Cisco Systems

PROFITEZ DU RÉSEAU. maintenant.

GUIDE SÉCURITÉ CISCO

SOMMAIRE

L'IMPORTANCE DE LA SÉCURITÉ 4

LES MENACES ET LES ENNEMIS 5

- Quelles sont les menaces ?
- Qui sont les ennemis ?

LES VECTEURS DE MENACES 6

- Virus et vers
- Chevaux de Troie
- Vandales
- Attaques
- Interception de données
- Social engineering
- Les nouvelles menaces

POLITIQUES DE SÉCURITÉ 8

- L'établissement d'une politique de sécurité
- 10 conseils pour définir une politique de sécurité

LES COMPOSANTES DE LA SÉCURITÉ . . . 10

- Pare-feu
- Contrôle d'accès
- Cryptage et réseaux VPN
- Détection d'intrusions
- Logiciel de sécurité de point d'extrémité

COMMENT RÉPONDRE À L'ÉVOLUTION DES MENACES DE SÉCURITÉ 13

- Les réseaux capables de se défendre tout seuls

L'IMPORTANCE DE LA SÉCURITÉ

Internet offre des possibilités à la fois riches et nouvelles pour la croissance et le développement commercial. Grâce à la diversité des services et des solutions désormais disponibles sur le réseau, les sociétés sont mieux à même de prendre soin de leur clientèle, de générer des synergies entre des employés géographiquement éloignés et de se créer des opportunités de nouveaux revenus par l'accès à une base de clients plus large et plus diversifiée.

Mais si Internet a transformé et nettement amélioré les transactions commerciales, ce vaste réseau et les technologies qui lui correspondent ont ouvert la porte à un nombre croissant de menaces relatives à la sécurité contre lesquelles les entreprises doivent se prémunir. Bien que les attaques des réseaux soient généralement plus graves lorsqu'elles visent des sociétés qui stockent des données critiques, comme des dossiers confidentiels médicaux ou financiers, les conséquences de ces attaques sur une entreprise peuvent aller d'un léger désagrément à une paralysie complète de l'activité, des données importantes peuvent être perdues, la confidentialité peut être transgressée et plusieurs heures ou jours d'interruption du réseau peuvent s'en suivre.

Maintenant, plus que jamais, il est impératif que les entreprises intègrent la sécurité au sein de l'architecture de leur réseau afin de limiter ces risques et de concrétiser le potentiel de croissance inhérent à l'environnement de réseau.

Ces menaces génèrent assez fréquemment des alertes jugées sérieuses. En effet, selon une étude récente (Octobre 2003) de ZDNet.fr réalisée auprès de 336 décisionnaires IT en France, seulement 4,4% des sondés estiment qu'ils n'en ont jamais constaté, alors que 65,5 % affirment en avoir subi durant les trois derniers mois et 41,5% avouent avoir déploré des dégâts, suite à une défaillance de la sécurité.

LES MENACES ET LES ENNEMIS

Quelles sont les menaces ?

Les menaces sur la confidentialité et l'intégrité des données proviennent d'un très petit nombre de vandales. Cependant, alors qu'un voleur de voiture ne peut voler qu'un seul véhicule à la fois, un seul pirate peut, à partir d'un simple ordinateur, engendrer des dégâts sur un grand nombre de réseaux informatiques, faisant des ravages dans le monde entier. Le fait le plus inquiétant est peut-être que le danger peut provenir de personnes que nous connaissons.

En effet, la plupart des experts en sécurité des réseaux déclarent que la majorité des attaques des réseaux sont effectuées par des employés travaillant dans des sociétés comportant des failles dans leur sécurité. Les employés peuvent sans difficulté endommager les réseaux de leur société et détruire des données, que ce soit par malveillance ou par erreur.

De plus, grâce à l'évolution récente des technologies de connexion à distance, les sociétés développent de plus en plus le télétravail, ouvrent plus facilement de nouvelles succursales et augmentent leur réseau de partenaires commerciaux. Ces employés et partenaires distants représentent les mêmes dangers que les employés internes, les risques seront d'autant plus élevés si leur accès à distance au réseau n'est ni sécurisé ni contrôlé.

