PROTECTION CONTRE LES INTRUSIONS : CISCO IPS VERSION 5.0

DESCRIPTION DU PRODUIT

La solution de prévention des intrusions Cisco IPS (Intrusion Prevention System) de Cisco Systems ® est une offre logicielle qui est conçue pour identifier, référencer et bloquer le trafic malveillant avant qu'il ne compromette la continuité de votre activité. Avec ses capacités éprouvées de détection et de prévention en ligne de qualité industrielle, la solution Cisco IPS réalise une protection complète de vos données comme de votre infrastructure informatique.

La solution Cisco IPS offre une protection précise et proactive qui permet à ses utilisateurs de bloquer davantage de menaces avec une confiance accrue grâce à :

- **l'identification globale des menaces** – L'inspection approfondie du trafic des couches 2 à 7 protège votre réseau des violations de politiques, de l'exploitation de ses vulnérabilités et des activités malveillantes ;
- **des technologies précises de prévention** – Elles vous permettent d'effectuer des actions de prévention en toute confiance sur un éventail élargi de menaces sans risquer de rejeter le trafic autorisé. Le système innovant d'évaluation des risques ainsi que le générateur de méta-événements MEG (Meta-Event Generator) de Cisco identifient les attaques avec précision et permettent de mettre rapidement en œuvre les actions de défense ;
- **une collaboration en réseau originale** – La collaboration de réseau, avec ses techniques efficaces de capture du trafic, ses fonctions d'équilibrage de charge et sa capacité d'analyse du trafic crypté, vous apporte encore plus d'évolutivité et de robustesse ;
- **des solutions complètes de déploiement** – L'offre logicielle Cisco IPS permet la mis en œuvre des solutions de détection et de prévention des intrusions dans tous les environnements. Environnements clients de tous types (depuis les PME et les agences d'entreprise jusqu'aux installations du siège social ou des fournisseurs de services), mais aussi environnements hardware adaptés. La gamme des équipements spécialisés Cisco IPS se compose des serveurs dédiés de la gamme Cisco IPS 4200 ainsi que des modules de commutation de la gamme Cisco Catalyst® 6500. Le module de détection des intrusions (IDS) destiné aux routeurs d'accès Cisco fournit des fonctionnalités évoluées qui renforcent les fonctions traditionnelles de détection. De plus, un ensemble spécialisé de fonctions de prévention des intrusions est disponible en tant que solution Cisco IOS® pour les routeurs Cisco. Pour la configuration des unités et la visualisation des événements, Cisco propose des solutions comme IPS Device Manager, destiné à la gestion des serveurs uniques et à la surveillance des événements, ainsi que CiscoWorks VMS (VPN/Security Management Solution), spécialisé dans la gestion de plusieurs unités avec corrélation d'événements multiples.

