Enterprise Strategy Group | Getting to the bigger truth.™

Livre blanc

L'architecture de sécurité réseau intégrée : les pare-feu de nouvelle génération axés sur les menaces

Jon Oltsik, analyste principal senior

Septembre 2014

Ce livre blanc ESG a été commandé par Cisco Systems et est distribué sous licence d'ESG.

Table des matières

Synthèse

Pour assurer la sécurité de leur réseau, la plupart des grandes entreprises mettent en place un ensemble d'outils tactiques ponctuels : des pare-feu, des passerelles VPN, des systèmes IDS/IPS, des proxys réseau, des sandbox d'analyse de logiciels malveillants, des passerelles web et e-mail, etc. Si cet enchevêtrement de technologies indépendantes était efficace il y a dix ans, il est aujourd'hui source de difficultés en termes d'efficacité opérationnelle, d'application des politiques et de surveillance. Pire encore, les systèmes de défense des réseaux parviennent de moins en moins à bloquer les menaces sophistiquées et ciblées, ainsi que les attaques de malwares avancés.

Quelle est l'étendue des risques ? Et comment les DSI peuvent-ils y faire face ?

- **Les réseaux sont de plus en plus difficiles à protéger.** Les redondances entre les processus et les contrôles, la multiplication des outils ponctuels et des procédures manuelles, ou encore le manque de compétences en matière de sécurité sont autant de challenges auxquels les professionnels de la sécurité doivent faire face quotidiennement. Devant ce cumul de problèmes, nouveaux ou de longue date, les solutions de protection du réseau ne sont plus en adéquation avec les besoins de l'entreprise.
- **Les outils modernes de protection du réseau ne suffisent pas.** De nombreuses entreprises adoptent de nouveaux outils de protection comme les pare-feu de nouvelle génération. S'il est vrai que ces pare-feu renforcent la sécurité, ils se concentrent trop souvent sur un contrôle limité des applications au lieu de proposer une solution de protection plus globale contre les attaques. De plus, les outils isolés comme les sandbox d'analyse de programmes malveillants restent une solution purement tactique, puisqu'ils n'offrent aucune protection ni davantage de visibilité sur la sécurité du réseau ou du cloud.
- **Les grandes entreprises ont besoin d'une architecture de sécurité réseau interopérable.** Il leur faut une architecture de sécurité intégrée, davantage axée sur les menaces, évolutive, qui automatise les processus manuels et qui remplace les outils ponctuels par des services de protection du réseau interopérables. L'architecture de sécurité réseau doit inclure des fonctions de commande et de contrôle centralisées, l'application des politiques aux systèmes distribués et des informations exploitables intégrées.

