cpl.thalesgroup.com

THALES

Protection du réseau SD-WAN

Solutions de chiffrement de bout en bout

Livre blanc

SD-WAN

Les réseaux informatiques s'agrandissent et deviennent de plus en plus dispersés. Avec des endpoints s'étendant sur plusieurs sites, frontières nationales et emplacements distants, les professionnels de l'informatique se tournent vers des systèmes plus sophistiqués afin de les gérer.

Le SD-WAN, ou réseau étendu à définition logicielle (software defined networking), est l'outil idéal. Conçu dans le but de simplifier le déploiement et la gestion de l'infrastructure WAN, ses avantages vont d'une agilité améliorée et d'un routage dynamique à une réduction des coûts et une normalisation des réseaux.

Le SD-WAN est l'un des segments du marché d'infrastructure réseau à la croissance la plus rapide : il devrait atteindre, selon IDC, 5,25 milliards USD d'ici 2023[1].

Le rôle des réseaux de données

D'ici 2023, Gartner prédit que plus de 90 % des initiatives d'actualisation des infrastructures de paramètres de réseau étendu seront basées sur des plateformes virtualisées vCPE (virtualized Customer Premises Equipment) ou des logiciels/appareils SD-WAN[2].

Comme les administrateurs réseau seront en mesure d'appliquer cette couche d'orchestration à distance, le SD-WAN dépend fortement des réseaux de données pour fonctionner correctement.

Alors que l'infrastructure informatique principale, dont les services de sauvegarde et les interconnexions de centre de données, nécessite des réseaux à une vitesse supérieure à 10 GB/s, les réseaux étendus ne fonctionnent généralement qu'à une vitesse de 1 GB/s maximum.

L'un des rôles du SD-WAN est d'optimiser les performances réseau avec le routage dynamique, ce qui signifie que tout logiciel de sécurité et de chiffrement déployé à ses côtés doit être rentable.

La composition de ces réseaux diffère également. Tandis que l'infrastructure principale continue de s'exécuter sur des réseaux privés, un grand nombre d'organisations utiliseront les réseaux publics dans un déploiement de réseau SD-WAN.

Infrastructure sans frontières

Dans le cadre de leur déploiement de SD-WAN, les organisations doivent accepter la réalité de leur infrastructure sans frontières.

Entre la transformation numérique, la demande en agilité et mobilité, et l'augmentation du nombre d'appareils IoT, il n'y a plus de séparation claire entre les réseaux.

Bien que ces tendances offrent de nombreux avantages, elles posent également le problème suivant en matière de sécurité : les réseaux qui sont généralement fermés au monde extérieur s'ouvrent et deviennent vulnérables aux attaques, tandis que chaque point de terminaison ajouté au réseau étendu présente un risque de sécurité supplémentaire.

Menaces sur le réseau SD-WAN

Les technologies de réseau étendu se sont développées au-delà des frontières traditionnelles de l'infrastructure informatique, augmentant le risque et la complexité du réseau.

Alors que les organisations peuvent se focaliser sur la protection des liens haute vitesse dans leur infrastructure réseau principale, elles ne doivent pas oublier de protéger les points de terminaison à l'extérieur du périmètre réseau.

Heureusement, la protection du WAN est une prouesse reconnue par la communauté informatique, avec 72 % des gestionnaires de technologies déclarant que leur plus grande préoccupation vis-à-vis des réseaux étendus est la sécurité[3], au-dessus du coût et des performances.

Le volume grandissant de données circulant dans les réseaux SD-WAN attire l'attention des cybercriminels, qui utilisent tous les moyens afin de les intercepter, des attaques simples de force brute aux techniques plus élaborées.

Une fois qu'ils réussissent à créer un accès, les acteurs malveillants peuvent soit manipuler les informations interceptées, soit les voler à des fins frauduleuses.

Les conséquences d'une fuite de données peuvent aller de la perte d'informations IP ou clients à des pertes financières et des dommages à la réputation.

En plus des menaces existantes, les organisations doivent également avoir connaissance des technologies émergentes, comme l'arrivée de l'ère de l'informatique quantique.

Sécurité du SD-WAN

Tandis que le réseau SD-WAN apporte indéniablement une myriade d'améliorations en matière d'efficacité, cette technologie pose également un risque de sécurité intrinsèque si la communication entre les endpoints n'est pas correctement protégée.

