Livre blanc

Secure Networks™ :

Une approche automatisée et rentable de la sécurité et de la continuité de l'activité à l'échelle de l'entreprise

enterasys™
Networks that Know

L’essentiel

Assurer la continuité de l’activité ainsi que la disponibilité des applications, des services et des systèmes clés demeure un objectif prioritaire pour les directions commerciale et informatique de l’entreprise. Et pourtant, les nouvelles exigences en matière de réseaux, notamment la nécessité de consolider les ressources voix/vidéo/données sur une infrastructure unique et de fournir un accès sans fil plus universel, vont de pair avec des menaces plus puissantes contre la sécurité et qui posent des défis plus importants que jamais. En résumé, devoir concilier une sécurité à l’échelle de l’entreprise et une dépendance encore plus grande vis-à-vis de l’infrastructure de communication conduit nombre d’entreprises à repenser leur stratégie réseau.

Jusqu’à présent, beaucoup d’entreprises adoptaient une stratégie au coup par coup en matière de sécurité réseau. Et même si des produits spécifiques comme les firewalls, les systèmes de détection d’intrusion, les logiciels antivirus et les technologies d’authentification des utilisateurs sont efficaces, ils ne fournissent pas la protection à l’échelle de l’entreprise requise pour protéger contre les attaques sophistiquées d’aujourd’hui. Par exemple, la périphérie du réseau peut être correctement sécurisée contre des menaces ciblées ou contre des prédateurs opportunistes, mais qu’en est-il du cœur du réseau vulnérable aux nouvelles attaques par déni de service distribué (DDoS) ou aux attaques émergentes par force brute et en cascade ?

Et la pression ne cesse d’augmenter à mesure que les réseaux évoluent et qu’apparaissent de nouvelles technologies, de nouvelles applications et de nouveaux équipements. Même si le nombre d’employés n’évolue guère, les entreprises devront administrer davantage de nœuds et faire face à davantage de risques de sécurité. Par exemple, si deux ou trois nouveaux équipements tels que des PDA, des téléphones IP ou des équipements sans fil sont régulièrement ajoutés à chaque réseau traditionnel, un réseau de 10 000 nœuds aujourd’hui pourra héberger 40 000 nœuds d’ici à quelques années, sans nouveaux utilisateurs supplémentaires. Et pourtant, la plupart des budgets et ressources informatiques des entreprises continueront d’être révisés à la baisse.

Alors que se cantonner à gérer la croissance du réseau peut déjà sembler insurmontable, garantir la sécurité absolue est d’un tout autre ordre. Pour la plupart des entreprises, la situation est inextricable. En effet, comment développer l’activité et le réseau et ajouter des technologies pour accroître les revenus tout en garantissant la fiabilité totale des applications, des ressources et des données de l’entreprise, de bout en bout, le tout sans compromettre les performances ?

Le présent livre blanc est destiné à aider les responsables réseau ainsi que les directeurs informatiques et commerciaux à comprendre ces bouleversements fondamentaux et pourquoi les besoins et les enjeux en matière de sécurité conduisent les entreprises à rechercher des solutions alternatives pratiques pour créer un réseau plus sécurisé, plus souple et plus évolutif. Ce document présente également la stratégie d’Enterasys en matière de déploiement de réseaux Secure Networks, une solution plus simple, plus intégrée, plus économique, plus souple et capable de répondre aux besoins métier croissants de l’entreprise.

La sécurité est au cœur de la continuité de l'activité

Pour maintenir et améliorer la sécurité aussi bien des applications métier que des données clients tout en garantissant la continuité de l'activité et les accords de niveau de service (SLA), la plupart des entreprises estiment nécessaire de réévaluer leurs plans réseau et de sécurité traditionnels. Ceci est particulièrement vrai pour un éventail croissant de défis en matière de sécurité informatique : les applications et les systèmes d'exploitation sont soumis à des attaques ; les vols d'informations vitales sont en hausse ; les réglementations coûtent de plus en plus cher et les nouvelles technologies sont en train d'effacer la distinction entre périmètres protégés et non protégés.

En outre, les enjeux sont désormais plus importants car les entreprises sont aujourd'hui plus dépendantes de leur infrastructure d'information hautes performances. Une panne du réseau de communication a des conséquences considérables sur les revenus, sur la productivité des employés, sur la satisfaction des clients et sur la réputation de l'entreprise.

Pour la plupart des entreprises, garder la même stratégie de sécurité n'est ni pratique ni efficace puisque les menaces de sécurité continuent d'évoluer avec la technologie. Ces dernières années, les entreprises ont dépensé des milliards de dollars pour tenter de protéger leurs ressources informatiques à l'aide de firewalls, de logiciels antivirus, de services de conseils en sécurité et autres technologies de sécurité. En dépit de tous ces efforts, les attaques restent tout aussi virulentes et le coût pour les combattre est monté en flèche.

Même si les virus et les accès réseau abusifs d'origine interne sont les deux types d'attaques détectées les plus courants, les attaques les plus coûteuses (soit 40% des pertes totales) sont liées à des attaques par déni de service (DoS), à des vols d'informations propriétaires ainsi qu'à des abus liés aux connexions sans fil et à une utilisation abusive d'Internet en interne. De même, une enquête IDC réalisée récemment a permis de constater que 75% des grandes entreprises avaient signalé au moins une infraction de sécurité réussie au cours des 12 derniers mois, 40% d'entre elles ayant signalé 11 attaques réussies ou plus.

Même si assurer la sécurité du réseau a toujours été à l'ordre du jour, les dommages potentiels liés à un nouvel éventail de menaces de sécurité obligent nombre d'administrateurs réseau à repenser leurs stratégies de sécurité existantes. Les menaces nouvelles et émergentes, notamment les vers visant les systèmes de messagerie instantanée, les logiciels espions, les attaques DDoS ainsi que les attaques par force brute et en cascade peuvent mettre un coup d'arrêt à l'activité de l'entreprise et entacher sa réputation.

