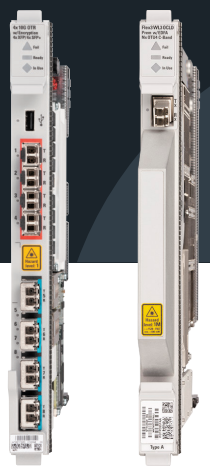
FICHE TECHNIQUE

Modules de chiffrement hautes performances haute capacité

Pour le système 6500 Packet-Optical Platform



Conçu pour assurer la confidentialité des données en vol, le système 6500 Packet-Optical Platform de Ciena permet d'obtenir une solution 10G, 100G ou 200G de chiffrement flexible hautes performances indépendante du protocole à la fois flexible et rentable qui allie facilité d'exploitation et d'administration afin d'activer une protection des données facile à mettre en œuvre pour les services Ethernet, Fibre Channel, SDH/SONET et OTN (réseau de transport optique).

La solution WaveLogic Encryption de Ciena combine une technologie de chiffrement éprouvée, déployée sur des plates-formes disposant d'une large base installée au niveau mondial démontrant la fiabilité du 6500, produit leader du marché déployé par plus de 600 opérateurs autour du monde. Les opérateurs peuvent bénéficier d'une solution qui simplifie le déploiement du chiffrement en intégrant la fonctionnalité de chiffrement directement dans les éléments au sein du réseau de transport, réduisant ainsi la complexité du réseau et éliminant le besoin de gérer différentes solutions de chiffrement pour différentes applications.

Une solution certifiée hautement sécurisée

Dans le cadre de l'approche multicouche de Ciena en matière de sécurité assurant la confidentialité, l'intégrité et la disponibilité des données sur le réseau, le chiffrement est toujours activé dans la solution WaveLogic Encryption de Ciena, ce qui garantit le meilleur niveau de sécurité possible, car l'intégralité du trafic est chiffrée en permanence. Même si la possibilité d'activer ou de désactiver le chiffrement paraît donner davantage de souplesse, une simple erreur humaine peut entraîner l'envoi non-chiffré de données confidentielles sur le réseau. Cette solution est validée en externe et certifiée de façon indépendante par une tierce partie pour lui assurer d'être mise en place avec les algorithmes et le moteur AES normalisés. La solution respecte les normes de sécurité les plus hautes reconnues, notamment les certifications Common Criteria et FIPS. Elle fournit ainsi un moteur de chiffrement AES-256, certifié FIPS, disposant de mécanismes d'authentification normalisés (tels que les certificats X.509), ce qui permet une simplification opérationnelle avec une intégration transparente aux PKI d'entreprise existants.

Fonctionnalités et avantages

- Offre une solution de chiffrement à hautes performances et délai de transit ultra-faible pour des communications de bout en bout transparentes et hautement sécurisées.
- Dispose d'un chiffrement indépendant du protocole offrant la flexibilité de prendre en charge toute une variété de services.
- Sécurise à la volée toutes les données sensibles avec une solution de chiffrement AES256 (norme de chiffrement avancé) conforme FIPS.
- Tire parti de deux ensembles distincts de clés pour les fonctions d'authentification et de chiffrement des données, avec une rotation rapide des clés de chiffrement de quelques secondes.
- S'intègre de façon transparente aux infrastructures PKI (à clé publique) existant en entreprise grâce à une authentification à certificat X.509.
- Permet une gestion sécurisée de la capacité de type EaaS (chiffrement en tant que service) par l'utilisateur final dans des infrastructures gérées par opérateur ou entreprise via un outil de gestion intégré.
- Offre une solution de chiffrement ayant fait ses preuves sur le terrain largement déployée dans le monde sur des réseaux de la finance, des services publics, de la santé, des armées et des gouvernements.

