Livre Blanc Secure Convergence

Enterasys Secure Convergence

L'essentiel

À l'heure où les déploiements des communications voix/vidéo/données convergentes s'accélèrent, Enterasys publie ce livre blanc pour expliquer son approche fondée sur une architecture ouverte et normalisée pour supporter une quelconque application convergente de n'importe quel fournisseur. Les nouvelles applications et les gains de productivité, plutôt que les économies de coût, sont aujourd'hui au cœur du déploiement des technologies de convergence. Grâce aux solutions de convergence Enterasys Secure Networks™, votre entreprise répond aux questions suivantes de manière concrète et réaliste tout en bénéficiant d'une rentabilité rapide :

- Le réseau peut-il répondre aux exigences de haute disponibilité en matière de services voix ?
- Comment disposer d'une architecture qui garantit la fiabilité et prévient automatiquement des problèmes ?
- Le réseau supporte-t-il une architecture ouverture et une interopérabilité multifournisseur ?
- Le réseau est-il assez rapide et le temps de latence ainsi que la gigue sont-ils maîtrisés ?
- Le réseau peut-il automatiquement vous protéger et protéger vos données sans sacrifier les performances ?
- Le réseau est-il assez intelligent pour découvrir, classifier et donner la priorité au trafic convergent grâce à des mécanismes de QoS performants et faciles à déployer ?
- Y a-t-il assez de ports physiques avec auto-alimentation sur Ethernet (PoE) pour connecter les nouveaux équipements convergents, y compris les téléphones IP et les caméras de sécurité ?
- Si un téléphone, une caméra et un poste de travail sont tous connectés à un seul port de commutation, les trafics voix, vidéo et données peuvent-ils être sécurisés et prioritisés séparément ?
- Le réseau est-il assez sécurisé pour protéger automatiquement la confidentialité, l'intégrité et la disponibilité du contenu des applications convergentes ?
- Existe-t-il un logiciel d'administration pour fournir la visibilité et le contrôle centralisés nécessaires à la prioritisation et à la sécurisation du trafic convergent de bout en bout sur de nombreux sites ?

Nos solutions de connectivité pour les niveaux Accès, Distribution et Cœur de réseau vous permettent de déployer en toute fiabilité des applications de convergence et d'éviter d'être dépendants d'un seul fournisseur. Partout dans le monde, des entreprises font confiance à l'offre Enterasys pour prendre en charge les solutions de téléphonie IP d'Avaya, Cisco, Nortel, Panasonic, Shoretel et Siemens. Nous restons à votre disposition pour vous démontrer concrètement comment notre stratégie unique permet de sécuriser le réseau d'un quelconque fournisseur tout en vous permettant de tirer parti de vos investissements existants.

Introduction

Ce livre blanc traite des défis auxquels le service informatique est confronté lors de la conception et du déploiement d'un réseau convergent. Il propose une approche architecturale unique pour répondre aux exigences de performance, de disponibilité et de sécurité d'une infrastructure réseau prenant en charge des communications convergentes.

Les réseaux IP Ethernet d'aujourd'hui sont l'infrastructure de base pour la grande majorité des communications critiques des entreprises. Les données applicatives, les communications textuelles et la recherche documentaire sont désormais des composantes fondamentales du réseau d'entreprise. Désormais, le service informatique compte sur ce même réseau puissant pour fournir un certain nombre de services supplémentaires auparavant fournis par des infrastructures distinctes.

Il est important de comprendre les motivations d'une migration vers un réseau convergent ainsi que les avantages et enjeux associés à cette entreprise importante. Jusqu'à maintenant, la convergence des services voix, vidéo et données était considérée comme un moyen de faire d'importantes économies de coût et de ressources. Cependant, une récente étude menée sur des entreprises ayant déployé des projets de convergence démontre clairement que ces dernières ne sont pas parvenues à profiter des économies de coût prévues, au moins pas à court terme. La principale motivation n'est plus les économies de coût, mais une amélioration des processus métier. Les progrès réalisés en matière de technologie applicative invitent les Directions Informatiques à s'engager sur la voie du réseau convergent pour optimiser l'interaction avec les actionnaires et améliorer sensiblement les processus métier et les performances de l'entreprise. Les entreprises cherchent à investir dans des technologies telles que la messagerie unifiée et la collaboration électronique pour travailler de manière plus productive. Ces technologies mettent généralement en jeu des applications de pointe et un réseau de communication convergent. Aujourd'hui, la Direction Informatique doit envisager de déployer un réseau convergent, pas seulement pour économiser de l'argent mais aussi pour prendre en charge la nouvelle génération d'applications convergentes qui apporte des améliorations importantes aux processus métier.

Selon une récente étude réalisée par IDC et InfoWorld en 2006, de nombreuses applications permettront de faire de futurs investissements dans le réseau données et téléphonie de l'entreprise. Il est évident que nombre de ces applications

s'appuieront sur une infrastructure simple et convergente pour fournir des services métier critiques. Plus de la moitié (52,3% exactement) des personnes interrogées déclarent que la messagerie unifiée sera au cœur de leurs futurs investissements et que les communications vidéo (36,9%), les téléphones bimode (WLAN/mobile) (35,7%) ainsi que les services audio (24,2%) sont des applications qui seront toutes fournies par l'infrastructure réseau Ethernet/IP simple et convergente.

Mais à ce partage du réseau Ethernet/IP commun pour ces services critiques vient s'ajouter un nouvel ensemble de besoins critiques. En effet, les traditionnelles mesures destinées à évaluer les performances et la capacité du réseau peuvent s'avérer totalement inappropriées pour un réseau convergent. La stabilité de l'infrastructure réseau et la disponibilité des services, qui peuvent être parfaitement adaptées à un réseau informatique traditionnel, peuvent ne pas correspondre aux besoins du réseau convergent. De plus, les contraintes de sécurité pour le réseau convergent peuvent exiger de planifier et de déployer des technologies supplémentaires.

Avantages et enjeux du réseau convergent

Les acteurs du marché se sont beaucoup interrogés sur les avantages du déploiement d'une infrastructure réseau convergente. Les nouvelles technologies applicatives sont au cœur d'exigences informatiques afin d'améliorer les processus métier. Les solutions d'entreprise s'appuient toujours plus sur les possibilités qu'offre l'intégration des services données, voix et vidéo afin de fournir des fonctionnalités plus puissantes. Prenons le cas des progrès réalisés par les applications de messagerie instantanée et de la manière dont ces applications sont utilisées pour améliorer la communication et la collaboration des employés. Les centres d'appel via le Web permettent de rapprocher une entreprise de ses clients en réagissant plus vite et plus efficacement à leurs demandes. Interrogez un quelconque employé concernant les applications les plus susceptibles d'améliorer son travail. Le plus souvent, il vous répondra qu'il s'agit d'applications qui intègrent les données et la voix et qui sont fournies via une infrastructure de communication sur IP convergente et unique. Même si le déploiement d'une infrastructure réseau convergente n'est pas synonyme d'économies de coût immédiates, la convergence de plusieurs réseaux distincts en un seul devrait optimiser l'efficacité du support technique et réduire les coûts d'infrastructure à long terme.

Cependant, quel est l'intérêt de faire converger sur la même infrastructure IP des applications traditionnellement distinctes avec des applications nouvelles et en évolution constante ?