Qu'il s'agisse de protéger une voiture, une maison, une nation ou un réseau informatique, il est essentiel de connaître les principaux ennemis ainsi que leurs modes d'action.

Qui sont les ennemis ?

Pirates informatiques (hackers)

Ce terme générique s'applique aux passionnés d'informatique s'amusant à accéder aux ordinateurs et aux réseaux d'autres personnes.

Personnel non avisé

Il arrive souvent que des employés, concentrés sur leurs activités professionnelles spécifiques outrepassent les règles de base de sécurité du réseau. Ils peuvent, par exemple, choisir des mots de passe simples à mémoriser afin de se connecter aisément au réseau. Ces mots de passe sont alors faciles à deviner ou à forcer par les pirates, de manière logique ou à l'aide d'un utilitaire logiciel de "cracking" (logiciel permettant de découvrir les mots de passe) largement répandu.
Les employés peuvent involontairement être la source de failles dans la sécurité, y compris la contamination accidentelle par des virus informatiques et leur propagation.

Employés mécontents

Ce problème est bien plus troublant que l'éventualité d'une erreur humaine endommageant le réseau : un employé mécontent peut vouloir nuire à l'entreprise. Les employés mécontents, souvent à la suite d'un licenciement ou d'une remontrance, peuvent infecter le réseau de leur entreprise par des virus ou intentionnellement supprimer des fichiers importants ou encore en accédant à des données confidentielles afin de fournir aux concurrents des informations qu'ils n'auraient pas pu obtenir d'une autre manière.

LES VECTEURS DE MENACES

• Virus et vers

Les virus représentent la menace sur la sécurité la plus largement connue car bénéficiant généralement d'une importante couverture médiatique. Les virus sont des programmes informatiques écrits par des programmeurs mal intentionnés et conçus pour se multiplier et infecter les ordinateurs lorsqu'ils sont activés par un événement spécifique.
Un ver informatique est un programme complet (ou un ensemble de programmes) qui est capable de répandre des copies fonctionnelles de lui-même (ou de ses segments) sur d'autres systèmes informatiques (en règle générale via un réseau). Contrairement aux virus, les vers n'ont pas besoin de programme hôte. Il existe deux types de vers : les vers de station de travail et les vers de réseau.

• Chevaux de Troie

Les chevaux de Troie sont des programmes véhiculant un code destructif. Ils apparaissent sous la forme d'un programme utile ou inoffensif, comme des jeux informatiques, mais ils sont généralement des ennemis cachés. Les chevaux de Troie peuvent supprimer des données, envoyer des copies d'eux-mêmes par courrier électronique à tout le carnet d'adresses et exposer les ordinateurs à des attaques supplémentaires (certains chevaux de Troie ouvrent simplement une brèche de sécurité par laquelle un ver pourra se répandre).

• Vandales

Les sites Web sont désormais animés grâce au développement d'applications logicielles telles que ActiveX et les applets Java. Ces dispositifs permettent d'exécuter des animations et d'autres effets spéciaux afin de rendre les sites Web plus attractifs et interactifs. Cependant, la simplicité de leur téléchargement et de leur exécution a donné lieu à un nouveau moyen d'endommager les réseaux.
Un vandale est une application logicielle ou un applet entraînant une destruction à différents niveaux : il peut effacer un seul fichier ou la majeure partie d'un système informatique.

• Attaques

De nombreux types d'attaques du réseau ont été identifiés. Ces attaques sont généralement classées en trois principales catégories : attaques dans le but de découvrir des informations, attaques par intrusion et attaques d'interruption de service.

