LES ÉLÉMENTS CLÉS DE LA STRATÉGIE DE RÉSEAU CAPABLE DE SE DÉFENDRE TOUT SEUL DE CISCO

Le point de vue technologique du Cisco Security Technologie Group
Février 2005

Beaucoup d'entre vous ont pu voir cette année les publicités Cisco sur son projet de réseau capable de se défendre tout seul, le Self-Defending Network (SDN) : à la télévision, une fillette qui télécharge à son insu un virus sur l'ordinateur de son père, les panneaux d'affichage entourés de fil de fer barbelé ou, dans les magazines, les publicités où les équipements de sécurité sont incarnés par des Dobermans.

Bien que Cisco soit un fournisseur réputé de technologies de réseau et de sécurité, notre compagnie n'est pas fréquemment associée à des campagnes marketing aussi percutantes. Il est donc naturel que l'on nous pose souvent la question : « Qu'est-ce que le réseau capable de se défendre tout seul ? Un réseau peut-il vraiment se défendre lui-même ? »

La réponse courte est « Oui ! ». La protection des réseaux est en train d'évoluer, remplaçant des produits bien identifiés, mais souvent cloisonnés à une seule fonction, par des solutions à l'échelle du système tout entier. Pour ouvrir la voie de ce nouvel univers de possibilités, Cisco a pris la tête du développement des technologies et du marché de la sécurité. La raison en est simple. Dans l'entreprise, l'un des éléments clés de toute charte informatique, et plus encore dans cette ère de réglementation, est la préservation de l'intégrité, de la confidentialité et de la longévité des informations. Depuis que nous marchons vers une économie mondiale informative, jamais la valeur de l'information et l'importance d'un accès contrôlé à cette information n'ont été plus grandes. L'objet de toute infrastructure informatique est de créer des systèmes capables de détecter et de combattre les intrusions tout en garantissant aux utilisateurs légitimes un accès rapide. Face à une attaque, le simple verrouillage des portes et fenêtres est devenu insuffisant. Les réseaux modernes doivent être capables de répondre aux attaques tout en garantissant la disponibilité et la fiabilité afin de permettre à l'entreprise de poursuivre ses activités. A de nombreux titres, l'objectif de la sécurité est de rendre les réseaux plus résistants en accroissant leur élasticité. Plutôt que de rompre sous l'attaque, le réseau doit pouvoir l'absorber et demeurer opérationnel, à l'instar de notre système immunitaire qui nous permet de continuer à vivre en présence d'un virus ou d'une autre infection bactérienne.

Le présent article présente les idées qui sous-tendent le réseau capable de se défendre tout seul Self-Defending Network, ses éléments fondamentaux et les approches successives adoptées par Cisco pour lui permettre de fournir ces fonctionnalités.

Le monde change, la sécurité aussi !

Ces trois dernières années, que cela nous plaise ou non, le paysage de la sécurité a davantage changé qu'au cours de la décennie précédente. Devant l'ampleur et le rythme de ces changements, les services de sécurité informatiques ont eu des difficultés à s'adapter. Avant d'espérer reprendre le contrôle des événements, il est nécessaire de mieux comprendre la manière dont ce paysage change.

Le périmètre de réseau sécurisé

Peut-être plus que toute autre, la notion de périmètre de réseau sécurisé s'est estompée à mesure que les grandes entreprises consolidaient leurs centres de calcul, faisaient converger leurs réseaux internes et adoptaient Internet. Ce qui était jusqu'ici un

environnement contrôlé et en vase clos est aujourd'hui le plus souvent ouvert aux partenaires par des extranets d'entreprise à entreprise (B-to-B), des connexions de points de vente et les solutions pour télétravailleurs et utilisateurs mobiles. En élargissant ainsi son réseau, l'entreprise a déplacé sa frontière de sécurité pour englober désormais des réseaux intermédiaires non sécurisés et des environnements qu'elle ne maîtrise pas. Il est fréquent que les équipements qui se connectent ainsi au réseau de l'entreprise ne respectent pas ses politiques, tandis que ceux qui les respectent accèdent souvent à d'autres réseaux non contrôlés avant de se connecter à celui de l'entreprise. Ceci explique comment les équipements installés sur ces réseaux extérieurs peuvent devenir des voies d'accès pour les attaques et favoriser les utilisations abusives.