Posez-vous les questions suivantes :

- L'infrastructure a-t-elle été architecturée pour intégrer la haute disponibilité ?
- Cette infrastructure fournira-t-elle le niveau de disponibilité auquel sont habitués les utilisateurs avec des services tels que le réseau voix classique par exemple ?
- Le réseau pourra-t-il satisfaire aux exigences de performances et d'accessibilité de toutes les applications ?
- Combien et quel type d'applications partageront dorénavant la même infrastructure sous-jacente et les services de data center ?
- Le réseau est-il assez sécurisé pour garantir un transport fiable et homogène du trafic applicatif convergent ?
- Le réseau est-il assez ouvert pour prendre en charge les applications convergentes d'un fournisseur, quel qu'il soit ?

En conclusion, la disponibilité, les performances et la sécurité des réseaux informatiques traditionnels ne sont pas particulièrement appropriées pour un réseau convergent. De plus, les technologies propriétaires qui peuvent être déployées aujourd'hui sur le réseau informatique peuvent empêcher le déploiement d'applications convergentes majeures.

Enfin, n'importe quelle entreprise peut grandement profiter d'une solution de convergence. Les processus métier et les performances de l'entreprise peuvent être améliorés tandis que le coût de possession total à long terme peut être réduit. Mais, pour veiller à ce que cette solution constitue bien un avantage plutôt qu'un inconvénient, il faut tenir compte des nouvelles exigences de l'infrastructure réseau commune. Par conséquent, une technologie appropriée doit être déployée.

Exigences d'un réseau convergent

Pour garantir le déploiement efficace d'une solution réseau convergente, plusieurs conditions doivent être remplies :

- Architecture ouverte — Prise en charge d'une quelconque application de convergence
- Capacité de l'infrastructure
- Réseau de communication hautement disponible
- Services applicatifs sécurisés
- Détection/classification du trafic applicatif
- Détection/classification du système d'extrémité
- Contrôle d'accès au réseau
- Qualité de service applicable

Une solution correctement architecturée pour un réseau convergent prendra en charge l'éventail des services disponibles sur l'infrastructure de communication unique. Il est également important de construire une **architecture ouverte**. L'infrastructure réseau devra être en mesure de fournir les performances, la disponibilité et la sécurité nécessaires pour prendre en charge n'importe quelle application d'un quelconque fournisseur. Si le réseau supporte uniquement les téléphones IP ou les services vidéo d'un seul fournisseur, c'est que la solution de convergence est mal conçue. Un bon réseau est un réseau souple et qui s'adapte pour répondre aux besoins présents et à venir de l'entreprise. À mesure que de nouvelles applications métier s'imposeront, un réseau bien architecturé sera capable de les prendre en charge. Concernant les services voix et vidéo sur un réseau IP convergent, ils doivent être envisagés simplement en tant qu'applications IP supplémentaires que le réseau doit intégrer. Chaque application a des besoins différents. Cependant, lorsque des applications sont exécutées sur un réseau

convergent, aucune dépendance propriétaire ne doit exister entre les applications et le réseau de communication. Un récent rapport de Gartner (référence G00136673) va dans ce sens en déclarant : « La voix étant une application, la sélection d'un fournisseur de solutions voix ne doit pas être liée à celle d'un fournisseur de l'infrastructure réseau. » Une approche ouverte du déploiement d'un réseau convergent sécurisé permet à l'entreprise d'acquérir l'application voix ou vidéo de son choix auprès d'un quelconque fournisseur et de l'exécuter efficacement et à moindre coût. Ainsi, l'entreprise pourra déployer les meilleures applications ou solutions pour répondre à ses besoins métiers, sans devoir tenir compte des dépendances vis-à-vis de l'infrastructure réseau et des coûts indirects potentiels.

Les besoins de **capacité de l'infrastructure** peuvent être très différents sur un réseau convergent et sur un réseau de données. Les systèmes d'extrémité capables de se connecter à un réseau convergent (téléphones IP, caméras IP, systèmes d'accès aux locaux - lecteurs de carte), sont nombreux et de différents types. Même des équipements comme les systèmes de télévision par Internet, les distributeurs automatiques et les cafétérias en libre-service augmentent sensiblement le nombre de ports Ethernet que l'infrastructure doit intégrer. En plus de devoir redimensionner la capacité du niveau Accès au réseau, les besoins accrus en bande passante de tous ces systèmes d'extrémité supplémentaires et des applications associées peuvent imposer d'améliorer les liaisons montantes (uplinks) aux niveaux Distribution et Cœur de réseau. En outre, la bande passante à destination du centre de données devra certainement être augmentée pour prendre en charge de nouveaux services applicatifs. Il faut en outre envisager d'ajouter de la bande passante au niveau du centre de données pour disposer d'un service vidéo en flux continu de qualité professionnelle. De plus, certains points d'extrémité convergents peuvent s'auto-alimenter électriquement depuis l'infrastructure réseau elle-même, sans dépendre de l'alimentation du bâtiment. Le meilleur exemple est celui des téléphones IP qui accèdent aux communications réseau et qui s'alimentent via le même câble Ethernet. Afin que le réseau puisse prendre en charge la norme d'auto-alimentation sur Ethernet (PoE), des commutateurs Ethernet supplémentaires dotés de cette fonctionnalité seront peut-être nécessaires au sein du réseau convergent. Des besoins supplémentaires en alimentation au niveau départemental peuvent également être nécessaires pour des déploiements PoE.

Fournir un réseau **de communication hautement disponible** est vital pour que les services critiques répondent aux attentes des utilisateurs en matière d'utilisation et de disponibilité. Attardons-nous sur l'opinion d'un utilisateur lambda concernant la disponibilité des services de téléphonie qui dépendent d'un système d'autocommutateur (PBX) traditionnel. Si vous demandez à ce même utilisateur combien de fois il n'a pas entendu la tonalité lorsqu'il a décroché le téléphone, il déclarera « presque jamais. » Les utilisateurs ont des opinions toutes faites sur la disponibilité intrinsèque de certains services et applications. Même si les utilisateurs acceptent parfois les problèmes de disponibilité pour une application de données métier, ils n'accepteront pas forcément la même chose d'un service voix fonctionnant via le réseau convergent. Le service informatique doit donc s'assurer que l'infrastructure réseau optimisée et le réseau convergent pourront répondre aux besoins de disponibilité, même les plus exigeants, de chaque application. Tous les aspects liés à la redondance et à la souplesse du réseau doivent être soigneusement analysés pour garantir que les défauts et les pannes n'entraîneront pas de perte de service pour l'utilisateur. L'utilisation appropriée de protocoles orientés topologie de niveaux 2 et 3 permet de créer une infrastructure capable de supporter des pannes majeures pour que les utilisateurs puissent continuer à communiquer avec leurs services nécessaires. L'intelligence intégrée aux équipements d'infrastructure réseau permet une reconfiguration dynamique de la topologie et un reroutage des flux de communication pour maintenir la disponibilité des services.

