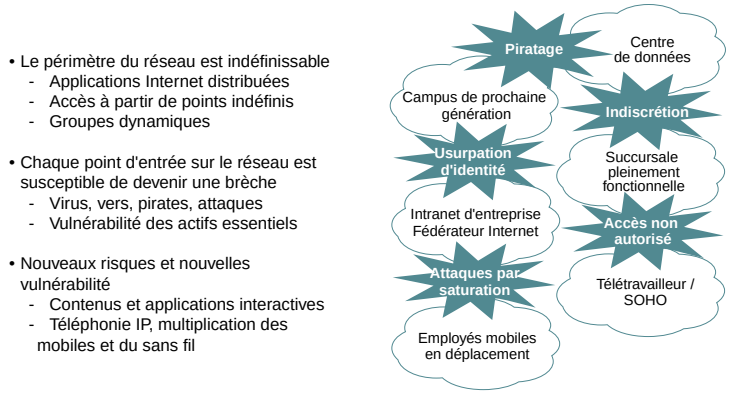
LIVRE BLANC : CISCO OUVRE LA VOIE DU RÉSEAU INFORMATIQUE INTELLIGENT

Par Jayshree Ullal, vice-Président Directeur et Directeur Général, Security Technology Group

Nous nous trouvons à un carrefour de l'avenir des réseaux et notre industrie voit deux chemins devant elle : continuer à construire des produits spécialisés ou créer des systèmes de réseau unifiés qui permettront aux entreprises d'améliorer leur productivité, de réduire leurs coûts et de prendre un avantage concurrentiel. Chez Cisco Systems, nous pensons que la solution la plus avantageuse pour nos clients proviendra de la création de réseaux intelligents où chaque élément s'intègre et travaille en harmonie avec les autres composantes de l'infrastructure de communications. Nous sommes en train, aujourd'hui même, de poser les fondations d'un tel système que nous avons baptisé Réseau informatique intelligent.

Mieux que tout autre aspect des réseaux modernes, la sécurité illustre à elle seule la criante nécessité d'une telle démarche. Aucune fonctionnalité de réseau ne fait l'objet d'une demande aussi importante. Voici encore deux ans, les administrateurs systèmes disposaient de quelques heures, voire de plusieurs jours, pour faire face aux nouvelles menaces pesant sur leurs réseaux : leur temps de réaction se mesure désormais en minutes quand ce n'est pas en secondes. Nous connaissons tous, malheureusement, des exemples d'introduction dans le réseau mondial de vers ou de virus qui se sont propagés rapidement et largement sur l'ensemble du globe. Ces logiciels nuisibles, conçus pour exploiter les environnements mal sécurisés, sont rarement bénins et leurs conséquences sont parfois très onéreuses. Le coût annuel supporté par les entreprises pour se prémunir contre virus et vers, ou pour en réparer les dégâts, se chiffre actuellement en milliards de dollars. Jusqu'ici, les opérateurs de réseaux devaient recourir à des correctifs logiciels ou à des produits spécifiques pour assurer leur défense, mais il devient clair que ces solutions n'apportent pas d'antidote contre l'ingéniosité et la malignité des menaces qui pèsent actuellement sur les réseaux.

Figure 1
La sécurité des réseaux telle qu'elle a évolué



Pour répondre aux nouvelles contraintes rencontrées pour obtenir une sécurité plus robuste, Cisco est en train de développer pour l'ensemble du réseau des défenses intégrées qui améliorent, tant en termes de rentabilité que de valeur ajoutée, les solutions spécifiques de sécurité traditionnelles. Le point commun entre tous les pirates informatique, virus, vers, logiciels espions et attaques diverses est qu'ils traversent un réseau pour se propager et atteindre leur cible. Chez Cisco, nous pensons que c'est un niveau du réseau que les mesures les plus efficaces peuvent être prises, et avons développé une approche exhaustive de la sécurité, le réseau à autodéfense de Cisco (Cisco Self-Defending Network). Une telle approche est de loin la manière la plus efficace de défendre les réseaux, leurs applications et leurs données contre les menaces d'aujourd'hui et de demain. En réalisant une sécurité à l'échelle du réseau tout entier, le concept Self-Defending Network permet à l'entreprise comme au particulier d'exploiter tout le potentiel des communications IP (Internet Protocol) pour relancer sa productivité et réduire ses frais d'exploitation.