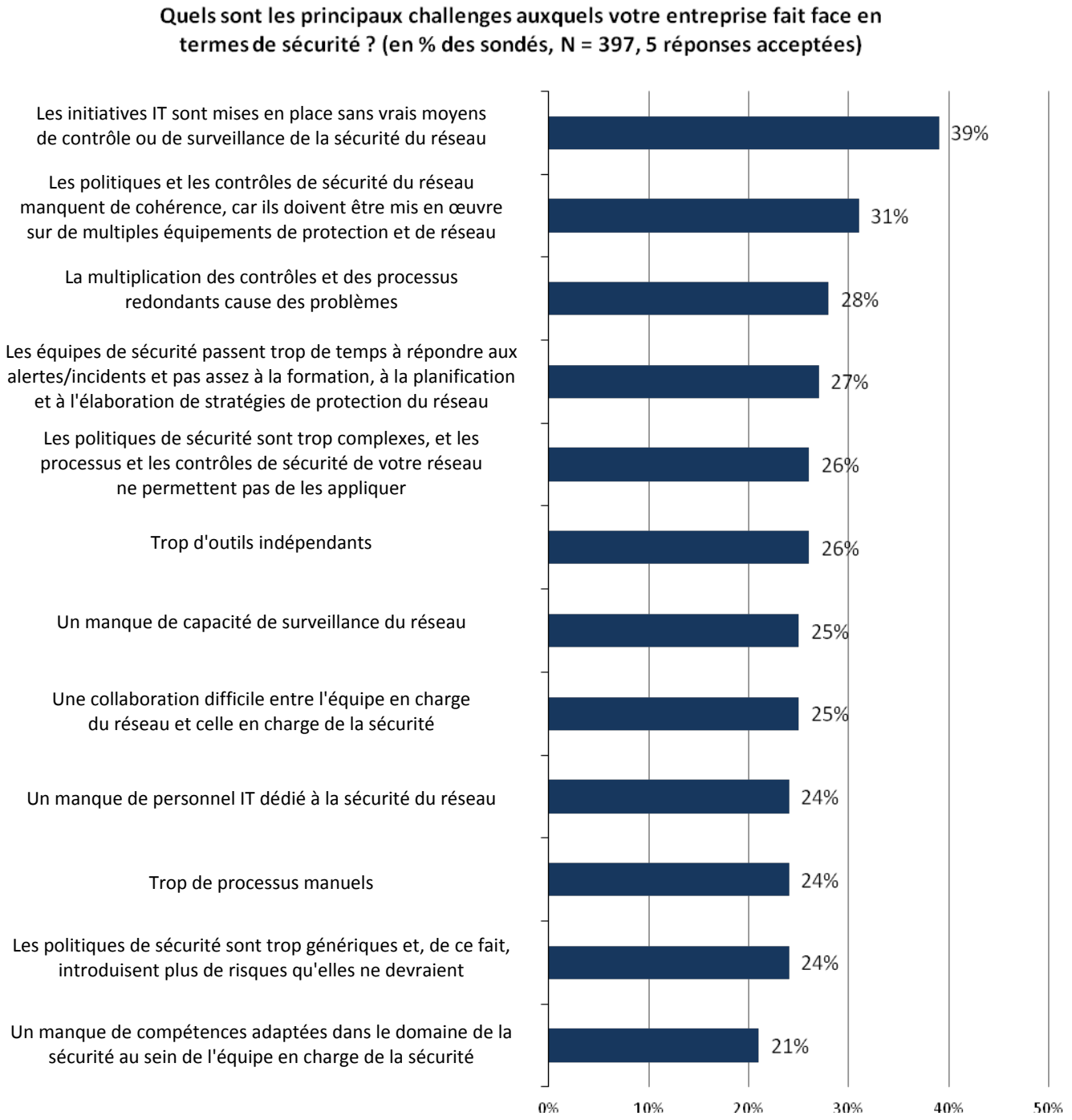
Les challenges de la sécurité réseau

Les grandes entreprises transforment rapidement leurs infrastructures IT en développant des initiatives autour notamment du cloud computing, du traitement analytique du Big Data, de la mobilité et des applications de l'Internet des objets. Ce sont autant de nouveaux risques pour la sécurité du réseau (voir Figure 1).[1] Les RSSI ont souvent du mal à protéger leur réseau pour plusieurs raisons :

- **Trop de silos technologiques et de solutions disparates.** Presque un tiers (31 %) des entreprises est touché par un manque d'homogénéité entre les politiques et les contrôles de sécurité réseau, 28 % rencontrent des difficultés avec des politiques et des contrôles redondants, tandis que 26 % ne s'y retrouvent pas dans la multiplicité des outils indépendants. Cet ensemble hétérogène de solutions et de silos technologiques complique la prévention, la détection et la résolution des incidents de sécurité.
- **Un excès de processus manuels.** Les données de ESG indiquent que les équipes en charge de la sécurité passent plus de temps à résoudre les situations de crise qu'à s'occuper de la sécurité du réseau en mettant en place des politiques et des procédures proactives. 24 % des entreprises ajoutent qu'elles souffrent de la multiplication des processus manuels. Agir dans l'urgence et de façon manuelle est incompatible avec les exigences actuelles en termes de gestion du risque et de réactivité pour la sécurité réseau.
- **Un manque de compétences dans le domaine de la sécurité réseau.** D'après ESG, 24 % des entreprises manquent de collaborateurs spécialisés dans la sécurité réseau et 21 % d'entre elles ne disposent pas des compétences appropriées en la matière. Étant donné la pénurie mondiale de spécialistes en cybersécurité, nous courons droit à la catastrophe.