Il est essentiel de **sécuriser les services applicatifs** d'un réseau convergent. Une fois un service applicatif tel que la voix déployé sur le réseau convergent, des services centralisés seront connectés au réseau, en général au niveau du centre de données. Les serveurs d'applications tels que les PBX, les passerelles voix, etc. doivent être étroitement sécurisés contre les attaques et autres abus. Dans la mesure où ces services applicatifs sont désormais hébergés sur des serveurs connectés au réseau IP, ils sont la cible potentielle d'attaques et sont également potentiellement vulnérables à des impacts collatéraux liés à d'autres activités indésirables sur le réseau. Si, par exemple, une application PBX logicielle est détournée sur le réseau convergent, l'entreprise pourrait perdre tous ses services voix. Les services traditionnels tels que Dynamic Host Configuration Protocol (DHCP) et Domain Name System (DNS) sont de plus en plus importants dans un environnement convergent. Si les points d'extrémité convergents ont besoin d'adresses IP dynamiques et de services de nommage, les serveurs qui hébergent ces services doivent être hautement disponibles et protégés contre tout compromis. Le service informatique de l'entreprise doit s'appuyer sur l'infrastructure réseau et sur des applications de sécurité spécifiques pour protéger tous les services applicatifs critiques. Les stratégies de communication réseau doivent être applicables là où les serveurs d'applications se connectent au réseau pour garantir le filtrage du trafic indésirable. Des technologies appropriées de détection et de prévention des anomalies comportementales et des intrusions doivent être déployées pour détecter les attaques malveillantes et non malveillantes sur les serveurs d'applications critiques. Une solution bien architecturée doit automatiquement réagir face au comportement dangereux ou menaçant envers un serveur d'applications critique. Elle doit aussi permettre d'atténuer la menace rapidement et efficacement pour garantir l'intégrité du service.

La détection et la classification du trafic applicatif sont des fonctionnalités importantes pour garantir le bon fonctionnement des applications métier critiques. Dans un environnement réseau convergent, de nombreuses applications différentes sont tributaires du réseau. Chaque application a sa propre importance pour l'entreprise. Pour établir des règles de communication pour ces différentes applications, il est nécessaire d'identifier le trafic associé à une application particulière. L'infrastructure réseau convergente doit pouvoir détecter un flux spécifique de trafic et le classifier comme appartenant à une application particulière. Une fois les flux de trafic classifiés, il est possible d'appliquer des politiques de sécurité et de qualité de service pour veiller au bon fonctionnement et à la sécurisation de l'application associée. Détecter et classifier le trafic de chaque application sur le réseau garantit une approche très granulaire de l'application des priorités et de la sécurité pour les services métier individuels qui s'appuient sur le réseau convergent.

La détection/classification des systèmes d'extrémité est une fonctionnalité critique pour identifier les types d'équipements qui se connectent au réseau. Comprendre la différence entre les systèmes d'extrémité permet d'appliquer des politiques de communication spécifiques à un équipement. Par exemple, la communication autorisée vers et depuis un ordinateur portable peut s'avérer très différente de celle autorisée vers et depuis une caméra de surveillance IP. Une solution capable de reconnaître les différences entre les systèmes d'extrémité qui se connectent au réseau est essentielle pour garantir la disponibilité des services appropriés aux utilisateurs ainsi qu'aux systèmes qui en ont besoin. L'infrastructure réseau convergente doit être en mesure d'identifier un système d'extrémité qui tente de se connecter puis d'utiliser différentes technologies pour déterminer automatiquement le type d'équipement qui se connecte. L'authentification des équipements, les

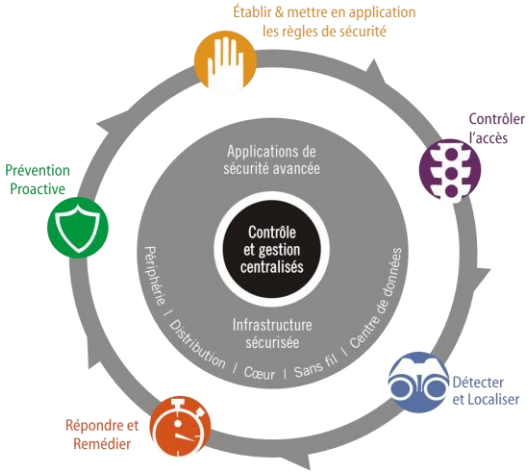
protocoles de découverte standards et propriétaires et même la surveillance des communications initiales doivent permettre de déterminer le type de système d'extrémité qui se connecte au réseau.

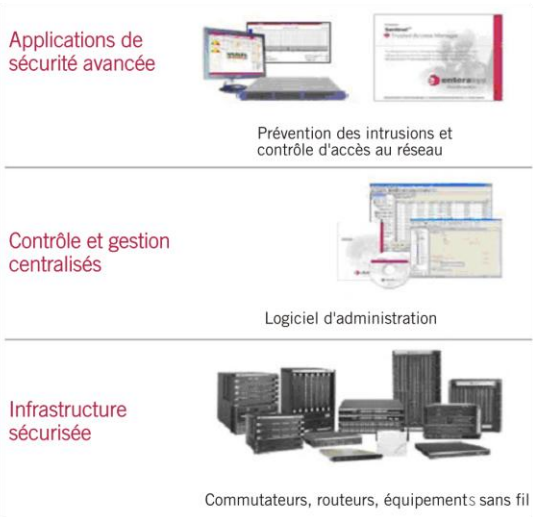
Fournir un **contrôle d'accès** à tous les systèmes d'extrémité est un critère important pour sécuriser l'environnement réseau et également autoriser les services appropriés. Dans un environnement de réseau convergent, il est important non seulement de contrôler l'accès à l'infrastructure réseau, mais aussi l'accès aux services sur ce réseau. Un téléphone IP ou une caméra IP doit être authentifié avant de pouvoir communiquer sur le réseau, au même titre qu'un utilisateur de PC. Une fois qu'un système d'extrémité est authentifié et autorisé à communiquer sur le réseau, l'accès aux applications et aux services nécessaires doit être contrôlé sur la base de critères tels que le type d'équipement, les certificats utilisateur, le rôle dans l'entreprise, l'emplacement et l'heure. Les équipements d'infrastructure auxquels un système d'extrémité se connecte doivent pouvoir interroger ce système lors de sa première tentative de connexion au réseau. Plusieurs méthodes d'authentification doivent être disponibles pour supporter les systèmes d'extrémité orientés humain et machine. L'infrastructure réseau convergente doit limiter l'accès aux services en fonction de l'identité du système d'extrémité. Des règles de communication réseau doivent s'appliquer au niveau du point d'entrée du système d'extrémité. Ainsi, ce dernier pourra communiquer avec les services auxquels il doit pouvoir accéder, tout en limitant la communication avec les services auxquels il ne doit pas avoir accès.