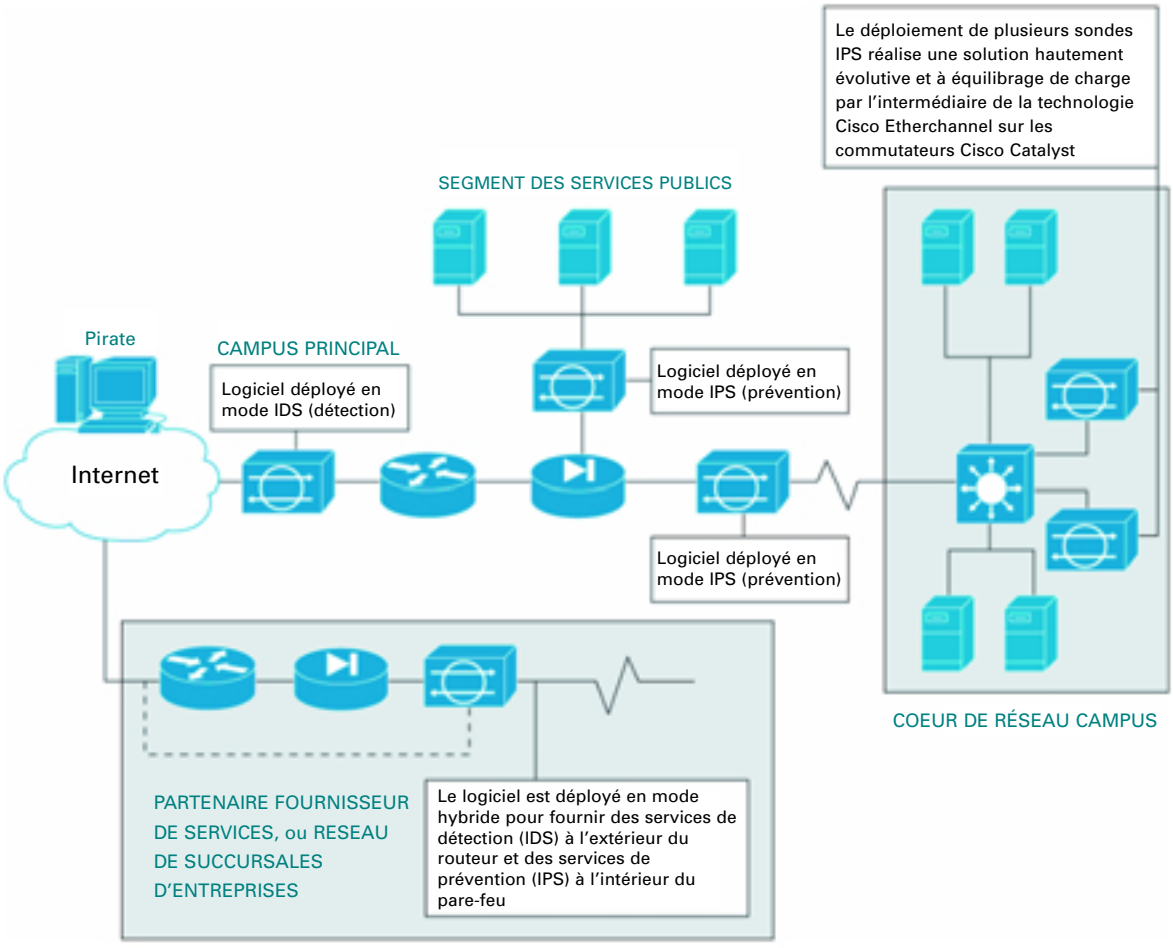
Lorsqu'ils sont associés, ces éléments réalisent une solution de prévention en ligne complète qui vous permet, en toute confiance, de détecter et de bloquer les types les plus variés de trafics malintentionnés avant qu'ils compromettent la continuité de vos activités et surtout, de quelque endroit qu'ils proviennent !.

CARACTERISTIQUES ET AVANTAGES

Des services IPS pour bloquer les vers et les virus

Destiné aux serveurs dédiés de gamme Cisco 4200 ainsi qu'au module IDSM-2 pour les commutateurs de la gamme Cisco Catalyst 6500, le logiciel Cisco IPS Version 5.0 fournit des fonctionnalités en ligne de prévention des intrusions qui bloquent efficacement les vers et les virus aux endroits stratégiques du réseau. La Figure 1 montre comment les serveurs dédiés et les modules Cisco IPS réalisent des solutions de déploiement complètes sur l'ensemble du réseau.

Figure 1. Le logiciel Cisco IPS Version 5.0 fournit du code convergent à l'ensemble de la gamme des produits Cisco IPS



- Support des services **hybrides IDS/IPS**, qui permet au même logiciel de travailler à la fois en mode de détection (IDS) et de prévention (IPS). La Figure 1 montre comment déployer stratégiquement des unités IPS pour qu'elles assurent, simultanément et individuellement, des services de détection et de prévention. Cette fonctionnalité permet de réduire considérablement le coût total d'acquisition en supprimant la nécessité de déployer de multiples unités sur un même réseau.
- Support d'un **large éventail d'actions de rejet des paquets**, notamment la possibilité de rejeter individuellement les paquets malveillants, tous les paquets d'un flux contenant plusieurs paquets malveillants ou tous les paquets provenant de l'adresse IP du pirate. Ces actions **en ligne** complètent les actions de défense existantes, comme la réinitialisation des connexions et les modifications des listes de contrôle d'accès sur les commutateurs, les routeurs et les pare-feu, pour fournir un ensemble de techniques de contrôle des attaques – le plus complet de l'industrie – **qui travaillent de concert** pour bloquer efficacement les vers et les virus.