[1] Source : Rapport de recherche ESG, *Network Security Trends in the Era of Cloud and Mobile Computing*, août 2014.

Figure 1. Les challenges de la sécurité réseau



Source : Enterprise Strategy Group, 2014.

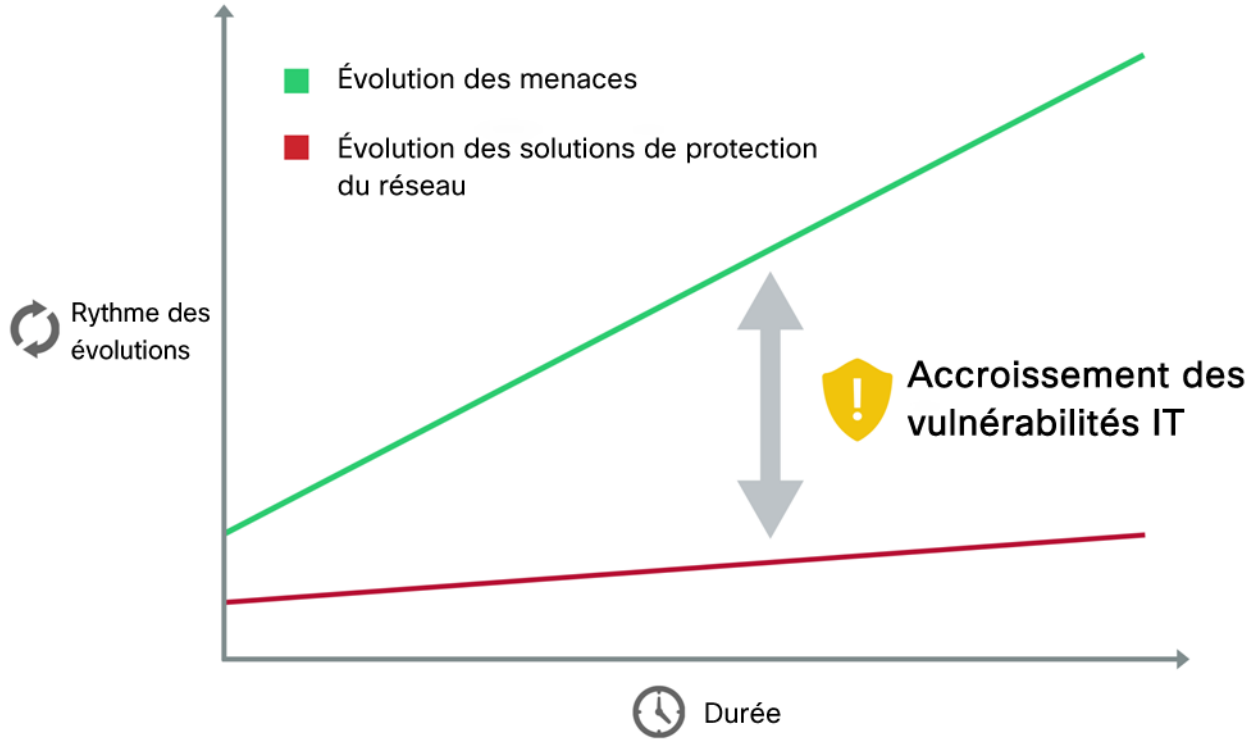
Les vulnérabilités croissantes du réseau

Les PDG et les directeurs doivent réaliser que les challenges liés à la sécurité font partie d'un problème de plus grande ampleur qui touche la cybersécurité et la gestion des risques. Les anciens systèmes de protection reposent sur des silos technologiques et des processus manuels. Les solutions actuelles nécessitent des compétences avancées en sécurité et elles ne sont pas adaptées à la quantité, à la variété et à la complexité des cybermenaces d'aujourd'hui. Les solutions déconnectées présentent des angles morts que les cybercriminels savent exploiter. C'est l'une des raisons pour lesquelles tant d'entreprises font l'objet de cyberattaques : les pirates profitent des

vulnérabilités des systèmes de sécurité, parviennent à contourner les contrôles du réseau et compromettent les ressources IT. Une fois que les pirates ont établi une « tête de pont » fiable qui leur permet de rester invisibles pendant plusieurs mois, ils peuvent naviguer sur le réseau, accéder aux systèmes stratégiques de l'entreprise et voler des données sensibles.