Sans fil et mobilité

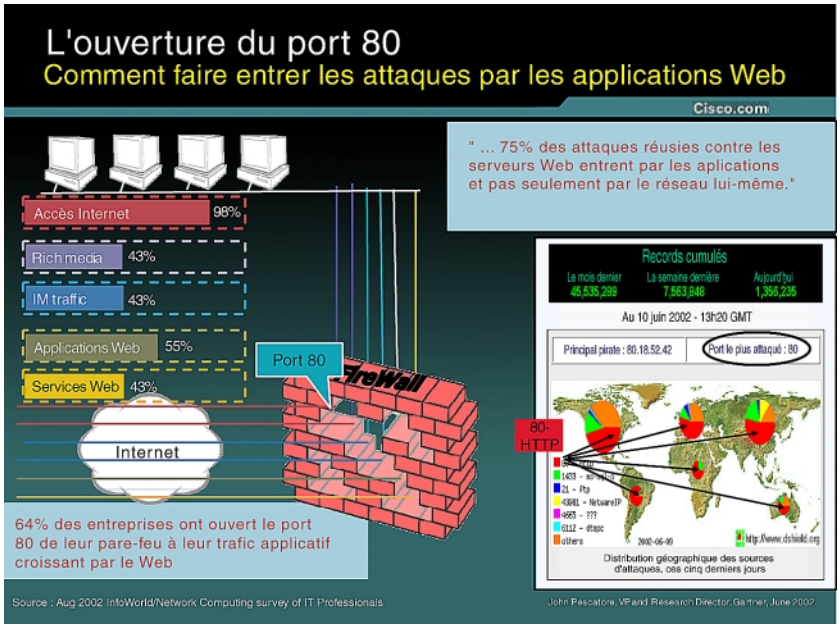
Toujours au cœur de cette notion de périmètre sécurisé, le déploiement des réseaux sans fil et la généralisation des applications et des terminaux mobiles (PC portables, PDA, téléphones convergeants, etc.) introduisent de nouveaux risque.

Ces hôtes aux multiples connexions sont capables de créer des réseaux sans fil ad-hoc qui facilitent les communications « peer-to-peer » et permettent, au niveau des applications, la transmission efficace de paquets d'une unité à l'autre. Avec de telles fonctionnalités, il devient encore plus difficile de déterminer où commence et où s'arrête la frontière d'un réseau. L'entreprise doit être en mesure d'installer un point de contrôle sur des unités mobiles afin de gérer la sécurité du système et de garantir la disponibilité du réseau.

Le commerce électronique, les extranets et l'évolution Internet des activités métiers

L'émergence d'interfaces d'application communes développées autour de protocoles de messagerie comme XML et SOAP s'est révélée une bénédiction pour le commerce électronique et la productivité des entreprises. Toutefois, comme souvent avec les nouvelles technologies, ces protocoles de messagerie ont apporté avec eux un vaste ensemble de vulnérabilités et de vecteurs d'attaques inédits que les sociétés doivent désormais combattre. Les données, autrefois éparpillées sur de multiples protocoles de réseau et aisément filtrables par les politiques de pare-feu, sont désormais agglutinées sur un petit nombre de protocoles de transport, quand ce n'est pas sur un seul comme HTTP sur le port TCP 80.

En conséquence, une grande partie des données jusqu'ici placées dans l'entête d'un paquet figurent maintenant parmi les données utiles, générant d'importants problèmes de traitement qui sont autant de moyens pour le pirate de contourner les défenses classiques du réseau. De plus, pour répondre aux exigences des entreprises en matière de confidentialité et d'intégrité des données, une partie croissante de ce trafic applicatif est désormais cryptée par les protocoles SSL/TLS et HTTPS. Cette évolution a pour effet de compliquer fortement la tâche des services informatiques chargés de faire appliquer les politiques d'accès de l'entreprise à la périphérie du réseau car l'inspection des données utiles des paquets devient impossible dès que le flux est crypté.



Virus, vers et vitesse de propagation

Le nombre et la diversité des virus et des vers apparus ces trois dernières années fait froid dans le dos. Toutefois, les deux facteurs qui ont eu la plus forte incidence sur les entreprises et sa rentabilité opérationnelle sont : 1) le raccourcissement des délais entre l'identification d'une vulnérabilité et son exploitation et 2) la vitesse à laquelle un grand nombre de ces attaques se propagent dans l'entreprise. Ces deux facteurs ont engendré des niveaux inacceptables de dysfonctionnements dans l'entreprise ainsi que des projets de remédiation coûteux qui consomment en personnel, en temps et en argent des ressources qui n'avaient pas été prévues pour ces tâches.

Conformité à la réglementation

Largement médiatisées, les brèches dans la sécurité des entreprises et les malversations internes de certains dirigeants de société ont poussé les organismes de réglementation de nombreux secteurs industriels à intervenir pour définir des règles de gestion des risques sur les informations d'entreprise. Aux Etats-Unis, ces nouvelles réglementations *(dont les plus connues sont Sarbanes-Oxley, Gramm-Leach-Bliley (GLB) et Health Insurance Portability and Accountability Act (HIPAA))* ont modifié de manière radicale l'organisation des réseaux, des serveurs, des bases de données et des hôtes de l'entreprise.

