, and Layer 4.

About Certes Networks

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you "Encryption without Compromise".

For more information visit **CertesNetworks.com**

Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: +1(888) 833-1142
Fax: +1(412)262-2574
CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East & Africa Sales
emea@certesnetworks.com

V1-04-27-2017