En septembre 2004, *Computerworld* avait par exemple signalé que la société de traitement de cartes de crédit Authorize.Net avait été la cible d'une attaque DDoS intermittente et de grande envergure avec comme conséquence des interruptions périodiques de service pour les clients. L'attaque avait été précédée quelques jours plus tôt par une demande de forte somme d'argent. Même si cette société s'en est remise depuis, son centre d'assistance à la clientèle a dû répondre à un nombre extrêmement important d'appels pendant l'attaque, ce qui a pu être préjudiciable à sa réputation.

Malheureusement, ces problèmes de sécurité ne sont pas des menaces qui se cantonnent à l'infrastructure informatique. Elles sont dirigées contre l'entreprise elle-même. Qu'il s'agisse de vers ou de virus ou de vol de propriété intellectuelle, d'une menace contre un site Web ou d'amendes envers des entreprises qui ne se conforment pas à la réglementation Sarbanes Oxley, tous ces événements sont liés entre eux et peuvent avoir un impact négatif énorme sur l'activité de l'entreprise s'ils ne sont ni gérés ni prévenus correctement.

Intégrer une sécurité intelligente au réseau

D'un point de vue technologique, l'infrastructure réseau ne se limite plus à connecter des utilisateurs ou à augmenter la capacité. Désormais, les réseaux doivent avoir l'intelligence non seulement de prévoir et de prévenir les risques de sécurité, mais aussi de s'adapter aux environnements changeants des utilisateurs. Par exemple, la plupart des entreprises ouvrent désormais des pans entiers de leur réseau à leurs fournisseurs, partenaires, clients et sous-traitants, ce qui augmente considérablement les risques. En outre, les entreprises ajoutent davantage de points d'accès sans fil et étendent leurs réseaux, ce qui les expose et les rend plus vulnérables aux failles de sécurité.

En conséquence, développer une solution de sécurité efficace ne se limite plus à ajouter des firewalls et des logiciels antivirus ou à résoudre le problème de sécurité du moment au moyen d'une technologie autonome ou des tout derniers produits spécifiques. Ce qu'il faut, c'est une stratégie de sécurité efficace pour bâtir une architecture de sécurité plus universelle. Une architecture capable d'affronter tout un éventail de menaces et de fournir tout un panel de réponses à une variété d'utilisateurs tout en assurant la disponibilité de l'ensemble de l'environnement technologique. Plus spécifiquement, l'application de politiques à l'échelle de l'entreprise doit s'effectuer via un modèle opérationnel commun et des outils d'administration de réseau coordonnés. Plutôt que de traiter les risques de sécurité au cas par cas, les stratégies de sécurité de nouvelle génération doivent s'appuyer sur une approche universelle basée sur l'infrastructure réseau.

C'est cette approche universelle et intégrée qui générera un système holistique capable de répondre aux besoins émergents, sans complexifier l'infrastructure réseau ni augmenter la charge de travail, le personnel ou les coûts opérationnels. Ce qui est nécessaire, c'est une solution Secure Networks : un réseau doté de l'intelligence nécessaire pour administrer les menaces de sécurité existantes et nouvelles et qui est directement intégrée à son architecture.

Plutôt que d'ajouter au fur et à mesure des fonctionnalités de sécurité au réseau de manière ponctuelle et réactive, les entreprises peuvent désormais s'appuyer sur l'infrastructure intelligente d'une architecture Secure Networks pour résoudre de manière proactive les risques de sécurité potentiels. Sans restreindre leur souplesse ni impact négatif sur les performances ou la disponibilité. Les principaux composants d'une architecture Secure Networks sont :

- La maîtrise hautement granulaire du contexte du trafic acheminé sur le réseau
- L'application universelle de politiques via un modèle opérationnel commun et des outils d'administration de réseau coordonnés
- La définition centrale de politiques et la capacité de pousser des politiques sur chaque équipement
- Des interfaces ouvertes pour le choix de l'architecture, sans sacrifier le potentiel d'une infrastructure sécurisée

Comme les analystes métier et technologiques de Gartner l'ont reconnu : « Le lieu idéal pour contrôler l'accès au réseau est au sein de l'infrastructure réseau. » Et Forrester Research d'insister également sur l'adoption de réseaux Secure Networks intelligents en déclarant : « La tendance est au remplacement d'une série d'appliances réseau isolées par un système de sécurité du réseau de campus intégré et bâti autour de commutateurs de troisième génération fonctionnant à la vitesse du lien. »

Les risques de sécurité étant de plus en plus évolués, il est vital que les entreprises commencent à adopter une infrastructure réseau plus holistique. Ceci afin de contrecarrer les menaces de sécurité provenant de l'extérieur du réseau, mais aussi via ou au sein du réseau, de manière à la fois coordonnée, facile à administrer et pratique. Neutraliser les menaces de sécurité sur un seul point d'entrée ne fait qu'encourager d'autres formes d'attaque. Par exemple, plus la sécurité déployée au niveau Accès et du centre de données sera efficace, plus les attaques ciblées sur le cœur du réseau iront crescendo. Il s'agit d'attaques qu'un réseau Secure Networks doit pouvoir empêcher et arrêter puisqu'une panne au niveau du cœur du réseau aura des conséquences sur un nombre bien plus importants d'utilisateurs et de services qu'une panne ou une interruption en périphérie de réseau.

Le réseau Secure Networks – Les 5 « C » pour le succès de l'activité

Pour la plupart des entreprises, un réseau Secure Networks n'est pas une solution de substitution standard et unique. Il s'agit plutôt d'un objectif à atteindre en évaluant l'infrastructure réseau existante. Et en comprenant les nouveaux enjeux de sécurité, notamment les besoins évolutifs au niveau du réseau et de l'activité de l'entreprise, et en alignant l'infrastructure réseau sur les nouveaux objectifs. Un directeur commercial ou informatique doit donc commencer par tenir compte des nouveaux besoins d'une infrastructure réseau.