Dans un environnement de réseau convergent, **une qualité de service (QoS) applicable** est un critère important pour certaines applications. Prenons le cas de la prioritisation et des besoins en bande passante pour les services voix ou vidéo sur une infrastructure réseau convergente. Si la signalisation entre le téléphone IP et le gestionnaire d'appels ou la passerelle est affectée par la perte de paquets ou tout simplement retardée en raison de l'encombrement du réseau, un utilisateur ne pourra pas obtenir la tonalité lorsqu'il décroche son combiné téléphonique ou qu'il ouvre son interface téléphonique logicielle. Si la bande passante nécessaire n'est pas disponible pour supporter un flux vidéo, l'affichage de la vidéo sera médiocre voire inexistant sur son poste de travail. Des paramètres de QoS doivent être applicables au niveau du point d'entrée d'un système d'extrémité puis sur l'ensemble du réseau entre le système d'extrémité et le service. Une application granulaire est importante pour garantir des paramètres de QoS appropriés pour les différents services utilisés par un système d'extrémité unique. L'infrastructure réseau convergente doit pouvoir identifier les paquets associés à une application particulière et donner la priorité à ces paquets de manière appropriée pour répondre aux besoins du service applicatif spécifique. En plus de donner la priorité au trafic au niveau du point d'entrée sur le réseau depuis le système d'extrémité, l'équipement d'infrastructure doit pouvoir baliser le trafic spécifique pour donner la priorité aux communications avec le service sur l'ensemble du chemin réseau, depuis le système d'extrémité jusqu'au serveur d'applications. L'utilisation de la bande passante doit être contrôlée en fonction du type de trafic. La capacité à limiter la quantité de bande passante utilisée par une application spécifique sur le réseau permet de garantir une bande passante suffisante aux applications critiques pour fournir le service.

Une approche architecturale

Enterasys Networks propose une approche architecturale du réseau convergent sécurisé. Contrairement à l'approche d'autres fournisseurs, Enterasys intègre pleinement une infrastructure dédiée à la sécurité, des applications de sécurité de pointe ainsi qu'une visibilité et un contrôle centralisés. Ainsi, le service informatique peut déployer des réseaux capables de s'adapter à n'importe quelle application convergente et qui fourniront des services sécurisés et hautement disponibles aux utilisateurs.





Cette approche architecturale des réseaux convergents sécurisés offre d'importantes fonctionnalités. L'architecture permet de **définir** de manière centralisée des **politiques** d'utilisation du réseau pour les utilisateurs et les équipements et de les **appliquer** à travers l'environnement réseau. Grâce à ces politiques de communication réseau, le service informatique peut garantir la qualité de service (QoS) nécessaire aux applications de convergence. Et aussi garantir un accès sécurisé à l'ensemble des services critiques dans l'environnement réseau convergent. Des politiques peuvent être appliquées à la communication à partir d'un quelconque point d'extrémité de convergence de n'importe quel fournisseur.

L'architecture applique le **contrôle d'accès** des utilisateurs et des équipements qui tentent de se connecter au réseau convergent et avec des services spécifiques. Il est possible de détecter et d'identifier les différents systèmes d'extrémité qui se connectent au réseau convergent. Une fois un système d'extrémité identifié, l'accès au réseau ainsi qu'aux services spécifiques de ce dernier peut être contrôlé en fonction du type de système, du rôle dans l'entreprise de ce même système et/ou de la personne susceptible de l'utiliser, ainsi que du lieu et de l'heure de connexion. Ainsi, il est possible d'identifier les

points d'extrémité de convergence (téléphones IP, caméra IP, etc.) qui se présentent sur le réseau convergent et de contrôler leurs communications sur le réseau afin de garantir un accès sécurisé et fiable aux services appropriés.

L'architecture **détectera** les menaces et anomalies en un quelconque point du réseau convergent et en **localisera** la source exacte. En raison de l'importance croissante de l'infrastructure réseau convergente pour l'entreprise, il est vital que les menaces contre les services critiques soient détectées et atténuées en temps réel. Enterasys s'appuie sur une technologie brevetée pour fournir une fonctionnalité unique qui détecte les problèmes au moment même où ces derniers surviennent sur le réseau et qui localise la source exacte du problème. Sur un réseau composé de milliers de systèmes d'extrémité et de points d'extrémité de convergence, il est ainsi possible de déterminer en quelques secondes seulement la source exacte d'une menace ou d'un problème sur le réseau.

L'architecture **réagira** aux menaces en déclenchant une action spécifique et mesurée qui permettra aux utilisateurs de **résoudre eux-mêmes** le problème le cas échéant. La capacité de l'architecture à identifier la source exacte de la menace pour l'environnement permet de mettre en place une réponse appropriée.

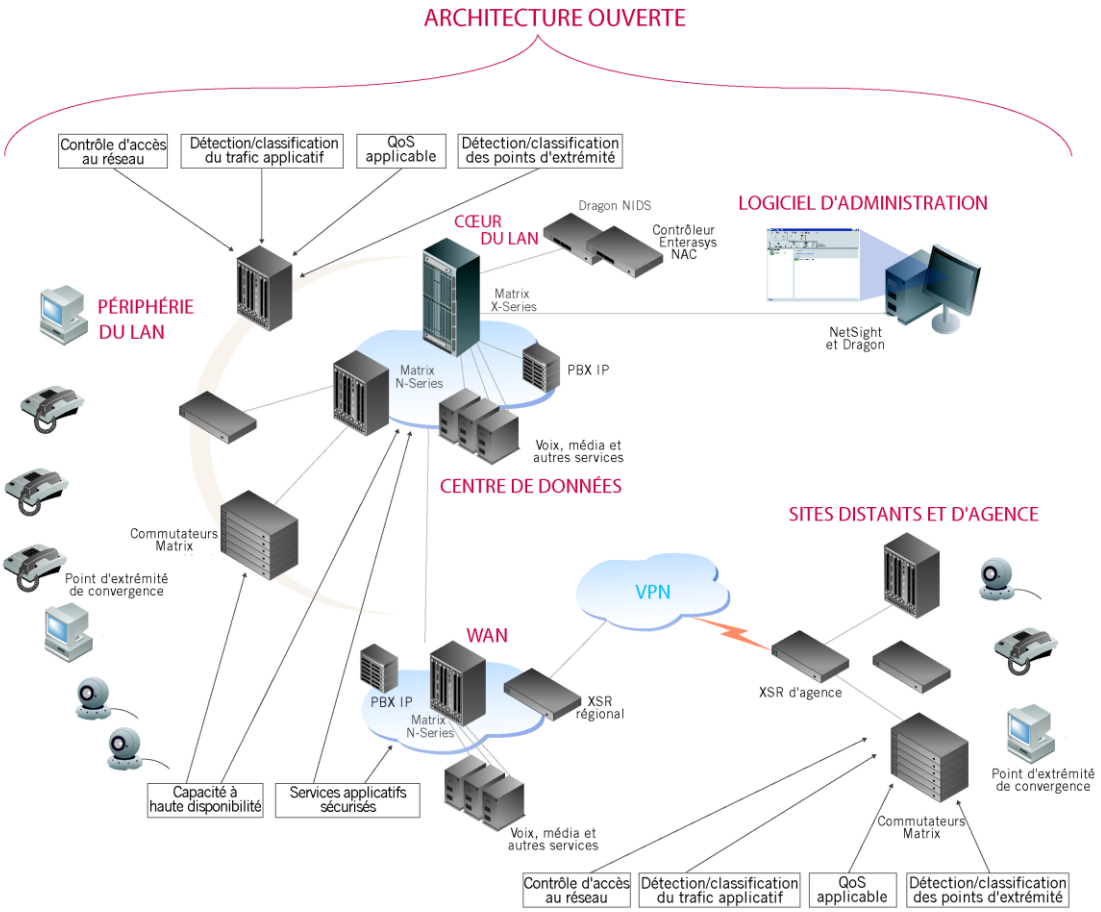
La réponse peut varier en fonction du type de menace ou d'anomalie réseau. La solution Enterasys offre des réponses mesurées telles que la désactivation d'un port, la modification d'un VLAN, l'application d'un ensemble complet de politiques de communication, la notification et la mise en quarantaine. Lorsque le problème à résoudre concerne un utilisateur, l'architecture permet d'appliquer des règles de politiques spécifiques pour protéger complètement tous les services réseau critiques. L'utilisateur garde néanmoins la possibilité de résoudre lui-même (auto remédiation) le problème afin de pouvoir à nouveau rapidement travailler de manière productive.

