CLES POUR UN DEPLOIEMENT : COMPARAISON ENTRE LES SERVEURS DE SECURITE UNIFIES ET DEDIES

CISCO ASA 5500, CISCO PIX, CISCO IPS 4200 OU CONCENTRATEUR CISCO VPN 3000 ? COMMENT CHOISIR ?

Cisco Systems® propose des solutions de sécurité personnalisables qui répondent aux exigences de n'importe quel environnement de déploiement. Avec sa nouvelle gamme ASA 5500, Cisco élargit encore ce choix grâce à des serveurs de sécurité adaptatifs capables de fournir sur une même plate-forme matérielle des services de sécurité et de connectivité VPN convergents. Leur éventail diversifié de services convergents – pare-feu, prévention des intrusions (IPS) et anti-virus de réseau – donne à l'utilisateur les moyens de déployer une solution élargie de Défense adaptative contre les menaces. Conçue pour les services VPN, la gamme Cisco ASA 5500 met à votre disposition des technologies souples qui réalisent des solutions sur mesure parfaitement adaptées aux besoins des connexions à accès distant et de site à site.

Chaque serveur de la gamme Cisco ASA 5500 est doté de ces services VPN et de sécurité, et une même unité peut remplir plusieurs fonctions. Sur le site central, elle peut être déployée en tant qu'unité convergente de prévention contre les menaces grâce à ses multiples technologies de contrôle d'accès, d'inspection des applications et de défense contre les vers, les virus et autres logiciels malveillants. Avec ses fonctionnalités VPN IPSec (IP Security) et SSL (Secure Sockets Layer), elle devient un serveur dédié d'accès distant. Sur le réseau interne, elle joue le rôle de passerelle de contrôle d'accès entre les services et assure une protection contre les vers, les virus et les logiciels malveillants que vos utilisateurs pourraient introduire à leur insu. Dans les environnements des petites sociétés ou des agences d'entreprise, les serveurs dédiés de la gamme Cisco ASA 5500 réalisent une solution «tout en un» de services VPN et de prévention complète contre les menaces et s'adaptent aux budgets et aux modèles opérationnels de ces déploiements.

Quels sont les facteurs de déploiement qui privilégient une unité multifonction de type Cisco ASA 5500 par rapport aux serveurs de sécurité «dédiés» comme Cisco PIX®, les unités de la gamme Cisco IPS 4200 ou les concentrateurs de la gamme Cisco VPN 3000 ? Dans ce livre blanc, nous explorons les raisons fonctionnelles, opérationnelles et économiques qui justifient le choix d'un serveur de sécurité multifonction par rapport à un serveur dédié. Le choix du déploiement entre un serveur convergent sécurité / VPN et un routeur Cisco sort du cadre du présent article, mais le lecteur trouvera une analyse détaillée de ce sujet dans le livre blanc «Positioning Integrated Router Security and Dedicated Security Appliances» disponible sur Cisco.com.

LES FAMILLES DE SERVEURS DE SECURITE DEDIES CISCO

Pour protéger les réseaux de ses clients, Cisco propose des solutions serveurs déclinées en quatre gammes : Cisco PIX, les serveurs Cisco IPS 4200, les concentrateurs Cisco VPN 3000 et les serveurs de sécurité Cisco ASA 5500. Chacun de ces produits offre une solution adaptée à un large éventail de déploiements et d'entreprises, depuis les petits bureaux jusqu'au site du siège social de l'entreprise, et des PME/PMI jusqu'aux géants multinationaux. De plus, les serveurs de sécurité Cisco PIX offrent des solutions qui s'adaptent parfaitement aux environnement des petits bureaux et des bureaux à domicile, ce que nous appelons SOHO (Small Office and Home Office). Voici un descriptif rapide des fonctionnalités de chaque produit et de leurs scénarios de déploiement.

Serveur de sécurité dédié Cisco PIX

Leader de son marché, la gamme des serveurs de sécurité dédiés Cisco PIX® offre, grâce à ses solutions économiques et faciles à déployer, des services robustes de pare-feu sensible aux applications et de connectivité VPN, la protection multi-niveaux contre les attaques et des services sécurisés de connexion de site à site.