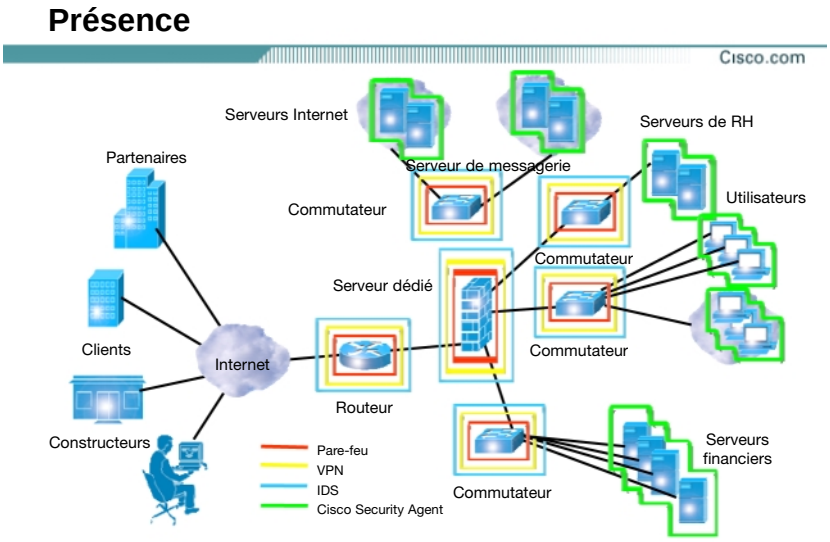
De nombreuses sociétés pensent, à tort, qu'elles renforcent la sécurité de leur infrastructure en se mettant en conformité avec la réglementation. Ce n'est souvent pas le cas. Selon la loi des conséquences involontaires, le simple fait de se mettre en conformité peut engendrer de nouvelles vulnérabilités. Les vers et les virus, par exemple, se propagent bien plus efficacement dans un réseau qui supporte les VPN de bout-en-bout car les nœuds intermédiaires sont aveugles au trafic qui les traverse. Dans un paquet sécurisé et crypté, ce type de trafic peut injecter un ver au cœur même des serveurs sensibles de l'entreprise. En plus d'allonger le temps nécessaire à l'identification de telles attaques, ces VPN de bout-en-bout risquent également de compliquer la mise en œuvre des défenses.

Les principes fondateurs du réseau moderne sécurisé

Face à une telle évolution du paysage de la sécurité, les capacités d'adaptation de l'entreprise sont limitées : au-delà d'un certain seuil, le changement devient totalement contre-productif. Dans l'idéal, le renforcement de la sécurité ne doit avoir qu'une incidence minimale sur l'infrastructure de routage et de commutation existante, sur les techniques de segmentation et de contrôle d'accès et sur les structures organisationnelles qui supportent ces systèmes. Dans cette section, nous décrivons les éléments fondamentaux du réseau capable de se défendre tout seul, le Self-Defending Network, qui soutiennent cet objectif : *Présence, Contexte, Liens et Confiance.*

Présence

Tout système sécurisé commence par des points de contrôle, un concept essentiel que nous appelons présence. Notre système immunitaire dépend de détecteurs et de récepteurs répartis dans tout l'organisme et qui assurent une présence. Dans un environnement de réseau, la présence se traduit par l'existence de certaines fonctionnalités dans des nœuds répartis sur le réseau. Ces fonctionnalités comprennent les technologies classiques d'identification, de contrôle d'accès, d'inspection des données et de sécurité des communications, ainsi que d'autres, plus originales et sensibles aux applications, qui permettent de faire face au développement du trafic peer-to-peer, des services Web, des services voix et des contenus mobiles dynamiques.



Contexte

Lorsqu'un utilisateur s'inscrit sur le réseau, le réseau exige et obtient un accès à un ensemble d'authentifiants aussi bien pour l'utilisateur que pour l'hôte qui constitue une entité d'extrémité. Il est important de remarquer que ces authentifiants peuvent changer avec le temps pour tenir compte des actions de l'hôte pendant qu'il est connecté au réseau. Ensemble, ces informations représentent le contexte. Alors que les réseaux traditionnels ont tendance à ne s'intéresser qu'aux permissions de l'utilisateur au moment où il entre sur le réseau, un système sécurisé accorde ou révoque les permissions en fonction des modifications de comportement et du contexte associé pendant toute la durée de l'association de l'entité avec le réseau. Par exemple, si le réseau constate qu'un hôte a été infecté par un virus, il réagit en mettant l'hôte en quarantaine dans un segment remédiateur du réseau..