Des technologies de prévention précises

- **Cisco Meta Event Generator (MEG)** – Le générateur de méta-événements MEG effectue une corrélation « on-box » pour classer les attaques de manière précise. Le logiciel Cisco IPS Sensor Version 5.0 intègre des fonctions évoluées de corrélation des événements au niveau de l'équipement qui fournissent aux administrateurs de la sécurité une méthode automatisée pour accroître le niveau de confiance dans la classification des activités malveillantes détectées par l'IPS. Ce mécanisme permet, par des actions appropriées, de contenir les vecteurs d'injection des vers et des virus et de bloquer la propagation des vers à l'échelle du réseau tout entier.

Ce mécanisme repose sur les techniques suivantes :

- **la corrélation des alertes** relatives aux vers qui exploitent des vulnérabilités multiples. La Figure 2 montre comment plusieurs alertes déclenchées sur une courte période peuvent être corrélées en temps réel afin de constituer un méta-événement unique qui assure une meilleure visibilité de l'activité d'un ver ;
- la corrélation d'une **séquence d'actions** caractérisant l'infestation par un ver. Les analyses de tendances historiques réalisées pour caractériser le cycle de vie des vers révèlent souvent une séquence particulière d'actions détectables juste avant qu'ils parviennent à s'infiltrer dans le système. Ces actions interviennent au cours de la « phase de sondage », une succession d'activités de reconnaissance du réseau cible. Le générateur MEG donne à l'utilisateur la possibilité de définir les précurseurs de l'infiltration du ver en désignant un algorithme logique qui se déclenchera en cas de détection d'une suite particulière d'événements. De telles corrélations engendrent des méta-événements qui permettent, avec un meilleur niveau de confiance, d'alerter l'utilisateur de la présence d'une activité malveillante ;
- la corrélation **de multiples événements** de faible dangerosité qui sous-entendent l'éventualité d'un événement unique bien plus grave. A mesure qu'un ver se propage dans le réseau, il génère des alertes plus ou moins sérieuses. Cisco MEG relie entre elles des alertes de faible gravité et apparemment indépendantes qui signent un événement grave ou à haut risque pour permettre à l'utilisateur de rejeter, avec un haut niveau de confiance, les paquets associés (Figure 3) ;
- **l'amélioration** du niveau de **fiabilité** des alertes par la simultanéité des réponses positives d'algorithmes hybrides de détection. Par exemple, lorsque des activités caractéristiques d'attaque par saturation sont détectées (identification via une signature classique de type « saturation »), le générateur MEG peut servir à corroborer l'un des événements avec l'autre et fournir ainsi un méta-événement unique qui indique, avec une plus grande probabilité, qu'une attaque est en cours.

Ces niveaux complémentaires de sécurité apportent la confiance nécessaire pour déployer une action de prévention des intrusions en ligne **sans risque de rejet du trafic légitime**, tout en identifiant les vers et en les empêchant de se propager dans votre réseau.

Figure 2. Le générateur MEG corrèle de multiples événements pour détecter la présence d'un ver