Sondes de sécurité Cisco IPS 4200

Les sondes de la gamme Cisco IPS 4200 protègent le réseau contre les attaques, les vers et les virus avant qu'ils puissent affecter vos données et vos ressources. Les sondes Cisco IPS réalisent une protection efficace de votre réseau en contribuant à la détection, à l'évaluation et au blocage des logiciels dangereux – vers, logiciels espions ou publicitaires, virus de réseau, etc. – et l'utilisation abusive des applications.

Concentrateurs de la gamme Cisco VPN 3000

Les concentrateurs de la gamme Cisco VPN 3000 sont des solutions de VPN à accès distant SSL et IPSec parmi les meilleures du marché. Intégrant un client VPN normalisé et facile à utiliser ainsi que des unités évolutives de raccordement des tunnels VPN, ils possèdent un système de gestion qui permet à l'entreprise d'installer, de configurer et de surveiller en toute simplicité ses VPN à accès distant.

Serveurs de sécurité adaptatifs Cisco ASA 5500

La gamme Cisco ASA 5500 réunit les plus récentes avancées en matière de technologies de sécurité et notamment les solutions éprouvées de Cisco en matière de pare-feu, de prévention des intrusions, d'antivirus réseau et de VPN. Equipés d'un progiciel de gestion unifiée et conçus pour des performances exceptionnelles, les serveurs de la gamme Cisco ASA 5500 sont faciles à administrer et fournissent aux grandes entreprises comme aux PME/PMI des services simultanés à haut débit.

COMPARAISON DES CARACTERISTIQUES ET DES FONCTIONS

La gamme Cisco ASA 5500 réunit, sur une même unité et dans une même architecture de gestion, les ensembles de fonctionnalités réputés des plates-formes Cisco PIX, IPS 4200 et VPN 3000 ainsi que les solutions antivirus de Trend Micro. La convergence ainsi réalisée offre des possibilités nouvelles comme la capacité de protéger les connexions VPN à distance contre les vers, les virus et les logiciels malveillants, une large protection contre ces mêmes menaces sur l'ensemble du périmètre et de l'intérieur de réseau, sans oublier des fonctions évoluées d'inspection et de contrôle des applications. En fait, et grâce à l'éventail hautement convergent de ses services coordonnés, la gamme Cisco ASA 5500 offre souvent un sur-ensemble des fonctionnalités proposées par les autres serveurs de sécurité et VPN dédiés de Cisco.

L'ampleur des fonctions de limitation des menaces offertes par une seule unité de la gamme Cisco ASA 5500 assure également une plus grande protection contre les attaques, quel que soit l'endroit où elle est déployée – dans un bureau distant, sur la zone démilitarisée du siège social ou à l'intérieur même du réseau. La protection contre les vers, les virus et les logiciels malveillants de même que la sécurité des applications s'applique ainsi dans des zones comme les sites distants ou l'intérieur du réseau qui, pour des raisons économiques ou de faisabilité sont généralement négligées. De ce point de vue, la gamme Cisco ASA 5500 améliore les défenses générales du réseau et renforce du même coup l'ensemble de la chaîne de sécurité.

En ce qui concerne l'intégration avec les déploiements existants, la gamme Cisco ASA 5500 est pleinement compatible avec toutes les installations Cisco PIX, IPS 4200 et VPN 3000 dont peut disposer l'entreprise. Comme nous l'avons mentionné plus haut, tous ces serveurs ont été construits autour des mêmes technologies éprouvées, avec pour conséquence de faire pratiquement disparaître les disparités fonctionnelles entre les unités de la gamme ASA 5500 et les autres produits dédiés. Mieux encore, le personnel chargé du déploiement de la gamme ASA 5500 peut s'appuyer sur la formation dont il dispose déjà et sur sa connaissance des produits PIX, IPS 4200 et VPN 3000. Le Tableau 1 décrit l'environnement et les fonctionnalités applicatives de chaque plate-forme :