Jusqu'à présent, les réseaux étaient considérés comme un moyen de transmission de l'information d'un point vers un autre. Par conséquent, les critères d'achat se concentraient sur trois caractéristiques principales : connectivité, capacité et coût, que nous appellerons les « 3 C classiques ». Même si le coût reste un critère important, aujourd'hui, les entreprises sont confrontées à des problèmes critiques supplémentaires au-delà des traditionnels problèmes de connectivité et de capacité. En effet, l'infrastructure intelligente moderne doit satisfaire à de nouvelles préoccupations métier et de sécurité : continuité, contexte, contrôle, conformité et consolidation, que nous appellerons les « 5 C ». Analysons maintenant en détail chacun de ces C :

- **Continuité**. Un réseau Secure Networks doit pouvoir garantir une communication métier ininterrompue et prévisible. Ce réseau doit être assez puissant pour résister aux attaques DoS, notamment à la variante Distribuée (DDoS) qui peut faire tomber un réseau d'entreprise tout entier. Il doit en outre ajouter des mécanismes d'auto-protection pour assurer la disponibilité des services critiques, y compris en cas d'activités malveillantes. La continuité est tout particulièrement cruciale pour les réseaux convergents sur lesquels une attaque soutenue pourrait provoquer la perte du trafic voix et données.

- **Contexte**. Un réseau Secure Networks doit pouvoir comprendre le contexte des flux de paquets qui traversent l'infrastructure et savoir comment ces mêmes flux se définissent par rapport à un comportement normal et prévu. Par exemple, les traditionnelles caractéristiques du trafic réseau produites par un directeur des ventes sont complètement différentes de celles générées par un administrateur système. Fort d'une conscience contextuelle évoluée, le réseau peut reconnaître le trafic légitime du trafic nuisible et prendre des décisions pour protéger les services métier qu'il fournit.

- **Contrôle**. Le contrôle granulaire est au cœur de toute infrastructure sécurisée. Un réseau Secure Networks doit pouvoir différencier et contrôler les nombreux flux de trafic qui le traversent. Pour ce faire, il opère une distinction entre les communications métier légitimes et les activités malveillantes ou interdites. Le contrôle s'applique aux utilisateurs, aux services et aux applications et le réseau peut être reconfiguré de manière dynamique depuis un point central pour répondre aux besoins de sécurité et métier en perpétuelle mutation.

- **Conformité**. Les gouvernements et les organismes de normalisation imposent de plus en plus des utilisations acceptables des informations métier. Citons par exemple les législations HIPAA et Sarbanes-Oxley aux États-Unis ainsi que la réglementation européenne sur la confidentialité des données. Ces règles influencent la manière dont les services informatiques traitent les informations et les transactions numériques, l'absence de conformité pouvant entraîner des pénalités financières conséquentes. Un réseau Secure Networks concerne chaque élément du système d'information, ce qui en fait le lieu le plus logique pour intégrer des technologies qui appliquent la conformité aux exigences de confidentialité.

- **Consolidation**. Les réseaux doivent s'adapter pour intégrer différents types de communications et de flux. Un réseau Secure Networks doit pouvoir s'adapter pour fédérer des applications, des utilisateurs et des sites supplémentaires sur une infrastructure universelle et commune. Ceci s'applique à tout, qu'il s'agisse de l'association de la voix et des données sur un réseau IP unique ou de l'extension de l'infrastructure avec de nouvelles fonctionnalités sans fil en passant par l'ajout de nouveaux bureaux et services suite à une fusion ou une acquisition.

En effet, les critères d'achat d'équipements réseau ont changé. L'infrastructure réseau du 21ème siècle doit satisfaire aux 5 C tout en continuant à fournir les traditionnels 3 C et sans compromettre les fonctionnalités majeures du réseau. En d'autres termes, un réseau Secure Networks doit participer activement à la sécurité et à la tranquillité d'esprit de l'entreprise, un objectif que les directeurs informatiques tentent d'atteindre non sans grandes difficultés.

Pour satisfaire aux 5 C et fournir un contrôle granulaire et une réaction automatisée, un réseau Secure Networks doit intégrer des technologies de sécurité de pointe à l'infrastructure réseau. Une solution Secure Networks adéquate garantit la conformité de l'entreprise et prévient les événements de sécurité, sans temps d'arrêt pour l'activité ni frais d'exploitation supplémentaires. Mais cette solution permet également à l'entreprise de devenir proactive et réactive face aux besoins de son activité.

Les entreprises qui ne bénéficient pas des fonctionnalités de sécurité intégrées d'un réseau Secure Networks doivent généralement consacrer davantage de temps et de ressources à l'administration de chaque problème de sécurité et réseau. Et concevoir des solutions ad-hoc pour les nouvelles menaces de sécurité. Plutôt que de devoir procéder de la sorte, un réseau Secure Networks doté d'une intelligence et de fonctionnalités de sécurité intégrées permet de recentrer les ressources et l'énergie de l'entreprise sur le développement à valeur ajoutée d'applications, sur des extensions du réseau et sur une administration proactive, plutôt que réactive, des menaces de sécurité.

Attributs d'un réseau Secure Networks

Les 5 C servant de leitmotiv pour répondre aux besoins critiques d'un réseau Secure Networks, analysons maintenant certains des attributs les plus tangibles de cette stratégie. En premier lieu, le réseau Secure Networks doit fournir une visibilité et un contrôle granulaire hors pair à travers toute l'entreprise pour faciliter le déploiement d'autres fonctionnalités et caractéristiques majeures. En outre, le réseau Secure Networks doit offrir l'extensibilité (via une architecture ouverte) et la réutilisabilité nécessaires pour s'adapter en permanence à de nouveaux processus métier.

