



Protection de l'entreprise par le
réseau : la sécurité simplifiée



Toutes les entreprises, quelle que soit leur taille, prennent à cœur la sécurité de leurs informations. Numéros de carte bancaire clients, données comptables confidentielles, données relatives aux achats, aux fournisseurs et au stock - personne ne souhaite laisser divulguer de telles informations. Alors comment construire votre infrastructure pour éviter toute fuite ?

Un système de sécurité efficace doit :

- Vous protéger contre les attaques internes et externes
- Garantir la confidentialité de toutes les communications, partout et à chaque instant
- Contrôler l'accès aux informations en identifiant les utilisateurs et leurs systèmes avec certitude
- Limiter les responsabilités engagées en matière de respect des réglementations
- Tenir compte de votre culture d'entreprise et de vos méthodes de travail
- Maintenir le niveau de productivité en permettant le déploiement rapide de nouvelles applications
- Garantir un retour sur investissement (ROI) rapide et réutiliser l'existant (matériel et logiciels) chaque fois que possible

Les technologies réseau Cisco® sont les plus avancées du marché pour préserver la confidentialité de votre entreprise. Dans le cadre de la stratégie « des réseaux capables de se défendre tout seuls », tous les éléments de l'infrastructure - applications, PC, portables, téléphones IP, serveurs, mais aussi périphériques réseau tels que routeurs, commutateurs, points d'accès sans fil - intègrent des fonctionnalités de sécurité qui visent à protéger votre entreprise.



Comprendre le fonctionnement de la sécurité

Pour une protection exhaustive de l'entreprise, reposer sur une seule méthode de sécurité ne suffit pas : vous devez mettre en place un ensemble de barrières qui vous défendent de plusieurs manières. Ainsi, même si une solution est mise en échec, les autres demeurent actives et protègent votre entreprise et ses données contre une multitude d'attaques.

Ces barrages multiples, directement intégrés au réseau qui supporte toutes vos autres technologies, protègent immédiatement et automatiquement l'ensemble de vos applications, équipements et périphériques. C'est le concept initial de la stratégie Cisco Self-Defending Network, des réseaux capables de se défendre tout seuls. La force de cette solution réside dans sa souplesse : que votre entreprise se trouve en phase d'expansion ou de concentration, qu'elle diversifie ses canaux de distribution, fasse évoluer son matériel ou change de locaux, le réseau protège invariablement l'ensemble de l'infrastructure.

Détail des offres de sécurité Cisco :

- **Déploiement de pare-feu** - les pare-feu isolent le réseau d'entreprise sécurisé d'autres réseaux non protégés, comme Internet, en bloquant le trafic indésirable. De plus, ils surveillent et contrôlent le trafic légitime en observant une « politique de sécurité » (ensemble de règles définissant le trafic autorisé). Les applications courantes telles que le courrier électronique, la messagerie instantanée et les navigateurs web sont protégées contre les utilisations abusives.
- **Établissement de communications sécurisées** - les réseaux privés virtuels (VPN) cryptent les informations avant de les envoyer, ce qui permet d'authentifier les utilisateurs et de protéger vos informations. Les VPN sont donc un outil essentiel pour les télétravailleurs qui utilisent Internet à leur domicile ou via des points d'accès publics et des hôtels équipés Wi-Fi.

- **Protection du réseau contre les intrusions et les attaques** - les systèmes de prévention des intrusions (IPS) balayent le réseau à la recherche de comportements nuisibles et malveillants. Ils peuvent même prendre des mesures de correction face à une attaque, et alerter les responsables du réseau.
- **Contrôle des menaces émanant d'Internet** - des défenses avancées protègent le contenu et les utilisateurs contre les virus, les spyware et le spam.
- **Gestion de la sécurité des terminaux** - le contrôle de l'admission sur le réseau (NAC) protège votre réseau en vérifiant l'identité de chaque utilisateur avant de l'autoriser à accéder à ses données.
- **Gestion de l'accès des utilisateurs** - les services AAA (Authentication, Authorization and Accounting) facilitent la vérification de l'identité des utilisateurs du réseau, permettent d'attribuer le niveau d'accès approprié et empêchent les utilisations non autorisées.

Pour vous aider à tirer pleinement avantage de tous ces outils, Cisco a mis au point une stratégie **Smart Business Roadmap** à l'usage des PME. Cette initiative propose un itinéraire structuré, qui met en corrélation les enjeux commerciaux et les « points faibles » avec des solutions techniques qui vous aideront à faire avancer votre entreprise et à vous rapprocher d'un niveau de performance optimal.

Meilleure sécurité associée à un meilleur contrôle des coûts

Le contrôle des coûts est une préoccupation majeure pour toutes les entreprises. La mise en œuvre d'une solution de sécurité réseau facile à déployer, à intégrer et à gérer confère aux entreprises une plus grande maîtrise de leurs frais. Tirer parti de votre investissement en infrastructure et applications Cisco vous aidera à réduire vos dépenses et à limiter les pertes imputables au piratage ou à la disparition de données. Avec un niveau de sécurité adapté :

- Internet peut être employé comme un canal peu coûteux pour des communications d'entreprise et des transactions commerciales sécurisées.