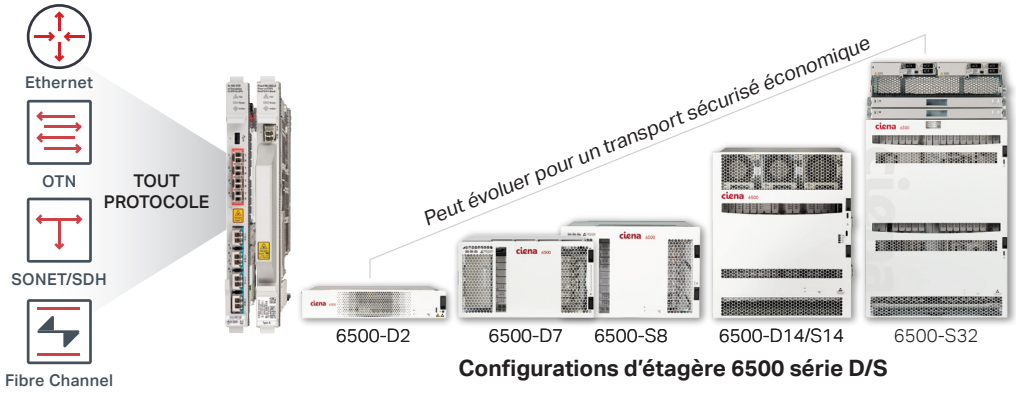


Figure 1 : Solution WaveLogic Encryption hautes performances indépendante du protocole pour 6500 pouvant évoluer et satisfaire les besoins de votre réseau

Une flexibilité sans précédent

Grâce à la flexibilité des 6500, les clients peuvent sélectionner la taille de baie optimale selon leurs besoins spécifiques sur site de capacité, d'espace et de puissance pour un transport rentable des services chiffrés. Un avantage clé supplémentaire est que la solution est totalement indépendante du protocole et prend en charge une large variété de clients flexibles pour répondre aux multiples applications parmi les clients soucieux de sécurité. Les clients peuvent déployer des services différenciés avec une connectivité à délai de transit ultra-faible et plusieurs options de protection d'équipement et de trajet.

Encryption Testing and Certification
Télécharger l'infobrief

Un chiffrement invulnérable

Pour mieux protéger les données, deux ensembles de clés distincts et indépendants sont utilisés pour les fonctions d'authentification et de chiffrement des données avec un intervalle de rotation des clés de chiffrement rapide, de quelques secondes au lieu de plusieurs minutes. Les clés de la session de chiffrement AES-256 des données font l'objet de négociation et de rotation à chaque seconde, de façon autonome et indépendante sur chaque ligne de port, sans impact sur le trafic ou sur le débit, ni intervention de l'utilisateur. Les opérateurs peuvent déployer la nouvelle génération d'algorithmes de cryptographie à clé publique avec une prise en charge ECC (encodage à courbes elliptiques), qui donne une stratégie plus sûre que les systèmes de cryptographie à clé publique de première génération.

Figure 2. 4x10G OTR à module de chiffrement

Chiffrement 10G hautes performances

Les opérateurs peuvent offrir de façon rentable des services 10G chiffrés en tirant parti d'un transpondeur optique à simple emplacement, 4x10G OTR, à module de chiffrement qui permet une capacité 40G de services chiffrés hautes performances via quatre ports de ligne chiffrés distincts et indépendants du protocole. Ce module conforme à la norme FIPS 140-2 de niveau 3 assure une protection améliorée aux informations sensibles contre les tentatives d'intrusion physique par « zéro-isation » : toutes les données sont remises à zéro dès détection de toute tentative d'intrusion matérielle sur le module de chiffrement, même quand la carte n'est pas branchée dans la baie.