Tableau 1. Comparaison fonctionnelle

	Application	Services complémentaires propres à ASA
Cisco ASA 5500 et Cisco PIX	• Serveur ASA destiné aux environnements PIX 515E et 525 classiques • Complète les PIX 501, 506E et 535 pour les SOHO et les sièges sociaux des grandes entreprises	• Services complets de prévention des intrusions • Prévention des vers et des virus • Antivirus de réseau • Inspection approfondie des applications • Groupement des VPN • Emplacement modulaire pour les services
Cisco ASA 5500 et IPS 4200	• Serveur ASA orienté pare-feu convergent et prévention des intrusions (IPS) • IPS 4200 est optimisé et particulièrement économique pour les déploiements IPS seuls	• Pare-feu complet • Services VPN complets • Emplacement modulaire pour les services
Cisco ASA 5500 et Cisco VPN 3000	• Serveur ASA destiné aux services VPN IPSec à accès distant et de site à site pour tous les sites • Serveur ASA interopérable avec les groupements VPN 3000 • VPN 3000 optimisé pour les déploiements VPN SSL	• Débit trois fois supérieur • Reprise des VPN avec inspection d'état • QOS et OSPF pour les VPN de site à site • VPN «propres» avec protection contre les vers, les virus et les logiciels malveillants

L'ARCHITECTURE DE SECURITE ET L'ORGANISATION DU SERVICE INFORMATIQUE

La taille, le modèle opérationnel et la segmentation du réseau ont une influence sur le choix d'une plate-forme de sécurité et de connectivité VPN. Dans certains scénarios, la consolidation de multiples fonctions de sécurité et de connectivité VPN sur un même équipement répond très exactement aux besoins, alors que dans d'autres, il est préférable de dédier un équipement à une tâche spécifique.

Si l'on considère leur taille, les réseaux des grandes entreprises acheminent un trafic si volumineux et si complexe qu'ils exigent souvent le déploiement d' équipements dédiés. Une infrastructure de sécurité et de connectivité VPN appuyée sur des équipements qui exécutent des fonctions spécialisées, voire uniques, permet une évolutivité optimale, simplifie le choix des versions logicielles et les cycles de mise à niveau, et permet un ajustement précis des configurations ainsi qu'une meilleure segmentation du réseau. D'un point de vue opérationnel, le déploiement d' équipements dédiés autorise également la répartition des responsabilités de sécurité sur le réseau entre les différentes équipes informatiques.

Voici quelques exemples classiques de segmentations fonctionnelles qui exigent des équipements dédiés de sécurité et de connectivité VPN :

- le déploiement dé équipements dédiés de VPN à accès distant,
- le déploiement d' équipements dédiés de prévention des intrusions pour faciliter les audits des politiques de sécurité et la conformité à la réglementation, ou encore la répartition des responsabilités informatiques organisationnelles,
- les déploiements haute vitesse des centres de calcul pour la protection des fermes de serveurs Web et de serveurs d'applications,
- les pare-feu de périphérie de réseau pour l'inspection du trafic et le contrôle d'accès résilients et à haute vitesse.

Pour les organisations et les réseaux de plus petite taille, le contraire est généralement vrai. Sur les petits réseaux, comme ceux des petites sociétés et des bureaux distants, ainsi que dans les petites organisations informatiques, on a tendance à regrouper autant de fonctions de sécurité et de connectivité VPN qu'il est possible sur le plus petit nombre d' équipements. La limitation du nombre d'équipement réduit la complexité du réseau et la somme des connaissances que l'équipe informatique doit maîtriser pour gérer un système composé de plusieurs plates-formes uniques. En soi et de manière générale, la consolidation des unités simplifie les opérations des sites qui ne disposent que d'une petite équipe informatique, souvent moins spécialisée dans le domaine de la sécurité.