L'architecture protège **de manière proactive** le réseau convergent contre les systèmes d'extrémité vulnérables et dangereux. Elle **empêche** ces derniers de compromettre les services métier critiques, les autres utilisateurs ainsi que les systèmes d'extrémité. Les défenses sont établies pour protéger l'environnement contre les menaces connues et contre une utilisation malveillante du réseau. En outre, la vulnérabilité et la menace potentielle que constituent les systèmes d'extrémité de tout type (y compris les points d'extrémité de convergence) peuvent être évaluées avant que ces systèmes ne soient autorisés à communiquer sur le réseau. Les vers et les virus dangereux pouvant infecter et se répandre via de nombreux et différents types de systèmes d'extrémité, il est vital que l'architecture puisse protéger de manière proactive l'environnement réseau convergent contre tout système d'extrémité dangereux.

En s'appuyant sur l'approche architecturale Secure Convergence, le service informatique peut déployer une solution Enterasys qui garantit un environnement de réseau convergent, efficace et rentable.

Principes de la solution Enterasys

Une solution Secure Convergence d'Enterasys répond à tous les besoins critiques pour garantir la continuité de l'activité et le bon fonctionnement de l'entreprise. Cet environnement de communication hautement disponible, sécurisé et dédié aux applications qui fournissent tous les services convergents nécessaires à l'environnement métier de nouvelle génération s'appuie sur des technologies clés. Le schéma suivant illustre l'évolutivité et l'exhaustivité d'une solution Secure Convergence d'Enterasys.


ARCHITECTURE OUVERTE
Contrôle d'accès au réseau
Détection/classification du trafic applicatif
QoS applicable
Détection/classification des points d'extrémité
CŒUR DU LAN
Dragon NIDS
Contrôleur Enterasys NAC
LOGICIEL D'ADMINISTRATION
Matrix X-Series
NetSight et Dragon
PÉRIPHÉRIE DU LAN
Matrix N-Series
PBX IP
Voix, média et autres services
CENTRE DE DONNÉES
Commutateurs Matrix
Point d'extrémité de convergence
SITES DISTANTS ET D'AGENCE
VPN
WAN
XSR d'agence
PBX IP
Matrix N-Series
XSR régional
Capacité à haute disponibilité
Services applicatifs sécurisés
Voix, média et autres services
Commutateurs Matrix
Point d'extrémité de convergence
Contrôle d'accès au réseau
Détection/classification du trafic applicatif
QoS applicable
Détection/classification des points d'extrémité

Architecture ouverte

Grâce à l'engagement de longue date d'Enterasys en matière de technologies normalisées et de conception d'architectures ouvertes, il est possible de déployer un réseau convergent et sécurisé adapté à n'importe quelle application de convergence d'un quelconque constructeur. La solution Enterasys permet d'identifier et de contrôler les applications de convergence exécutées sur le réseau et de garantir leur sécurisation et prioritisation en fonction des besoins métier. Ceci s'effectue à l'aide de classificateurs de paquets intégrés à l'infrastructure matérielle pour différencier le trafic grâce à des attributs de niveau 2, 3 et 4 (modèle OSI normalisé). Il est possible de contrôler des applications de convergence spécifiques grâce à une mise en file d'attente par priorité matérielle au point d'entrée même sur le réseau convergent. Ce contrôle est également possible grâce à un balisage normalisé des paquets tel que IEEE 802.1Q, 802.1p et RFC Type of Service (ToS) 1349. Avec une solution Enterasys, il est possible d'identifier et d'appliquer des politiques de communication sur les points d'extrémité de convergence des principaux fournisseurs. En s'appuyant sur le protocole d'authentification IEEE 802.1X, sur la technologie d'authentification basée MAC, sur des protocoles de découverte des points d'extrémité de convergence normalisés tels que Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED) ainsi que sur plusieurs protocoles de découverte spécifiques à un fournisseur, la solution Enterasys peut détecter, authentifier et contrôler l'accès à un quelconque point d'extrémité de convergence. Des téléphones IP classiques de fournisseurs tels qu'Avaya, Cisco, Nortel, Panasonic, Shoretel et Siemens sont des exemples de points d'extrémité de convergence qu'un réseau convergent sécurisé d'Enterasys peut détecter et contrôler.

Avec cette architecture ouverte, les entreprises peuvent déployer la bonne application métier au bon moment et pour les bonnes raisons. Aucune dépendance au niveau de l'architecture réseau ne peut empêcher le déploiement d'applications convergentes.

Capacité d'infrastructure

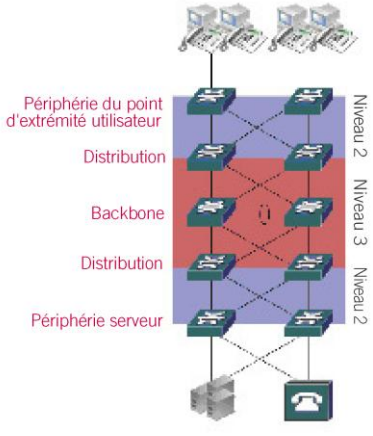
Les équipements d'infrastructure Enterasys sont bien positionnés pour s'adapter aux besoins de capacité du réseau convergent. Grâce à la modularité des commutateurs à base de flux Matrix N-Series, une densité de ports supplémentaire peut être ajoutée rapidement et en toute transparence là où elle s'impose pour supporter des points d'extrémité de convergence. De conception empilable, la gamme de commutateurs SecureStack C-Series et B-Series permet d'ajouter des ports supplémentaires en étendant simplement la pile. La modularité et la variété des technologies de liaison montante (uplinks) intégrées aux commutateurs Enterasys pour le niveau Accès, Distribution et Coeur de réseau permettent d'augmenter la bande passante en fonction des besoins, sans mise à niveau majeure de l'infrastructure réseau. En outre, l'offre Enterasys permet, de manière exclusive et en temps réel, de collecter des informations sur la planification de la capacité à partir de l'infrastructure réseau. L'application Enterasys NetSight® Inventory Manager génère des rapports qui indiquent les ports utilisés et inutilisés sur un réseau. L'administrateur réseau bénéficie ainsi d'une vue claire de la capacité de l'infrastructure courante à gérer des points d'extrémité de convergence supplémentaires.

Afin d'alimenter électriquement les points d'extrémité de convergence via l'infrastructure réseau, Enterasys intègre la technologie d'auto-alimentation sur Ethernet Power-over-Ethernet 802.3af (PoE) normalisée à ses gammes de commutateurs de niveau départemental Matrix N-Series, SecureStack C-Series et SecureStack B-Series.