Par le passé, les RSSI répondaient aux menaces de cybersécurité par l'ajout progressif de technologies, de processus et d'équipes dédiées à la protection de leur réseau. Aujourd'hui, cette stratégie ne suffit plus. Les cyberattaques se développent de façon exponentielle au gré des nouvelles technologies et des nouvelles techniques d'exploitation des vulnérabilités. D'autre part, les investissements progressifs n'améliorent que légèrement le niveau de protection du réseau, notamment face aux challenges opérationnels mentionnés précédemment. Cette situation fragilise la sécurité du réseau et accentue chaque jour un peu plus la vulnérabilité de l'infrastructure IT (voir Figure 2).

Figure 2. Les solutions de protection tactique du réseau accentuent les risques IT



Source : Enterprise Strategy Group, 2014.

L'entreprise a besoin d'une architecture de sécurité réseau intégrée axée sur les menaces

Les grandes entreprises font face à un dilemme : les réseaux doivent être disponibles, évolutifs, dynamiques et ouverts pour inclure les processus IT et commerciaux actuels, mais ce modèle conduit à une hausse alarmante des risques de cybersécurité. Les contrôles de sécurité du réseau actuels ne sont pas à la hauteur de cet environnement IT fluide où les menaces évoluent constamment.

Alors que faire ? Selon ESG, il faut aborder la protection du réseau sous un nouvel angle. Les RSSI doivent envisager la protection du réseau comme un nouveau modèle d'architecture qui couvre l'ensemble du réseau et du cloud. ESG définit une architecture de sécurité réseau intégrée en ces termes :

Un système intégré de solutions matérielles et logicielles de sécurité réseau, où tous les services de protection peuvent être mis en œuvre partout sur le réseau interne ou étendu, de façon physique ou virtuelle. Une architecture

de sécurité réseau offre également un système de communication sous-jacent qui permet à tous les services et composants de sécurité de partager des informations et de réagir en temps réel pour ajuster les contrôles de sécurité, détecter les incidents et intervenir sur les systèmes compromis.

Une architecture de sécurité réseau intégrée axée sur les menaces s'appuie sur les mêmes types de pare-feu (standard et de nouvelle génération), d'IDS/IPS et de technologies de protection utilisées aujourd'hui. Ce modèle d'architecture se démarque par ses appareils individuels, qui interopèrent et coopèrent de façon plus fluide sur le réseau. En partageant leurs données télémétriques, ils s'informent mutuellement en permanence pour réagir de façon plus coordonnée. De plus, les fonctionnalités de sécurité réseau (pare-feu ou IDS/IPS) peuvent être pensées comme des services et appliquées de façon homogène sur un réseau LAN, dans un data center d'entreprise ou chez un fournisseur de cloud externe, là et où elles sont nécessaires.

Pour réellement conjuguer intégration, protection complète et interopérabilité, l'architecture de sécurité réseau intégrée axée sur les menaces doit s'appuyer sur 3 éléments :

1. **Des commandes et des contrôles centralisés.**
2. **L'application des politiques aux systèmes distribués.**
3. **Des informations exploitables intégrées.**

Des commandes et des contrôles centralisés

La gestion et les opérations représentent l'un des principaux challenges associés aux anciennes technologies de protection des réseaux. Chaque appareil de protection a son propre moteur de politiques et son propre modèle de provisionnement, de configuration et de reporting. Cela entraîne des problèmes majeurs en matière de coûts de fonctionnement et de redondance des tâches. Il est par ailleurs difficile, voire impossible, de déterminer le niveau de protection de l'entreprise simplement en consultant un assortiment de rapports tactiques.