En chiffrant les données en transit dans le réseau SD-WAN, il est possible de garantir l'intégrité des données puisqu'elles seront illisibles, et donc inutilisables, si elles venaient à être volées.

De plus, les organisations doivent trouver une méthode rentable pour protéger les données WAN en transit, le déploiement d'un chiffrement matériel sur chaque endpoint n'étant pas une solution viable financièrement.

Ce livre blanc analyse les menaces existantes pour les organisations qui déploient un réseau SD-WAN, explique l'importance du chiffrement des données en transit et donne des conseils pour sélectionner la solution de chiffrement appropriée.

1 Prévisions concernant les infrastructures SD-WAN, IDC, juillet 2019

2 Magic Quadrant de Gartner pour l'infrastructure de périmètre de réseau étendu, par l'intermédiaire de SDxCentral

3 Analyse d'enquête Gartner : Répondre aux inquiétudes de sécurité et des systèmes numériques pour conserver une croissance rapide pour son réseau SD-WAN, par l'intermédiaire de Fortinet

Pourquoi chiffrer ses données ?

En utilisant des réseaux privés et publics plutôt que de faire confiance à des réseaux MPLS isolés par exemple, les données transmises entre les points de terminaison par le biais du SD-WAN sont vulnérables aux attaques.

Des technologies de prévention telles que les pare-feux garantissent que les données inactives sont protégées, mais elles restent exposées lorsqu'elles sont en transit.

Afin de garantir la sécurité et l'intégrité des données transmises, les organisations doivent agir pour les protéger contre des menaces très variées.

Topographie des fuites de données

Tandis que les fuites de données se produisent dans toutes les industries, elles sont le plus fréquentes dans les secteurs de la technologie, des réseaux sociaux, du commerce de détail et gouvernemental, en raison de la quantité et la composition des données échangées.

Les entreprises mettent en moyenne 197 jours pour identifier une fuite de données, et 69 jours supplémentaires pour la maîtriser[4]. Parmi les conséquences de fuites de données :

- Vol de propriété intellectuelle
- Perturbation des opérations
- Problèmes de conformité
- Perte de données client
- Infractions de confidentialité
- Pertes financières

De plus, les entreprises doivent réagir face à la perte de réputation et de confiance des parties prenantes, une perte qui est très difficile à chiffrer.

Tendances et menaces émergentes

En plus des menaces existantes, les organisations doivent avoir connaissance des technologies qui gagnent en popularité et celles qui sont sur le point d'arriver.

La croissance des déploiements de SD-WAN est en elle-même un domaine de grand intérêt, avec un taux de croissance composé annuel du marché estimé à 40,4 % d'ici 2022[5].

Lorsqu'ils sont interrogés sur les raisons principales pour lesquelles ils utilisent la technologie SD-WAN, les leaders du domaine de l'infrastructure et l'optimisation indiquent quatre motivations clés : augmenter la disponibilité (41 %), augmenter les performances/la fiabilité (41 %), réduire les coûts récurrents des réseaux étendus en utilisant des moyens de transports plus économiques (38 %) et gagner en agilité (36 %)[6].

De plus, 64 % des augmentations de budget informatique sont motivées par le besoin de mettre à jour une infrastructure informatique obsolète[7].

La croissance rapide des dispositifs IoT et l'introduction d'infrastructures sans frontières par défaut ont également un impact considérable sur la sécurité des données. En ne parvenant pas à protéger leurs appareils dans le périmètre réseau (couches 3 et 4), les organisations donnent aux hackers l'opportunité d'accéder aux réseaux et de collecter des données sensibles ou d'introduire des données frauduleuses.

Le nombre de vols de métadonnées (données concernant les données) a également considérablement augmenté. Malgré les idées reçues, ces données sont sensibles et peuvent fournir une source riche de données exploitables, si elles ne sont pas chiffrées correctement.

L'arrivée de l'ère quantique joue également un rôle de plus en plus important dans la cybersécurité. Tandis que les capacités de calcul incommensurables des ordinateurs quantiques transformeront le secteur informatique, il existe également le risque que cette technologie soit utilisée à mauvais escient.

Les ordinateurs quantiques pourront craquer les normes de chiffrement AES actuelles en une fraction du temps nécessaire pour les ordinateurs traditionnels, menaçant les protocoles sur lesquels repose la sécurité des données mondiale.

