Multilayer Group Encryption: Myth or Reality?

October 2010

Franjo Majstor
Sr. Technical Director - EMEA
CipherOptics Inc.
franjo@cipheroptics.com

CIPHEROPTICS

Problem Description?

Modern networks are done with direct fiber and allow country-wide network communications at Layer 2. MPLS networks carry today Layer 3 or Layer 2 while all is load balanced, redundantly designed with fast failover carrying unicast, multicast or anycast traffic…

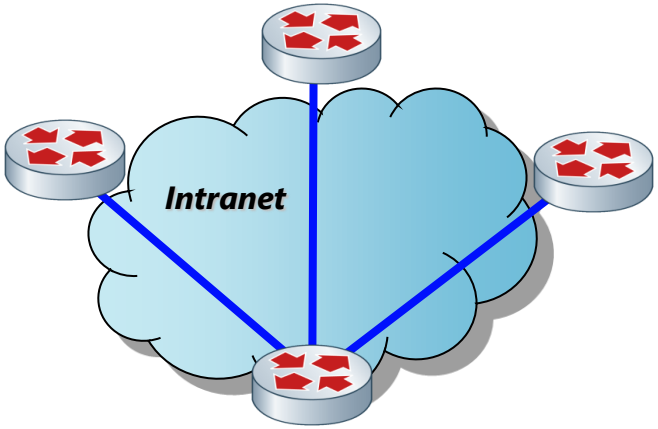
So how do you encrypt all of this today? How do you comply with any auditor wishes for protecting your data in transit over the modern networking infrastructure without impacting any of its existing functionality?

The answer is multilayer group encryption.