Personne ne contestera que la sécurité des réseaux est devenue plus importante que jamais. Si les communications convergentes voix, vidéo et données sont devenues indispensables aux entreprises et aux particuliers, le périmètre d'un réseau sécurisé reste mal défini. La multiplication des clients, la prolifération des équipements mobiles et le développement de la téléphonie VoIP (Voix sur IP) font peser des exigences croissantes sur les relations entre les points d'extrémité et la sécurité du réseau. Les réseaux contiennent des renseignements sur la quasi-totalité des aspects du commerce et de notre existence, y compris les informations les plus confidentielles comme les dossiers médicaux ou financiers. La gestion de ces réseaux n'est plus une activité secondaire mais, bien au contraire, le moyen d'accomplir sa tâche dans pratiquement n'importe quel métier, notamment grâce aux communications voix et vidéo. Aujourd'hui, le réseau est l'entreprise et l'entreprise est le réseau.

LES LIMITES DE LA SÉCURITÉ TRADITIONNELLE

Les méthodes traditionnelles de sécurité informatique (qui dépendent largement de produits spécialisés et indépendants, d'une litanie de correctifs de systèmes d'exploitation et de la mise à jour continue des logiciels antivirus) montrent leur inadéquation à répondre efficacement aux exigences actuelles de la protection des réseaux. Ces méthodes sont limitées parce qu'elles ne peuvent défendre qu'une partie du réseau tandis que les nouvelles formes d'attaques les contournent facilement. De plus, chaque produit exige sa propre interface et ses propres politiques ce qui signifie que la plupart de ces produits spécialisés sont incapables de dialoguer avec les autres. Enfin, les défenses dont disposent actuellement les réseaux reposent sur des contrôles et des interventions manuelles qui se sont montrées trop lentes et pas assez réactives pour s'opposer aux dernières générations de vers et de virus.

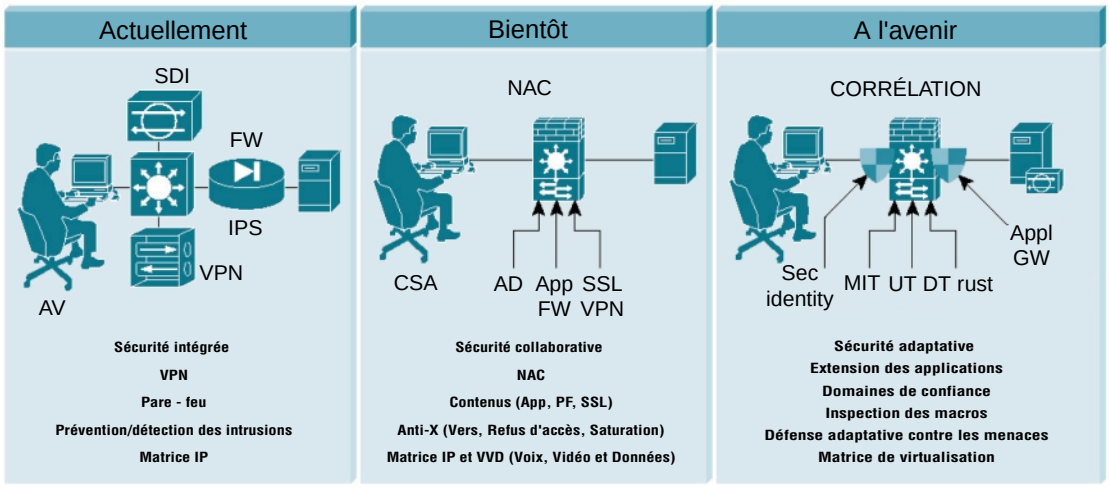
En raison de ces limitations, les défenses de réseau traditionnelles coûtent aux entreprises autant, si ce n'est davantage, en frais de gestion que les dégâts qu'elles cherchent à éviter. Les opérateurs de réseaux se trouvent désormais contraints d'intégrer en nombre toujours croissant les mises à jour antivirus et les correctifs de systèmes d'exploitation ou d'applications, une activité qui absorbe souvent une telle quantité de ressources informatiques que les projets les plus cruciaux sont mis sur la touche. L'entreprise doit fréquemment « monter au créneau », quel que soit son planning, pour lutter contre des virus qui la forcent à prendre des mesures de sécurité réactives et gênantes pour son fonctionnement.

