



Sécurisation pour les entreprises



Introduction

La brochure que vous tenez en main est consacrée à la sécurisation des réseaux. La sécurisation est l'un des problèmes les plus importants auxquels les entreprises sont confrontées. Une étude a révélé que 64% des PME dépendent dans une large mesure de l'informatique et d'Internet, mais que 80% d'entre elles n'ont pas de politique structurée en matière de sécurisation. Cette brochure vous apprend comment aborder de façon structurée la sécurisation de votre entreprise.

Nous utilisons un scénario de croissance pour vous montrer les étapes à suivre lorsque votre entreprise développera de nouveaux services qui exigeront une utilisation plus intensive d'Internet. Vous lirez comment un réseau Cisco Self-Defending Network est élaboré, et quels produits se prêtent le mieux à votre situation et à la taille de votre entreprise. Dans la dernière partie, vous en apprendrez plus sur les services de nos Select Partners, certifiés pour les solutions PME, et sur nos conditions de financement attrayantes.

Cisco aide les personnes et les entreprises à travailler plus intelligemment, plus efficacement et de façon plus sûre. En mettant vos problèmes au centre de nos préoccupations, nous sommes en mesure de développer une technologie qui aide votre entreprise à se développer. Nous commençons toujours par analyser les problèmes rencontrés par votre entreprise, et c'est sur cette base que nous déterminons quelles technologies se prêtent le mieux à y répondre. C'est dans ce but précis que Cisco a développé l'approche 'Smart Business Communications', une approche par étapes qui vous aide à atteindre des objectifs essentiels : augmentation de la productivité, réduction des coûts, meilleure réaction aux questions des clients et sécurisation de vos informations critiques.

Cette série comprend une brochure consacrée à l'approche Cisco Smart Business Communications. Cette brochure vous apprendra tout sur cette méthodologie. Les autres brochures de cette série abordent les thèmes de Cisco Unified Communications pour les entreprises et des solutions sans fil pour les entreprises. Pour de plus amples informations, visitez le site web Cisco consacré aux PME : www.cisco.be/pme - petites et moyennes entreprises.



Objet

- 5 Augmentation des risques de sécurité
- 8 Qu'est-ce qui est possible ?
- 10 Composants d'un réseau Cisco Self Defending Network
- 16 Exemples de solutions de sécurisation Cisco
- 22 Nos services



Augmentation des risques de sécurité

La sécurisation des informations : le plus grand défi des PME

Une étude indique que la sécurisation des informations est le plus grand défi auquel sont confrontées les entreprises de 250 salariés ou moins. À l'heure actuelle, la grande majorité des entreprises possèdent une connexion fixe à large bande. Le réseau de ces entreprises est donc exposé en permanence à des menaces telles que les virus, vers et autres attaques. Nous énumérons ici quelques aspects qui ont un impact sur les mesures de sécurisation que vous devriez prendre.

E-commerce

Le commerce électronique (E-commerce) est en plein essor : de plus en plus d'entreprises possèdent un site sur lequel leurs clients peuvent effectuer des transactions. Le site web a évolué d'une brochure en ligne à un outil transactionnel. Ceci impose cependant des contraintes spécifiques en termes de sécurisation, non seulement pour le site web mais également pour l'environnement ICT dans son ensemble.

Logiciel en ligne

Les services hébergés deviennent de plus en plus populaires. Ils vous permettent d'utiliser des logiciels sous la forme de services en ligne comparables aux systèmes de banque en ligne. Les logiciels comptables et de gestion de clientèle, notamment, sont très souvent proposés sous cette forme. Cela signifie que les informations critiques de l'entreprise, comme les informations financières et les informations clients, sont stockées sur un serveur dans les locaux du prestataire de service et mises à disposition, via Internet, de tous les collaborateurs disposant d'un nom d'utilisateur et d'un mot de passe. Sans une bonne sécurisation, la confidentialité de ces données n'est absolument pas garantie.