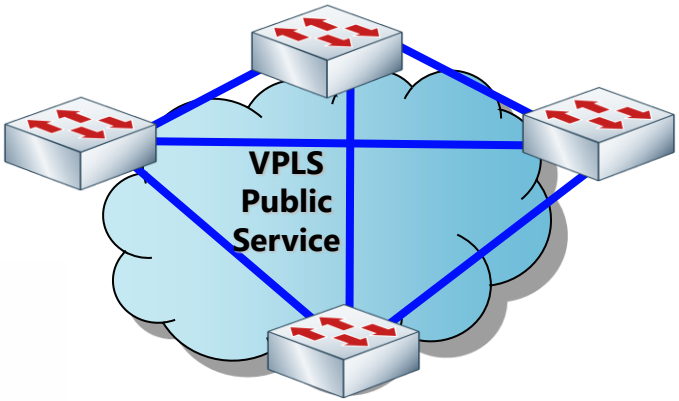
© CIPHEROPTICS

CIPHEROPTICS

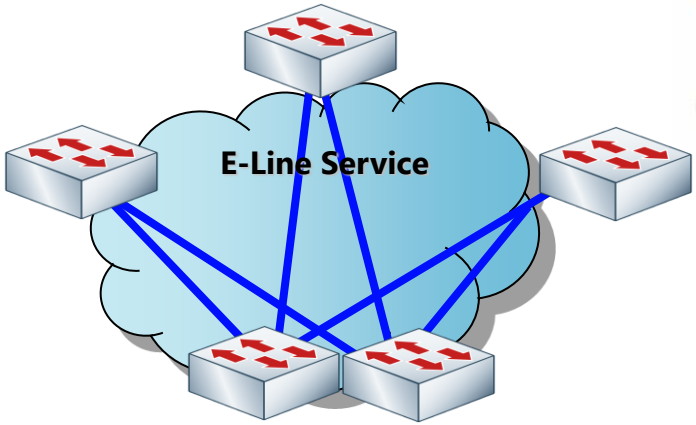
Network Topologies & Protocols



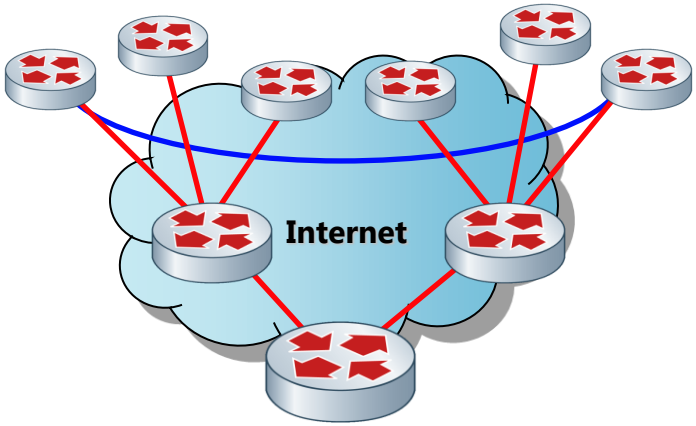
Hub and Spoke



L2
Mesh



Redundant Hub
And Spoke



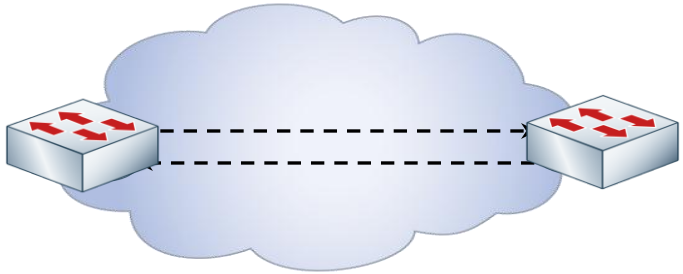
Multicast

CIPHEROPTICS

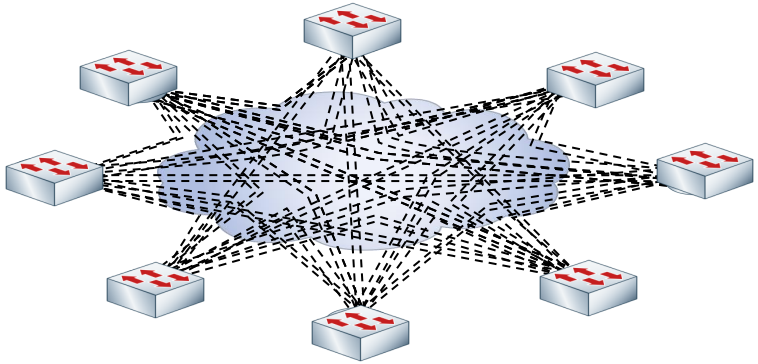
How Scalable this is?

Companies that want network encryption are forced to use a policy and key exchange technology that was designed only for point-to-point links.

IKE was designed for this…



…not this



Using IKE for network-wide encryption:

- **Is complicated - It gets worse at an exponential rate.**
- **De-optimizes networks - IKE tunnels "break" load balancing and multicast and also negatively impact resiliency and availability.**
- **Impacts application performance - The tunnel set-up and look-up processing adds latency and increases router CPU load, which adds more latency.**

"Encryption" often gets the blame, but it's a policy and key creation and management problem.

© CIPHEROPTICS

CIPHEROPTICS

How Easy this is?

Encryption Standard

Policy Definition	➢ Policy Definition ➢ Elements defined by standards ➢ Facilitates interoperability
Key Exchange	➢ Key Exchange Protocol ➢ IKE is standard for IPSEC ➢ Use of Diffie-Hellman
Encryption	➢ Encryption Algorithm ➢ AES is the current standard (also 3DES) ➢ Supports tunnel and transport mode

The right Tool for the right Job

Appliance Based
Point-to-Point Encryption

Easy installation and set-up

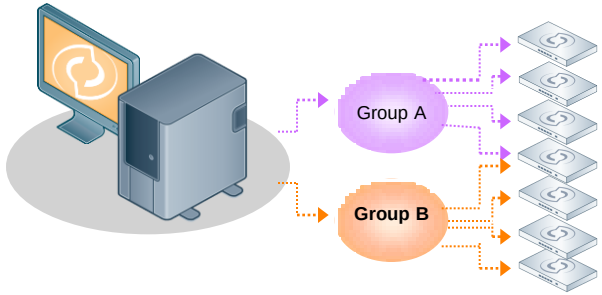
Wire-speed performance

IKE used for key exchange

AES-256 Encryption

Per-frame authentication provides additional security

Group Multilayer
Network-wide Encryption



Easy installation and set-up

Layer 2, Layer 3, or Layer 4

Network-wide policy and key management with CipherEngine

Wire-speed performance

Automatic re-key option

One-click adds, changes and re-keys

Traffic flows and application performance are preserved

© CIPHEROPTICS

CIPHEROPTICS

WHO is CipherOptics?

2000
The Year CipherOptics was Founded

1st
2002
Gigabit IP Encryptor

1st
2005
Gigabit Ethernet Encryptor

1st
2006
Group Encryption Solution

1st
2008
Multilayer Encryptor

1st
2009
L2-10M Encryptor

© CIPHEROPTICS

CIPHEROPTICS

We fixed the Problem!