Analysons de plus près certains des principaux attributs inhérents à une infrastructure Secure Networks :

- **Visibilité totale du réseau** pour voir non seulement les événements de sécurité et les anomalies mais aussi les utilisateurs présents sur le réseau et pour savoir où ils se trouvent et ce qu'ils font, et ce depuis leur point de connexion. Sans cette visibilité, le réseau ne peut pas fournir le niveau de conscience requis pour un réseau Secure Networks.
- **Identité et intelligence contextuelle**, ou bien Qui, Quoi, Quand, Où et Pourquoi ? Le réseau doit comprendre qui et quoi se trouve sur le réseau et pouvoir distinguer un téléphone IP d'une imprimante ou d'un poste de travail. Il doit également comprendre la relation entre les utilisateurs et l'entreprise.
- **Application de politiques distribuées**. Le réseau est si vaste et distribué qu'il faut un moyen simple pour déployer et appliquer une politique en temps réel. Dans le cas contraire, le fardeau administratif devient insupportable.
- **Contrôle centralisé et granulaire via des politiques**. Le réseau doit pouvoir examiner en profondeur les caractéristiques de communication pour comprendre ce qui se produit et exercer un contrôle au niveau de chaque utilisateur et équipement. Par exemple, le contrôle peut prendre la forme de configurations centralisées de politiques applicables via une infrastructure intelligente.
- **Interopérabilité ouverte**. Chaque entreprise utilise du matériel de différents équipementiers au sein de sa structure informatique. Un réseau Secure Networks doit donc être en mesure de garantir l'interopérabilité dans un environnement hétérogène.
- **Administration au niveau système et en une seule action** pour exécuter de nombreuses tâches d'un seul clic. Le système d'administration de réseau, ainsi que les composants réseau eux-mêmes, doivent pouvoir réagir rapidement à des tâches de haut niveau et avec un niveau élevé d'automatisation pour permettre une action d'un seul clic.
- **Réaction et protection dynamiques**. Les nombreux équipements et processus actuellement utilisés pour gérer la sécurité nécessitent un traitement manuel trop longtemps. Un processus rationalisé s'impose pour que, lorsqu'une menace est détectée, et même si la réaction doit être autorisée, les informations soient pré-agrégées et que le système puisse informer sur la menace, sur son emplacement et sur les moyens de la traiter.
- **Solutions intégrées**. Un réseau Secure Networks doit garantir la réutilisabilité à travers toute l'infrastructure du réseau et avec d'autres technologies, quel que soit le constructeur.
- En conclusion, les **éléments d'un réseau Secure Networks doivent être disponibles aujourd'hui** et auront été éprouvés dans des environnements clients. Les entreprises tireront des avantages financiers, opérationnels et métier énormes d'une telle infrastructure.

Une approche concrète des réseaux Secure Networks

Même si le concept de réseau Secure Networks n'est pas étranger à la plupart des directeurs informatiques ou commerciaux, une approche concrète du déploiement d'un réseau Secure Networks peut parfois sembler floue, en particulier pour les entreprises ayant déjà investi lourdement dans des solutions réseau et de sécurité. Cependant, cette même préoccupation est une raison supplémentaire qui donne toute sa légitimité au concept de réseau Secure Networks. Souplesse et évolutivité figurent parmi les avantages concrets d'une solution Secure Networks. Les entreprises peuvent déployer cette stratégie où et quand elles en ont besoin, avec l'ampleur souhaitée et en fonction de leur contraintes spécifiques, de leur architecture réseau existante et des solutions de sécurité qu'elles ont déjà installées.

Cerner les objectifs déjà spécifiés (les 5 C) et déployer le bon cocktail de technologies ainsi qu'une conception de réseau stratégique permet aux entreprises de bénéficier de la sécurité et du contrôle nécessaires à leur métier. Non seulement pour atténuer les menaces, externes ou internes, mais aussi pour multiplier les chances de succès de leur activité et assurer leur avenir.

Plus précisément, les entreprises doivent choisir des composants et des architectures réseau répondant à leurs principales exigences pour une sécurité et un contrôle supérieurs, une meilleure facilité d'utilisation et des performances réseau accrues. Par exemple, pour répondre aux importants besoins d'évolution et notamment à la multiplication par trois ou par quatre du nombre d'équipements connectés à un réseau au cours des prochaines années (même si le nombre d'utilisateurs réels ne changera pas), les entreprises devront appliquer des politiques communes sur leurs réseaux pour réduire le temps d'administration, une activité potentiellement très grosse consommatrice de ressources. Trouver des solutions qui garantissent l'application de politiques communes est une application concrète de la philosophie Secure Networks.

La solution Secure Networks exige également une plate-forme d'administration commune et opérationnelle pour fournir une visibilité totale sur la périphérie du réseau (Niveau Accès) et au niveau Distribution, du cœur de réseau et du centre informatique. Cette vue globale du réseau ainsi que des fonctionnalités distribuées pour opérer des modifications à grande échelle d'un seul clic profitent à la fois à la communauté informatique et des utilisateurs. En effet, d'un côté, les administrateurs réseau peuvent réagir plus rapidement aux événements, et contribuer ainsi à la réduction du coût de possession, tandis que de l'autre côté les employés et autres utilisateurs disposent d'un accès sécurisé et à la demande aux ressources nécessaires pour améliorer leur productivité, même sur une connexion sans fil.

Bien entendu, les entreprises doivent continuer à améliorer les performances de base et la disponibilité de leurs réseaux, plus particulièrement lorsqu'elles migrent vers un déploiement sécurisé d'applications de nouvelle génération et gourmandes en bande passante, notamment pour la collaboration interactive, la vidéo en flux continu sur IP ou l'informatique en grille.

Dotées de la bonne stratégie et des solutions prenant en charge le concept d'un réseau Secure Networks, les entreprises peuvent protéger leurs investissements et créer une infrastructure évolutive, sans compliquer la situation ni créer involontairement des failles de sécurité à mesure que le réseau, le nombre d'utilisateurs ou le nombre d'équipements connectés au réseau augmentera.

Comprendre ses besoins – Comment créer un réseau Secure Networks

Une fois qu'une entreprise s'est donnée pour objectif de déployer un réseau Secure Networks, d'inévitables questions se posent :

Avec les sommes déjà investies dans différents équipements réseau et de sécurité, quel est le meilleur moyen pour bâtir un réseau Secure Networks ?

Dans quelle mesure une entreprise doit-elle faire un compromis entre performances accrues et moindre sécurité ?