Par le passé, bon nombre d'initiatives de protection des réseaux ont été limitées par leur approche conceptuelle de la sécurité. Certaines ont adopté le modèle de la « forteresse » avec ses pare-feu et autres technologies destinés à maintenir à l'extérieur du réseau toutes les personnes non autorisées. Cette démarche est aujourd'hui mise à mal par les nouveaux besoins métiers qui, à tout moment et en tout lieu, nécessitent un accès pour des groupes de personnes très variés : employés, fournisseurs, sous-traitants, invités, etc. De plus, les menaces internes continuent de poser aux entreprises de graves problèmes de sécurité. D'autres tentatives ont négligé d'inclure les ordinateurs personnels, les serveurs et les autres « points d'extrémité » dans la structure de sécurité du réseau, ignorant par la même des points de contrôle essentiels pour bloquer la prolifération des vers et des virus.

L'INTELLIGENCE DE RÉSEAU OUVRE LA VOIE À LA SÉCURITÉ ADAPTATIVE

Heureusement, la technologie fondamentale qui permet de protéger les informations numériques et les infrastructures de communications contre les menaces actuelles existe déjà. Les routeurs et les commutateurs de réseau disposent de manière inhérente d'une visibilité du réseau et de ses activités car ce sont eux qui voient et contrôlent le flux de toutes les données et des communications IP. Moyennant l'association bien conçue avec des technologies et des services de sécurité spécialisés (comme les logiciels de surveillance des points d'extrémité) ces composantes de cœur de réseau permettent de déployer progressivement des fonctions de sécurité sans équivalent.

Figure 2
L'étape suivante : le réseau à autodéfense



Cisco exploite maintenant l'infrastructure du Réseau informatique intelligent pour tisser une « cotte de mailles » multicouche intégrée qui évite les défaillances des mesures de sécurité traditionnelles. A la différence des produits spécialisés, le Self-Defending Network est un système de défense qui exploite les fonctionnalités omniprésentes de détection et de contrôle du réseau, chacun de ses éléments communiquant avec les autres pour renforcer la protection sur l'ensemble de l'infrastructure. Un tel système intégré génère un environnement coordonné, cohérent et proactif qui identifie les menaces, en limite la portée et les bloque. Résultat : une sécurité de réseau de référence unifiée contre les menaces, capable de réagir à vitesse informatique aux alertes de sécurité et de réduire les créneaux de vulnérabilité tout en allégeant le travail administratif.