- La première catégorie d'attaque consiste à récolter des informations que les pirates utiliseront par la suite pour détruire les réseaux. Généralement, des outils logiciels tels que les "renifleurs de paquets" (sniffers) ou les scanneurs (scanners) sont utilisés pour analyser les ressources d'un réseau cible, d'un hôte ou d'une application et en exploiter les éventuelles faiblesses. Par exemple, il existe des logiciels spécialement conçus pour découvrir les mots de passe. Ces logiciels ont été créés à l'origine à l'intention des administrateurs système afin de leur permettre de retrouver les mots de passe oubliés des employés ou de déterminer les mots de passe des employés ayant quitté la société sans communiquer cette information. Aux mains de pirates, ces logiciels peuvent se transformer en une arme redoutable.

- Les attaques par intrusion sont entreprises afin d'exploiter les faiblesses de certaines zones du réseau telles que les services d'authentification afin d'obtenir un accès aux comptes de messagerie électronique, aux bases de données et à d'autres informations confidentielles.

- Les attaques d'interruption de service saturent l'accès à une partie ou à l'intégralité d'un système. Elles s'exécutent généralement par l'envoi massif de données brouillées ou inexploitables à une machine connectée à un réseau d'entreprise ou à Internet, bloquant ainsi le trafic normal des données. Les attaques d'interruption de service distribué (DDOS, Distributed Denial of Service) qui consistent à saturer ainsi plusieurs machines ou hôtes sont encore plus nuisibles.

Il existe encore des attaques par saturation appelées attaques en «buffer overflow» qui saturent la mémoire cache des CPU de n'importe quel élément du réseau. Ces attaques sont particulièrement dévastatrices car elles peuvent rendre un nœud de réseau totalement indisponible.

• Interception de données

Les données transférées via un type de réseau quelconque peuvent être interceptées par des personnes non autorisées. Celles-ci peuvent procéder à l'interception électronique de communications ou même dégrader les paquets de données transférées. Ils peuvent intercepter les données au moyen de différentes méthodes. Par exemple, l'usurpation d'adresse (IP Spoofing) consiste à se faire passer pour une machine autorisée dans la transmission des données en utilisant l'adresse IP d'un des destinataires des données.

• Social engineering

Il s'agit d'une méthode, de plus en plus répandue, pour obtenir des informations confidentielles relatives à la sécurité du réseau par des moyens non techniques. Par exemple, un fraudeur peut se présenter comme un membre du support technique et appeler les employés pour obtenir leurs mots de passe. Obliger un collègue à accéder à un serveur ou fouiller le bureau d'un collègue à la recherche d'un document contenant son mot de passe sont d'autres exemples de social engineering.

• Les nouvelles menaces

Les pirates attaquent ce qu'ils connaissent. Dans un premier temps, ils se sont intéressés à l'interception des mots de passe et des "login", puis aux serveurs. On entre aujourd'hui dans une 3ème phase : ils se font passer pour une application ou un utilisateur pour saboter le système d'information. Demain, ils prendront possession du poste client et procéderont de même pour se glisser partout et attaquer le réseau en tant que tel. En d'autres termes, autrefois, on sécurisait la périphérie des systèmes d'information et on était à l'abri. Aujourd'hui ce n'est plus suffisant, le poste client et les serveurs sont au cœur des problématiques actuelles de sécurité : ils doivent être protégés. Il faut anticiper les comportements des pirates et élaborer des schémas directeurs et des architectures capables de s'adapter en permanence aux nouvelles formes d'attaques. Il faut penser en termes de prévention et non plus de réaction. C'est d'autant plus primordial que les attaques ont gagné en rapidité : là où on raisonnait en semaines auparavant, tout se joue désormais en quelques heures.

POLITIQUES DE SÉCURITÉ

Lors de la configuration d'un réseau, qu'il s'agisse d'un réseau local (LAN), d'un réseau local virtuel (VLAN), ou d'un réseau étendu (WAN), il est important de définir dès le début les politiques de sécurité. Les politiques de sécurité sont des règles électroniques programmées et stockées dans un dispositif de sécurité destinées à contrôler des aspects comme les droits d'accès. Ces politiques de sécurité sont, bien sûr, également des règlements écrits ou oraux régissant le fonctionnement d'une société. De plus, les sociétés doivent désigner le responsable de l'application et de la gestion de ces politiques et déterminer le mode d'information des employés à propos des règles et des protections.