Bien que cette préoccupation semble lointaine, elle est en réalité bien plus proche qu'on ne le croit. Selon les estimations, un ordinateur quantique capable de craquer les codes du chiffrement actuel sera disponible dans les 10 prochaines années, ce qui signifie que les organisations doivent introduire des méthodes de chiffrement adaptées à l'informatique quantique dès maintenant, sous le risque de compromettre l'intégrité de leurs données.

Protection et prévention

Beaucoup d'organisations pensent à tort qu'un pare-feu solide suffit à prévenir les accès non autorisés à leur réseau. Une autre idée erronée qu'elles partagent est que les réseaux privés et les hébergeurs sont sécurisés par nature.

Malheureusement, ce n'est pas le cas. Tandis que le pare-feu peut détecter et éliminer une variété de tentatives de pénétration ou d'attaques par déni de service, il n'offre aucune protection contre les tentatives d'interception physiques, que ce soit à l'intérieur ou à l'extérieur du pare-feu.

La seule solution fiable pour garantir que les données sont sécurisées lorsqu'elles sont en mouvement dans le réseau est le chiffrement. De plus, votre solution de chiffrement doit être séparée de toute architecture réseau spécifique et conforme aux normes de sécurité reconnues à l'international.

4 Étude sur le coût d'une fuite de données 2018 – Ponemon Institute

5 Prévisions concernant les infrastructures SD-WAN, IDC

6 Gartner Technology Insight pour le SD-WAN

7 L'état de l'informatique en 2019, Spiceworks

Protection du réseau SD-WAN

En interceptant les données en transit traversant les réseaux utilisés par une solution SD-WAN, les hackers peuvent contourner les systèmes en place autour des données au repos.

Dès qu'ils réussissent à accéder au réseau, les cybercriminels peuvent intercepter et voler les données qui circulent entre le point de départ et le point de terminaison. En obtenant un accès indésirable, les hackers peuvent également introduire des données frauduleuses dans le réseau, compromettant l'intégrité des données et de la plateforme dans son ensemble.

Les administrateurs réseau doivent prendre des mesures pour protéger ces données en mouvement, tout en assurant une performance optimale du réseau.

Chiffrement de bout en bout

Le chiffrement est vital pour le réseau SD-WAN et doit faire partie des solutions de sécurité choisies par la communauté informatique. De plus, il doit être déployé en tant que solution de bout en bout.

Autre critère important, cette solution de chiffrement de bout en bout doit également être indépendante des couches de transport réseau, permettant un déploiement sur toutes les couches du réseau (couches 2, 3 et 4), étendant ainsi le paramètre virtuel. Elle doit aussi protéger les métadonnées accompagnant les paquets de données principaux.

En cas de fuite de données, les données chiffrées interceptées par les hackers sont illisibles, et donc inutilisables. De plus, la confidentialité persistante fournie par les solutions de chiffrement empêche l'introduction de données frauduleuses dans les systèmes.

Le chiffrement des données facilite également la vie des organisations vis-à-vis de la conformité, les règlementations sur la protection des données comme le RGPD faisant une distinction entre les fuites de données considérées comme « sécurisées » et celles qui ne le sont pas ; les entreprises peuvent ainsi échapper à des amendes lourdes en prouvant qu'elles attachent une grande importance à la protection des données sensibles qu'elles collectent.

Performance des réseaux et des applications

Il est crucial que la solution de chiffrement n'ait pas un impact négatif sur la vitesse ou la performance des réseaux.

Toute augmentation de la latence aura un impact sur la performance du réseau étendu. C'est un problème que la solution SD-WAN tente d'améliorer par le biais du routage dynamique.

Autre préoccupation d'importance égale, certaines organisations optent pour des technologies de chiffrement « bas de gamme » qui semblent être efficaces, mais ne sont pas sans conséquences :

- Performance réseau réduite
- Coûts cachés dus à la perte de bande passante

Choisir la solution de chiffrement appropriée

Lors de la sélection du fournisseur de solution de chiffrement pour votre réseau SD-WAN, il est important de prendre en compte toutes les applications. Il est tout aussi important de comprendre que toutes les solutions de chiffrement n'offrent pas la même qualité.

Par nature, le SD-WAN voit un mouvement des données des appareils dans le réseau ; les données doivent donc être protégées tout au long de leur circulation.