Travail mobile

Les risques augmentent sans cesse parce que les employeurs travaillent de plus en plus de façon mobile. Ils emportent leur ordinateur portable (fourni par l'entreprise) chez eux. Le réseau qu'ils utilisent à domicile est rarement protégé, ou il est mal protégé. La connexion sans fil est souvent entièrement ouverte, avec tous les risques qui y sont associés pour les informations critiques de l'entreprise qui se trouvent sur l'ordinateur portable. La popularité croissante du travail mobile signifie que vos contacts professionnels apprécient de pouvoir profiter d'un quart d'heure perdu pour brancher leur portable sur votre réseau et consulter leur courrier électronique. Vous ne savez pas quels virus, vers ou logiciels espions pénètrent ainsi le réseau de votre entreprise. Ces services avancés nécessitent une sécurisation avancée.

Spam

Le spam représente lui aussi un risque important. D'une part parce que vos collaborateurs reçoivent tellement de courriels indésirables qu'ils risquent d'oublier un message important, mais aussi parce que ce spam impose une charge inutile à vos serveurs. Les filtres anti-spam sont heureusement de plus en plus efficaces, mais il faut faire attention à ce que votre filtre ne bloque pas les 'vrais' messages. Les filtres anti-spam doivent bloquer les bons messages. En outre, le spam invite souvent ses destinataires à visiter des sites web infectés de logiciels espions et d'autres programmes nocifs, ce qui représente un risque supplémentaire.

Législation

Les menaces toujours changeantes en matière de sécurisation, tant à l'intérieur qu'à l'extérieur du réseau d'entreprise, peuvent avoir des conséquences graves sur les activités et donc sur la rentabilité de l'entreprise et sur la satisfaction de ses clients. Vous devez en outre respecter de nouvelles réglementations et de nouvelles lois sur la protection des données personnelles et sur la sécurisation des transactions électroniques imposées par l'Union Européenne et la Belgique. Un exemple en est la norme de protection des données pour l'industrie des cartes de paiement ("Payment Card Industry", PCI), applicable à toutes les entreprises qui effectuent des transactions avec des cartes de crédit.

Frais

Une attaque réussie sur votre réseau entraîne des coûts visibles et invisibles. La plupart des attaques, comme un virus sur un PC, etc. provoquent relativement peu de dommages. Les coûts concernés concernent principalement le temps perdu à supprimer le virus des systèmes infectés, et le temps de travail perdu parce que le collaborateur doit attendre que son PC ait été nettoyé.

La situation est plus grave lorsque l'infection se répand dans le réseau au point de provoquer sa défaillance. Il ne s'agit plus alors uniquement de temps perdu, mais aussi de commandes perdues, de clients qui s'en vont et d'une réputation qui souffre.

La conséquence la plus grave d'une mauvaise sécurisation est souvent le vol ou la fuite de données. Si votre fichier clients est rendu public, il y a de fortes chances pour que la nouvelle se répande, avec toutes les conséquences néfastes sur la réputation, sans parler du risque de procès que ces clients pourraient tenter à votre rencontre. Dans le cas d'une chaîne de distribution qui rassemble les adresses électroniques de ses clients pour pouvoir leur envoyer régulièrement un mailing, la fuite de ces données ne sera peut-être pas trop grave. Dans le cas d'une agence de recouvrement ou d'une fiduciaire, le risque est grand de perdre entièrement la confiance de ses clients.

Qu'est-ce qui est possible ?

Cisco Self Defending Network

Personne ne peut prévoir ce que l'avenir nous réserve. Il est en tout cas évident que plus notre économie dépendra des réseaux informatiques, plus ces réseaux présenteront d'intérêt pour les criminels, les spammeurs et d'autres hôtes indésirables. La meilleure défense est celle qui s'adapte facilement aux menaces futures tout en restant abordable.

La sécurisation n'est pas un problème qu'il est possible de résoudre une fois pour toutes. Une entreprise qui a peu d'activités sur Internet et qui communique principalement en interne, a besoin d'une autre sécurisation qu'une entreprise qui dépend largement de l'Internet, comme par exemple un magasin en ligne. Cela signifie que pour chaque nouveau service que vous développez ou contractez, vous devrez évaluer son impact sur les risques en matière de sécurisation et déterminer les mesures à prendre. Vous envisagez de vous abonner à un logiciel en ligne ? Faites l'inventaire des risques que cela comporte. Vous souhaitez permettre à vos collaborateurs d'accéder au réseau de votre entreprise depuis leur domicile ? Idem.