Pour atténuer ces problèmes, une architecture de sécurité réseau intégrée doit d'abord inclure la centralisation des commandes et des contrôles pour :

- **La gestion des services.** Les services de provisionnement, de configuration et de modification de la sécurité réseau doivent être gérés de façon centralisée, pris en charge par une interface utilisateur et un moteur de workflow intuitifs, et assurer l'interopérabilité des outils d'opérations IT. Par exemple, les équipes chargées de la sécurité réseau doivent pouvoir provisionner et configurer des règles de pare-feu, des VLAN et des listes de contrôle d'accès pour les routeurs/commutateurs à partir d'une seule interface. Cela devrait suffire à simplifier les contrôles et à améliorer la protection du réseau, tout en rationalisant les opérations de sécurité.
- **L'interopérabilité avec la virtualisation des serveurs et l'orchestration cloud**. Les outils de configuration générale des charges de travail virtuelles pour VMware, Hyper-V, OpenStack ou AWS doivent être pris en charge et contrôlés de manière adaptée. Avec la centralisation des commandes et des contrôles, l'architecture de sécurité réseau doit pouvoir offrir des API permettant de s'aligner sur les bénéfices du cloud, tels que le provisionnement rapide et le libre-service sur les couches de protection du réseau appropriées**.**
- **La surveillance et le reporting.** Outre des fonctionnalités opérationnelles et de gestion, une architecture de sécurité réseau intégrée doit également proposer une surveillance et un reporting centralisés pour des activités telles que la gestion des événements. Les analystes doivent pouvoir passer d'un rapport à l'autre et corréler plusieurs rapports rapidement pour observer l'état de protection du réseau de façon plus précise et opportune. Pour limiter les angles morts, ces fonctionnalités centralisées doivent également permettre la surveillance des commandes virtuelles et cloud en même temps que les appareils de sécurité réseau physiques.
- **La visibilité avancée.** Les analystes ne veulent pas seulement surveiller leur environnement, ils veulent une visibilité complète. Ils doivent avoir les moyens de repérer les attaques et de savoir quels utilisateurs, applications, contenus et appareils sont sur le réseau, et ce qu'ils y font, pour mettre en œuvre des politiques de sécurité efficaces, détecter les attaques et réagir plus rapidement.

L'application des politiques aux systèmes distribués

La centralisation des commandes et des contrôles permet aux RSSI de créer des politiques de sécurité globales, mais elles doivent tout de même être appliquées par les divers services de protection locaux du réseau. L'architecture de sécurité réseau intégrée répond également à ces besoins avec :

- **La prise en charge de tous les formats, partout sur le réseau.** Les services de protection du réseau doivent être disponibles quels que soient leur emplacement, leur format ou leur combinaison. Cela permet aux équipes chargées de la sécurité d'appliquer des politiques de sécurité granulaires aux segments, aux flux, aux applications ou à des groupes d'utilisateurs spécifiques du réseau. Par exemple, dans les commerces on peut mettre en place un ensemble de contrôles de sécurité physiques et virtuels pour s'assurer que les systèmes des points de vente ne sont connectés qu'avec des adresses IP spécifiques via une combinaison de pare-feu, d'IDS/IPS et d'outils de détection de programmes malveillants avancés. Les utilisateurs d'un réseau LAN d'entreprise peuvent également faire l'objet de politiques d'accès différentes de celles applicables aux employés en télétravail utilisant des réseaux publics.
- **Une gamme de services de protection du réseau.** Une architecture de sécurité réseau doit accomplir les tâches des couches 2 à 7 et prendre en charge tous les types de filtrage de paquets sur l'ensemble des réseaux LAN, WAN et du cloud. Le filtrage de paquets est une vaste catégorie qui comprend la détection de nombreuses menaces : les virus, les vers, les attaques par déni de service (DDoS), les SPAM, l'hameçonnage, les menaces web, les fuites d'informations et les attaques au niveau de la couche d'applications. La multiplicité des formats et des services permettent aux entreprises de créer des piles de sécurité avancées multicouches qui peuvent être adaptées en fonction du trafic du réseau, des groupes d'utilisateurs et des besoins de mobilité, ou ajustées rapidement pour faire face à de nouveaux types de menaces.
- **L'intégration de la sécurité des terminaux et des réseaux.** Par le passé, la sécurité des terminaux et des réseaux était généralement gérée par différents groupes de sécurité à l'aide de processus et d'outils disparates. Du fait de la nature insidieuse des menaces actuelles, cette approche n'est plus possible. Pour combler ce fossé, une architecture de sécurité réseau doit assurer une intégration étroite entre les contrôles de prévention des terminaux et des réseaux, et l'analytique à des fins de détection. Par exemple, les contrôles des applications doivent être homogènes entre les pare-feu de nouvelle génération et les terminaux, afin de protéger les ressources sensibles lorsque les utilisateurs se connectent en utilisant le réseau LAN de l'entreprise ou des réseaux distants publics partout dans le monde. Pour améliorer la détection des incidents, les sandbox d'analyse et les agents des terminaux doivent fonctionner de concert pour établir une corrélation entre un trafic réseau suspect et une activité système anormale.