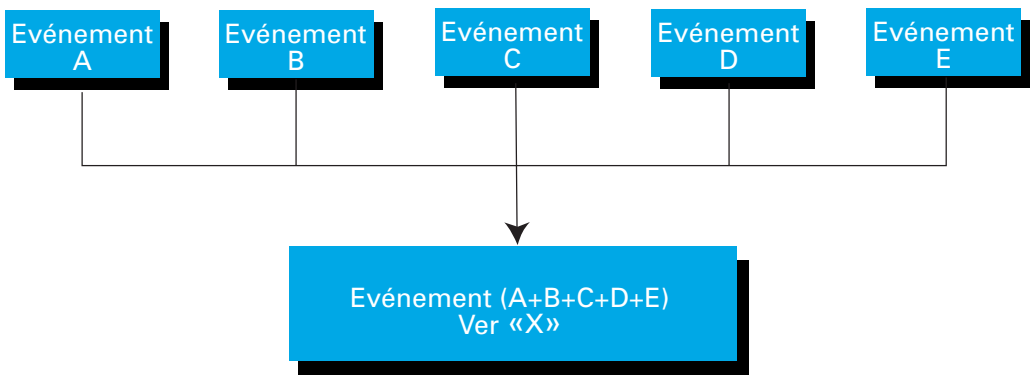
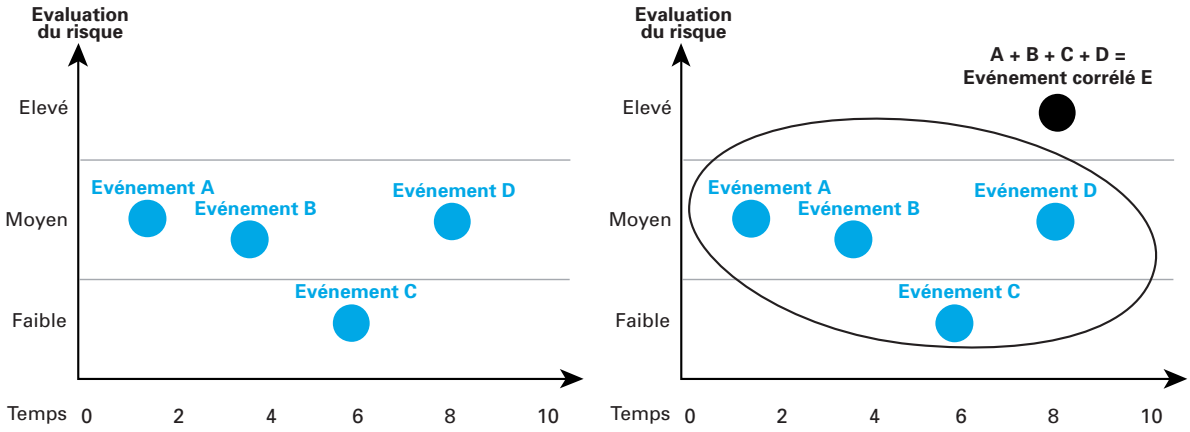


Figure 3. Le générateur MEG corrèle de multiples événements de faible gravité pour générer un unique événement de présence de ver d'un haut niveau de gravité.

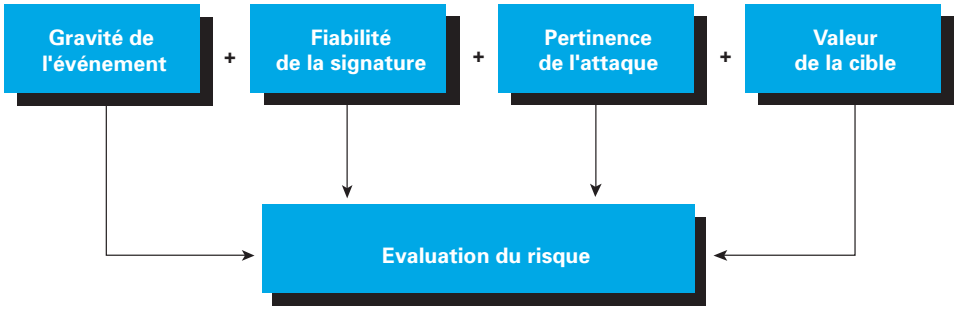


L'Evaluation du risque augmente la précision et le niveau de confiance des actions de prévention (IPS) de rejets des paquets en classant les menaces en fonction des risques encourus (Figure 4). De manière automatisée, l'Evaluation du risque utilise un algorithme pluridimensionnel unique qui tient compte de différents facteurs, et notamment de :

- **la gravité de l'événement** – Valeur dont la pondération est modifiable par l'utilisateur et qui caractérise les dégâts potentiels du trafic suspect ;
- **la fiabilité de la signature** – Valeur dont la pondération est modifiable par l'utilisateur et qui définit dans quelle mesure la signature est susceptible de caractériser la menace ;
- **la valeur de l'équipement** – Paramètre défini par l'utilisateur et représentant la valeur qu'il attribue à l'hôte cible ;
- **la pertinence de l'attaque** – Pondération interne qui rend compte de tous les faits complémentaires que le logiciel possède sur la cible de l'événement.