Haute disponibilité

Sur un réseau convergent, la disponibilité des services est absolument critique. Plus il y a d'applications critiques qui convergent vers une infrastructure unique, plus la tolérance de pannes et la résilience du réseau sont importantes. Les réseaux convergents doivent être conçus selon les principes du traditionnel modèle de réseau hiérarchique. La plupart des réseaux peuvent être segmentés en trois niveaux, même si les plus petits d'entre eux peuvent être composés de deux niveaux seulement. Chaque niveau est configuré pour gérer des services spécifiques au sein de l'environnement. Les utilisateurs et les systèmes d'extrémité, y compris les équipements d'extrémité convergents, sont connectés au réseau au niveau Périphérie. Les commutateurs de périphérie sont connectés au campus via des commutateurs de niveau Distribution. Des commutateurs de niveau Distribution sont connectés aux commutateurs du Backbone. Les serveurs et autres systèmes qui fournissent des services applicatifs, notamment les passerelles et les contrôleurs de téléphonie IP, se connectent au réseau au niveau Périphérie spécifiquement déployé pour prendre en charge ces systèmes. Le niveau Périphérie serveur ne fournira généralement pas de connectivité utilisateur.

Les commutateurs qui intègrent le niveau Périphérie sont généralement configurés en tant qu'équipements d'acheminement de niveau 2. Les protocoles de topologie de niveau 2 tels qu'IEEE 802.1w, 802.1s et 802.3ad sont essentiels pour garantir une reprise rapide en cas de panne d'une liaison ou d'une défaillance des composants réseau. Les commutateurs de périphérie Enterasys Matrix et SecureStack prennent en charge ces normes de topologie critiques ainsi que des fonctionnalités de haute disponibilité supplémentaires telles que la détection Link Flap Detection, SpanGuard et le pont racine de sauvegarde. Ils garantissent ainsi une récupération rapide de la topologie réseau en cas de panne. Les commutateurs de niveau Distribution doivent être configurés de manière à router le trafic vers le backbone et à isoler chaque domaine de niveau 2. Ils doivent intégrer les mêmes fonctionnalités de niveau 2 de redondance et de tolérance aux pannes que le commutateur de périphérie. Ces mêmes commutateurs doivent également prendre en charge les protocoles de redondance de niveau 3 pour interagir avec le niveau Backbone routé. Ils intègrent en outre les protocoles de redondance de niveau 3 tels que Open Shortest Path First (OSPF) et Virtual Router Redundancy Protocol (VRRP) afin de garantir une conception réseau hautement redondante.



Le niveau Backbone permet d'interconnecter de larges segments au LAN. Les commutateurs de backbone doivent être configurés pour fonctionner comme des routeurs de niveau 3 et se connecter à des commutateurs de distribution. Le

Backbone doit prendre en charge la redondance et la tolérance de pannes au moyen de protocoles normalisés tels qu'OSPF et VRRP. Le commutateur/routeur de cœur sécurisé Enterasys Matrix X est une plate-forme de cœur de réseau de nouvelle génération à la pointe de la technologie. Il supporte des fonctionnalités critiques de redondance et de haute disponibilité dont les protocoles de redondance de niveau 3.

Services applicatifs sécurisés

Sur un réseau convergent, des serveurs hébergeront certainement des applications spécifiques qui supportent le service convergent. Il est essentiel que ces serveurs soient complètement protégés contre les attaques et la malveillance. Si, par exemple, une application de gestion d'appels ou une passerelle voix est connectée à l'infrastructure réseau convergente, elle doit être sécurisée et disponible afin que les utilisateurs puissent disposer du service téléphonique. Si ces serveurs d'applications sont compromis ou victimes d'une attaque par déni de service, l'entreprise essuie alors une perte majeure d'un service métier essentiel.

Les commutateurs Enterasys Matrix et SecureStack fonctionnant à base de politiques et le logiciel NetSight Policy Manager protègent les serveurs d'applications contre les attaques ou les compromissions en établissant et en appliquant des politiques de sécurité. Ces politiques permettent d'interdire les communications externes et indésirables vers et depuis le serveur d'applications. Des règles de politiques peuvent également être configurées pour empêcher l'émulation des adresses IP de serveurs d'applications critiques. Ainsi, ces serveurs indispensables ne peuvent pas être détournés et l'intégrité du service applicatif convergent est maintenue. Des services critiques tels que DHCP et DNS peuvent être isolés et protégés à l'aide de règles de politiques. Un profil de politique peut être appliqué sur tous les points du réseau. Il permet de veiller à ce qu'aucun serveur DHCP ou DNS non conforme ne puisse communiquer sur le réseau et de protéger les points de connexion de serveurs valides contre des caractéristiques de trafic inattendues.

Les formateurs de débit sortant peuvent être configurés sur des ports de commutation Enterasys en tant que profil de politique spécifique pour des serveurs d'applications critiques. Ainsi, des services comme les gestionnaires d'appels ne pourront pas être surchargés par des attaques malveillantes ou par un effet collatéral lié à une anomalie réseau.

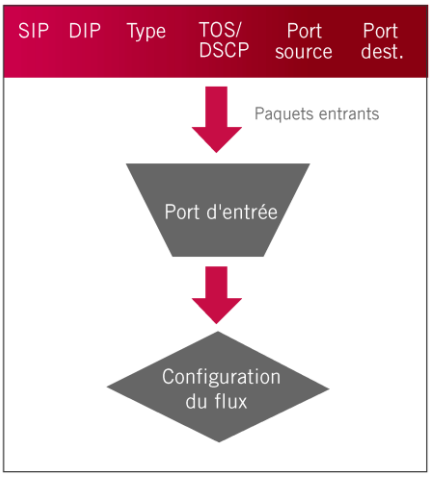
En plus d'appliquer des politiques de sécurité sur les ports de commutation via lesquels des serveurs d'applications de convergence critiques se connectent au réseau, la solution Dragon® Intrusion Detection System d'Enterasys utilise des capteurs basés sur un hôte et résidant sur des serveurs d'applications de convergence critiques pour détecter en temps réel des attaques et autres événements de sécurité. Lorsqu'un de ces capteurs détecte un événement de sécurité, le logiciel NetSight Automated Security Manager d'Enterasys peut éliminer le trafic associé à la menace, identifier la source exacte de l'attaque et lancer une action d'atténuation sur le port source du réseau.

Détection/classification du trafic applicatif

Afin d'appliquer des règles de politiques de communication granulaires pour l'utilisation d'applications critiques, pouvoir détecter et classifier le trafic applicatif individuel est indispensable sur le réseau convergent. La solution Enterasys offre des fonctionnalités de pointe pour identifier de manière dynamique le trafic applicatif qui arrive sur le réseau convergent, ainsi que pour classifier le trafic en fonction du type de service et de son importance pour l'entreprise.

Les paquets qui pénètrent sur les commutateurs Enterasys sont analysés et classifiés en tant que flux de trafic d'après un ensemble de variables :

- Adresse IP source
- Adresse IP de destination
- Type IP
- Champ ToS / Point de code DiffServ
- Port source
- Port de destination



Ces variables permettent d'identifier des flux de trafic applicatif spécifiques afin d'appliquer des politiques de communication au flux du trafic. Ainsi, chaque paquet entrant sur le commutateur peut être examiné lors de son acheminement pour déterminer l'application à laquelle il appartient. Cette technologie étant intégrée aux commutateurs Matrix et SecureStack, les services de classification de paquets d'un réseau Enterasys ne subissent aucune baisse de performances. Le schéma ci-contre décrit la classification des paquets au sein d'un commutateur Enterasys.