CipherEngine™ is the only purpose-built policy and key manager for network-wide group encryption!

Using a policy and key management solution that is designed for network-wide deployments makes encryption:

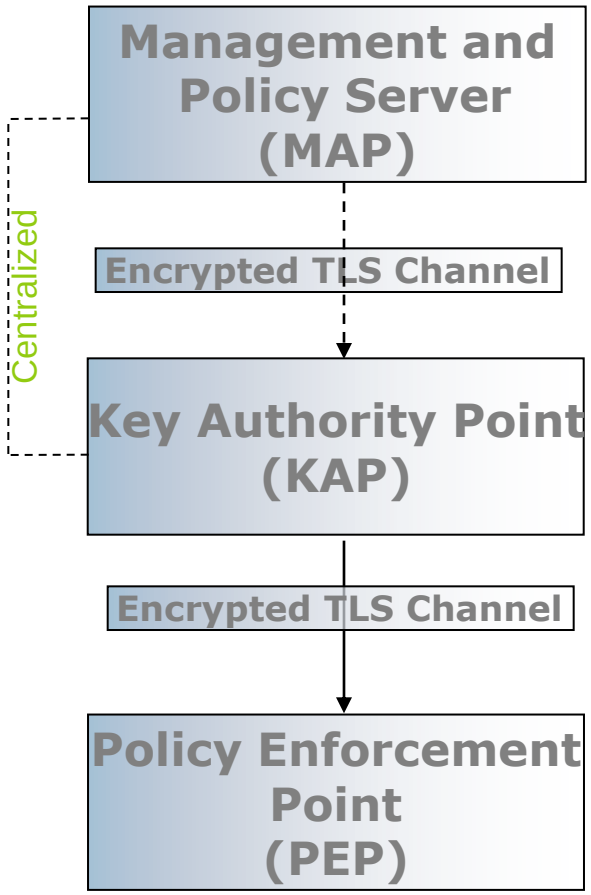
- ✓ **Scalable** without increasing complexity
- ✓ **Easy** to install and manage
- ✓ **Transparent** to your network traffic requirements
- ✓ **Compatible** with your throughput needs

© CIPHEROPTICS

CIPHEROPTICS

Distributed Encryption Approach

CipherEngine™



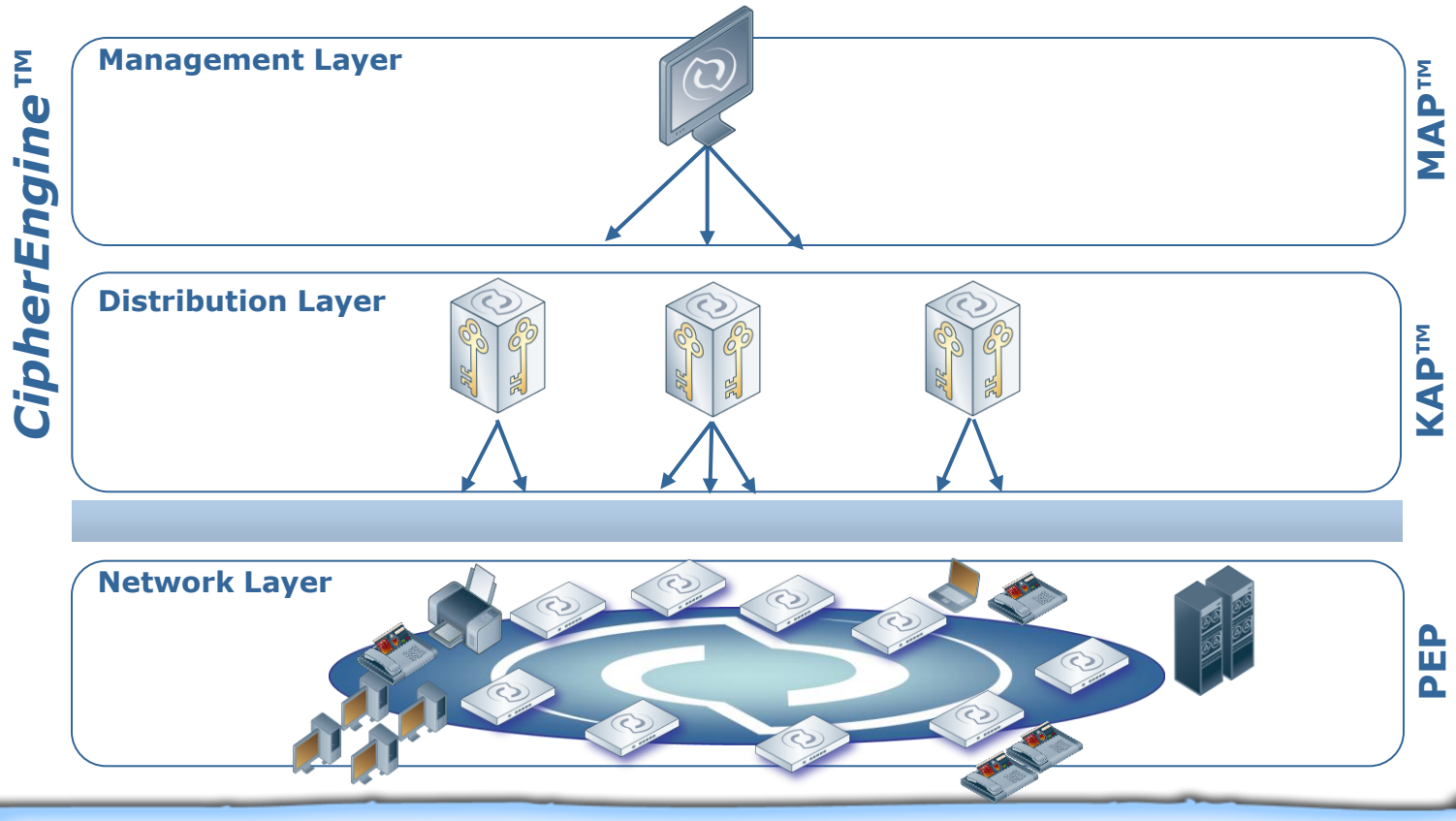
- Interface for policy definition or interface to others
- Centralized management
- Authenticates each KAP
- Pushes and enforces policy with KAPs
- Group/Community of Interest definition and support