L'établissement d'une politique de sécurité

Une politique de sécurité repose essentiellement sur quatre piliers :

1. Décrire clairement votre modèle métier.

Il serait absurde de concevoir ou de déployer une solution de sécurité qui ne serait pas fondée sur la nature de vos objectifs métier. Identifiez clairement vos objectifs métier en y incluant le type de services et d'accès qui vous sont nécessaires pour les atteindre.

2. Identifier en détail les risques associés.

Si vous prévoyez d'héberger un segment de services au public (encore appelé zone démilitarisée ou DMZ) et d'offrir des activités de commerce électronique, vous devez comprendre toutes les manières dont les pirates chercheront à exploiter vos systèmes et vos services. Quels sont les risques si la page Web est saccagée, si un pirate s'introduit sur un serveur ou si une base de données de clients est attaquée ? De quelle manière ces attaques sont-elles menées ? Les pirates contournent-ils le pare-feu en se cachant dans le trafic Web autorisé ou cherchent-ils à exploiter des vulnérabilités dans des systèmes d'exploitation mal mis à jour ? Ces questions doivent être soigneusement examinées et comprises avant de pouvoir passer à l'étape suivante. A mesure que vous ajoutez de nouveaux systèmes ou de nouveaux services à votre réseau, vous introduisez de nouveaux risques. Les procédures régulières d'administration du réseau doivent comprendre une évaluation régulière et complète des faiblesses du système.

3. Adopter une démarche systématique de limitation de ces risques.

Tout dans un réseau peut constituer une cible, qu'il s'agisse des routeurs, des commutateurs, des hôtes, des applications, des réseaux et des systèmes d'exploitation. Pour être efficace, une politique de sécurité doit tenir compte de chacune de ces composantes. La mise en œuvre des solutions de sécurité repose sur les trois "P" : les Personnes, les Produits et les Procédures. Vous devez disposer de techniciens compétents pour mettre en œuvre votre politique, vous devez utiliser des outils spécifiquement conçus pour supporter votre stratégie e-business et vous devez associer à tout cela une administration système et une politique d'analyse efficaces.

4. Garder à l'esprit que la sécurité est un processus.
Une politique de sécurité n'est pas une solution "gravée dans le marbre". La sécurité exige des études, des analyses et des améliorations régulières pour offrir le niveau de protection dont votre entreprise a besoin. Vous pouvez également envisager l'acquisition d'un utilitaire d'évaluation des vulnérabilités ou encore signer un contrat avec un partenaire extérieur de contrôle de la sécurité afin de vérifier votre politique, vos procédures et votre mise en œuvre et, dans certains cas, vous décharger de certaines tâches à forte composante de main-d'œuvre comme la surveillance. Lorsque vous élaborez votre politique de sécurité, gardez à l'esprit la liste des dix conseils de sécurité les plus importants, mise au point par l'équipe Security Consulting Services de Cisco.

10 conseils pour définir un politique de sécurité

1. **Inciter ou obliger les employés à choisir des mots de passe qui ne soient pas évidents à trouver,**
2. **Exiger des employés qu'ils changent leurs mots de passe tous les 90 jours,**
3. **Vérifier que l'abonnement à la protection antivirus est à jour,**
4. **Sensibiliser les employés aux risques relatifs à la sécurité des pièces jointes aux messages électroniques,**
5. **Mettre en œuvre une solution de sécurité du réseau complète et adéquate,**
6. **Evaluer régulièrement l'infrastructure de sécurité,**
7. **Supprimer immédiatement les droits d'accès au réseau d'un employé quittant la société,**
8. **Si des employés sont autorisés à travailler à distance, mettre en place un serveur sécurisé et géré de façon centralisée pour le trafic distant,**
9. **Mettre à jour régulièrement le logiciel du serveur Web,**
10. **Ne pas exécuter de services de réseau superflus.**

LES COMPOSANTES DE LA SÉCURITÉ

Pare-feu
Un pare-feu est une solution matérielle ou logicielle qui administre l'accès au réseau ou à un segment du réseau. C'est l'équivalent électronique d'une porte verrouillée qui ne permet de passer qu'à ceux qui en possèdent la clé ou une carte d'accès. Il crée une barrière de protection entre le réseau et le monde extérieur et, placé au point de contact entre les deux, il négocie les accès au réseau et interdit l'entrée des documents non autorisés ou potentiellement dangereux.