Des informations exploitables intégrées

Alors que certaines technologies de sécurité réseau telles que les appareils de protection contre les cybermenaces, les IDS/IPS et les passerelles antivirus reposent sur des signatures et des informations venant du cloud, de nombreuses autres technologies dépendent du personnel de sécurité pour la modification de leur configuration ou l'écriture de nouvelles règles de blocage des connexions réseau. À l'inverse, une architecture de sécurité réseau intégrée est conçue dès le départ pour exploiter les informations qu'elle reçoit :

- **Elle est basée sur plusieurs sources de données.** Tandis que les systèmes de gestion des informations des événements de sécurité (SIEM) basent leurs analyses de sécurité sur les événements des journaux, l'architecture de sécurité réseau présente beaucoup d'autres types de données à analyser. Notamment les technologies réseau de base comme NetFlow et la capture intégrale des paquets, mais également des informations détaillées sur le profilage et l'analyse des terminaux, les modes d'accès aux données des utilisateurs/appareils, ainsi que les audits des applications cloud. Lorsqu'elles sont combinées, corrélées et analysées correctement, ces nouvelles données aident l'entreprise à améliorer la gestion des risques, à détecter les menaces et à intervenir plus rapidement.

- **Elle intègre les informations sur les menaces axées sur le cloud.** Une architecture de sécurité réseau doit inclure ce type d'informations et offrir des données détaillées sur les vulnérabilités logicielles, les adresses IP incorrectes, les URL non autorisées, les canaux de commande et de contrôle, les fichiers malveillants, les indicateurs de compromission (IoC) et les modes attaques qui évoluent rapidement.
- **Elle est conçue pour l'automatisation.** Le but d'une architecture de sécurité réseau est d'aider les entreprises à automatiser la protection de leur réseau en tirant parti des informations de sécurité internes et externes. Par exemple, un trafic anormal au sein du data center peut déclencher une règle de pare-feu automatisée qui interrompt les flux de données selon une combinaison de facteurs tels que l'IP source, le port, le protocole et les activités DNS. Lorsqu'un programme malveillant est détecté, le réseau peut consulter les téléchargements de fichiers, découvrir rétroactivement les terminaux à l'origine du téléchargement de ces fichiers suspects à partir d'une URL particulière et y remédier. De telles activités de résolution automatisée permettent d'améliorer en permanence les contrôles de sécurité des réseaux et contribuent à systématiser les analyses de sécurité pour répondre plus rapidement aux attaques.

Pour résumer, une architecture de sécurité réseau peut non seulement répondre aux challenges existants, mais également présenter des bénéfices pour l'entreprise en matière de protection et d'infrastructure IT (voir le Tableau 1).