WaveLogic Encryption 100G ou 200G programmable

La solution WaveLogic Encryption de Ciena tire parti de la technologie cohérente WaveLogic, leader du secteur, pour permettre une solution de chiffrement hautes performances, flexible et adaptable sur mesure via le nouveau module de ligne WaveLogic 3 (WL3) Extreme. Le WL3 Extreme repose sur les capacités du WL3 et offre des performances extrêmes pour toutes les applications de mise en réseau cohérent grâce à des schémas de modulation supplémentaires et en réduisant mieux les détériorations, qu'elles soient

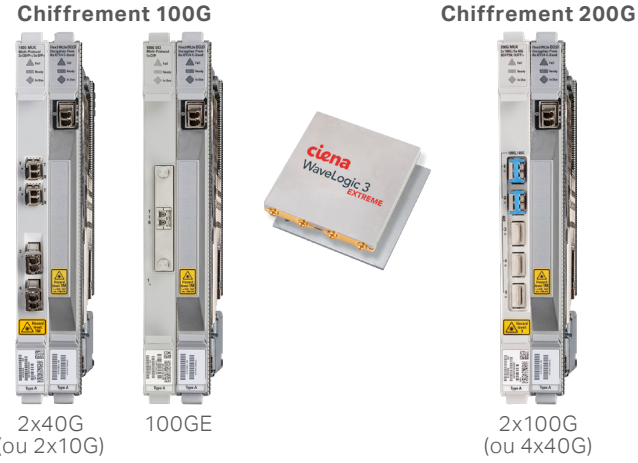


Figure 3. Exemples de chiffrement programmable 100G ou 200G hautes performances avec un module de ligne WL3 Extreme

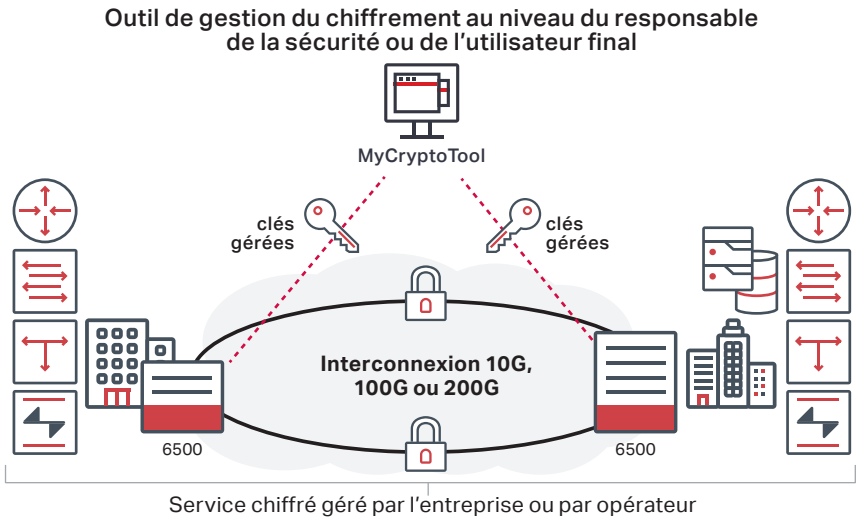


Figure 4. Interface de gestion de chiffrement dédiée MyCryptoTool

Sécurité des données avec un chiffrement optique
Télécharger maintenant l'infographie

linéaires ou non. Cette solution de pointe répond à toutes les exigences de l'infrastructure, depuis le niveau métropolitain jusqu'aux longues distances, et fournit une modulation programmable par logiciel pour permettre à la fois un chiffrement 100G par modulation QPSK et un chiffrement 200G par modulation 16QAM, une première sur le secteur.

En intégrant ce module de ligne WL3 Extreme à n'importe quelle interface client, les opérateurs ont la flexibilité de déployer une solution adaptée sur mesure pour satisfaire leurs besoins spécifiques de trafic, qu'il s'agisse de transport de service 10G, 40G ou 100G. À mesure que la demande augmente, le même module de ligne WL3 Extreme peut être programmé pour transporter 200G de trafic chiffré simplement en ajoutant une autre carte client. De plus, les opérateurs peuvent déployer des services chiffrés de haute capacité à travers le réseau en tirant parti de la matrice haute capacité hybride paquets/OTN du système 6500 et ainsi optimiser l'efficacité des ressources du réseau.