Tous les composants de votre réseau travaillent en étroite collaboration pour échanger des informations, améliorer encore la sécurisation et peuvent être gérés depuis un seul point. Ils s'avertissent mutuellement de l'existence d'une nouvelle menace. Ils reconnaissent un danger possible grâce à un logiciel innovant de reconnaissance de comportement qui identifie les menaces. S'ils reconnaissent un nouveau virus ou une attaque de hacker, les composants du réseau développent en un clin d'œil de nouveaux mécanismes de défense. Le réseau est protégé de l'intérieur comme de l'extérieur.

Votre collaborateur chargé de l'informatique est content qu'on ne l'appelle plus en pleine nuit pour lui demander d'intervenir. Cela lui permet de gagner du temps et lui évite un stress inutile. Étant donné que la sécurisation est largement intégrée aux composants du réseau qu'il doit de toute façon administrer, la maintenance de l'environnement de sécurisation ne lui demande que très peu de temps supplémentaire. Il a en outre choisi une plateforme de sécurisation distincte qui contrôle tous les composants et toutes les fonctions de sécurisation. Cela lui permet d'économiser encore plus de temps.

Avec un Cisco Self Defending Network, vous serez prêt à respecter toutes les réglementations et les lois en matière d'intégrité des données financières et de protection de la confidentialité de vos données clients. Vous économiserez également les coûts liés aux infections par des virus et au vol de données. La probabilité de tels dommages est en effet réduite au maximum.



Composants d'un Cisco Self Defending Network

Les mesures que vous devez prendre pour protéger votre entreprise dépendent bien sûr entièrement de votre situation, c'est-à-dire de la façon dont vous menez vos activités. Un magasin en ligne rencontre d'autres problèmes qu'une entreprise qui, hormis pour le courrier électronique, n'utilise presque pas Internet. Vos projets d'avenir doivent également être pris en compte. Il est toutefois possible de définir un certain nombre d'étapes standard. Cisco collabore avec des Select Partners PME locaux qui peuvent vous assister à réaliser le plan par étapes présenté ci-dessous.

- **Étape 1. Inventaire**

Testez vos propres compétences et l'expertise de vos collaborateurs et collègues pour savoir si vous avez besoin d'aide. Dressez la liste des informations et systèmes (y compris le matériel et le logiciel) nécessitant une protection. Déterminez les menaces et les risques auxquels l'entreprise peut avoir à faire face et les mesures déjà prises. Rédigez une liste d'éléments à sécuriser par ordre de priorité.

- **Étape 2. Planification**

Écrivez des procédures sur la prévention et la détection de menaces, et sur la façon d'y réagir. Désignez aussi clairement la personne responsable, au sein de l'entreprise, de la réalisation du contrôle de ces procédures. Établissez un calendrier d'implémentation. Établissez des règles indiquant aux salariés comment ils doivent utiliser les ordinateurs et le réseau de l'entreprise (réseau, Internet, courriel, etc.)

- **Étape 3. Réalisation**

Mettez les plans à exécution et présentez la politique. Communiquez le progrès à vos collaborateurs et proposez-leur des formations si nécessaire.

- **Étape 4. Contrôle**

Contrôlez régulièrement le respect des procédures et des accords et vérifiez si des ajustements sont nécessaires. Il peut en effet être nécessaire de modifier vos plans en cas de modification du personnel, du matériel ou des logiciels.

- **Étape 5. Recommencer**

Un incident peut être l'occasion de revoir vos plans et vos procédures. Mais quoi qu'il en soit, il est recommandé de réévaluer vos plans et vos procédures régulièrement (par exemple une fois par an) et de les modifier si nécessaire. Continuez à faire l'inventaire des menaces possibles pour garder une sécurisation optimale.