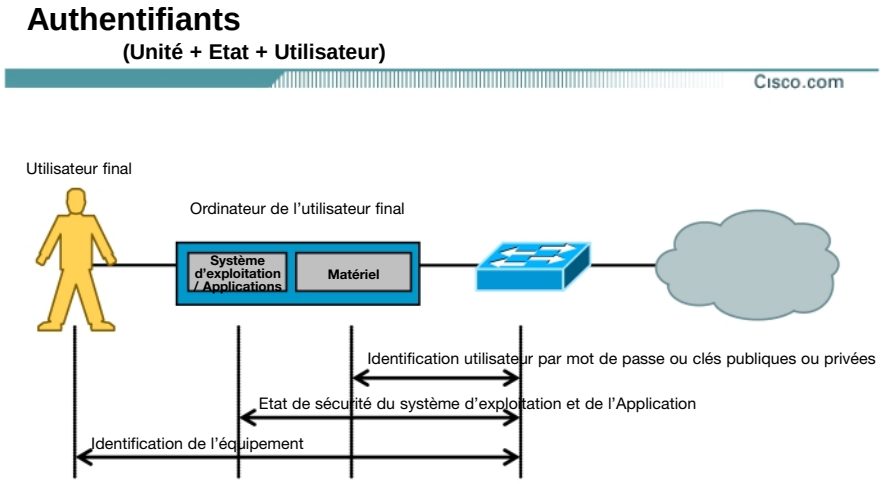
Liens

Les liens entre des entités distinctes permettent les échanges et réalisent un « système ». Traditionnellement, les liens que les réseaux établissent entre les unités passent par des protocoles de routage comme BGP (Border Gateway Protocol). Pour contrer efficacement les formes les plus récentes de menaces et d'utilisation abusive, il est désormais nécessaire d'étendre ces liens de la source jusqu'à la destination du trafic réseau. Or, compte tenu de la multiplication des équipements mobiles à connexions multiples, ces liens ont commencé à franchir des bornes que l'agencement des réseaux traditionnels considère comme extérieures à son domaine de supervision. Les privilèges qu'une entité reçoit en entrant sur un réseau, et la manière dont ils peuvent évoluer tout au long de la connexion, sont liés au contexte de cette entité comme à ses liens vers un ou plusieurs réseaux.

Confiance

Un système sécurisé n'est jamais meilleur que les informations qu'il détient, mais il travaille nettement mieux s'il dispose d'un ensemble complet de relations de confiance. Par le passé, la confiance reposait essentiellement sur l'identité d'une unité ou d'un utilisateur. Des progrès récents ont montré que les capacités des systèmes sécurisés doivent être augmentées pour intégrer la compréhension de l'état et de l'emplacement de cette unité. A de nombreux titres, les activités des utilisateurs et des équipements d'un réseau peuvent être comparées à la manière dont nous conduisons une automobile sur la route. De même qu'il faut posséder un permis de conduire pour prendre le volant d'un certain type de véhicules, l'utilisateur doit disposer d'une forme ou d'une autre d'identification pour ouvrir une session sur un réseau. Et, de même qu'une voiture possède une plaque et un numéro d'immatriculation attribué par la Préfecture, tous les équipements de réseau et les points d'extrémité devront bientôt disposer d'un certificat numérique installé lors de leur fabrication et d'une forme d'immatriculation lorsqu'ils seront déployés dans une entreprise. Cependant, comme les authentifiants appropriés peuvent ne pas être présents en un lieu ou à un moment donnés, le réseau capable de se défendre tout seul utilise des méthodes innovantes de confiance induite et de détermination des efforts maximums afin d'authentifier et

d'autoriser une entité. Au minimum, le réseau SDN (Self-Defending Network) doit être capable d'acquérir des garanties quant à l'identité de l'unité et de l'utilisateur, à l'état de l'unité et à l'emplacement qu'elle occupe dans l'environnement. La technologie qui permettra d'acquérir ces garanties devra être omniprésente et soutenue par des formats et des protocoles de messages bien définis et normalisés comme 802.1x et EAP (Extensible Authentication Protocol).



Individuellement, aucun de ces concepts n'a d'intérêt particulier, mais associés dans le Cisco Self Defending Network, ils deviennent particulièrement puissants. Dans la suite de cet article, nous présentons quelques-unes des manières dont ces concepts interagissent dans le cadre du réseau capable de se défendre tout seul Cisco SDN.

Le réseau capable de se défendre tout seul : une nécessité

Les réseaux d'entreprise, comme les attaques utilisées pour les exploiter, ont atteint un niveau de complexité tel qu'aucun mécanisme ne peut, à lui seul, en assurer la défense. Cette constatation a conduit au concept de « Défense en profondeur » qui, jusqu'à présent, s'est appuyé sur la notion de défenses proactives. Cependant, compte tenu du type de vulnérabilités et d'attaques qui ont accompagné l'évolution constante des réseaux, Cisco estime qu'il est grand temps de commencer à bâtir des solutions adaptatives plus efficaces. C'est pour cela que Cisco a recherché dans le monde réel des modèles, comme notre propre système immunitaire, pour bâtir son projet de réseau capable de se défendre tout seul. D'autres systèmes réels ont également contribué à ce modèle, comme l'épidémiologie et les méthodes qu'utilisent les communautés pour lutter contre la délinquance. Tous ces systèmes ont ceci en commun qu'ils emploient des techniques de défense adaptatives aussi bien que proactives.

Si l'on approfondit un peu cette observation, les défenses qui protègent un système de cette nature doivent être inscrites dans chacun de ses blocs fonctionnels. Les principales qualités de ces défenses adaptatives sont leurs capacités à :

- demeurer actives en permanence,
- agir sans perturber,
- minimiser la propagation des attaques,
- réagir rapidement aux attaques jusqu'ici inconnues.

Ces systèmes reposent sur l'idée première que les ressources sont limitées et qu'elles doivent être soigneusement gérées pour éviter qu'elles ne s'épuisent.

Elles sont également conçues pour exploiter pleinement l'infrastructure existante avec un minimum de perturbations pour les activités informatiques de l'utilisateur.

Le réseau capable de se défendre tout seul fournit des solutions systèmes qui permettent aux utilisateurs d'exploiter leur infrastructure au maximum et de manière innovante pour réduire les fenêtres de vulnérabilité, minimiser l'impact des attaques et améliorer la disponibilité et la fiabilité d'ensemble de l'infrastructure. L'objectif est également de bâtir des systèmes autonomes capables de réagir rapidement à une infestation, avec un minimum d'intervention humaine. Ce type de réaction rapide est indispensable pour contrer les formes les plus récentes d'utilisation abusive qui s'avèrent bien plus nuisibles que celles qui les précédaient.