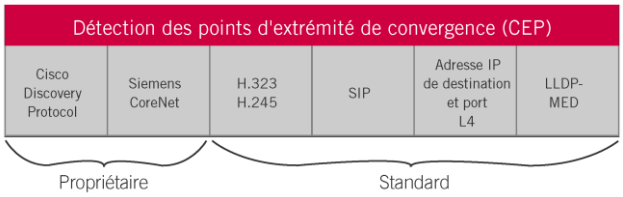
Détection/classification d'un système d'extrémité

La capacité de l'infrastructure réseau à détecter les systèmes d'extrémité qui se connectent au réseau et à déterminer si le système est un point d'extrémité de convergence (CEP) est un aspect critique d'une solution réseau convergente bien architecturée. Connaître le type de système d'extrémité est important pour déterminer les politiques de communication appropriées qui doivent être appliquées au point de connectivité réseau.

Les solutions de commutation Enterasys Matrix et SecureStack intègrent des fonctionnalités avancées de détection et de classification des systèmes d'extrémité. Ces systèmes peuvent être détectés lorsqu'ils se connectent au réseau convergent sécurisé en forçant l'authentification et/ou la détection des points CEP sur les commutateurs d'accès. Des certificats peuvent être transmis à un service d'annuaire via le protocole IEEE 802.1X normalisé où un système d'extrémité peut être classifié sur la base de données préétablies. Les systèmes d'extrémité peuvent également être classifiés en transmettant leur adresse MAC en guise de certificat lors du processus d'authentification. En plus de ces options fournies via un service d'authentification, il est possible de détecter et classifier des points d'extrémité de convergence à l'aide de la technologie de détection de points CEP unique intégrée aux commutateurs Matrix et SecureStack. LLDP-MED, l'adresse IP de destination et

le port de niveau 4, SIP et H.323/H.245 figurent parmi les méthodes normalisées pour détecter des points CEP sur des commutateurs Matrix. En outre, ces commutateurs peuvent utiliser des méthodes spécifiques à un fournisseur pour la détection des points CEP telles que : Cisco Discovery Protocol et Siemens CoreNet. La figure ci-dessous décrit les fonctionnalités de détection des points CEP d'un commutateur Enterasys.

Pouvoir identifier les nombreux systèmes d'extrémité connectés à un seul port Ethernet est un aspect important de la détection des points d'extrémité dans un environnement de réseau convergent. Notamment lorsqu'un PC est connecté via un téléphone IP et que les deux équipements se connectent au commutateur réseau à l'aide du même câble Ethernet. Les commutateurs Enterasys Matrix intègrent une capacité unique d'authentification multi-utilisateur pour authentifier séparément de nombreux équipements qui se connectent via le même port Ethernet au réseau convergent sécurisé. Utiliser des méthodes d'authentification des systèmes d'extrémité à l'aide de certificats et pouvoir détecter un système d'extrémité via différents protocoles de signalisation permet au réseau de classifier un système d'extrémité de manière dynamique. Cela permet aussi d'ajuster les politiques de communication en fonction du type d'équipement et de son rôle dans l'environnement du réseau convergent.



Contrôle d'accès au réseau

Lors de la détection d'un système d'extrémité qui se connecte au réseau convergent sécurisé, il convient de déterminer l'accès à l'infrastructure de communication et aux services disponibles dont doit bénéficier ce système. Au sein d'une solution bien architecturée, plusieurs paramètres permettent de déterminer si un tel système peut ou non accéder au réseau et à chacun des services qu'il supporte.

Enterasys utilise plusieurs technologies pour contrôler l'accès à l'infrastructure de communication et aux différents services disponibles. Avec la solution de contrôle d'accès au réseau (NAC) d'Enterasys, des politiques d'accès sont appliquées sur tous les types de systèmes d'extrémité, y compris les points d'extrémité de convergence ou CEP. La solution Enterasys NAC s'intègre pleinement aux technologies d'évaluation des systèmes d'extrémité basées sur un agent ou sur le réseau. Elle permet de déterminer la vulnérabilité potentielle et la menace possible que constitue un système d'extrémité qui tente de se connecter au réseau convergent sécurisé. Ceci revêt une importance toute particulière sur un réseau comprenant des points d'extrémité de convergence afin de s'assurer que ces points d'extrémité (téléphone IP, caméra IP, etc.) ne sont pas vulnérables aux attaques ou qu'ils n'ont pas été compromis et qu'ils ne représentent donc pas une menace pour l'ensemble de l'environnement réseau. Avant de pouvoir communiquer sur le réseau, tout système d'extrémité fait l'objet d'une évaluation. Si un système d'extrémité est défini comme étant vulnérable ou dangereux, il n'est pas autorisé à communiquer avec des services métier, ceci afin de protéger l'environnement. Si un système d'extrémité est considéré comme fiable et sécurisé, il peut communiquer avec les services appropriés déterminés par des paramètres tels que l'identité du système d'extrémité, son profil dans l'entreprise, l'emplacement et l'heure de connexion. L'accès à des applications et à des services réseau spécifiques s'effectue à l'aide de règles de politiques associées de niveau 2, 3 et 4 pour le contrôle du trafic VLAN, le filtrage, la limitation du débit et la prioritisation du trafic réseau depuis le système d'extrémité.

Qualité de service applicative

Les réseaux informatiques ont été conçus pour fournir assez de bande passante et prendre en charge toutes les applications métier en évitant de recourir à des technologies de QoS. Ceci peut s'avérer suffisant pour des réseaux supportant seulement des applications de données, mais ce n'est pas assez pour les réseaux convergents. Les applications de données peuvent généralement compenser une perte de paquets occasionnelle ou les délais variables constatés sur les réseaux sous-utilisés. Au contraire, le trafic téléphonique IP ne tolère aucune perte de paquets et toutes les communications doivent être transmises avec le strict minimum de variation au niveau du délai de transmission (gigue) de la voix. Les applications de convergence peuvent s'avérer très sensibles à la perte et au retard de paquets ainsi qu'aux variations de temporisation au niveau des flux de paquets. En raison de la nature sporadique des applications de données et de l'utilisation de chemins réseau uniques pour les applications de données et de convergence, une congestion peut se produire. Cet encombrement du réseau peut entraîner des pertes de paquets et induire une qualité de service inacceptable pour une application de convergence. Pour compenser ces périodes de congestion, les commutateurs Enterasys Matrix fournissent un ensemble de services de QoS qui garantissent la viabilité des données et du trafic des applications de convergence sur un réseau.

Les commutateurs Enterasys Matrix et SecureStack intègrent une classification de paquets multiniveau de pointe, une limitation granulaire du débit en entrée et en sortie ainsi que des files d'attente programmées très précises. Le schéma ci-dessous décrit le flux de trafic associé à la QoS d'une application classifiée par un commutateur Enterasys.

