Cipher Box M

Application note: Cipher Box powered SD-WAN and LAN security solutions

What is Cipher Box M?

Cipher Box is the next generation IP encryption device with clean hardware design for modern security requirements in IP networked world.

The unique Cipher Box gains from multiparty protocol ("MPP") which handles identity and cipher key exchanges between multiple entities. MPP protocol is XXLSEC proprietary multiparty consensus protocol with no visible *META DATA* on transmission and complete device forensic security.

Cipher Box with MPP is fully meets the functional requirements under modern zero trust cyber security strategy.

Cipher Box device runs PriveOS, vanilla Linux based Operating System and selected software components. They meet essential base for highest level of security requirements for any business critical system or infrastructure. The hardware and all software components are auditable to source code level. Therefore there are no hidden elements or binary code from unknown sources.

Encrypting IP connections with Cipher Box upgrades traditional VPN device approach, including multicast encryption. Cipher Box encrypts IP traffic with any symmetric algorithm user choose to use and enables crypto modernization to reach required security level.

Cipher Box physics and electronics are designed to secure your cipher primitives at strictest professional level. Abloy lock on the unit prevents any physical intrusion while in transport and in use.

Cipher Box M features

Form factor:	Table stand or rack mount
Processor:	Cortex ® -A9 NXP i.MX6 Quad
Memory:	2GB RAM, 8 GB MassStorage
Comms:	Wired Ethernet (10/100 MBits)
OS:	PriveOS (vanilla Linux kernel)
Source code:	100% visibility and auditable
Software:	META DATA Free IP encryptor with MPP protocol for secure key consensus
Security:	No META DATA on traffic Forensic security Supply chain security Tamper protected aluminum case Multi key ciphering
IP encryption	Supports p2p and multipoint configurations with MPP key delivery. Multicast encryption support.
Power Supply:	5 V DC (2.5 A)

Multiparty protocol (MPP) features

- Anonymization of all networked identities
- Secure encryption key delivery and consensus (layer 2 and 3)
- Authentication of nodes in constellation
- All devices are part of a multiparty constellation
- No centralized infrastructure required
- Support for user defined cipher paramethers
- Distributed computing model
- No third party Trust Anchor models

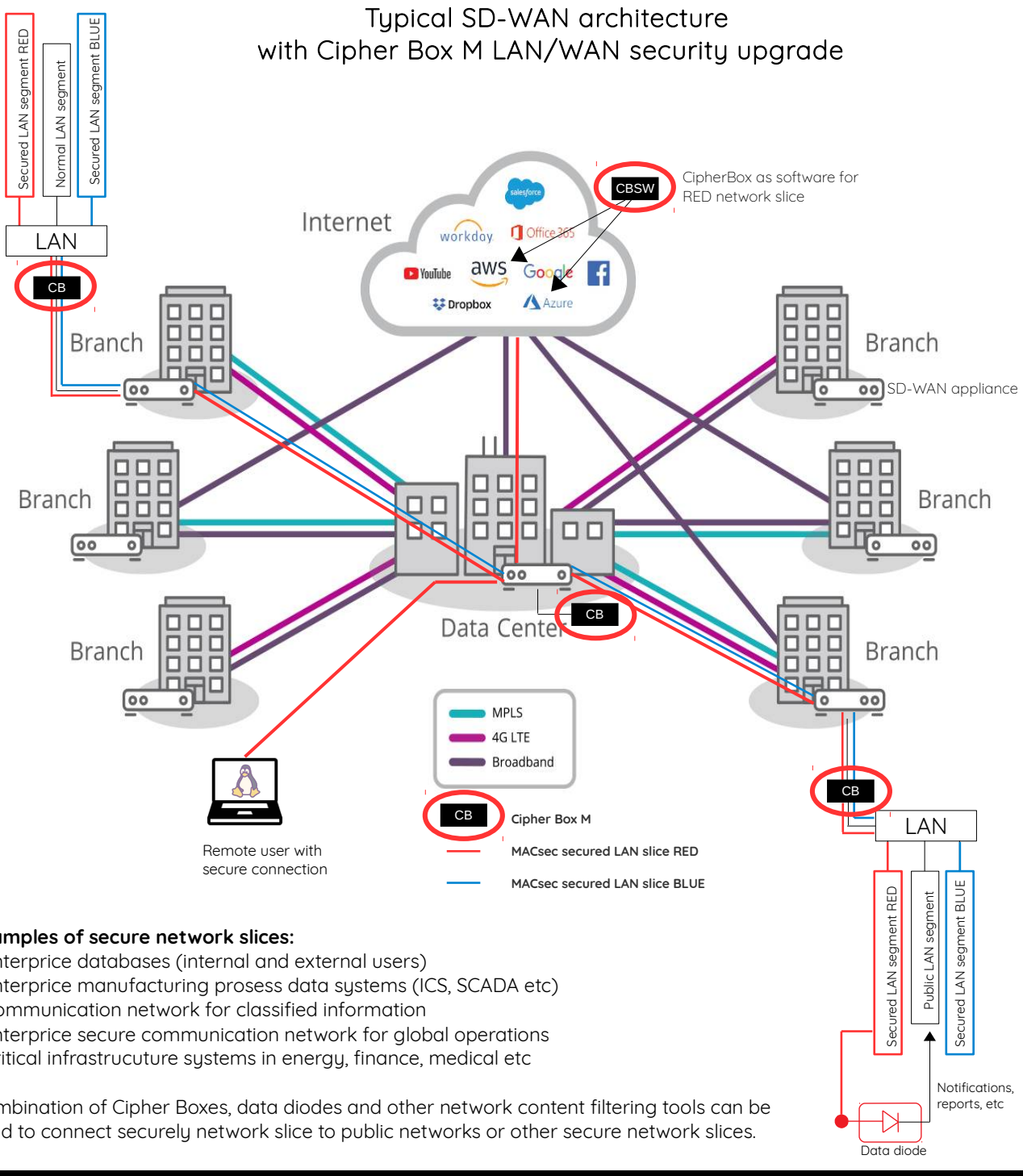
MPP protects Cipher Box devices against forensic threats, no keys to steal.