Le projet Cisco SDN continue d'améliorer sa capacité de réaction aux nouvelles menaces. La première phase, **Sécurité intégrée,** renforce la capacité de sécurité des éléments du réseau comme les commutateurs et les routeurs. La deuxième phase, **Collaboration de sécurité**, comprend la création de liens entre les éléments de sécurité et l'extension de la présence réseau jusqu'aux points d'extrémité qui s'y connectent. **La phase ultime** du projet SDN comprend des fonctionnalités de **Défense adaptative contre les menaces** qui, grâce à un nouvel ensemble de technologies Anti-X, donnent au réseau encore plus de moyens pour réagir aux menaces.

Les blocs fonctionnels du réseau capable de se défendre tout seul

Il est évident que la plupart de nos utilisateurs ne pourront pas adopter en une seule fois l'ensemble des composantes d'un réseau capable de se défendre tout seul. L'une des raisons est qu'il est difficile de reprendre d'une seule pièce la totalité des sous-systèmes nécessaires sans compromettre l'intégrité des services informatiques. Une autre raison est qu'il est encore plus difficile de confier le contrôle de la sécurité à un système automatisé tant que l'on n'est pas certain de la fiabilité de son fonctionnement. Le projet SDN (Self- Defending Network) répond à cette problématique en commençant par fournir à l'utilisateur des produits efficaces qu'il pourra déployer de manière indépendante, puis des solutions capables de relier ces produits les uns aux autres à mesure qu'il prend confiance dans l'efficacité des composantes et des sous-systèmes individuels. Cette progression s'appuie sur une politique mixte de développement et d'acquisitions de produits, d'élaborations de systèmes et de partenariats. Dans cette optique, il est intéressant d'étudier les principales étapes franchies à ce jour par le projet Cisco SDN.

Protection des points d'extrémité

L'une des principales nouveautés de ces dernières années est une modification profonde des stratégies d'attaques : les pirates utilisent les stations « légales » (authaurisée) pour véhiculer et déclancher l'attaque. C'est le cas par exemple des vers : ils provoquent des congestions réseaux en raison de leur propagation rapide et de l'infestation des points d'extrémité. Cisco a constaté que l'on pouvait trouver un début de solution aux deux problèmes en proposant aux clients un produit de prévention des intrusions des points d'extrémité mis au point par Okena et désormais appelé Cisco Security Agent (CSA). CSA utilise des techniques originales de sécurité comportementale afin de détecter les virus et les vers et de les empêcher de s'établir sur un système d'extrémité. Il bloque du même coup leur propagation sur le réseau. En fait, CSA constitue un atténuateur de premier ordre de l'effet de propagation des vers et des virus.

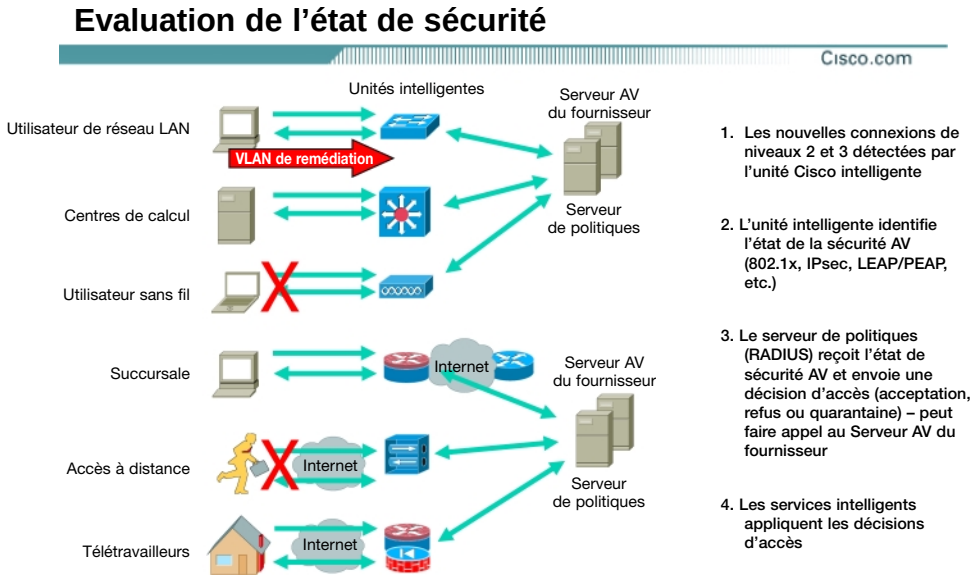
Une seconde raison, tout aussi décisive, de choisir CSA est qu'il établit sur les points d'extrémité une présence qui peut servir à acquérir des rapports d'état parfois difficiles à obtenir en périphérie du réseau. Il se crée ainsi une boucle de retour d'informations entre le point d'extrémité et le réseau dont l'avantage est de permettre une adaptation rapide aux menaces émergentes.