Quel est le meilleur moyen pour optimiser les investissements existants, rationaliser l'administration, garantir l'ouverture et créer l'infrastructure la plus souple possible ?

Pour la plupart des entreprises, il n'est pas aisé de répondre à ces questions, en particulier en raison du large choix de composants de solution à la disposition des sociétés. Traditionnellement, il existe des **approches propres à un fournisseur**, **des solutions spécifiques à un problème** et des **solutions de sécurité basées sur le réseau**.

Même si la plupart de ces approches peuvent théoriquement résoudre les mêmes problèmes et défis, les différences entre elles sont importantes et peuvent avoir un impact non négligeable sur l'activité de l'entreprise, sur les ressources informatiques et sur le chiffre d'affaires global. Par exemple, procéder à l'application universelle de politiques basées sur un modèle opérationnel commun est une opération très difficile dans le cas d'une stratégie s'appuyant sur des solutions spécifiques. Et pourtant, il s'agit d'une conséquence pratique de l'approche en réseau ou intégrée. Pour mieux comprendre les différences, examinons l'éventail des différentes approches possibles :

- **Approche mono-fournisseur**. Dans ce cas de figure, l'entreprise recherche un fournisseur qui lui procurera les composants de réseau et de sécurité pour son infrastructure de communication, notamment les services voix, données et sans fil.

  Points importants :

  - La fonctionnalité de détection pêchera parce qu'aucun constructeur ne peut être toujours à la pointe de l'innovation
  - La fonctionnalité de localisation et l'analyse peuvent s'avérer difficiles
    - Les possibilités de réaction seront souvent limitées, complexes et coûteuses et n'offriront qu'un choix restreint
    - Les entreprises sont enfermées dans une solution propriétaire qui fournit peu de souplesse lors de l'ajout de nouvelles technologies et applications

- **Approche basée sur une solution spécifique**. En règle générale, cette approche tente de résoudre le problème de la sécurité avec des solutions spécifiques destinées à contrer des menaces de sécurité ou des besoins réseau spécifiques : une approche à base de solutions superposées. Cependant, une telle approche peut nécessiter un certain nombre d'équipements spécifiques et difficiles à gérer, souvent de différents constructeurs, pour répondre aux problèmes de sécurité. Le résultat est une infrastructure complexe difficile à administrer et à adapter avec le temps.

  Points importants :

  - La détection est limitée.
  - Analyse de localisation limitée. Localisation de l'équipement au niveau agrégation, mais présence de lacunes sans technologie de sécurité.
  - Possibilité d'arrêter les réactions entre les différentes zones mais pas au sein de chacune d'entre elles.
  - La remédiation et l'analyse peuvent être très bonnes. Un riche ensemble de technologies et d'outils est généralement disponible.
  - Pas de vue unifiée de l'infrastructure.

- **Approche pratique et intégrée**. Cette approche se fonde sur une infrastructure réseau dotée d'une intelligence sécuritaire intégrée pour créer une solution holistique de bout en bout. L'idée est qu'une sécurité optimale ne peut être obtenue que sous la forme d'une architecture au niveau système qui est ouverte aux deux extrémités. Un large éventail de fonctionnalités de sécurité et d'administration doit permettre de superviser l'activité de différents systèmes et composants réseau et d'appliquer des politiques sur une variété tout aussi large de ressources réseau et de types d'utilisateurs.

  Cette approche s'appuie sur un paradigme d'administration actif qui relie les événements aux actions, avec le contexte approprié. Elle est également ouverte au niveau des fonctions et de la diversité des équipements réseau devant être protégés. Grâce à sa capacité à augmenter le nombre de fonctionnalités spécifiques à un équipement, ou à les compléter, cette stratégie peut même comprendre une infrastructure de sécurité en plus d'améliorer des technologies de sécurité existantes ou tierces, ainsi qu'un niveau unifié d'administration active. Au sein de ce modèle, un gestionnaire de politiques peut coordonner et orchestrer les activités de sécurité et d'administration sur le réseau. Enterasys appartient typiquement à cette catégorie de fournisseurs de solutions.

  Points importants :

  - Le plus large éventail de détections. Capacité à comprendre des informations associées à un quelconque type d'équipement envoyant des informations, sans se limiter à des solutions matérielles d'un seul constructeur.
  - Le réseau est impliqué dans les services de localisation pris en charge par une infrastructure d'administration unifiée.
  - L'application est aussi universelle que le réseau. Application la plus rudimentaire comme la plus sophistiquée. La réaction peut être adaptée à l'équipement réseau qui la reçoit et peut être omniprésente.
  - Remédiation des problèmes beaucoup plus aisée puisque la qualité de l'information et de l'application est élevée.

Avantage de la « sécurité intégrée »

Peu d'entreprises sont touchées par tous les nouveaux virus ou toutes les nouvelles menaces de sécurité. Mais lorsque c'est le cas, les conséquences peuvent être dévastatrices et entraîner la fermeture de l'entreprise. Sans une approche intégrée de la sécurité, les entreprises peuvent être contraintes de limiter l'accès au réseau ou aux applications, voire de modifier leurs pratiques métier afin d'adopter des solutions de rechange moins efficaces, tout simplement parce qu'elles ne sont pas en mesure de garantir la sécurité de leur réseau.

Prenons l'exemple d'une importante société internationale du secteur des médias contrainte de fermer son système de messagerie instantanée après une attaque par le ver Kelvir. Le ver, qui s'est propagé en envoyant de faux messages instantanés à des personnes via des listes de contact des utilisateurs les renvoyant vers un site Web destiné à infecter leur ordinateur, a contraint cette société à suspendre l'utilisation de son système de messagerie instantanée. Malgré la fermeture du système aux communications publiques et une utilisation réservée aux messages internes, la société avait dû se résoudre à fermer le système de crainte que ce ver ne se propage à ses clients.