Une gestion du chiffrement simplifiée

La solution WaveLogic Encryption de Ciena comprend MyCryptoTool, une interface dédiée à la gestion du chiffrement conçue pour une gestion distribuée du réseau donnant au responsable de la sécurité, ou à l'utilisateur final, la possibilité de gérer indépendamment les paramètres de sécurité et les alertes des services 10G, 100G ou 200G gérés par l'entreprise ou par opérateur. MyCryptoTool est une interface conviviale qui se connecte en toute sécurité au module de chiffrement et assure une authentification mutuelle, en limitant l'accès au personnel de sécurité autorisé.

La solution WaveLogic Encryption de Ciena combine un haut degré de flexibilité et de sécurité à une facilité d'exploitation et d'administration pour activer une solution rentable de chiffrement 10G/100G/200G, indépendante du protocole, à délai de transit ultra-faible et ainsi sécuriser pratiquement toutes les applications actuelles de communication à l'échelle du web.

Note d'application : Solution de chiffrement hautes performances
Télécharger maintenant

Informations techniques

Pack de circuit	4x10G OTR avec chiffrement	Module de ligne WaveLogic 3 Extreme avec chiffrement
Configuration système requise	Fonctionne dans tous les châssis 6500 de série S ou D	Fonctionne dans tous les châssis 6500 de série S ou D, sauf le 6500-D2
Format des ports **Interfaces client prises en charge**	OC-192/STM-64 LAN 10GbE, WAN 10GbE FC400, FC800, FC1200 OTU2, OTU2e	OC-192/STM-64 LAN 10GbE, WAN 10GbE, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
Interfaces de ligne prises en charge	OTU2 OTU2e	100G cohérent (QPSK) ; 1 port OTU4 200G cohérent (16QAM) ; 2 ports OTU4
Options de protection	Protection de ligne 1+1 Protection client et équipement 1+1	Protection de ligne 1+1 Protection client et équipement 1+1
Modes FEC	RS-8 FEC, UFEC et OFF conformes G.709	FEC souple
Caractéristiques environnementales Température de fonctionnement Humidité relative Altitude	 De +5° C à +40 °C De -5 °C à +55 °C à court terme - pour les 6500-D2/D7/S8/D14/S14 De -5 °C à +50 °C à court terme - pour les 6500-S32 De 5 % à 85 % (sans condensation) 4 000 m ; 13 000 pieds	
Caractéristiques physiques	288 mm (H) x 25 mm (L) x 237 mm (P) 11,34 pouces (H) x 0,99 pouces (L) x 9,34 pouces (P)	
Fonctionnalités de sécurité	• Solution de chiffrement AES-256 certifiée NIST pour le chiffrement des données • Algorithmes ECC (encodage de courbes elliptiques) • Échange de clés sécurisé Diffie-Hellman (comprenant les courbes elliptiques) • Prise en charge du certificat X.509 pour l'authentification • Prise en charge de la liste de révocation des certificats (CRL) • Rotation de clés AES-256 sans à-coups, chaque seconde • Interface mutuellement authentifiée et sécurisée par TLS pour la gestion du chiffrement • Prise en charge d'authentification Radius • TACACS + AAA • Prise en charge SNMPv3	
	• Certificats RSA 2048 bits • Certificats à courbe elliptique	• Certificats à courbe elliptique
Certifications	• Profil de protection collaborative en appareil réseau Common Criteria • BSI (office fédéral allemand pour la sécurité en matière de technologies de l'information) • FIPS 140-2 niveau 3 - certificats n°2379, n°2635 • FIPS 197 - AES–256 - certificats n°2963, n°2964, n°3599, n°3600 • GDPS IBM • EMC, Brocade	• Profil de protection collaborative en appareil réseau Common Criteria • BSI (office fédéral allemand pour la sécurité en matière de technologies de l'information) • FIPS 140-2 niveau 2 - certificats n°2697, n°2843 • FIPS 197 - AES–256 - certificats n°3601, n°3602, n°4231, n°4232, n°5241 • GDPS IBM • EMC, Brocade

Se connecter à Ciena maintenant