- Key Authority for policy enforcement points
- Allows for Federated/redundant deployment
- Generates and distributes Security Associations info and Keys to PEPs
- Authenticates PEPs and monitors operations
- Designed to support keying for any key-enabled app.

- Hardware or software-based PEP
- Support for clients, blades and appliances
- Policy and keys distributed by KAPs
- Mutually authenticates KAPs
- Supports Tunnel, Transport and Network modes

CIPHEROPTICS

CipherEngine™



Software & Hardware:

Dated June 2006

CE SW & KAP SW&HW

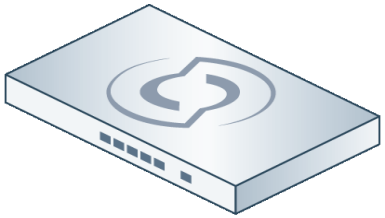
CipherEngine™ **makes group network encryption easy to install, simple to manage and transparent to any infrastructure, topology or application.**

© CIPHEROPTICS

CIPHEROPTICS

How Easy it could be…1, 2, 3.

1. CEPs are installed in seconds

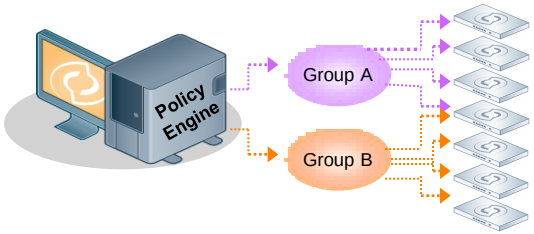


Can be installed by non-technical branch personnel

Connect 3 Ports:
- Local (LAN side)
- Remote (WAN side)
- Management

Management IP Address get assigned

2. Policies are defined in CipherEngine

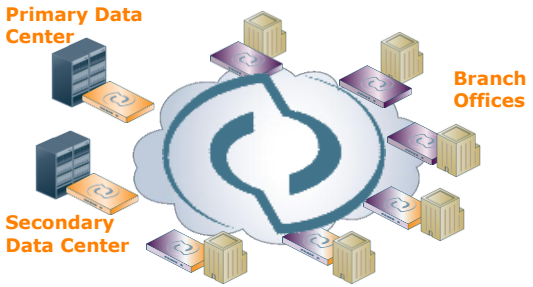


Groups are created based on security policies

CipherEngine used to provision CEPs (SNMP, logging, etc..)

Keys and policies are securely delivered to CEPs

3. Encryption is in effect



Data is encrypted, sent in the clear, or discarded at wire-speed

Traffic flows and application performance are preserved

No tunnels are created

© CIPHEROPTICS

CIPHEROPTICS

How transparent it is?