Approche Smart Business Communications

Un environnement informatique sécurisé permet à l'entreprise d'atteindre ses objectifs, et c'est de cela qu'il s'agit en fin de compte. Pour adapter vos projets informatiques aux priorités de votre entreprise, Cisco propose l'approche Smart Business Communications : un projet technologique et d'entreprise intégré permet à votre environnement informatique de croître avec votre entreprise et d'adapter sa sécurisation à la situation.

Afin de guider les entreprises à travers toutes les phases de leur croissance: lancement, croissance et optimisation, l'approche Cisco Smart Business Communications se compose de trois phases. La première phase permet de poser les fondements, appelés Secure Network Foundation : une sécurisation de base suffisante pour les entreprises qui utilisent peu l'Internet en dehors du courrier électronique, et qui constitue un point de

départ idéal pour ajouter des fonctionnalités de sécurisation à un stade ultérieur. Lors de la seconde phase, des risques nouveaux apparaissent du fait que les collaborateurs souhaitent accéder au réseau depuis leur domicile et que des clients souhaitent passer des commandes via Internet. Les mesures de cette phase sont étudiées pour répondre à ces besoins. Dans la troisième phase, l'Internet devient une ressource importante pour votre entreprise. Vous adaptez votre réseau en le configurant de telle façon qu'il puisse se défendre seul. Vous donnez également accès à vos données et à vos applications via Internet. Cisco appelle ce concept "Self Defending Network", le réseau qui se défend lui-même.

Cisco Self Defending Network

Le Cisco Self Defending Network est une solution de sécurisation avancée qui permet de développer des réseaux extrêmement fiables et capables de se défendre seuls. La sécurisation est intégrée dans une large mesure aux composants déjà présents, comme les routeurs et les switches. Cette approche intégrée assure non seulement que tous les composants de votre réseau sont sécurisés, mais facilite également leur installation, leur maintenance et leur administration. Un Self Defending Network est capable de s'adapter à l'évolution des circonstances. Il peut par exemple développer lui-même de nouveaux mécanismes de défense. Vous dépendez donc moins de votre administrateur système ou de votre Select Partner PME Cisco.

Composants d'une stratégie de sécurisation intégrée

Le Cisco Self Defending Network se compose de différents éléments :

- **Pare-feu**

Les pare-feu et dispositifs IPS installés à chaque point d'accès au réseau vous protègent des vers, logiciels espions et hackers afin d'empêcher tout vol d'informations présentes sur le réseau de l'entreprise. Les pare-feu permettent également d'empêcher les utilisateurs de l'entreprise d'accéder à certaines informations sensibles. Les pare-feu internes peuvent être configurés de façon à bloquer, par exemple, l'accès des utilisateurs non autorisés aux ordinateurs du département financier, des ressources humaines ou de la comptabilité. Il est également impossible d'épier les échanges de données.

- **Cisco Intrusion Prevention Systems (IPS)**

Ces systèmes anti-intrusion sont disponibles sur les machines de sécurisation, les routeurs et les switches de Cisco. Ils scannent et examinent en temps réel tout le trafic entrant à la recherche d'irrégularités susceptibles d'indiquer une attaque. Lorsqu'une irrégularité est constatée, l'IPS évalue la gravité du risque et communique ensuite avec les autres composants du réseau dotés de fonctionnalités de sécurisation afin de neutraliser la menace à la source et d'éviter qu'elle ne se répande à travers le réseau. L'IPS est comparable au système d'alarme d'une maison : le pare-feu est la serrure de la porte d'entrée, l'IPS est l'alarme. En cas d'intrusion malgré la serrure, l'IPS veille à ce que les intrus soient détectés et appréhendés.

- **Réseaux privés virtuels (VPN)**

La technologie des réseaux privés virtuels permet aux petites filiales et aux collaborateurs externes (à domicile) de communiquer entre eux et avec le siège principal en toute sécurité, même lorsqu'ils se connectent via l'Internet public. La vérification des utilisateurs veille à ce que seuls les utilisateurs compétents aient accès au réseau. Le cryptage rend les données illisibles pour quiconque tenterait d'intercepter la communication VPN via le réseau public. Si vous le souhaitez, vos collaborateurs peuvent même utiliser une solution VPN sans devoir installer de logiciel spécifique sur leur PC (VPN web). Le collaborateur peut ainsi accéder à Outlook, à ses fichiers et aux applications de l'entreprise depuis son navigateur Internet.