Les commutateurs Enterasys utilisent une classification multiniveau pour associer le trafic reçu avec l'un des différents niveaux de priorité. Ces niveaux de priorité sont associés à des classes de service définies. À chaque niveau correspond une file d'attente de transmission physique. Différents algorithmes de planification sont utilisés pour administrer l'acheminement du trafic depuis les files d'attente d'un commutateur. Les commutateurs Enterasys supportent trois types d'algorithmes de planification de file d'attente. Chaque commutateur prend en charge un algorithme de planification avec priorité stricte et pondérée. La priorité stricte est l'algorithme le plus simple. Il assure la transmission des données stockées dans la file d'attente prioritaire avant celles se trouvant dans des files d'attente de plus faible priorité. Les commutateurs Enterasys supportent également les algorithmes de formatage de bande passante avec mise en file d'attente pondérée (WFQ) ou Round Robin (WRR). Les programmateurs pondérés offrent un mécanisme qui garantit l'allocation d'un pourcentage minimum de bande passante à une file d'attente spécifique.

Les commutateurs Enterasys et le logiciel NetSight s'appuient sur un modèle à base de profil pour associer le trafic à la QoS appropriée. Des rôles sont définis dans des profils de politique qui peuvent être associés à différents utilisateurs, systèmes, services ou ports. Grâce aux profils de politiques Enterasys, les administrateurs réseau peuvent définir un ensemble de règles pour contrôler différents types de trafic réseau et établir une priorité entre ces derniers. Les règles qui composent un profil de politique contiennent à la fois des définitions de classification et des actions à appliquer lors de la correspondance d'une classification. Les classifications comprennent des champs de niveau 2, 3 et 4. Les actions à base de politiques applicables comprennent l'affectation de VLAN, le filtrage, la limitation du débit entrant, le formatage du débit sortant ainsi que le mappage et la consignation de classes de priorité.

Le modèle de QoS d'Enterasys présente l'avantage de pouvoir établir des politiques de hiérarchisation et de limitation de débit à partir d'un profil et depuis une console de contrôle centralisée. Ce modèle permet aussi aux commutateurs d'appliquer automatiquement des politiques appropriées lors de l'identification de systèmes d'extrémité et d'applications spécifiques sur le réseau.

Enterasys fournit un ensemble complet de technologies pour le déploiement d'un environnement de réseau convergent de nouvelle génération. Le tableau ci-dessous indique les technologies nécessaires à un réseau convergent sécurisé et les produits Enterasys qui les fournissent.

Secure Convergence – Besoins	Technologies/Fonctionnalités		Produits Enterasys
Architecture ouverte	• IEEE • API ouvertes • Intégration d'événements tiers • Support et type de CEP	• IETF • Politique de niveau Distribution • Application de sécurité tierce	• Commutateurs Matrix et SecureStack • Logiciel d'administration NetSight • Dragon IDS/IPS • Contrôle NAC Enterasys
Capacité de l'infrastructure	• Châssis modulaire • Liaisons montantes modulaires • Commutateurs empilables • Agrégation de liens	• Densité de ports (de 24 à plus de 500 ports par commutateur) • PoE • Reporting de la capacité	• Commutateurs Matrix N-Series • Commutateurs/routeurs Matrix X • Commutateurs SecureStack B- et C-Series • NetSight Inventory Manager
Haute disponibilité	• Alimentation redondante • Matrice de commutation distribuée • IEEE 802.1w • IEEE 802.1s	• IEEE 802.3ad • Enterasys Span Guard • OSPF • VRRP	• Commutateurs Matrix N-Series • Commutateurs/routeurs Matrix X • Commutateurs SecureStack B- et C-Series • NetSight Console
Services applicatifs sécurisés	• Politique – Filtres de trafic • Politique – Limitation de débit • Politique – Prévention de l'émulation des services • Flow Setup Throttling	• Détection d'intrusions • Isolement de flux • Atténuation des menaces	• Commutateurs Matrix N-Series • Commutateurs SecureStack B- et C-Series • Logiciel d'administration NetSight • Dragon IDS/IPS/SIM
Détection/classification du trafic applicatif	• Inspection niveau 2/3/4 • Tagging prioritaire • Politique – Association de rôles	• Par port/vitesse du lien • Inspection du trafic entrant/sortant	• Commutateurs Matrix N-Series • Commutateurs SecureStack B- et C-Series • Logiciel d'administration NetSight
Détection/classification d'un système d'extrémité	• IEEE 802.1X • Authentification basée MAC • Authentification multi-utilisateur • Détection des CEP - SIP	• Détection des CEP - H.323/H.245 • Détection des CEP - LLDP-MED • Détection des CEP – CDP • IP de destination + Port source	• Commutateurs Matrix N-Series • Commutateurs SecureStack B- et C-Series • Logiciel d'administration NetSight
Contrôle d'accès au réseau	• Authentification basée MAC • Évaluation basée sur l'agent et le réseau • Mise en quarantaine/auto-remédiation	• Utilisation du réseau/des applications – Politique appliquée • Base de données des emplacements • Reporting de conformité	• Commutateurs Matrix N-Series • Commutateurs SecureStack B- et C-Series • Logiciel d'administration NetSight • Enterasys NAC
Qualité de service applicable	• Formateurs de débit entrant et sortant • Tagging de paquets (ToS/802.1p) • Routage de politiques	• Mise en file d'attente par priorité - Matériel • Classe de service applicatif	• Commutateurs Matrix N-Series • Commutateurs/routeurs Matrix X • Commutateurs SecureStack B- et C-Series • Logiciel d'administration NetSight

En résumé

Il est indispensable de déployer un réseau IP convergent pour tirer parti des progrès considérables qu'offrent les processus métier qui s'appuient sur la technologie.

Les avantages de la messagerie unifiée, des services complètement intégrés et mobiles et des technologies interactives inciteront le service informatique à faire converger les services critiques traditionnellement dispersés. Comprendre les avantages de la convergence pour l'activité de l'entreprise est important. Cependant, afin qu'un service informatique puisse bâtir son réseau d'entreprise de nouvelle génération, il est essentiel de maîtriser la gestion des risques supplémentaires liés à un environnement réseau sensiblement plus complexe. La sécurité, la souplesse et l'intégration sont les objectifs à atteindre et l'offre Enterasys Secure Networks™ vous apporte la solution de convergence sécurisée qui vous aidera à répondre à relever ces défis.

La solution de convergence sécurisée d'Enterasys offre les principaux avantages suivants :

- La meilleure disponibilité du réseau et des services métier critiques qui en dépendent
- Le niveau de sécurité le plus élevé pour les applications et les systèmes d'extrémité convergents
- L'infrastructure d'exploitation la plus simple pour que le service informatique puisse accorder la priorité aux services les plus critiques et garantir leur efficacité.

Avec la solution Secure Convergence d'Enterasys, vous pouvez choisir l'application d'entreprise convergente du fournisseur de votre choix et la déployer pour une sécurité, une disponibilité et une conformité garanties. Enterasys vous propose les meilleures solutions du marché pour faire migrer votre infrastructure réseau vers la dernière génération d'applications d'entreprise convergentes.

Contactez-nous

Pour plus d'informations, appelez Enterasys Networks au + 33 (0) 1 40 84 61 80
et visitez notre site Web à l'adresse www.enterasys.com

Thought Leadership
Over 500 global patents

9014183 3/07

enterasys Secure Networks™

Nous tenons nos promesses, dans le temps et le budget impartis