Les pare-feux de la gamme Cisco PIX sont des équipements matériels qui offrent une protection forte dans un serveur dédié intégrant matériel et logiciel. La famille des pare-feux Cisco PIX convient à tous les types d'utilisateur final, du pare-feu économique de bureau pour les utilisateurs distants jusqu'aux pare-feux de type opérateur de télécommunication pour les entreprises les plus exigeantes et les environnements de fournisseur d'accès. Les pare-feux de la gamme Cisco PIX sont conçus dans une logique de sécurité totale et de déploiement facilité grâce à une mise en œuvre simple, un coût d'exploitation réduit et des performances maximales supportant des interfaces de 1Go.

Le pare-feu embarqué dans l'IOS Cisco enrichit les possibilités du système d'exploitation réseau IOS Cisco en intégrant les fonctionnalités du pare-feu PIX et la détection des intrusions dans les unités de réseau, ce qui permet de faire profiter l'ensemble de l'infrastructure de la protection et des fonctionnalités du pare-feu. Une mise en œuvre large permet de créer des zones de défense au sein de votre conception de réseau pour une protection par couches. En association avec le logiciel Cisco IOS VPN IP Sec, le pare-feu Cisco IOS offre une solution de réseau privé virtuel complète et intégrée. Comme le pare-feu est disponible avec un grand nombre de routeurs Cisco, il laisse le choix d'une solution capable de s'adapter à la bande passante, à la densité du réseau local ou distant et aux exigences du multiservice, tout en offrant des fonctions de sécurité évoluées. Il répond à une logique d'intégration de la sécurité au sein même du routeur, permettant l'administration à distance et facilite la maintenance.

Contrôle d'accès
Avant qu'un utilisateur ne puisse accéder au réseau au moyen d'un mot de passe, le réseau doit en vérifier la validité. Les serveurs de contrôle d'accès valident l'identité de l'utilisateur et déterminent, à partir des profils d'utilisateur en mémoire, à quelles zones ou informations l'utilisateur peut accéder.

Le serveur de contrôle d'accès Cisco Secure ACS est une unité haute performance et extensible qui fonctionne comme un système serveur centralisé et assure l'identification, le contrôle des autorisations et le suivi des utilisateurs qui accèdent aux ressources de l'entreprise par l'intermédiaire du réseau. Cisco Secure ACS supporte le contrôle d'accès et le suivi pour les accès traditionnels au réseau, les serveurs à accès commuté, les VPN, les pare-feux, le protocole voix sur IP (VoIP) et l'accès sans fil.

Cryptage et réseaux VPN

La technologie de cryptage garantit que les messages ne peuvent être interceptés ou lus par personne d'autre que le destinataire autorisé. Le cryptage est généralement utilisé afin de protéger les données transportées via un réseau public et utilise des algorithmes mathématiques pour "brouiller" les messages et leurs pièces jointes. Il existe plusieurs types d'algorithmes de cryptage, mais certains sont plus sûrs que d'autres. Le cryptage fournit la sécurité nécessaire à la prise en charge de la technologie en pleine expansion des Réseaux Privés Virtuels (VPN). Les VPN sont des connexions privées, ou des tunnels, vers des réseaux publics comme Internet. Ils sont déployés afin de connecter des télétravailleurs, des employés mobiles, des succursales et des partenaires commerciaux entre eux et aux réseaux d'entreprise.

Tous les dispositifs matériels et logiciels de VPN prennent en charge la technologie de cryptage afin de fournir la meilleure protection possible des données transportées.