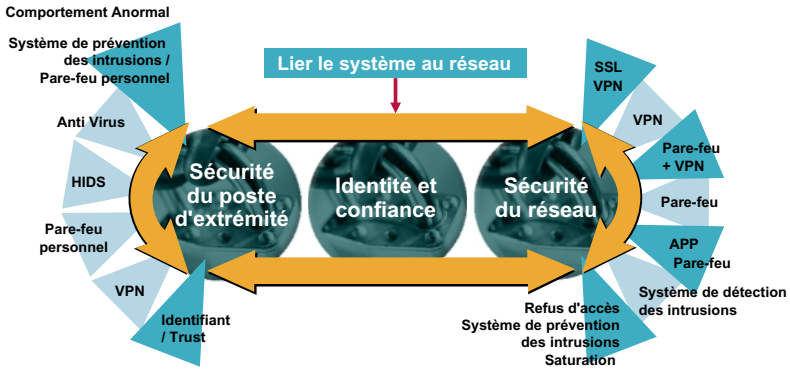
Pour son réseau à autodéfense, Cisco a pris modèle sur la manière dont notre corps se défend et lutte contre les infections et maladies. Comme la peau et les membranes du corps humain, le réseau à autodéfense possède plusieurs couches de protection : les VPN, les pare-feu, la prévention des intrusions et la réduction des anomalies. Associé aux fonctions de virtualisation évoluée, à une meilleure intelligence des paquets et à des liens comportementaux avec les systèmes d'extrémité, le système Self-Defending Network est capable de repousser les éléments dangereux. Toutefois, comme le corps humain, le réseau ne peut pas interdire totalement l'infiltration de tels éléments. Si l'être humain doit manger, boire et respirer, les réseaux doivent traiter et livrer des informations provenant d'une multitude de sources extérieures. Dans cet esprit, Cisco est en train de permettre au réseau à autodéfense de travailler à pleine capacité ou presque, même lorsqu'il est envahi par des entités nuisibles, tout comme le corps humain continue de fonctionner malgré une infection ou une maladie.

DE L'IDENTIFICATION DES POINTS D'EXTRÉMITÉS AUX LIAISONS DE RÉSEAU SÉCURISÉES

Plus important encore, Cisco prévoit que le réseau à autodéfense puisse évoluer avec les besoins de sécurité du Réseau informatique intelligent ainsi qu'avec les modifications apportées aux ordinateurs de bureau, aux serveurs et aux applications. Pour supporter la première phase du Réseau informatique intelligent, Cisco Self-Defending

Network établit des positions de défense à la périphérie du réseau : contrôles d'accès des utilisateurs et de leur PC, pare-feu plus intelligents, outils de prévention des intrusions et protection des points d'extrémité par des logiciels proactifs qui analysent les comportements. S'appuyant sur le protocole IP comme base d'échanges, Cisco élargit cette structure de protection grâce à des technologies de réseaux privés virtuels qui placent plus efficacement les utilisateurs distants et mobiles sous l'ombrelle protectrice du réseau à autodéfense. Tous ces outils sont liés les uns aux autres par une gestion centralisée qui coordonne les réactions et synchronise les politiques.

Figure 3
Exécuter les politiques de sécurité



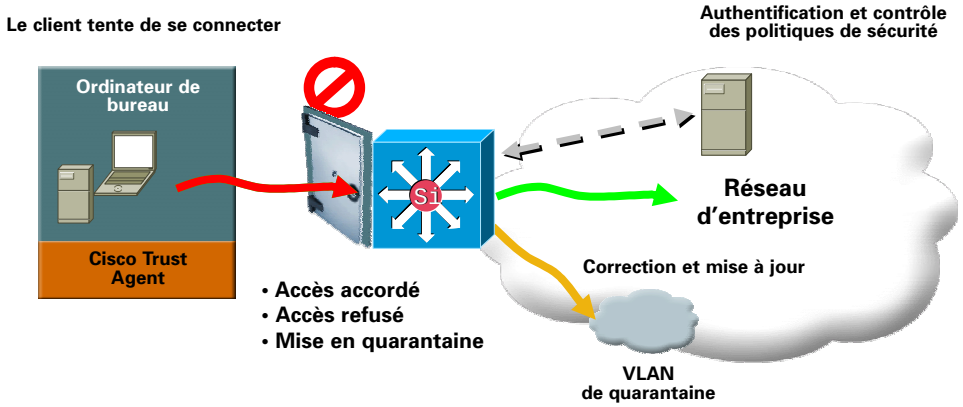
- **Le niveau de conformité du poste d'extrémité conditionne l'accès aux ressources réseaux**
- **Les "serveurs de politiques" centralisent la gestion de politiques de sécurité**
- **Le réseau fournit les mécanismes dynamiques et la sécurisation active**