Tableau 1. Caractéristiques des architectures de sécurité réseau

Propriétés des architectures de sécurité réseau	Détails	Fonctionnalité	Bénéfices
Des commandes et des contrôles centralisés	Gestion des services, interopérabilité de l'orchestration et de la virtualisation cloud/serveur, surveillance et reporting centralisés	Centralise le provisionnement et la gestion des politiques, de la configuration, des modifications, des événements, etc.	Opérations de sécurité rationalisées, facilité d'utilisation, contrôle centralisé et visibilité sur tous les éléments de sécurité du réseau, quels que soient leur emplacement ou leur format
L'application des politiques aux systèmes distribués	Prise en charge de l'ensemble des services de sécurité du réseau, des emplacements et des formats, intégration entre sécurité du réseau et des terminaux	Coordonne les divers services du réseau et étend l'application des politiques de sécurité au cloud	Couches de sécurité adaptées aux divers exemples d'utilisation pour protéger les utilisateurs, les appareils et les applications ; facile à modifier et à améliorer pour répondre aux nouvelles menaces
Des informations exploitables intégrées	Diverses sources de données, intégration des informations sur les menaces axées sur le cloud	Fournit des détails granulaires sur le trafic des applications et du réseau, sur les activités des terminaux et sur les nouvelles menaces non détectées	Prise de décision basée sur des informations en temps réel, automatisation des processus de résolution

Source : Enterprise Strategy Group, 2014.

Architecture de sécurité réseau intégrée Cisco : les pare-feu de nouvelle génération axés sur les menaces

Si Cisco Systems a toujours été reconnu pour ses produits de sécurité réseau, la société a dû transformer sa technologie et sa vision pour répondre aux exigences des entreprises et aux menaces toujours plus dangereuses. C'est pour cette raison qu'en 2013, Cisco a décidé d'acquérir Sourcefire, entreprise innovante dans le domaine de la sécurité réseau.

Bien que la fusion entre Cisco et Sourcefire ait rapproché deux géants de la sécurité, il restait encore beaucoup à faire pour intégrer les technologies qui formeraient le type d'architecture de sécurité réseau d'entreprise que nous avons décrite. Ce travail commence à porter ces fruits, avec l'annonce de la solution Cisco ASA avec les fonctionnalités FirePOWER. En combinant le pare-feu Cisco ASA au système de prévention des intrusions de nouvelle génération et aux fonctionnalités de protection avancées contre les programmes malveillants de Sourcefire, Cisco propose désormais une offre complète de services de sécurité réseau qui garantit :

- **La visibilité et le contrôle granulaires des applications.** Comme d'autres, le pare-feu de nouvelle génération Cisco peut détecter et générer des rapports sur les connexions des applications et appliquer des politiques basées sur les utilisateurs, sur les groupes ou encore sur les appareils. Mais avec FirePOWER, Cisco va très certainement étendre le contrôle et la visibilité des applications à l'ensemble du réseau et intégrer ces fonctionnalités à ces autres ressources, telles que TrustSec et Cisco ISE (Identity Services Engine).
- **La protection axée sur les menaces sur l'ensemble du réseau et des terminaux.** L'architecture de sécurité réseau de Cisco protège contre les menaces avancées et comprend des fonctions complètes de détection et de prévention des malwares. Elle tire parti de FirePOWER pour la protection du réseau et de FireAMP pour la sécurisation des terminaux. La détection et la prévention des menaces sont encore renforcées par le système de prévention des intrusions de nouvelle génération FirePOWER, le filtrage d'URL par catégorie et par réputation et les nombreuses informations sur les risques. FireAMP peut également suivre l'activité des terminaux pour une analyse de l'historique. Lorsqu'un nouveau programme malveillant est découvert, FireAMP peut appliquer des politiques de sécurité de façon rétrospective afin d'identifier et de corriger les terminaux qui ont rencontré le fichier par le passé. Enfin, en combinant les événements IPS, les informations sur les risques et les événements liés à des programmes malveillants pour générer des IoC détaillés, Cisco permet à l'équipe chargée de la sécurité d'améliorer et d'automatiser les analyses de sécurité et les processus de résolution.
- **De nombreux services de sécurité et une visibilité totale.** Cisco offre maintenant une gamme de services de sécurité physiques et virtuels pour les pare-feu, le contrôle des applications, les IDS/IPS, le filtrage d'URL, ou encore la détection/prévention des programmes malveillants avancés. Les entreprises peuvent ainsi personnaliser leurs couches de protection selon les utilisateurs, les applications, les segments et le trafic du réseau, pour tous les formats et sur l'ensemble du réseau. Cisco permet également de surveiller tous les services/sites afin d'éliminer les angles morts.
- **L'évaluation de l'impact.** L'architecture de sécurité réseau Cisco est conçue pour mettre en corrélation les intrusions et l'impact qu'une attaque peut avoir sur une cible donnée. Cisco présente cette corrélation en utilisant une série de 5 « indicateurs d'impact ». Un indicateur d'impact de niveau 1 décrit un événement révélant une vulnérabilité chez un hôte donné nécessitant une intervention immédiate. Les autres indicateurs ont des priorités inférieures. Les équipes de sécurité déjà surchargées peuvent ainsi mieux déterminer où déployer leurs ressources limitées. De cette façon, elles améliorent leur niveau de protection et leur efficacité opérationnelle.