360 security model for data in rest – data in use – data in transit.

SD-WAN and LAN security with MACsec (IEEE 802.1AE)

SD-WAN networks are cost efficent and suitable global networks for enterprices and governments. SD-WAN can be upgraded with XXLSEC Cipher Box and MPP technology to create MACsec encrypted network slices, which are protected from ransomwares, APT and ARP attacks and other most common LAN network related security issues (application level DDOS/DOS, Man-In-The-Middle eavesdropping, repuditation, replay etc). Cipher Box as software element can be also installed to cloud server which creates layer 2 connectivity between LAN segments and clould services.

LAN security with Cipher Box means secure MACsec key delivery between networked computers and servers inside single LAN segment and between LAN segments connected to SD-WAN network. Brigding LAN segments and cloud services with Cipher Box MACsec key delivery solution creates a layer 2 level network security with lower costs and better protection than current IP-security tools. XXLSEC Cipher Box MACsec key delivery client supports currently LinuxOS devices and servers. MACsec network slice is independent and isolated group of personal computers, servers and cloud services which are secured and isolated from any other potential malicous computers in the same network. Cipher Box is method of securing business and operation critical data from public networks with special network slice.



Examples of secure network slices:

* Enterprice databases (internal and external users)
* Enterprice manufacturing prosess data systems (ICS, SCADA etc)
* Communication network for classified information
* Enterprice secure communication network for global operations
* Critical infrastrucuture systems in energy, finance, medical etc