La gamme de concentrateurs Cisco VPN 3000 est une famille de plates-formes spécialisées de réseau privé virtuel à accès à distance qui réunit des qualités de haute disponibilité, de hautes performances et d'extensibilité avec les techniques les plus avancées de codage et d'identification actuellement sur le marché.

Détection d'intrusions

Les sociétés continuent à déployer des pare-feux comme protecteurs principaux contre l'entrée d'utilisateurs non autorisés sur le réseau. Cependant, la sécurité des réseaux est très similaire à la sécurité physique et une seule technologie ne répond pas à tous les besoins, c'est pourquoi une protection par niveaux présente les meilleurs résultats.
Les sociétés recherchent de plus en plus des technologies de sécurité permettant de lutter contre les risques et la vulnérabilité pour lesquels les pare-feux sont insuffisants. Un système de détection d'intrusions reposant sur le réseau fournit une surveillance constante du réseau. Ce système analyse les flux de paquets de données du réseau à la recherche d'activités non autorisées, telles que les attaques de pirates, et permet aux utilisateurs de répondre aux failles dans la sécurité avant que les systèmes ne soient compromis. Lorsqu'une activité non autorisée est détectée, le système peut envoyer des alarmes à une console de gestion comportant des détails de l'activité et peut souvent commander à d'autres systèmes comme les routeurs d'interrompre les sessions non autorisées.

La gamme de produits Cisco Secure IDS se compose de capteurs (serveurs dédiés capables de réaliser à grande vitesse des analyses de sécurité) et des modules de carte. Ces capteurs IDS analysent les paquets qui traversent le réseau afin de déterminer si le trafic est autorisé ou s'il est dangereux. Si le flux de données du réseau présente une activité suspecte ou dangereuse, des capteurs peuvent détecter en temps réel la violation de politique, et envoyer des messages d'alerte vers une console centrale d'administration. L'administrateur réseau peut alors surveiller l'activité de nombreux capteurs, et bloquer les attaques.

Logiciel de sécurité de point d'extrémité

Comme l'ont montré les récentes attaques hautement visibles telles que Code Red ou le ver SQL Slammer, les technologies classiques n'offrent qu'une capacité limitée de lutte contre les répercussions des types d'intrusion nouveaux et mutants. Les clients ont besoin d'une sécurité intégrée qui protège leurs systèmes dans toutes les phases d'une attaque et assurent en outre une protection efficace contre les menaces nouvelles et inconnues. Les intrusions sur les systèmes de réseau se déroulent généralement par étapes. Cisco pense que seule une approche en couches s'avère efficace contre les brèches de sécurité qui peuvent se produire à n'importe quel stade, à l'extérieur du périmètre, sur le serveur ou au niveau des fichiers.

La nouvelle génération de logiciels de sécurité de réseau Cisco® Security Agent (CSA) protège contre les menaces les systèmes serveur et station de travail, également nommés « points d'extrémité ». CSA va plus loin que les solutions de sécurité de point d'extrémité classiques, car il identifie et empêche les comportements malveillants avant qu'ils ne se produisent, éliminant ainsi des risques de sécurité connus et inconnus qui pèsent sur les réseaux et les applications d'entreprise. CSA procède par analyse de comportement plutôt que par correspondance de signature, garantissant ainsi une protection robuste et des coûts d'exploitation réduits.

COMMENT RÉPONDRE À L'ÉVOLUTION DES MENACES DE SÉCURITÉ :