Contrôle des admissions

L'une des initiatives les plus remarquables à ce jour du projet Cisco Self Defending Network est le programme Cisco NAC (Network Admission Control). NAC permet au réseau de se doter d'un moyen de reconnaissance poussé pour savoir précisément qui, et surtout quoi (quel terminal, avec quel niveau de confiance) cherche à accéder aux ressources. Autrement dit la protection de son système d'exploitation et des applications associées, et non plus seulement son identité. En plus du contrôle d'accès, NAC donne à l'administrateur informatique les moyens de mettre automatiquement en quarantaine les points d'extrémité non conformes, puis de corriger les problèmes. La vérification de la conformité des points d'extrémité (autrement dit des mises à jour des correctifs de système d'exploitation et des signatures antivirus) constitue un efficace atténuateur de second ordre des effets de la propagation des virus et des vers. [(1)]

[(1)] On peut également considérer NAC comme un outil *à la demande* d'évaluation de la vulnérabilité et de la gestion des correctifs.

Une des caractéristiques originales de NAC est de fournir des interfaces clients ainsi que des interfaces administratives AAA (Authentification, Autorisation et Administration) qui permettent à l'utilisateur d'installer les produits des fournisseurs de sécurité d'extrémité et de politiques de son choix pour piloter le plan NAC. Le programme NAC réunit aujourd'hui plus de 30 constructeurs leaders de leurs secteurs qui travaillent activement à l'intégration de leurs technologies sur le réseau.



Le contrôle NAC est particulièrement important pour les petites et moyennes entreprises et c'est pour ce segment de marché que Cisco a acquis Perfigo et commercialise une solution globale de contrôle de conformité appelée Cisco Clean Access.

Confinement des infections

Mêmes fortes, les politiques d'admission au réseau ne sont pas une panacée et ne suppriment pas la nécessité de maintenir une surveillance des unités une fois qu'elles sont connectées au réseau. Un pirate résolu est capable de contourner pratiquement n'importe quel contrôle d'admission. Une multitude de « vecteurs » différents sont susceptibles de véhiculer l'infection dans un équipement conforme après son admission sur le réseau, par exemple, une clé USB dont le contenu serait infecté. Pour cela, le réseau capable de se défendre tout seul est conçu pour élargir à toute la durée de la connexion réseau les contrôles de sécurité réalisés au moment de l'admission. Le principal défi est que le réseau ne peut pas toujours faire confiance à un élément infecté pour se dénoncer. Or, nous nous sommes aperçus que le réseau capable de se défendre tout seul peut s'appuyer sur les autres éléments du réseau, comme des points d'extrémité, qui détecteront si l'un d'entre eux est devenu « mauvais », un peu comme le 112 permet aux services de police de surveiller la criminalité au sein d'une communauté. Cisco considère le Confinement des infections comme un atténuateur de troisième ordre de l'effet de propagation des vers et des virus.

Cependant, les protocoles d'authentification actuels ne sont pas conçus pour intervenir après l'échange initial, et le réseau capable de se défendre tout seul doit proposer de nouvelles manières de transmettre l'état de sécurité d'une unité (le contexte) et d'évaluer la véracité de ces informations au travers de formes de confiance à la fois induites et directes.

Un administrateur peut, par exemple, créer une règle qui attribue aux notifications envoyées par un point d'extrémité exécutant CSA une valeur de confiance supérieure à celle accordée aux notifications des unités non protégées. C'est ainsi que Cisco a lancé le développement de nouveaux types de corrélation et de d'informations en retour en fonction des attributs induits.

Corrélation intelligente et réaction aux incidents

Pour que les mécanismes permanents d'informations en retour comme le Confinement des infestations fonctionnent de manière efficace, le réseau capable de se défendre tout seul doit pouvoir fournir des services comme la corrélation en temps réel des événements, l'évaluation rapide de leur impact sur la sécurité, la prise de décision contextuelle, la détermination du point de contrôle le plus proche pour lancer une contre-attaque, etc. Dans ce but, Cisco a récemment annoncé l'acquisition de Protego Networks, dont la famille de produits MARS offre des méthodes pour recouper les informations provenant d'un large éventail de points de présence (pare-feu, SDI-N, routeurs, commutateurs et hôtes) avec le contexte obtenu en découvrant la topologie des niveaux 2 et 3 du réseau. Ceci permet à l'équipe d'intervention de déterminer rapidement les points du réseau sous attaque.

Cisco travaille également avec netForensics et d'autres partenaires afin d'améliorer leurs capacités de corrélation qui leur permettront de mieux analyser le réseau capable de se défendre tout seul.

Détection et Prévention des Intrusion et des anomalies

L'un des domaines importants du développement actuel des solutions de sécurité Cisco est celui de la Détection des Intrusion (IDS). L'une des premières innovations de Cisco à cet égard a été l'intégration des IDS dans ses routeurs et ses plates-formes de commutation. Toutefois, pour que les IDS puissent donner pleinement leur mesure, ils doivent évoluer pour devenir des Systèmes de Prévention des Intrusions (IPS) disposant de fonctionnalités de filtrage en ligne et offrant une capacité de coupure du trafic indésirable grâce à des moteurs de classification programmables avec réglage fin.