Les entreprises qui utilisent des produits spécifiques pour garantir la sécurité de leur réseau éprouvent souvent des difficultés à se maintenir à niveau en termes de menaces de sécurité toujours changeantes. Ces sociétés doivent souvent recourir à des mesures de sécurité anti-faille draconiennes pour gérer les nouvelles menaces qui débarquent sur leur réseau. Une alternative préférable est une intelligence sécuritaire intégrée et inhérente sur l'ensemble de l'infrastructure (c'est-à-dire Secure Networks). Ainsi, le réseau peut détecter la propagation de menaces perverses et isoler des événements malveillants avant qu'ils n'entraînent l'arrêt complet d'applications ou de composants réseau critiques.

L’approche Enterasys en matière de réseaux Secure Networks

Même si les entreprises peuvent continuer à tenter de bâtir un réseau sécurisé à partir d’un ensemble de technologies de sécurité « superposées » et réactives face aux menaces changeantes, une approche plus stratégique fournit un retour supérieur au niveau sécurité, moins complexe et qui nécessite beaucoup moins d’administration. Un bon exemple de cette approche plus stratégique est la manière dont Enterasys fournit ses solutions Secure Networks.

Un réseau Secure Networks garantit la visibilité de bout en bout avec une application unifiée du contrôle et des politiques, le tout bâti sur une architecture de sécurité à haute disponibilité avec une détection et un contrôle des menaces au niveau système. La solution Secure Networks est étendue à toutes les zones du réseau, même à la communauté sans fil, pour garantir des performances et une sécurité homogènes et fiables.

La philosophie d’Enterasys repose sur la participation active de l’ensemble de l’infrastructure réseau à la stratégie de sécurité. En intégrant l’intelligence sécuritaire à tous les niveaux, depuis la périphérie jusqu’au cœur du réseau, le réseau est mieux armé pour anticiper le flot de menaces et garantir le bon déroulement de l’activité, même dans le cas d’un large éventail d’attaques. En outre, la solution Enterasys fonctionne avec les offres d’autres constructeurs pour améliorer de manière spectaculaire la sécurité dans un quelconque environnement réseau.

À la différence des constructeurs qui ne satisfont qu’une partie de ces besoins ou qui imposent l’achat d’une solution homogène, « verticale » et complète pour bénéficier de ce type de sécurité, Enterasys propose une architecture réseau supportée par un large portefeuille de produits pour permettre à une entreprise de bâtir progressivement un réseau stratégique et fiable. En développant des produits qui s’intègrent à une infrastructure de sécurité et qui s’appuient sur des fonctionnalités communes d’administration à base de politiques, Enterasys permet aux entreprises de profiter concrètement et efficacement des avantages du concept Secure Networks.

L’un des avantages d’une stratégie Secure Networks est l’application universelle de politiques via un modèle opérationnel commun rendu possible grâce à des outils d’administration de réseau coordonnés. Avec un réseau Secure Networks garantissant une supervision et une communication en temps réel sur le réseau, les administrateurs peuvent rapidement localiser et modifier le comportement de chaque utilisateur, équipement et service avec une interruption minimum des opérations en réseau. Cette application de politiques s’appuie sur des fonctionnalités d’administration d’événements existantes, sur des services topologiques et des architectures de politiques intégrées pour fournir des réponses plus rapides et moins gourmandes en ressources humaines et qui sont à la fois efficaces et commodes pour les entreprises.

Anatomie d'un réseau Secure Networks

Afin de mieux comprendre les solutions Secure Networks et la manière dont Enterasys a créé une gamme de produits permettant aux entreprises de résoudre leurs failles de sécurité les plus critiques et de satisfaire les besoins réseau les plus importants, penchons-nous sur les trois principaux domaines d'un réseau Secure Networks : la **périphérie**, le **niveau Distribution** et le **cœur du réseau**.

Même si relever les défis de sécurité dans chacun de ces trois domaines est un objectif honorable, la plupart des entreprises se rendront compte de la nécessité d'adopter une approche évolutionniste pour créer un réseau Secure Networks complet. Heureusement, déployer un réseau Secure Networks n'est pas un exercice du type « tout ou rien », en particulier pour les entreprises disposant déjà d'une stratégie de sécurité. Plutôt que d'adopter une approche « tout ou rien », les entreprises peuvent s'engager dans une voie incrémentielle qui les conduira à l'adoption d'un réseau Secure Networks complet capable de résoudre de manière tactique les risques les plus importants au sein d'un contexte stratégique. Elles devront bâtir un réseau Secure Networks « niveau par niveau » ou « segment par segment » en fonctions de leurs besoins et des opportunités qui se présenteront.

Il est important d'étudier étroitement chaque domaine du réseau et de comprendre les différents types de sécurité et de fonctionnalités qui participent à la création d'un réseau Secure Networks. Cette étape est d'une importance vitale dans la mesure où chaque composant de l'infrastructure réseau joue un rôle essentiel au sein de l'infrastructure de sécurité globale.

- **Réseaux Secure Networks en périphérie** : La périphérie du réseau est un composant clé pour défendre une entreprise contre des menaces telles que les prédateurs opportunistes (pirates,…) et les attaques malveillantes (par exemple les vers et les virus). En règle générale, la périphérie représente le premier point d'entrée de ces menaces. Le défi consiste donc à compliquer l'accès au réseau.

  Les solutions Acceptable Use Policy et Enterasys Sentinel™ permettent d'appliquer la sécurité de manière inverse, en attribuant des privilèges à tous les utilisateurs et équipements afin de pouvoir accéder au réseau. Si ces derniers n'ont pas d'autorisation ou s'ils ont tenté d'acheminer du trafic « douteux » sur le réseau, un large éventail de réponses de sécurité peut être appliqué pour éviter que la menace ne se propage.

  Avec le modèle Secure Networks, ce type de contrôle granulaire et de sécurité peut être étendu au domaine sans fil, généralement une technologie plus vulnérable qui peut être désormais aussi sécurisée que la périphérie « filaire ». Une solution sans fil sécurisée entièrement déployée assure l'identification et l'application des politiques au niveau du point d'accès. Ceci garantit la protection de centaines d'utilisateurs et d'équipements sans fil contre diverses menaces, ainsi que les uns par rapport aux autres.