Les appareils de chiffrement dits « hybrides », tels que les routeurs/commutateurs réseau avec chiffrement intégré ou ceux utilisant une norme MACSec ou similaire (non adaptée à la sécurité des réseaux WANs), offrent une protection des données à niveau d'assurance faible.

Pendant ce temps, les réseaux MPLS n'ont plus la cote, en raison des avantages que les réseaux SD-WAN offrent en comparaison en terme de coûts et d'efficacité.

La plupart des infrastructures modernes sont constituées de plusieurs couches réseau, avec généralement des éléments de couches 2, 3 et 4. Les organisations doivent donc trouver un fournisseur qui propose une solution de chiffrement qui tient compte des différentes couches, si possible.

Le facteur coût est également à prendre en compte lors du chiffrement du trafic WAN. La protection de chaque lien réseau avec un chiffrement matériel dédié n'est pas une solution économique.

Tandis que le chiffrement matériel (comme la série CN de dispositifs de chiffrement haute vitesse Thales) doit être utilisé pour protéger l'infrastructure informatique principale et l'infrastructure réseau, les organisations doivent penser à protéger leur CPE virtuel et leur réseau étendu virtualisé avec un chiffrement virtualisé.

La série de chiffreurs virtualisés haute vitesse (HSE) CV de Thales offre un chiffrement multicouches simultané et une prise en charge de la technologie DPDK pour une performance jusqu'à 5 GB/s.

Tout comme les chiffreurs matériels de la série CN, notre chiffrement virtualisé prend en charge toutes les topologies, de P2P à Hub & Spoke (réseau en étoile), ainsi que les réseaux entièrement maillés. C'est l'application idéale à déployer avec un réseau SD-WAN.

Le chiffrement virtualisé de la série CV est également très rentable. Il élimine le besoin de déployer un grand nombre de chiffreurs matériels et peut être déployé en toute simplicité en tant qu'implémentation logicielle, avec un approvisionnement « zéro contact ».

Chiffreur virtuel Thales CV1000

Le modèle CV1000 est un dispositif VNF (fonctions réseau virtualisées) fournissant une sécurité de chiffrement des données solide et efficace avec crypto-agilité intégrée. Conçu pour les virtualisations à grande échelle, le CV1000 propose un chiffrement qui tient compte des couches de transport pour les réseaux haute vitesse au-dessus de 1 GB/s.

En tant que dispositif VNF, le CV1000 se démarque de ses concurrents. L'évolutivité instantanée permet un déploiement rapide sur des milliers de liens réseau. Il offre la même flexibilité et la même évolutivité que d'autres fonctions réseau virtualisées.

Le CV1000 fournit une sécurité de chiffrement et une gestion de clé de pointe, sans impact négatif sur les performances de réseau ou d'applications*. Contrairement aux solutions de chiffrement de type IPSec, le CV1000 est transparent sur le réseau, ce qui en fait l'outil idéal pour protéger votre réseau étendu, jusqu'au paramètre virtuel.

Comment le CV1000 est-il implémenté ?

Le CV1000 est une machine virtuelle invitée qui s'exécute sur les hôtes et hyperviseurs x86 standard de l'industrie.

Les clients de réseau étendu à grande échelle n'ont pas besoin d'opérer la virtualisation réseau afin d'implémenter le CV1000 en tant que solution de sécurité sécurisée et efficace.

Comme toutes les machines virtuelles, les performances du CV1000 est spécifique aux objectifs du client et dépend de l'environnement et de la plateforme d'exploitation. Les spécifications d'implémentation sont donc présentes à titre de référence uniquement.

- Matériel x86 qui tient compte du fournisseur
- Configuration d'hôte minimum requise :
  - Nombre de noyaux : 3
  - RAM : 2 GB
  - Stockage de disque virtuel : 2 GB
- Prise en charge de l'accélération de paquets des bibliothèques Intel du DPDK :permet des performances de bande passante supérieures à 1 GB/s et jusqu'à 5 GB/s.