Les grandes qualités de flexibilité de la gamme Cisco ASA 5500 en font une solution idéalement adaptée à la plupart des scénarios qui exigent des fonctions dédiées ou consolidées. Avec son vaste éventail de services VPN et de sécurité, elle permet de réunir sur un même appareil de multiples solutions. Les serveurs de la gamme Cisco ASA 5500 peuvent être déployés sur le site central en tant qu'unités convergentes de prévention contre les menaces grâce à leurs multiples technologies de contrôle d'accès, d'inspection des applications et de défense contre les vers, les virus et autres logiciels malveillants. Vous pouvez les installer en périphérie de réseau comme des pare-feu classiques ou comme des unités dédiées d'accès distants en exploitant leurs fonctionnalités VPN. Dans les environnements des petites sociétés ou des agences d'entreprise, ils réalisent une solution «tout en un» de services VPN et de prévention complète contre les menaces et s'adaptent aux budgets et aux modèles opérationnels de ces déploiements.

Dans les déploiements de prévention des intrusions, comme les environnements où le système IPS doit fournir des données pour l'audit des politiques de sécurité et la conformité aux réglementations, les plates-formes de la gamme Cisco IPS 4200 demeurent le choix idéal. Cette infrastructure d'audit offre une vision de type «contrôle et équilibrage» pour la sécurisation et la validation de l'état du réseau tout en assurant une protection polyvalente contre les attaques, les vers, les virus et les logiciels publicitaires ou malveillants, qui se superpose aux équipement d'application des politiques. De plus, et comme il est courant de dissocier les équipes informatiques qui gèrent les systèmes IPS et celles chargées des autres fonctions de sécurité – les pare-feu, notamment – l'organisation qui gère l'infrastructure IPS préfère généralement disposer d' équipements dédiés.

Pour le déploiement de VPN SSL, les concentrateurs de la gamme Cisco VPN 3000 offrent les fonctions les plus évoluées comme Cisco Secure Desktop pour la sécurité des points d'extrémité, Clientless Citrix et la tunnellisation des VPN SSL pour un accès complet au réseau et aux applications. Dans les environnements où les VPN SSL sont la principale application, le concentrateur VPN 3000 demeure la plate-forme de prédilection.

LE COUT DES PLATES-FORMES ET DE LEUR EXPLOITATION

Coût des plates-formes

Dans la plupart des cas, les fonctionnalités convergentes de la gamme Cisco ASA 5500 coûtent autant, voire moins qu'un serveur dédié analogue des gammes Cisco PIX ou VPN 3000. Le prix de l'appareil n'a donc pas d'incidence particulière sur le choix d'une solution convergente du type Cisco ASA 5500, ou dédiée, du type Cisco PIX ou VPN 3000. La décision doit s'appuyer sur la comparaison des fonctionnalités offertes par les produits ainsi que sur l'architecture de sécurité et le modèle opérationnel de l'organisation, comme nous l'avons fait ci-dessus.