L'innovation la plus marquante de Cisco dans le développement initial du concept de Self- Defending Network est la surveillance par contrôle d'accès NAC (Network Admission Control) de la liaison entre le réseau IP sécurisé et les points d'extrémité. Le contrôle NAC est une première industrielle en matière de sécurité car il crée un précédent essentiel de collaboration entre de multiples sociétés. A l'origine, Cisco avait développé le contrôle NAC en association avec les principaux constructeurs de logiciels anti-virus comme Network Associates, Symantec et Trend Micro. IBM et Microsoft ont depuis manifesté leur soutien au projet NAC et travaillent en étroite collaboration avec Cisco. NAC permet au réseau de contrôler l'accès d'un point d'extrémité donné en fonction de sa conformité à une politique de sécurité. Il peut vérifier si l'ordinateur portable, l'ordinateur de bureau ou le serveur qui demande l'accès au réseau est bien conforme à ce qui est prévu, comme par exemple la présence d'un logiciel antivirus et de correctifs de système d'exploitation à jour. NAC peut également interdire l'accès à tous les équipements non conformes en utilisant les routeurs et les commutateurs Cisco.

A mesure que le Réseau informatique intelligent passera à la phase deux, d'ici deux ou trois ans, et commencera à permettre une utilisation plus dynamique des ressources, notamment au niveau des datacenters, le système de sécurité évolutif sera en mesure de répondre automatiquement aux menaces. Cisco donnera la priorité à l'accélération des réactions aux nouvelles attaques en consolidant les informations fournies par des technologies variées de détection et en les réunissant dans des systèmes dynamiques de contrôle des politiques. La clé de cette étape sera la capacité à identifier, localiser et isoler les systèmes infectés, puis à coordonner l'exclusion du réseau du trafic nuisible. Ceci permettra d'empêcher la propagation du virus au reste de l'environnement ainsi qu'aux autres réseaux qui y sont reliés.

Le réseau à autodéfense de Cisco collaborera avec les fournisseurs de produits de sécurité afin de maîtriser le potentiel de détection des virus et des comportements anormaux des différentes unités du réseau comme les serveurs de courrier électronique, les passerelles antivirus et même les autres ordinateurs personnels. Au sein du projet de réseau à autodéfense, ces unités pourront « dénoncer » d'autres éléments du réseau présentant des comportements anormaux, autrement dit, qui laissent entendre que ces éléments sont sous le contrôle d'un programme malveillant ou d'un pirate. Le système de routeurs et de commutateurs pourra alors servir à isoler les unités infectées ou les systèmes non protégés tandis que les équipes réseau et système mettront leurs défenses à jour.

Figure 4
Contrôle de l'accès au réseau : solution de sécurité basée sur la confiance et les identifiants