Parmi les plateformes prises en charge par le CV1000 :

- VMware
- KVM/QEMU
- Microsoft Hyper-V

Parmi les autres fonctionnalités et technologies prises en charge par le CV1000 :

- Interopérabilité avec tous les chiffreurs matériels de la série de HSE CN
- ransport Independent Mode : chiffrement multicouches simultané (couches 2, 3 et 4)
- Chiffrement symétrique et asymétrique
- Sentinel : pour une gestion des licences simplifiée
- Interfaces virtualisées : cartes réseau para-virtualisées x3

CV1000 : avantages clés

Parmi les avantages inégalés du CV1000 décrits par les utilisateurs finaux et les fournisseurs de services :

- Le CV1000 permet l'adoption d'une solution de chiffrement virtualisée qui n'a aucun impact négatif sur la sécurité ou les performances de réseau et d'application
- Évolutivité instantanée afin de prendre en charge l'ampleur et la flexibilité des réseaux virtuels et à définition logicielle
- Ne requiert pas de déployer un grand nombre d'appareils de chiffrement matériel pour obtenir une implémentation à grande échelle du chiffrement réseau.
- Le modèle de sécurité de chiffrement et de gestion de clé du CV1000 est optimisé pour une sécurité du chiffrement solide et efficace.
- Grâce au mode indépendant au transport, le CV1000 convient aux environnements réseau multicouches
- Compétitif, le CV1000 fournit une performance jusqu'à 30 % supérieure aux autres solutions
- Simplicité de déploiement avec approvisionnement centralisé, « zéro contact »
- 100 % d'interopérabilité avec les chiffreurs de la série de HSE CN
- En tant qu'implémentation logicielle de la plateforme de chiffrement à niveau d'assurance élevé Thales, le CV1000 fournit une méthode flexible et rentable pour le chiffrement intégral, jusqu'au paramètre virtuel.
- Les fournisseurs de services de centre de données ont désigné le CV1000 comme solution idéale, offrant une sécurité de chiffrement solide et efficace pour les appareils contenus dans le centre de données même.

Performance optimale

Accélération DPDK : performance jusqu'à 5 GB/s

Les bibliothèques Intel du DPDK permettent une accélération des performances de l'appareil hôte x86. Si l'appareil hôte x86 et le DPDK sont configurés de manière optimale, le CV1000 fournira des performances améliorées supérieures à 1 GB/s et jusqu'à 5 GB/s.

La performance continue jusqu'à 5 GB/s dépend de la configuration de l'hôte et de l'expertise en matière d'installation et de configuration du DPDK.

Les facteurs environnementaux et architecturaux peuvent également jouer un rôle dans les performances du chiffrement virtualisé, tout comme ils ont un impact sur les performances des réseaux virtualisés.

Transport Independent Mode : chiffrement multicouches simultané

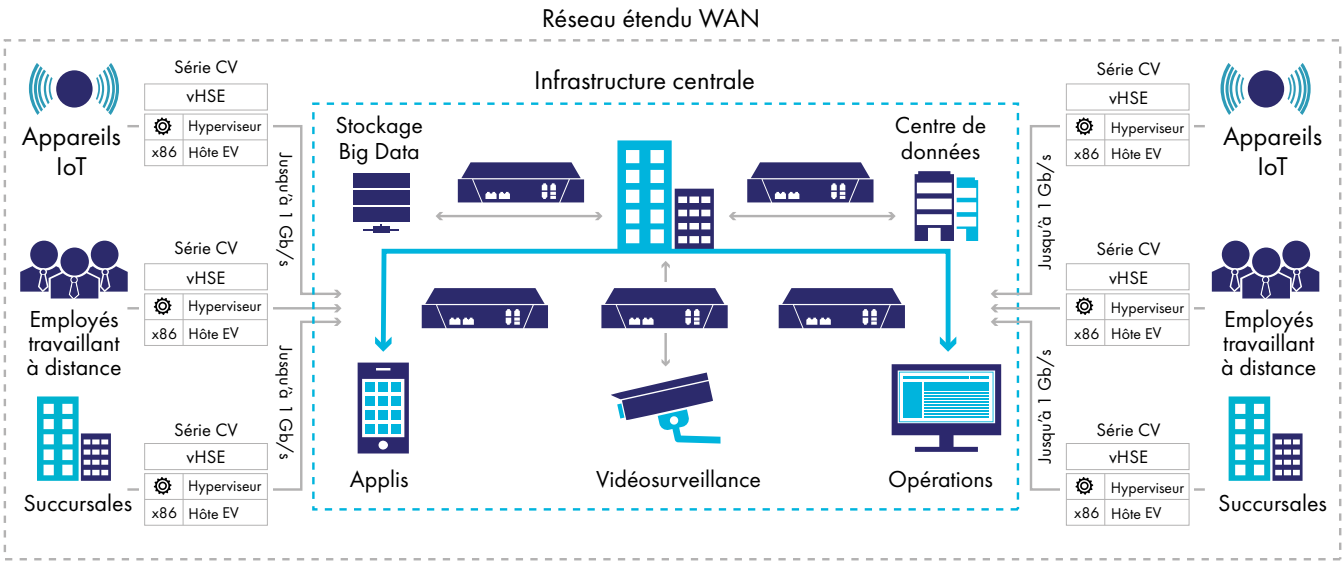
De nombreuses organisations utilisent plusieurs protocoles de couches pour les réseaux de données (couches 2, 3 et 4) pour les aider à fournir leurs applications d'entreprise et services de communication. Dans cette optique, Thales a conçu un mode indépendant au transport (Transport Independent Mode ou TIM) intégré.