Original Packet - Not protected

Original L2 Header	Original IP Header	Original L4 Header	Original IP Data

CipherEngine L2 Ethernet Frame Encryption - Protect Ethernet Payload

Original L2 Header	ESP Header	Original L3 Header	Original L4 Header	Original Layer 3 Data

CipherEngine L3 IP Packet Encryption with Virtual IP

Original L2 Header	Public IP Header	ESP Header	Original IP Header	Original L4 Header	Original IP Payload

CipherEngine L3 IP Packet Encryption Network Mode - *protocol changed to 50 (ESP)

Original L2 Header	Original IP* Header	ESP Header	Original IP Header	Original L4 Header	Original IP Payload

CipherEngine L4 Encryption TCP/UDP - **Protocol ID and Ports in clear

Original L2 Header	Original IP Header	Original TCP/UDP*** Header	ESP Header	Original TCP/UDP Payload

CipherEngine L4 Encryption Non-TCP/UDP - ***Protocol ID in clear

Original L2 Header	Original IP*** Header	ESP Header	Original IP Payload

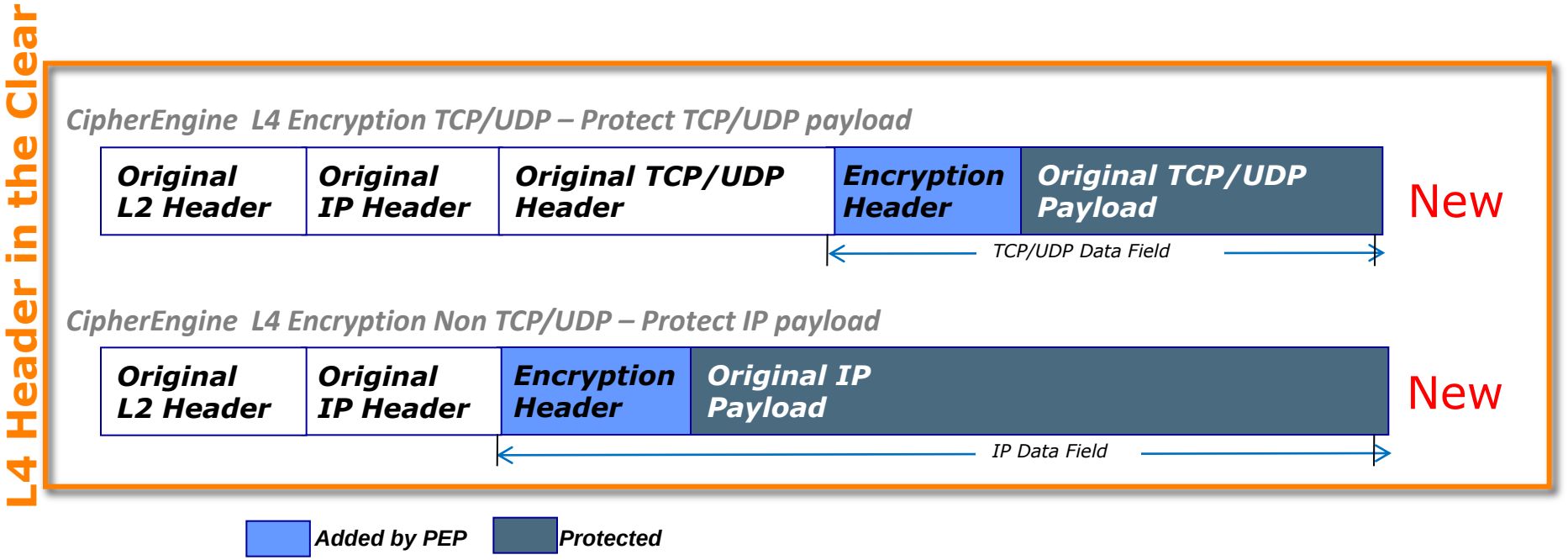
Encapsulating Security Payload Header

Encrypted

© CIPHEROPTICS

CIPHEROPTICS

Encryption at L4?