Les réseaux capables de se défendre tout seuls

Les virus et les vers qui interrompent la bonne marche des systèmes continuent de désorganiser les entreprises en faisant baisser leur productivité et en les contraignant à corriger en continu les failles de leurs systèmes de sécurité. La nature autoreproductible des attaques les plus récentes les rend particulièrement virulentes et dangereuses. Les solutions anti-virus existantes, qui reposent sur la reconnaissance de la signature de l'attaque, sont incapables de détecter et de neutraliser les virus inconnus et les attaques par déni de service qu'ils génèrent. L'entreprise est fréquemment confrontée à des serveurs et des ordinateurs de bureau qui ne respectent pas sa politique de sécurité. Ces unités sont difficiles à détecter, à isoler et à nettoyer.
La localisation et la mise en quarantaine de ces systèmes consomment beaucoup de temps et de ressources, et même lorsque les infections qu'ils propagent semblent avoir disparu du réseau d'entreprise, elles sont susceptibles de réapparaître par la suite. Le problème est encore multiplié par la complexité des environnements de réseau modernes qui comprennent des types très variés :

- ⇨ utilisateurs finaux – employés, constructeurs et sous-traitants
- ⇨ points d'extrémité – ordinateur de bureau dans l'entreprise ou à domicile, serveurs
- ⇨ accès – filaire, sans fil, réseau privé virtuel (VPN) ou accès commuté

Aujourd'hui, les politiques de sécurité sont gérées avec 2 logiques : une logique réseau (authentification de l'utilisateur, mise à disposition des services réseau –VLANs, ACLs, serveurs et ressources), et une logique système et applicative (Firewalls, détection d'intrusion, anti virus, etc.). Le fait que ces deux logiques soient gérées indépendamment pose des problèmes de montée en charge, d'administration et de sécurité. Par exemple, personne ne peut empêcher un utilisateur de connecter son PC de chez lui à Internet et de potentiellement ramener un virus dans le réseau d'entreprise lors de sa connexion suivante.

L'objectif de Cisco avec NAC (Network Access Control) est de lier ces 2 approches et de les mettre en cohérence : ne permettre l'accès au réseau que si la machine est conforme à la politique de sécurité, qui dépend elle-même de l'identifiant et du mot de passe de l'utilisateur.

Pour assurer ce service, Cisco NAC repose sur 2 composantes :

- Des fonctionnalités IOS qui seront intégrées progressivement par Cisco dans ses plateformes.
- Un Agent, le Cisco Threat Agent (CTA) résident sur la station. C'est cet agent qui servira à faire le lien entre IOS et Système.

Exemple : un utilisateur cherche à se connecter au réseau, il tape son identifiant et son mot de passe, un agent scanne sa machine et constate que son antivirus n'est pas à jour. Au lieu de recevoir ses paramètres réseau normaux, il est mis dans une zone où il n'accède qu'au serveur lui permettant de télécharger une mise à jour d'anti-virus. Une fois l'opération effectuée, il peut accéder au réseau.

Essentiellement, Cisco NAC tire le meilleur parti des investissements existants en matière d'infrastructure de réseau et de technologie de protection des hôtes en associant les deux fonctionnalités pour réaliser un système de contrôle d'admission au réseau. L'entreprise peut, par exemple, s'assurer que les éléments du réseau Cisco – routeurs, commutateurs, équipements sans fil ou serveurs de sécurité dédiés – contrôlent l'usage d'un logiciel anti-virus. De la sorte, Cisco NAC complète plus qu'il ne remplace les technologies classiques de sécurité déjà couramment utilisées – passerelle pare-feu, systèmes de protection contre les intrusions, authentification d'identité et sécurité des communications.

Cisco NAC est une étape cruciale dans la mise au point du réseau capable de se défendre tout seul – Cisco® Self-Defending Network – initiative innovante de sécurité qui améliore de manière spectaculaire la capacité des réseaux à identifier et prévenir les menaces de sécurité et à s'y adapter. Le projet Cisco Self-Defending Network renforce considérablement la stratégie de Cisco pour l'intégration des services de sécurité sur l'ensemble des réseaux IP en fournissant de nouvelles méthodes de défense au niveau système contre les menaces de sécurité.

Pour en savoir plus, contactez nos conseillers au
0 800 770 400
(appel gratuit)
www.cisco.fr/go/secu

Siège social Mondial et Amérique
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 Européen
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com

Tél. : +31 0 20 357 1000
Fax : +31 0 20 357 1100

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 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