  L'Evaluation du risque ainsi obtenue est un nombre entier appliqué de manière dynamique à chaque signature IPS, politique ou algorithme de détection des anomalies. Plus cette valeur est élevée et plus le risque de sécurité est grand en cas de déclenchement de l'alerte correspondante. On obtient ainsi un mécanisme qui permet à l'utilisateur de développer des politiques de prévention des attaques contre son réseau ou de mieux classer les événements pour les étudier par la suite en fonction de leur priorité. L'utilisateur est ainsi mieux informé pour prendre des décisions concernant des actions de prévention en ligne et élimine pratiquement tout risque de rejet du trafic légitime.

Figure 4. L'Evaluation du risque améliore la précision des actions de prévention IPS



EXTENSIONS VERS L'IDENTIFICATION MULTIVECTORIELLE DES MENACES

- Le recours aux technologies d'inspection permet l'application de décisions politiques en fonction des contenus détectés au niveau de la couche applicative.
- La détection et la prévention de la tunnellisation sur le port 80 – qui permet à un utilisateur de faire passer secrètement des applications interdites – donne à l'administrateur les moyens de constater plus facilement les infractions à la politique de sécurité de l'entreprise. Le principal avantage de cette fonction est la préservation de la bande passante au sein du réseau en interdisant les applications comme les outils de partage de fichiers qui ont tendance à consommer des quantités disproportionnées de bande passante.
- Le contrôle de conformité RFC des méthodes HTTP permet de s'assurer qu'un pirate ne manipule pas les transactions HTTP. L'utilisateur peut ainsi autoriser ou interdire certaines méthodes HTTP comme « GET » ou « POST ».
- Le filtrage du trafic en fonction de types MIME particuliers comme les extensions JPEG, permet à l'administrateur de bloquer avec précision les activités de vers et de virus qui peuvent être associées aux contenus malveillants que l'on trouve dans certains types MIME. De plus, l'en-tête de contenu du type MIME en question est comparé au contenu réel afin d'empêcher le pirate de contourner cette fonctionnalité en dissimulant du code malveillant sous l'en-tête d'un type MIME accepté.
- L'utilisateur peut contrôler le trafic autorisé grâce à des politiques qu'il définit lui-même. Contrairement aux méthodes traditionnelles d'inspection et de prévention, le logiciel Cisco IPS Version 5.0 permet également à l'utilisateur de prendre des décisions en fonction des politiques pour accepter ou refuser certains types de trafic comme le « Peer to Peer » susceptible de consommer une grande partie de la bande passante.
- Cisco IPS v5.0 protège les réseaux contre les logiciels espions ou publicitaires – spywares et adwares – en permettant à l'entreprise de préserver l'intégrité de ses informations confidentielles que des applications malveillantes comme Gator, Bonzi Buddy et SaveNow pourraient divulguer. Cisco IPS v5 dispose d'algorithmes originaux capables de bloquer efficacement les communications entre les serveurs qui hébergent des logiciels espions et les unités du réseau infectées par ces logiciels. De plus, Cisco IPS v5 peut également bloquer les communications non désirées générées par les applications publicitaires les plus courantes.
- Un moteur VoIP (Voix sur IP) vérifie la conformité aux protocoles des messages de passage d'appel H.225. Ce moteur protège également contre les attaques dirigées vers les passerelles voix grâce à ses fonctions évoluées de contrôle de dépassement de mémoire tampon et de saturation URL.
- Le système supporte l'inspection et l'atténuation des menaces dans les environnements MPLS (Multiprotocol Label Switching). Le trafic MPLS peut être important sur les sites des fournisseurs de services ou les réseaux d'entreprise. La visibilité des paquets MPLS est indispensable pour détecter avec précision les contenus malveillants dans les en-têtes et les données utiles des paquets. Le logiciel Cisco IPS Version 5.0 examine en profondeur les paquets MPLS pour classer et prévenir les menaces.
- Les fonctionnalités anti-virus de réseau facilitent l'identification précise et la prévention des épidémies virales. En plus des menaces classiques détectées par les unités de prévention (IPS), le logiciel Cisco IPS Version 5.0 élargit les fonctions de classification des menaces afin d'englober la détection et la prévention précises des activités virales identifiées sur le réseau. Suivant la manière dont il est déployé, le logiciel peut contenir les activités des virus les plus récents au niveau de la couche réseau pour une protection efficace des points d'extrémité contre ce type de menaces. Le logiciel Cisco IPS Version 5.0 améliore également la livraison des mises à jour et accélère de manière inégalée le renouvellement des mises à jour concernant les menaces les plus récentes.
- Le logiciel Cisco IPS Version 5.0 supporte les algorithmes évolués de normalisation du trafic comme le réassemblage après fragmentation.
- Les attaques sur l'environnement IPv6 sont identifiées grâce à l'inspection du trafic IPv4 tunnellisé dans IPv6.