  – **Produits à évaluer** : Pour sécuriser la périphérie du réseau, les entreprises s'intéresseront aux commutateurs SecureStack et Matrix N-Series, au commutateurs et points d'accès sans fil sécurisés RoamAbout, et à NetSight Console avec l'application NetSight Policy Manager. Pour disposer d'une solution de sécurité plus automatisée, les entreprises peuvent également ajouter Dragon IDS et NetSight Automated Security Manager.

  – **Solutions à évaluer** : Acceptable Use Policy, Enterasys sentinel™ et Dynamic Intrusion Response

- **Secure Networks au niveau Distribution** : Si une entreprise n'est pas prête à s'engager à sécuriser la périphérie de son réseau, elle peut envisager une solution de sécurité au niveau Distribution (Distribution Layer Security). Dans ce cas, l'application de politiques de sécurité à base de profils s'effectue sur le point d'agrégation du niveau Accès au réseau. Moyennant un investissement minimal dans des commutateurs Matrix au niveau Distribution et une administration NetSight, les entreprises peuvent immédiatement améliorer leur capacité à identifier et à isoler tout un éventail de menaces de sécurité : vers, attaques DDoS, intrus, utilisation abusive du réseau en interne, etc.

  Ce faisant, les entreprises réduiront au minimum l'impact de ces menaces sur leur fonctionnement, garantissant ainsi une meilleure continuité de l'activité. Elles protégeront en outre les investissements réalisés dans des équipements de périphérie, quel qu'en soit le constructeur. Qui plus est, la solution DLS s'inscrit dans la stratégie globale Secure Networks d'Enterasys pour assurer une migration transparente vers d'autres solutions lorsque les entreprises sont prêtes à les déployer.

  – **Produits à évaluer :** Pour sécuriser leur niveau Distribution, les entreprises s'intéresseront aux commutateurs Matrix N- et E-Series et à NetSight Console avec l'application NetSight Policy Manager.

  – **Solutions à évaluer** : Acceptable Use Policy, Dynamic Intrusion Response

- **Secure Networks au niveau Cœur de réseau** : Le cœur de réseau est au centre de l'infrastructure et transmet tous les flux indispensables à l'activité de l'entreprise. Aussi, lorsqu'une attaque est dirigée contre le cœur de réseau, cette dernière peut arrêter toutes les communications de l'entreprise et également causer des dommages irréparables à la réputation de l'entreprise. Une solution Secure Networks permet d'atténuer ces types d'attaques et de garantir la continuité de l'activité. Ceci est d'autant plus important que de nombreux services métier sont désormais basés sur le réseau/sur IP, y compris les systèmes d'administration de bâtiments, la surveillance périmétrique, les systèmes de diagnostic médical. De même qu'un nombre toujours plus important de services et d'applications critiques pour la mission, notamment la VoIP, la vidéo sur le poste de travail et la collaboration virtuelle.

  Le cœur de réseau doit participer activement à la sécurité du réseau. L'infrastructure de cœur est plus vitale que jamais pour l'entreprise et son importance ne cesse de croître dans la mesure où davantage d'applications, d'utilisateurs et de trafics différents la traversent. C'est pourquoi elle devient la principale cible de menaces de sécurité à la fois puissantes et sophistiquées. Citons notamment les attaques par déni de service distribué (DDoS) qui peuvent échapper aux défenses périmétriques pour atteindre le réseau de cœur. Sans oublier les attaques par force brute ou en cascade capables d'épuiser les solutions de sécurité en périphérie du réseau avec un déluge constant d'événements qui consomment une précieuse bande passante et qui entraînent l'arrêt de l'ensemble du système de communication.

  La solution qui s'impose est un routeur pour cœur de réseau. Ce dernier fournit non seulement des performances à la vitesse du térabit et avec une disponibilité de classe opérateur, mais aussi une sécurité intégrée pour identifier et aider à remédier les menaces avant qu'elles ne nuisent au cœur de réseau. Ce routeur de cœur doit pouvoir communiquer avec le reste de l'infrastructure, notamment des composants tiers, pour optimiser la disponibilité du réseau, même pendant des événements de sécurité.

  – **Produits à évaluer** : Pour sécuriser leur réseau de cœur, les entreprises s'intéresseront au routeur de cœur sécurisé Matrix X et à NetSight Console avec l'application NetSight Policy Manager.

  – **Solutions à évaluer** : Acceptable Use Policy, Dynamic Intrusion Response et Enterprise Intrusion Prevention

Abordons maintenant de manière brève d'autres déploiements de l'infrastructure Secure Networks associés à des technologies ou à des applications spécifiques, notamment le sans fil et la convergence, deux points sensibles pour les entreprises d'aujourd'hui :

- **Sans fil sécurisé** : Les technologies sans fil sont en train de faire évoluer rapidement la manière dont les entreprises s'appuient sur le réseau pour obtenir un avantage concurrentiel. Mais les technologies sans fil augmentent également le risque de sécurité pour l'entreprise. Afin de bâtir un véritable réseau Secure Networks, il convient de résoudre les lacunes associées à la sécurité sans fil. Des moyens doivent être mis en œuvre pour étendre et appliquer des politiques d'entreprise homogènes à l'ensemble des utilisateurs et équipements mobiles. Les points d'accès et les utilisateurs non conformes doivent être détectés, isolés et supprimés. Les sessions des utilisateurs mobiles et les caractéristiques du trafic doivent pouvoir être analysées pour identifier les failles de sécurité potentielles. Quant au réseau, il doit pouvoir arrêter ou mettre en quarantaine toute activité malveillante.

  – **Produits à évaluer** : Pour sécuriser leurs composants réseau sans fil, les entreprises s'intéresseront à la gamme de commutateurs et de points d'accès sans fil RoamAbout, ainsi qu'aux applications d'administration .