- **Cisco Secure Desktop**

Cisco Secure Desktop évite que des données telles que des cookies, historiques de navigation, fichiers provisoires et contenus téléchargés ne restent sur la machine lorsque la connexion VPN via Internet est interrompue.

- **LAN virtuels (VLAN)**

Les LAN virtuels permettent de segmenter encore plus la communication interne d'une entreprise. Les informations financières sensibles et les données clients peuvent être placées sur un LAN virtuel séparé du LAN sur lequel travaillent vos collaborateurs.

- **Sécurisation anti-X**

Cette fonctionnalité comprend un antivirus, anti-spyware, anti-spam, un filtrage d'URL et le scanning de pages.

- **Network Admission Control**

La fonctionnalité de contrôle d'admission contrôle tous les appareils, identifie les utilisateurs et vérifie que les appareils sont équipés des dernières mises à jour antivirus.



Exemples de solutions de sécurisation Cisco

Ce chapitre vous présente quelques exemples de solutions de sécurisation Cisco. Pour définir la solution qui convient à votre entreprise, nous vous recommandons de contacter un Cisco Select Partner PME. Ce partenaire vous fera volontiers profiter de son expertise et de ses conseils.

PME jusqu'à 50 collaborateurs

Pour les entreprises de 50 collaborateurs maximum, Cisco a développé la solution ASA5505 avec les fonctionnalités suivantes :

- Infrastructure réseau : 8 ports LAN dont 2 avec alimentation électrique sur Ethernet
- Pare-feu avec contrôle approfondi, par exemple pour la messagerie instantanée (débit jusqu'à 150 Mbps)
- VPN remote access server permettant aux utilisateurs d'établir une connexion sûre au réseau interne depuis Internet. Pour les VPN IPsec et les VPN Web (VPN SSL), débit jusqu'à 100 Mbps.
- VPN site-to-site pour créer des VPN entre différents sites, débit jusqu'à 100 Mbps
- Possibilité d'extension future des fonctionnalités
- Gestion intégrée de toutes les fonctionnalités de sécurisation. L'ASA5505 est facile à configurer. Il est également possible d'examiner avec précision les risques qui se présentent.

Jusqu'à 10 utilisateurs

ASA5505 pare-feu et VPN	
ASA5505-BUN-K9	solution ASA 5505 avec logiciel, 10 utilisateurs, 8 ports, 3DES/AES
ASA5505-SEC-PL	ASA 5505 Sec. Plus Lic. avec HA, DMZ, VLAN Trunk, plusieurs connexions.
	en option : nécessaire uniquement pour la prise en charge d'une DMZ, de VLAN et d'un backup ISP
ASA5500-SSL-10	ASA 5500 SSL VPN 10 User License
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 10

Jusqu'à 50 utilisateurs

ASA5505 pare-feu et VPN	
ASA5505-50-BUN-K9	solution ASA 5505 avec logiciel, 50 utilisateurs, 8 ports, 3DES/AES
ASA5505-SEC-PL	ASA 5505 Sec. Plus Lic. avec HA, DMZ, VLAN Trunk, plusieurs connexions.
	en option : nécessaire uniquement pour la prise en charge d'une DMZ, de VLAN et d'un backup ISP
ASA5505-SSL25-K9	ASA 5505 VPN Édition avec 25 utilisateurs SSL, 50 utilisateurs de pare-feu, 3DES/AES
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 25

Nombre d'utilisateurs illimité

ASA5505 pare-feu et VPN	
ASA5505-UL-BUN-K9	Solution ASA 5505 avec logiciel, nombre d'utilisateurs illimité, 8 ports, 3DES/AES
ASA5505-SEC-PL	ASA 5505 Sec. Plus Lic. avec HA, DMZ, VLAN Trunk, plusieurs connexions.
	en option : nécessaire uniquement pour la prise en charge d'une DMZ, de VLAN et d'un backup ISP
ASA5505-SSL25-K9	ASA 5505 VPN Édition avec 25 utilisateurs SSL, 50 utilisateurs de pare-feu, 3DES/AES
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 25

PME entre 50 et 250 collaborateurs

Cisco a développé la solution ASA5510 pour les entreprises entre 50 et 250 salariés.