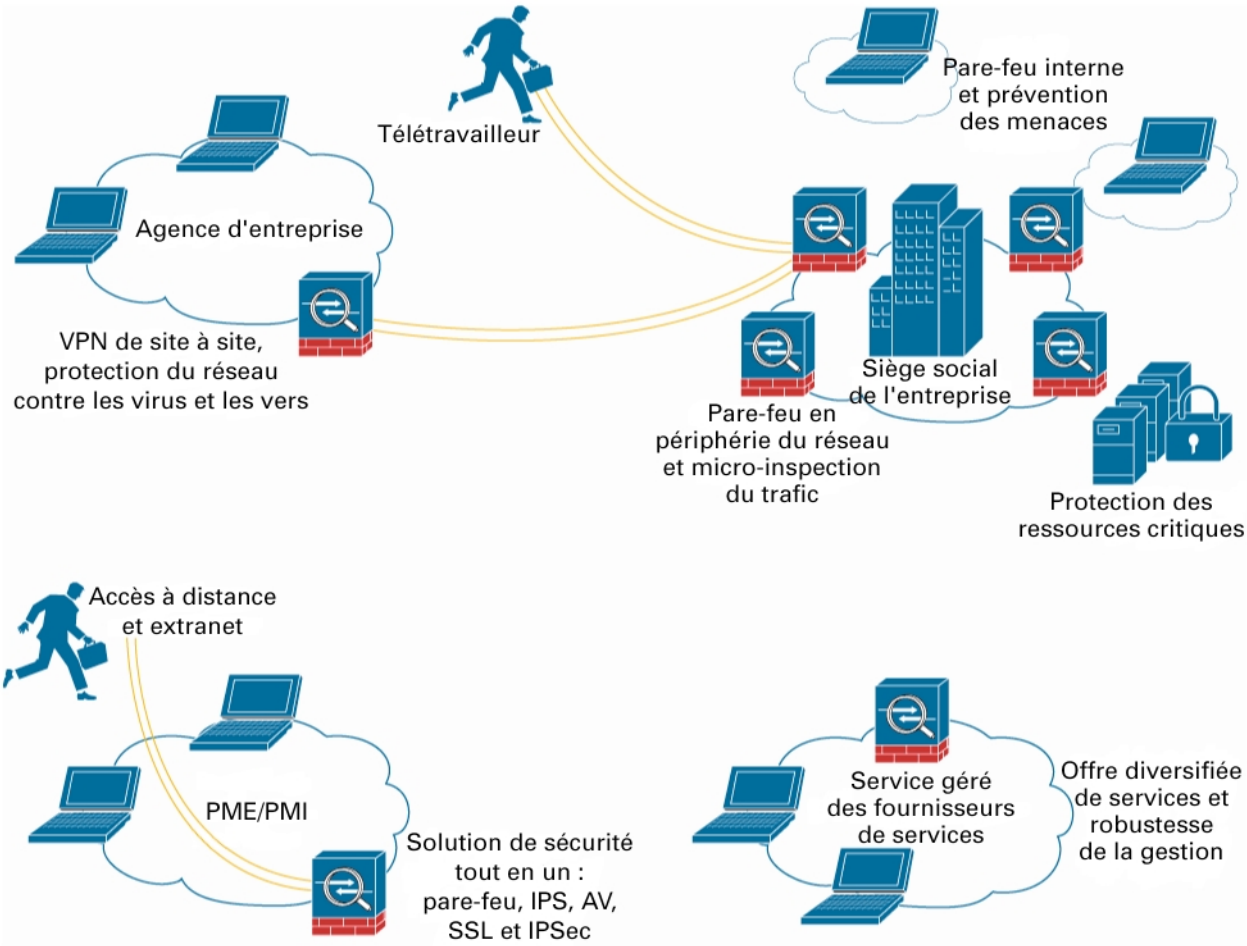
Pour les déploiements IPS purs, les serveurs de la gamme Cisco IPS 4200 offrent un rapport coût / performances plus intéressant que ceux de la gamme Cisco ASA 5500. Cette dernière est optimisée pour de larges fonctions de protection contre les menaces et de sécurité des applications offertes par la convergence de son pare-feu, de son système IPS et de son antivirus de réseau, tandis que la gamme IPS 4200 est spécifiquement conçue pour les environnements IPS spécialisés.

Pour les petits bureaux et les télétravailleurs (SOHO), les pare-feu des grandes sociétés ou encore le déploiement de VPN de site à site, les serveurs de sécurité Cisco PIX 501, PIX 506E et PIX 535 sont incontestablement les plates-formes les plus économiques. La gamme Cisco ASA 5500 est conçue pour les applications de services convergents sur les sites de petite taille. Si vous avez besoin d'une partie des fonctions de protection contre les menaces ou encore d'une connectivité VPN pure, les serveurs Cisco PIX 501 et PIX 506E sont plus économiques pour les sites de type SOHO. Le serveur de sécurité haut de gamme Cisco PIX 535 offre quant à lui des performances particulièrement élevées à 1,7 Gbits/s, et offre le meilleur rapport coûts / performances de la gamme Cisco ASA 5500. De plus, comme nous l'avons déjà dit, les fonctionnalités des produits Cisco ASA 5500 et Cisco PIX sont pleinement compatibles, car ces appareils sont prévus pour travailler ensemble, en fonction des besoins de l'architecture de réseau.