L'AVENIR DE LA SÉCURITÉ CISCO

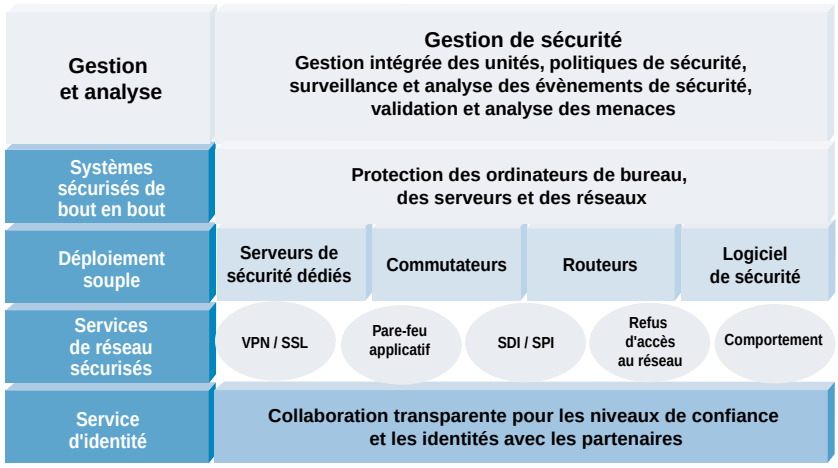
A l'horizon de trois à cinq ans, les exigences de sécurité ne pourront qu'augmenter devant la complexité croissante des réseaux. Au cours de cette troisième phase, le Réseau informatique intelligent commencera certainement à proposer des applications et des services virtualisés, permettant ainsi aux utilisateurs d'accéder facilement aux applications et aux informations dont ils ont besoin, quand ils en auront besoin et de la manière dont ils le souhaiteront. Toutefois, l'ouverture des applications ouvre aussi la porte à de nouveaux risques. Si les applications et les ressources transitent plus fréquemment sur un nombre croissant de réseaux, le code malveillant risque d'emprunter les mêmes chemins. Pour se protéger contre de telles attaques, le réseau à autodéfense devra pouvoir examiner le trafic encore plus en détail, et même analyser les informations des applications et des messages afin de vérifier leurs « bonnes intentions » et d'identifier avec davantage de fiabilité et de rapidité les utilisations abusives et les menaces. Bien que le défi technique correspondant soit de taille, de telles fonctionnalités assureront une sécurité dynamique de bout-en-bout au niveau des applications et des contenus. Parallèlement à ces inspections en profondeur, le réseau à autodéfense de l'avenir exigera également un cadre de sécurité à base de politiques à la fois transparent pour toutes les applications et applicable en toute autonomie.

Pour faciliter ces processus de sécurité encore plus détaillés, Cisco cherche à « inscrire » davantage de fonctions de sécurité dans les schémas de routage et de commutation. Tout comme Cisco a piloté l'industrie vers l'amélioration des performances de traitement des paquets, nous avons bien l'intention de montrer une fois encore la voie vers les réseaux sécurisés à hautes performances. La troisième phase de Self-Defending Network nécessitera également des progrès supplémentaires dans les ASIC et les processeurs pour permettre cette analyse détaillée des paquets et le contrôle au niveau des applications. Dans le même temps, un grand nombre des outils logiciels actuels migreront vers des unités matérielles de traitement, pour devenir des fonctions standard qui contribueront à réduire l'impact des fonctions de sécurité sur les performances des réseaux.

Tout au long de ces différentes phases, Cisco s'associera à d'autres fournisseurs pour diversifier les capacités de défense de son projet Self-Defending Network. Pour que cette approche de la sécurité devienne réalité, l'essentiel n'est pas que toutes ses composantes proviennent d'un unique système monolithique mais, bien au contraire, que chacune s'appuie sur des normes industrielles afin de communiquer efficacement et économiquement avec les autres dans un effort de défense coordonnée. Ces partenariats d'unification industrielle peuvent faire progresser la sécurité de manière spectaculaire, par exemple au travers d'un système universel d'identification numérique des applications et des unités.

Il est clair que les sociétés et les équipes réseau et système ont besoin d'une solution de remplacement au concept traditionnel de sécurité ponctuelle. Chez Cisco, nous pensons que le réseau à autodéfense est cette solution. Quelles que soient les technologies qui le constitueront, le réseau à autodéfense a un but unique : améliorer les communications en rendant les réseaux plus sûrs, car de meilleures communications se traduisent par de meilleurs résultats pour l'entreprise. A ce titre, les fonctionnalités de défense automatisées du réseau Cisco offrent une sécurité non seulement renforcée mais également plus économique en éliminant un grand nombre des processus manuels coûteux qui accaparent aujourd'hui les ressources des services informatiques.

Figure 5
Le réseau à auto défense Cisco



Lorsqu'elles savent que leur réseau est protégé, les entreprises comme les personnes sont plus libres de profiter des avantages nombreux (et en constante augmentation) des communications IP. Avec une meilleure sécurité, les utilisateurs du réseau ont plus rapidement et plus facilement accès aux applications et aux services. Une telle liberté est source de gains de productivité et resserre en même temps les relations avec les clients et les partenaires. Toutefois, le plus important de tous les biens que nous apporte une sécurité plus efficace, c'est la tranquillité d'esprit.

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

XXXXXXXXX