Elle présente les fonctionnalités suivantes :

- Infrastructure réseau : 4 ports LAN pour la connexion des switches
- Pare-feu avec contrôle approfondi, par exemple pour la messagerie instantanée (débit jusqu'à 300 Mbps)
- VPN remote access server permettant aux utilisateurs d'établir une connexion sûre au réseau interne depuis Internet. Pour les VPN IPsec et les VPN Web (VPN SSL), débit jusqu'à 170 Mbps.
- Pour les VPN IPsec et les VPN Web (VPN SSL), débit jusqu'à 170 Mbps.
- Possibilité d'extension future des fonctionnalités grâce à des cartes modulaires de services sécurisés comme :

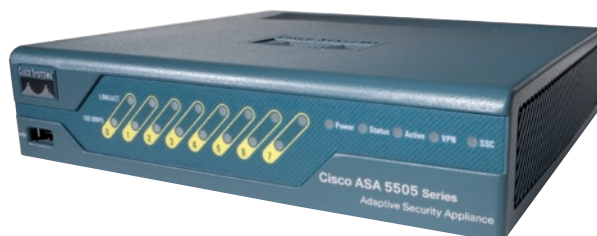
Intrusion Prevention Service (IPS) :

pour détecter et stopper le trafic mal intentionné, y compris les vers et les virus sur réseau avant que votre réseau ne soit infecté.

Sécurisation anti-X :

cette fonctionnalité comprend un antivirus, anti-spyware, anti-spam, un filtrage d'URL et le scanning de pages.

- Gestion intégrée de toutes les fonctionnalités de sécurisation. L'ASA5510 est facile à configurer. Il est également possible d'examiner avec précision les risques qui se présentent.



Pour plus de 50 utilisateurs

ASA5510 pare-feu et VPN	
ASA5510-BUN-K9	Solution ASA 5510 avec logiciel, 3FE, 3DES/AES
ASA5510-SEC-PL	ASA 5510 Security Plus Licence avec A/S HA, plus de VLAN + connexions
	en option : pour prise en charge de la disponibilité élevée, 5 ports Ethernet 10/100
ASA5510-SSL50-K9	ASA 5510 VPN Edition avec 50 licences SSL, 3DES/AES
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 50

Pour plus de 50 utilisateurs

ASA5510 pare-feu et VPN, avec module Anti-X	
ASA5510-CSC10-K9	Solution ASA 5510 avec CSC10, logiciel, 50 utilisateurs AV/spy, 1 an d'abonnement
ASA5510-SEC-PL	ASA 5510 Security Plus Licence avec A/S HA, plus de VLAN + connexions
	en option : pour prise en charge de la disponibilité élevée, 5 ports Ethernet 10/100, le nombre de VLAN passe de 50 à 100
ASA5510-SSL50-K9	ASA 5510 VPN Edition avec 50 licences SSL, 3DES/AES
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 50
ASA-CSC10-PLUS	ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1 an d'abonnement)
	en option : le module anti-X prend en charge de série l'anti-virus et l'anti-spyware, ceci étend les possibilités à l'anti-spam, l'anti-phishing. Filtrage du contenu
ASA-CSC10-USR-100	ASA 5500 Content Security SSM-10 Licence 100 utilisateurs
	en option : le module anti-X prend en charge de série 50 utilisateurs actifs et extension à 100