Cette technologie de chiffrement avancée qui tient compte des couches de transport permet un chiffrement multicouches simultané basé sur les politiques de destination.

Plus important, les clients ont toujours la garantie d'un chiffrement de bout en bout solide pendant la circulation des données protégées d'une couche réseau à l'autre, par exemple de l'Ethernet en couche 2 au réseau IP en couche 3.

Exemples de cas d'utilisation du CV1000 de Thales

Protection du réseau étendu jusqu'au paramètre virtuel (déploiements WAN à grande échelle)



Le cas d'utilisation le plus courant pour le chiffrement des données de réseau virtualisé est le déploiement sur un WAN étendu. Le client peut ou non adopter la virtualisation de l'environnement réseau même, mais il recherchera les avantages suivants :

- Utilisation efficace des ressources informatiques et réseau physiques
- Augmentation de la réactivité et de la flexibilité
- Coût du chiffrement par lien réseau réduit
- Surmonter les contraintes du déploiement d'actifs physiques sur les réseaux à grande échelle
- Une solution qui tient compte des couches de transport : sécurité réseau multicouches (couches 2, 3 et 4)

Ayant choisi une solution de réseau virtualisée pour son réseau étendu à grande échelle, le client soucieux de la sécurité envisage désormais les solutions de sécurité du chiffrement.

De la même manière que le client utilise des liens réseau Ethernet de couche 2 parmi ses actifs d'infrastructure principale, il est probable qu'il protège ces liens avec des chiffreurs matériels (comme illustré). Pour protéger les données circulant dans le réseau plus étendu, une solution de sécurité de chiffrement virtualisée peut être plus appropriée :

- Offre la possibilité d'évoluer rapidement
- Simplifie le déploiement par le biais d'une implémentation logicielle
- Permet une sécurité solide et efficace à un coût par lien réduit

Le CV1000 tenant compte des couches de transport, il fournit une sécurité de chiffrement multicouches (couches 2, 3 et 4) simultané basé sur les politiques de destination.

Les environnements clients peuvent inclure :

- Un hôte x86 haute performance à plusieurs noyaux (le nombre minimum de noyaux recommandé est de 4) pour le CV1000
- Accélération de paquets des bibliothèques Intel du DPDK
- Liens réseau multicouches (couches 2, 3 et 4)
- VMware ou environnement de virtualisation similaire
- Chiffreurs matériels de la série CN utilisés pour l'infrastructure réseau Ethernet principale : 100 % d'interopérabilité avec le CV1000

Un problème important posé par la croissance des systèmes d'entreprise est l'infrastructure nécessaire pour sa prise en charge. Les organisations comprennent que les systèmes nécessaires pour accompagner leur croissance n'ont pas besoin d'être physiques. La virtualisation de certains actifs physiques offre des avantages considérables en ce qui concerne le coût et l'utilisation. Le réseau en est un parfait exemple.

À propos de Thales

Les personnes à qui vous faites confiance pour protéger votre vie privée font confiance à Thales pour protéger leurs données. En matière de sécurité des données, les entreprises sont confrontées à un nombre croissant de moments décisifs. Qu'il s'agisse de mettre en place une stratégie de chiffrement, de passer au cloud ou de respecter les obligations de conformité, vous pouvez compter sur Thales pour sécuriser votre transformation numérique.

Une technologie décisive pour des moments décisifs.

THALES

Contactez-nous

Retrouvez nos coordonnées sur notre site Internet cpl.thalesgroup.com/fr/contact-us

> cpl.thalesgroup.com <

© Thales - juin 2020 • RMv4