- Les pertes de données dues aux attaques de virus ou de vers sont éradiquées.
- Les directeurs informatiques peuvent superviser le réseau depuis des sites distants, avec des déplacements réduits et une productivité accrue.
- L'investissement en équipement de sécurité requis par votre société est moindre.
- Votre entreprise est mieux préservée des pertes résultant de contentieux éventuels.
- Vous vous êtes assuré de votre conformité aux directives réglementaires, y compris aux exigences communes telles que les normes PCI de sécurité des cartes bancaires.
- La bande passante réseau est correctement attribuée en fonction de l'utilisation, ce qui améliore les performances et la réactivité du réseau.

Amélioration de l'efficacité opérationnelle

La stratégie Cisco Self-Defending Network permet d'intégrer la sécurité aux opérations de votre société, ainsi qu'à votre réseau. Votre système de sécurité sait détecter les menaces et y réagir automatiquement, empêchant les fichiers infectés ou les activités malveillantes de nuire à votre activité. Vos transactions sécurisées peuvent être étendues à des sites distants ainsi qu'à vos fournisseurs, revendeurs et partenaires.

Avantages de la sécurité intégrée :

- Tous les employés - locaux, mobiles et télétravailleurs - restent productifs partout et à tout moment, grâce à un accès sécurisé aux ressources et aux outils de la société.
- Vous pouvez travailler avec une totale confiance dans l'intégrité de vos informations.
- La confidentialité des données sensibles de vos clients et fournisseurs est préservée.
- Les périodes d'inactivité du réseau dues à des actes malveillants sont limitées au minimum.

- La productivité des employés augmente du fait que le réseau et les applications commerciales critiques réagissent plus rapidement.
- Les transactions commerciales sont traitées électroniquement et en temps utile ; les rapports financiers sont disponibles en temps réel.
- Les documents des fournisseurs et de conformité sont fournis avec un effort minimal.
- Votre société gagne en efficacité en établissant des relations en ligne avec ses clients et ses fournisseurs.
- La gestion des flux de travail est améliorée pour une production maximale.
- Les applications de courrier électronique et de messagerie instantanée sont protégées contre les utilisations abusives.

Réactivité des clients

À un niveau élémentaire, améliorer la réactivité des clients face à votre entreprise se traduit par un certain nombre d'avantages :

- Employés plus faciles à joindre
- Les employés disposent de nombreux moyens de rester connectés et en contact avec les clients
- Site web fiable et à jour mis à la disposition des clients
- Accès rapide et sûr aux données historiques des clients pour les employés

La sécurité des réseaux est un facteur essentiel pour que votre entreprise atteigne ce degré de réactivité, car elle permet aux employés et aux vendeurs autorisés de bénéficier des services de voix et de données de la société via une connexion réseau sécurisée et ce, quel que soit l'endroit où ils se trouvent. La productivité des employés dans le traitement des demandes de service et de renseignements augmente donc puisqu'ils peuvent répondre dans les meilleurs délais aux messages électroniques ou vocaux et aux appels importants lorsqu'ils sont en déplacement, qu'ils travaillent chez eux ou se trouvent chez un client.

En outre, un site web professionnel et sécurisé donne une image extrêmement positive aux clients, et l'impression que votre société est à même de répondre à leurs attentes. La technologie de sécurité Cisco protège votre site web afin qu'il soit toujours prêt à fournir des informations exactes et à recevoir des commandes client en toute sécurité.

Un site web sécurisé offre les avantages suivants :

- Les clients obtiennent les informations qu'ils recherchent rapidement et sans effort.
- Les clients se sentent tout à fait tranquilisés par la certitude que leurs données sensibles sont protégées.
- Les clients vous perçoivent comme une société compétitive et moderne.
- Les employés assurent leur service aux clients depuis leur bureau, en déplacement ou en travaillant à distance grâce à un accès complet au réseau voix et données.
- Les clients peuvent acheter vos produits et services simplement et en toute sécurité sur votre site web.
- Les sites web d'entreprise mis à la disposition des clients sont protégés contre le piratage et les abus.

Étape suivante

La sécurité est le service intégré le plus demandé par les entreprises, quelle que soit leur taille. Grâce à l'initiative Smart Business Roadmap, Cisco fournit des solutions de sécurité plébiscitées, dont les fonctionnalités intelligentes, résilientes et adaptables garantissent la protection de vos données. Chaque facette du réseau est protégée par des fonctions de sécurité intégrées qui mettent votre organisation à l'abri de toutes les menaces.

Pour faire bénéficier votre entreprise des solutions de sécurité Cisco, contactez votre partenaire Cisco. Pour en savoir plus, visitez le site :

www.cisco.fr/go/securitePME/

**Siège Etats-Unis**

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 : 408 527-0883

Siège Asie Pacifique

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tél. : +65 6317 7777
Fax : +65 6317 7799

Siège Europe

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

Cisco possède plus de 200 agences dans le monde. Vous trouverez les adresses, numéros de téléphone et de fax de ces agences sur le site web de Cisco à l'adresse www.cisco.com/go/offices.

©2006 Cisco Systems, Inc. Tous droits réservés. CCVP, le logo Cisco et le logo Cisco Square Bridge, sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, est une marque de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FollowMe Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux Etats-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0609R)

C02-378290-00 11/06