- **Solution Secure Convergence** : Représentant la majorité des applications de convergence actuellement disponibles sur le marché, la voix sur IP et les communications unifiées sont en augmentation rapide. Pour la plupart des entreprises, les traditionnels systèmes de communication basés sur un autocommutateur (PBX) ont vécu, si bien que nombre de sociétés prévoient de migrer vers des solutions de communication convergentes basées sur des PBX et des serveurs IP.

  Cependant, même si ces solutions de convergence offrent des options de communication plus souples, elles entraînent également des changements fondamentaux de l'infrastructure réseau et exposent le réseau à de nouveaux risques. Entre autres problèmes de sécurité associés à la voix, citons les attaques DoS, la menace Intercepteur (ou « Man in the middle »), le spam et le SpIT ainsi que les attaques par usurpation d'identité qui peuvent affecter la qualité de service ainsi que la continuité de l'activité des systèmes de communication convergents. Il est donc vital de garantir la continuité de l'activité des réseaux convergents. La solution Secure Convergence permet de prioritiser les applications lors d'un événement de menace ou d'une période de trafic intense afin de garantir une véritable continuité de l'activité.

  Par exemple, la solution Secure Convergence satisfait aux critères uniques de sécurité sensible à la latence pour les réseaux convergents données/voix en garantissant la qualité de service (QoS). Secure Convergence donne également la priorité à la fourniture des applications critiques pour la mission, même à différents moments.

  – **Produits à évaluer** : Les composants de la solution Secure Convergence peuvent comprendre un large éventail de produits, d'applications et de solutions Enterasys. Enterasys sécurise les points d'extrémité de différents fournisseurs de solutions VoIP et IP d'aujourd'hui. Ainsi, les entreprises peuvent bâtir une infrastructure de communication sécurisée et prévisible prenant en charge la convergence en tant que partie intégrante d'un réseau d'entreprise évolutif.

Solutions Secure Networks d'un coup d'œil

- **Acceptable Use Policy**. Un système à base de politiques et unique qui permet au réseau de fournir automatiquement les services métier nécessaires aux utilisateurs, tout en empêchant le trafic indésirable et malveillant de pénétrer l'infrastructure.
- **Dynamic Intrusion Response**. Une solution qui détecte tout comportement anormal sur le réseau d'entreprise puis qui intervient pour mettre en quarantaine l'utilisateur contrevenant ou l'équipement déviant. Dynamic Intrusion Response isole et classe chaque événement de sécurité, identifie la source et reconfigure automatiquement le réseau pour atténuer la menace. Le réseau d'entreprise peut être protégé à la fois contre les risques de sécurité connus et non renseignés.
- **Enterasys Sentinel™**. Une offre qui relève de manière unique le défi consistant à protéger l'entreprise contre les systèmes d'extrémité pouvant se connecter à l'infrastructure d'entreprise sans avoir bénéficié des toutes dernières mises à jour de sécurité. Ce qui rend l'infrastructure vulnérable à des attaques malveillantes pouvant compromettre des ressources critiques. La solution Enterasys Sentinel permet de déployer un contrôle efficace d'admission des systèmes d'extrémité pour chaque utilisateur ou équipement connecté au LAN.
- **Enterprise Intrusion Prevention**. Une solution qui intègre des fonctionnalités de pointe de prévention/détection/réaction face aux intrusions sur l'infrastructure Secure Networks pour fournir le niveau le plus élevé de protection du réseau. Lorsque cette solution est totalement déployée, l'entreprise a la garantie que l'intégralité du trafic suspect est identifiée et inspectée au niveau du point d'entrée, sans perturber les activités de l'entreprise ni compromettre les données réseau sensibles. La solution Enterprise Intrusion Prevention réduit également les coûts en évitant d'acquérir des produits spécifiques hétérogènes de prévention et de détection d'intrusions (IPS/IDS).

Conclusion

Les principaux avantages d'une infrastructure réseau d'entreprise ne se limitent plus à fournir connectivité et capacité. En effet, le réseau est devenu le principal vecteur de succès pour l'entreprise. Il achemine toutes les communications métier via la voix sur IP ou la messagerie électronique. Il permet de connecter les systèmes de contrôle et de sécurité physique. Il garantit le fonctionnement sans faille des équipements de production. Le tout en assurant l'une de ses fonctions d'origine, à savoir l'échange de fichiers et l'impression de rapports. Cependant, plus l'infrastructure du réseau de l'entreprise devient critique, plus il est vital pour l'entreprise de garantir la continuité de ce même réseau, quel que soit le type de menace de sécurité attendu ou inattendu qui se présente.

Une architecture Secure Networks est une approche holistique de la création d'un réseau capable de fournir une protection efficace à l'échelle de l'entreprise, y compris à des réseaux composés d'éléments réseau hétérogènes de différents constructeurs. Quels que soient les composants réseau individuels déployés en périphérie, au niveau Distribution et au cœur du réseau d'entreprise, l'essentiel pour un réseau Secure Networks est de pouvoir disposer d'une approche coordonnée pour garantir la visibilité de bout en bout avec une application unifiée du contrôle et des politiques. Le tout sur un réseau hautement disponible avec détection et contrôle des menaces à l'échelle de l'entreprise.

Enterasys est le seul fournisseur de solutions Secure Networks depuis la périphérie jusqu'au cœur du réseau en passant par le niveau Distribution. Le fondement de l'architecture réseau d'Enterasys s'appuie sur une administration dynamique à base de politiques, sur une supervision du trafic et sur une réaction automatisée aux atteintes à la sécurité grâce à des produits et solutions spécifiques qui fonctionnent ensemble pour créer une infrastructure sécurisée. Chaque produit prend en charge des technologies clés, notamment le contrôle d'accès, la protection proactive, la réponse dynamique et la remédiation assistée. Ces produits et technologies s'associent pour créer l'offre Secure Networks, la solution réseau la plus originale et complète du marché des réseaux qui garantit la continuité de l'activité, la protection des revenus ainsi que la productivité des employés.

Pour de plus amples informations, veuillez contacter Enterasys au 01 40 84 61 80 ou **rendez-vous sur enterasys.com**.

Lit. #9013993 4/05

enterasys™
Networks that Know