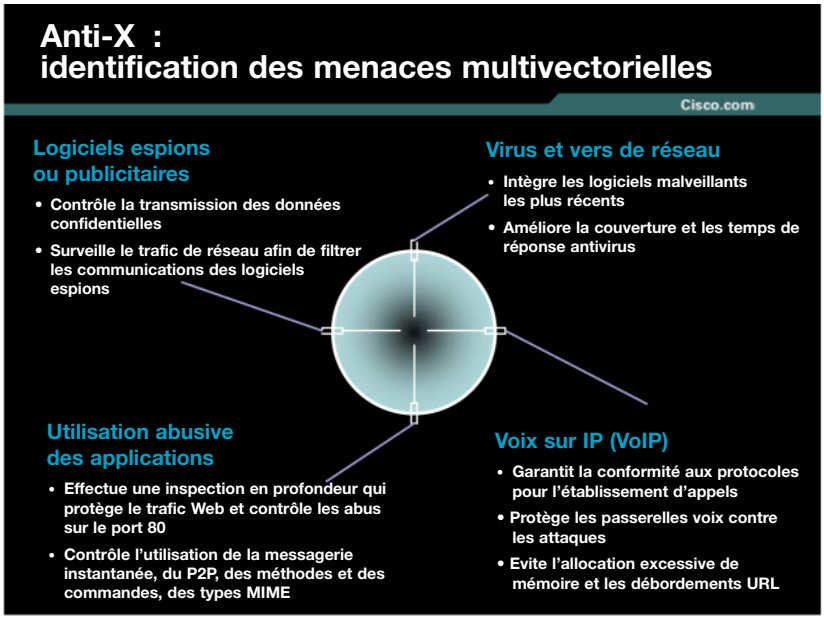
Malheureusement, la plupart des IDS génèrent bien trop de faux positifs pour qu'ils puissent assumer le rôle de services de sécurité en ligne. Le problème vient en partie de la nécessité de réunir de grandes quantités d'informations (le contexte) et de les traiter dans un délai raisonnablement court – surtout en raison de la quantité d'informations contextuelles qui doivent être réunies pour les protocoles à base d'applications. Ceci est plus particulièrement vrai pour les applications comme la téléphonie IP qui sont très sensibles aux délais de transmission des paquets. Ainsi, Cisco a développé plusieurs méthodes qui garantissent une signalisation haute fidélité vers ces moteurs de classification en ligne.

Un grand nombre d'activités légitimes peuvent être prises pour anormales, surtout dans les réseaux où le nombre de variables est important. C'est pour cela que Cisco a volontairement adopté une approche prudente et progressive de la détection des anomalies. Cela a commencé par CSA, car on considère que les systèmes d'exploitation sont plus faciles à modéliser que les environnements de réseau. Comprenant que les activités qui saturent le réseau sont nettement plus gênantes que les autres, Cisco a ensuite acquis Riverhead, un vrai système de prévention en ligne avec un taux de faux positif faible.

Tirant les enseignements de CSA et des fonctions de lutte contre les attaques par saturation de la gamme Riverhead DoS Guard, Cisco présente un système de prévention des intrusions (IPS) en ligne qui réduit le taux de faux positifs en appliquant des techniques innovantes de détection des anomalies et en échangeant des informations d'état de la sécurité (le contexte) entre les points d'extrémités et les éléments du réseau (liaisons). L'IPS de Cisco dispose également de fonctionnalités d'identification des menaces multivectorielles et de corrélation des méta-événements afin d'évaluer en temps utile les vulnérabilités et les attaques du réseau. Par l'introduction progressive de ces technologies sur le marché, Cisco pense rassurer sa clientèle quant à leur potentiel de sécurité et par extension à celui du réseau capable de se défendre tout seul.

Sécurité des applications et défense Anti-X

Ces dernières années, plusieurs nouveaux produits de réseau pour la couche applicative ont fait leur apparition pour permettre de gérer de nouvelles catégories de menaces que les pare-feu et les SSI-N classiques sont incapables de contrer efficacement : les virus et les vers, le courrier électronique indésirable (Spam) et le phishing, les logiciels espions, l'utilisation abusive des services Web et de la téléphonie IP, les activités Peer-to-Peer non autorisées, etc. Cisco a conçu la prochaine génération de services d'inspection des contenus et des paquets, capable de gérer ce type de menaces et d'abus. Cette convergence permet aux principaux points d'application de la sécurité de réseau de disposer de services granulaires d'inspection du trafic, et donc de confiner le trafic malveillant avant qu'il puisse se propager dans le réseau.