Pour Cisco, associer ASA et FirePOWER améliore la sécurité à tous les stades de l'attaque : avant, pendant et après. Avant l'incident, l'architecture de sécurité réseau Cisco peut être utilisée pour identifier les ressources du réseau, appliquer les politiques de sécurité et renforcer les contrôles pour une meilleure protection. Pendant l'incident, ASA et FirePOWER peuvent détecter les activités suspectes/malveillantes (sur les réseaux et sur les terminaux), bloquer les connexions réseau et défendre le réseau dans son ensemble. Enfin, après l'incident, l'architecture de sécurité réseau Cisco permet également aux analystes d'évaluer l'impact de l'attaque, de modifier les contrôles pour améliorer le confinement et de tirer parti des données d'analyse pour accélérer la résolution.

Cisco sait qu'il reste beaucoup à faire et prévoit d'ajouter de nombreuses fonctions à son architecture au cours des 12 à 18 prochains mois. Beaucoup de RSSI devront évaluer le niveau de protection actuel de leur réseau et planifier la création d'une architecture de sécurité réseau. Avec son offre de services spécifiques, Cisco pourra les y aider.

Conclusions

Aujourd'hui, la cybersécurité est façonnée par un certain nombre de problématiques :

1. La virtualisation, la mobilité et le cloud computing complexifient l'IT.
2. Les menaces sont de plus en plus dangereuses et il est particulièrement difficile d'empêcher les attaques ciblées, de les détecter et d'y remédier.
3. Les anciennes mesures de protection des réseaux sont moins efficaces que par le passé.
4. De nombreuses entreprises ne disposent pas des compétences nécessaires pour sécuriser leurs réseaux.

Le constat est alarmant : en matière de cybersécurité, les risques augmentent tous les jours.

Albert Einstein a dit un jour que « la définition de la folie, c'est de faire toujours la même chose et de s'attendre à un résultat différent ». C'est pourtant bien ce que font les RSSI lorsqu'ils cherchent à protéger leurs réseaux. Il est temps que les entreprises, les départements IT et les responsables de la sécurité s'aperçoivent qu'ils mènent un combat perdu d'avance. Les cybercriminels utilisent de nouveaux types d'armes et de tactiques que les entreprises ne peuvent contrer qu'avec de nouveaux types de défenses améliorant les mesures de protection, de détection et de réponse.

Nous pensons que ces améliorations ne proviendront pas de changements tactiques progressifs apportés aux anciennes solutions de protection du réseau. Les entreprises doivent aller de l'avant avec un changement plus stratégique : une architecture complète de sécurité réseau intégrée. La fusion entre Cisco et Sourcefire en 2013 a ouvert un monde de possibilités. En incluant les meilleures fonctionnalités du pare-feu ASA, le système de prévention des intrusions de nouvelle génération FirePOWER, la protection contre les programmes malveillants avancés et la mutualisation des informations sur la sécurité à son architecture de sécurité réseau intégrée, Cisco pourrait encore renforcer sa position de leader du secteur.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 États-Unis | Tél. : 508 482 0188 Fax: 508 482 0218 | www.esg-global.com