Pour plus de 50 utilisateurs

ASA5510 pare-feu et VPN, avec module IPS	
ASA5510-AIP10-K9	Solution ASA 5510 avec AIP-SSM-10, logiciel, 3FE, 3DES/AES
ASA5510-SEC-PL	ASA 5510 Security Plus Licence avec A/S HA, plus de VLAN + connexions
	en option : pour la prise en charge de la disponibilité élevée, 5 ports Ethernet 10/100, augmentation du nombre de VLAN de 50 à 100
ASA5510-SSL50-K9	ASA 5510 VPN Edition avec 50 licences utilisateurs SSL, 3DES/AES
	en option : la licence standard permet jusqu'à 2 sessions VPN SSL, cette licence en permet jusqu'à 50
ASA-CSC10-PLUS	ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1 an d'abonnement)
	en option : Le module anti-X prend en charge de série l'antivirus et l'anti-spyware, ceci élargit les possibilités à l'anti-spam et l'anti-phishing. Filtrage du contenu
ASA-CSC10-USR-100	ASA 5500 Content Security SSM-10 Licence 100 utilisateurs
	en option : le module anti-X prend en charge de série 50 utilisateurs actifs et extension à 100



Nos services

Cisco PME Select Partners

Cisco travaille avec un réseau local de 110 PME Select Partners. Nos Select Partners PME sont là pour vous offrir un service optimal. Depuis des solutions utiles jusqu'à un soutien fiable et précieux. Les partenaires de Cisco sont des spécialistes qui savent exactement comment tirer le meilleur de votre infrastructure réseau en matière de routage et de switching, de Unified Communications, de réseaux sans fil et de sécurisation. Ils possèdent également une connaissance et une expertise approfondies dans les domaines de la conception, de l'installation, de l'entretien et de la maintenance. Ils peuvent vous aider à configurer votre infrastructure de façon à répondre parfaitement aux exigences spécifiques de votre entreprise. Pour vous aider à atteindre vos objectifs.

Services Cisco : SMARTnet & PME Support Assistant

Cisco vous propose deux services : SMARTnet et PME Support Assistant. SMARTnet signifie Software Maintenance Advance Replacement et Technical Assistance. Cela signifie qu'en cas de défaillance d'une machine, celle-ci est remplacée le jour ouvrable suivant. Vous profitez en permanence des mises à jour et des mises à niveau logicielles. Nos clients sous contrat SMARTnet bénéficient d'un support en ligne 24 heures sur 24 depuis notre Technical Assistance Centre de Bruxelles. Nos collaborateurs vous en diront volontiers davantage sur les conditions applicables.

Le PME Support Assistant Cisco est un programme avantageux et facile à utiliser qui vous aide à faire face aux problèmes les plus fréquents et qui assure en permanence la disponibilité et la sécurité de votre réseau. Il signale en temps utile où des problèmes sont apparus, comment les résoudre et quand il convient de commander un nouveau composant. Le portail Cisco PME Support Assistant est une série d'outils en ligne permettant aux clients de restaurer des mots de passe, de consulter la documentation de soutien, de contrôler le réseau, de télécharger des patches logiciels et de créer des dossiers de support si nécessaire.

Solutions de financement Cisco

Votre entreprise peut profiter rapidement des dernières technologies Cisco grâce aux solutions de financement de Cisco Capital EasyLease, qui vous proposent des financements abordables, simples et clairs. Vous pouvez ainsi relâcher la pression sur votre budget et libérer des liquidités.

Les principaux avantages d'une solution de financement via Cisco Capital EasyLease sont les suivants :

- Maintien du capital. Les paiements prévisibles et abordables vous aident à conserver vos liquidités et vos lignes de crédit.
- Pas d'obsolescence technologique. Le contrat de leasing peut prévoir une option de mise à niveau technologique. Vous pouvez ainsi passer aux dernières technologies à un certain moment de votre période de leasing.
- Flexibilité maximale. Choisissez et implémentez une solution en fonction des besoins de votre entreprise et non de restrictions budgétaires éventuelles. Votre technologie reste ainsi récente et en ligne avec les besoins de vos utilisateurs.

EasyLease

EasyLease est un programme de financement souple que Cisco Capital™ propose aux petites et moyennes entreprises. EasyLease propose des conditions claires à des prix compétitifs. Il a été conçu pour proposer aux entreprises un réseau avancé pour leur permettre de fonctionner avec plus de succès encore.



Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam Pays-Bas
www-europe.cisco.com
Tél : +31 0 800 020 0791
Fax : +31 0 20 357 1100

Plus d'informations via 0800 73639
www.cisco.be/pme

08/2008