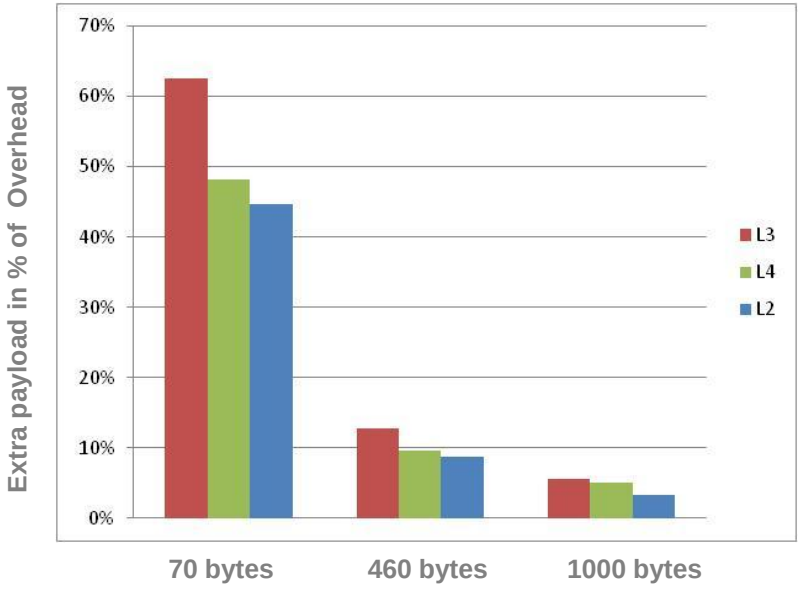
- **L4 encryption use cases:**
  - Passing through NAT devices
  - Netflow/Jflow support - accounting, statistics
  - Policy based routing/load balancing
  - Easy (encrypted) network troubleshooting
  - Lower packet overhead (~5-10% on average faster than L3).

© CIPHEROPTICS

CIPHEROPTICS

Where to encrypt?

Data Payload (bytes)	IP packet in clear (bytes)	L2 encrypted (bytes)	L3 encrypted (bytes)	L4 encrypted (bytes)
70	112	162	182	166
460	502	546	566	550
1000	1042	1076	1100	1094



- **L2 encryption use cases:**
  - Direct fiber or direct link
  - Metro Ethernet
  - Any modern network design at L2

- **L3 encryption use cases:**
  - Legacy L3 networks or „old VPN" devices

- **L4 encryption use cases:**
  - Passing through NAT devices
  - Netflow/Jflow support - accounting, statistics
  - Policy based routing/load balancing
  - Easy (encrypted) network troubleshooting
  - Lower packet overhead (~5-10% on average faster than L3).

© CIPHEROPTICS

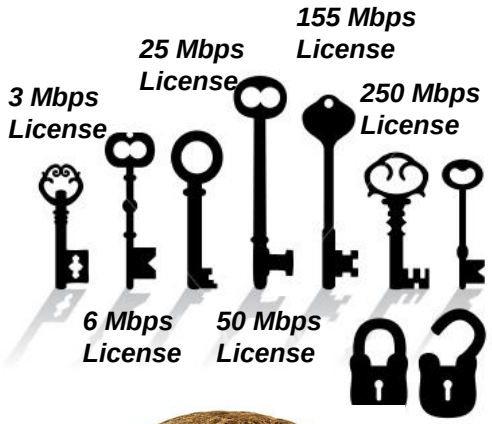
CIPHEROPTICS

How compatible it is?

Hardware Platforms:

Platforms that grow with you

From small/home office to data canters, there is a right size appliance



Bandwidth Licenses:

Unlock the throughput you need

You can unlock the throughput you need with a new bandwidth license- without an upgrade penalty

© CIPHEROPTICS

CIPHEROPTICS

CEP Family of Encryptors + CipherEngine ™

Family of Encryptors

CipherEngine

	CEP10	CEP100	CEP1000	CEP10G	CE
					
Traffic Ports	(2) 10/100Mbps	(2) 100/1000Mbps	(2) 1Gbps	(2) 10Gbps	N/A
Group SA's	1,200	9,600	9,600	9,600	N/A
Thru-put	3-50Mbps	100-250Mbps	500M-1Gbps	2.5-10Gbps	N/A
Encryption	3DES, AES-256	3DES, AES-256	3DES, AES-256	3DES, AES-256	N/A

© CIPHEROPTICS

CIPHEROPTICS

CipherOptics Youtube Channel

http://www.youtube.com/user/cipheroptics

© CIPHEROPTICS

CIPHEROPTICS

Questions?

© CIPHEROPTICS

CIPHEROPTICS


Merci
Gracias
Thank you
Tänan
Labai aciu
Paldies
Vielen Dank
Takk De
谢谢你。
Dank U
Děkujeme Vám
Hvala
Teşekkürler
CIPHEROPTICS