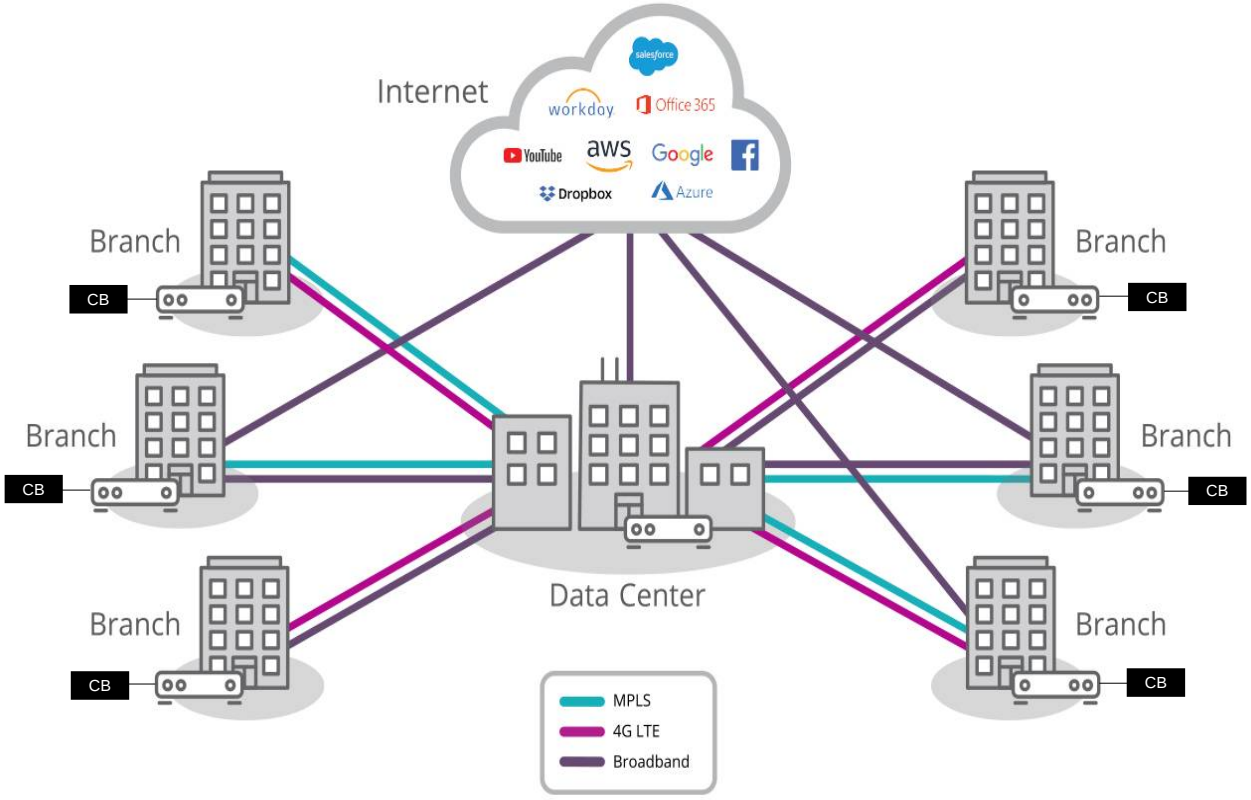
Combination of Cipher Boxes, data diodes and other network content filtering tools can be used to connect securely network slice to public networks or other secure network slices.

“Post VPN world” - secure management plane connections and key security

Cipher Boxes can be used to replace VPN or SSH connections of SD-WAN management plane or other VPN connections. Solution is based on creating better key security and authentication with layer 3 security. No more problems with lost or compromized security keys. Cipher Box is suitable for tunnel solutions where meta data of the connections is required to mimize and also device location and integrity risks must be eliminated. Also when user defined encryption paramethers and local audit is required, Cipher Box is capable of supporting these critical connections in energy, finance, governments, critical communication etc. Cipher Box itself is also a secure hardware element and secure software solution with user defniable crypto paramether capability for critical infrastructure users meeting regulatory domain.

SD-WAN management plane control security with Cipher Box creates secure connectivity over public networks to SD-WAN applicances with Post VPN world security level and user controlled trust anchor and full authentication.

Normal SD-WAN management plane with
Cipher Box M “Post VPN world” solution



Multiparty Protocol benefits – save costs and reduce risks

Legacy IP-security technologies like VPN, PKI and IPsec requires a lot of mangement efforts and the security has many vulnerabilities, restricitions and shortages. MPP is a multiparty connection capable protocol which reduces critical the meta data and creates easy and fast way to manage and create encryption keys. MPP allows users to reduce life time costs and upgrade security and reduce attack surface. MPP offers totally new way to manage encryption keys secure way and creates cost savings compared to current mechanisms. No more lost or stolen keys.

MPP controlled Cipher Boxes are automatically authenticated and all nodes in the constellation are verified and information is confirmed to be valid. MPP is a dispersed, secure and authenticated identity for machines and softwares in defined user group based on multiparty computation.