AUTRES FONCTIONNALITES

- Configuration automatique et manuelle de contournement du logiciel – De nombreux mécanismes permettent de garantir la haute disponibilité des sondes Cisco IPS. La robustesse et la redondance sont assurées par une collaboration de réseau originale, comme la configuration du protocole HSRP (Hot Standby Router Protocol) et l'équilibrage de charge Cisco EtherChannel® sur les commutateurs Cisco Catalyst qui permettent de dérouter le trafic vers une unité IPS secondaire en cas de défaillance de l'unité principale. Le logiciel Cisco IPS Version 5.0 dispose également de mécanismes de contournement on-box qui lui permettent de se mettre automatiquement en mode « fail-open » en cas de défaillance particulière. Le mécanisme de contournement peut également être configuré manuellement – dans ce cas, l'utilisateur doit basculer la sonde en mode contournement (« bypass ») pour passer en mode « fail-open » – ce qui améliore encore la fiabilité de l'unité IPS.
- Support SDEE (Security Device Event Exchange) – SDEE est un protocole de communication IPS normalisé développé par Cisco pour le consortium IDS d'ICSA (International Computer Security Association). Grâce à ce protocole SDEE, le logiciel Cisco IPS 5.0 offre une interface API souple et normalisée qui facilite l'intégration de solutions tierces de gestion et de surveillance avec la solution Cisco IPS. L'utilisateur dispose ainsi d'un choix entre de nombreuses solutions tierces pour la surveillance des événements générés par la sonde Cisco IPS.
- Extensions des mécanismes de surveillance et de notification grâce à la transmission des alertes du logiciel par l'intermédiaire de pièges SNMP (Simple Network Management Protocol) – En plus des formats d'alertes existants, le logiciel Cisco IPS Version 5.0 offre également à l'utilisateur un outil de transmission des alertes IPS de la sonde vers les outils de surveillances qui exigent le format SNMP. Le protocole SNMP peut également servir à obtenir de la sonde IPS des informations critiques de diagnostic et d'état qui fournissent à l'utilisateur des renseignements vitaux sur son bon fonctionnement.

CONFIGURATION SYSTÈME NÉCESSAIRE

Les services IPS en ligne exigent plus d'une interface de surveillance sur les sondes de la gamme Cisco IPS 4200. Pour toute information sur les options de mise à niveau, veuillez consulter la fiche technique de la gamme Cisco IPS 4200 à l'adresse :

http://www.cisco.com/go/ips

Le logiciel Cisco IPS Version 5.0 est supporté par les serveurs dédiés Cisco IDS 4215, IDS 4235, IPS 4240, IPS 4255 et IDS 4250-XL ainsi que sur le module IDSM-2. Il est supporté en mode IDS espion seulement sur le serveur dédié Cisco IDS 4210 et le module réseau Cisco IDS (NM-CIDS).

COMMANDE DE MATÉRIEL

Le Tableau 1 présente les informations de commande pour le logiciel Cisco IPS Version 5.0.

Tableau 1. Informations de commande pour le logiciel Cisco IPS Version 5.0.

Référence	Description
IPS-SW-K9-U	Logiciel CISCO IPS Version 5.0

Pour passer commande, visitez Cisco Ordering Home Page.

POUR PLUS D'INFORMATIONS

Pour toute information complémentaire sur le logiciel Cisco IPS Version 5.0, contactez votre Responsable de compte local ou visitez :

http://www.cisco.com/go/ips

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