Frais d'exploitation

«Un seul équipement, des utilisations multiples» : telle est la caractéristique de la gamme Cisco ASA 5500 qui lui confère des avantages tous particuliers en matière de coûts, tant pour la sécurité que pour la connectivité VPN (Figure 1). Le vaste éventail des services offerts par la gamme Cisco ASA 5500 – et notamment le pare-feu, la prévention des intrusions, les VPN et l'antivirus de réseau – permet le déploiement de la plate-forme dans des environnements très variés aux multiples exigences fonctionnelles. Ces services proviennent tous des serveurs de sécurité et de connectivité VPN dédiés de Cisco ce qui permet le déploiement de la gamme Cisco ASA 5500 sans avoir à transiger sur les fonctions, les performances ou la simplicité de gestion. Ce concept limite le nombre de plates-formes à déployer et à gérer tout en réalisant un environnement commun d'exploitation et de gestion sur l'ensemble de ces déploiements, avec une simplification évidente des tâches de configuration, de surveillance, de dépannage et de formation du personnel de sécurité.

Figure 1. Une seule unité, des utilisations multiples



Voici quelques exemples de scénarios de déploiement courants qui utilisent les plates-formes uniques et normalisées de la gamme Cisco ASA 5500 :

- les solutions convergentes de contrôle d'accès, d'inspection du trafic et des applications, et la protection contre les vers, les virus et les logiciels malveillants en périphérie du réseau ou sur la zone démilitarisée,
- les solutions convergentes de contrôle d'accès, d'inspection du trafic et des applications, et la protection contre les vers, les virus et les logiciels malveillants à l'intérieur du réseau,
- les solutions de pare-feu classique et d'inspection des applications en périphérie du réseau ou sur la zone démilitarisée,
- les solutions de pare-feu classique et d'inspection des applications à l'intérieur du réseau,
- la connectivité VPN «propre» à accès distant avec inspection convergente du trafic et des applications, et protection contre les vers, les virus et les logiciels malveillants,
- le raccordement autonome classique des VPN à accès distant,
- les services de VPN de site à site
- les solutions «tout en un» de contrôle d'accès, d'inspection du trafic et des applications, de protection contre les vers, les virus et les logiciels malveillants et la connectivité VPN à accès distant ou de site à site en tous lieux.

CONCLUSION

Quel que soit le type de serveur – convergent ou dédié – choisir le déploiement de fonctions de sécurité et de connectivité VPN est indispensable à la protection des réseaux modernes. Le choix repose essentiellement sur la taille du réseau, l'architecture qui en découle, l'emplacement sur le réseau et le modèle d'assistance informatique. Les serveurs de la gamme Cisco ASA 5500 et leur vaste éventail de services de sécurité et de connectivité VPN sont particulièrement adaptables et peuvent être déployés aussi bien en tant qu'unités convergentes que dédiées.

En uniformisant la diversité des environnements de déploiement et des fonctions de sécurité du réseau, la gamme Cisco ASA 5500 simplifie l'architecture du réseau et réduit du même coup les frais de déploiement et d'exploitation. La gamme Cisco ASA 5500 est une solution de remplacement avantageuse dans les scénarios de déploiement classiques des serveurs de sécurité dédiés Cisco PIX 515E et PIX 525 ainsi que pour les services VPN IPSec fournis par les concentrateurs de la gamme Cisco VPN 3000. Toutefois, la gamme Cisco ASA 5500 reprend les technologies propres aux gammes Cisco PIX et VPN 3000 et offre donc une compatibilité complète en termes de fonctions et de fonctionnalités avec les déploiements actuels de Cisco PIX et VPN 3000. Pour les solutions IPS et VPN SSL autonomes, les serveurs dédiés de la gamme Cisco IPS 4200 et les concentrateurs Cisco VPN 3000 sont respectivement le meilleur choix possible. Pour les petits bureaux et les bureaux à domicile (SOHO), les pare-feu des grandes sociétés ou encore le déploiement de VPN de site à site, les serveurs de sécurité Cisco PIX 501, PIX 506E et PIX 535 sont incontestablement les plates-formes les plus économiques et peuvent renforcer toutes les installations multisites de la gamme Cisco ASA 5500.

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :
www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas Pérou • Philippines •Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine Russie • Singapour • Slovaquie •Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

205226.s_ETMG_KM_4.05