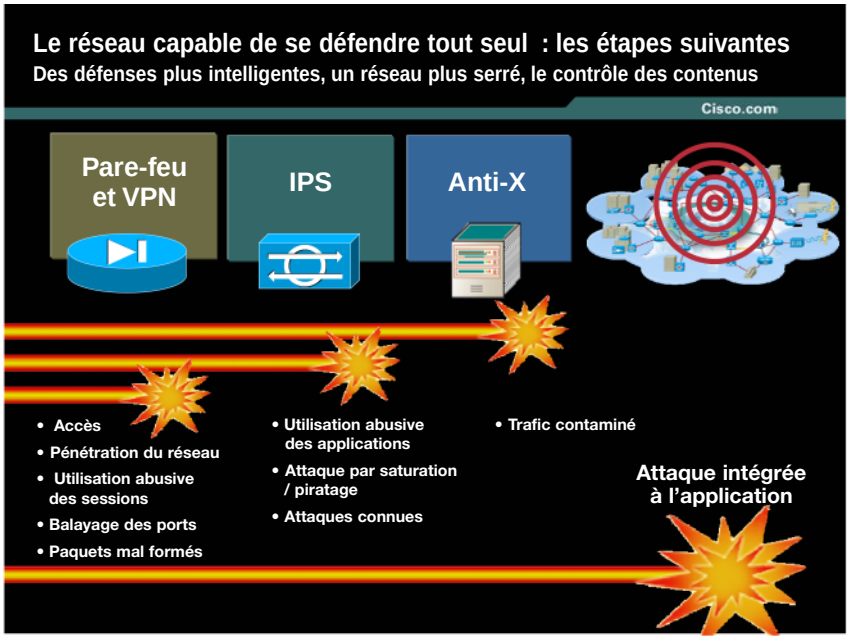


La consolidation de ces services sur des plates-formes multi-services offre aux constructeurs une chance d'innover et au client, la possibilité de réduire ses coûts de propriété. Cisco a développé le serveur dédié ASA (Adaptive Security Appliance) en tant que plate-forme multi-services destinée à ce segment de marché. Le serveur ASA réunit des fonctionnalités innovantes et originales d'inspection des paquets et de corrélation avec les services existants de pare-feu, de VPN et de'IPS. La dernière génération des routeurs à services intégrés Cisco propose également des fonctionnalités similaires. Par ailleurs, le réseau capable de se défendre tout seul deviendra davantage sensible aux applications une fois que ces services auront été intégrés dans son cadre.

Il est à noter que lorsque des applications utilisent un cryptage de bout-en-bout, le réseau capable de se défendre tout seul peut récupérer les informations transmises par les points d'extrémité afin de compenser la perte de visibilité à la périphérie du réseau.

Les prochaines étapes

Cisco va poursuivre ses investissements lourds dans la réalisation de réseaux capables de se défendre tout seuls et capables de créer des liens entre les points de présence dans tout le réseau, y compris les systèmes de points d'extrémité. De cette manière, Cisco permettra à l'entreprise de gagner considérablement en visibilité et en contrôle des équipements, des utilisateurs et des applications qui communiquent sur son infrastructure. C'est une évolution nécessaire et importante de ce que l'on attend classiquement du réseau, exactement comme l'introduction des protocoles de routage intelligent a pu l'être pour la transmission de paquets sur la matrice de communication.



Cet article ne présente que quelques aperçus des possibilités du projet Cisco SDN (Self-Defending Network). Il est nécessaire de les étudier plus en profondeur, tant pour mieux comprendre ce qu'il est possible de réaliser aujourd'hui que pour poser les fondations des futurs projets de sécurité et d'architecture des réseaux. Les choix que vous ferez dépendent des problèmes spécifiques de sécurité, de risque et de conformité que votre entreprise rencontre jour après jour :

- Pour le personnel chargé de la sécurité périmétrique, nos nouvelles plates-formes PIX 7.0, notre serveur dédié ASA et notre gamme de routeurs à services intégrés permettent une inspection détaillée des données. Ils offrent également le contrôle d'un vaste éventail de protocoles et des vecteurs d'attaques qui leur sont associés, ainsi que de nombreuses autres fonctionnalités de sécurité et de gestion de réseau.
- Les groupes de sécurité opérationnelle qui perdent un temps et une énergie considérables à répondre aux incidents, devraient étudier la technologie que nous venons d'acheter à Protego (Cisco MARS), et chercher à en savoir davantage sur les nouvelles fonctionnalités de protection en ligne contre les intrusions de nos serveurs dédiés d'infrastructure et de sécurité.
- Les responsables des environnements à forte composante de données, qui doivent régulièrement lutter contre les attaques par saturation et leurs dérivées, trouveront une aide précieuse dans la technologie Anomaly Guard que nous avons achetée à Riverhead.
- Les entreprises qui sont régulièrement infectées par des vers ou des virus, comme celles qui ont besoin de solutions de conformité des points d'extrémité, auront intérêt à examiner les solutions Cisco Security Agent, Network Admission Control et Cisco Clean Access que nous avons acquises auprès de Perfigo.
- Les vérificateurs responsables de l'évaluation de la conformité aux réglementations pourront étudier les possibilités de NAC ainsi que celles de CiscoWorks SIMS, un outil qui fournit des informations détaillées sur l'utilisation de l'intégralité de l'infrastructure de communications.

Enfin, ceux d'entre vous qui ont la charge de la conception et du déploiement des systèmes de sécurité et de l'infrastructure réseau peuvent contacter leur représentant local Cisco pour obtenir des détails complémentaires sur le projet de réseau capable se défendre tout seul Cisco et la manière dont il peut modifier, à leur avantage, leur environnement informatique.

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