Livre Blanc Network Access Control (Contrôle d’accès au réseau)

There is nothing more important than our customers.

Contrôle d’accès au réseau (NAC) Enterasys

L’essentiel

Le contrôle d’accès au réseau (NAC) tient un rôle toujours plus important dans la stratégie globale de sécurité du réseau de l’entreprise. Le présent livre blanc a donc pour mission d’expliquer l’approche basée sur des normes et sur une architecture ouverte d’Enterasys en matière de NAC. Les solutions Enterasys permettent de sécuriser n’importe quel réseau d’un quelconque fournisseur en détectant intelligemment les menaces de sécurité et en y réagissant automatiquement. L’offre Secure Networks™ d’Enterasys identifie qui et ce qui est connecté, son emplacement ainsi que son rôle dans l’entreprise. Ainsi, les utilisateurs ont accès aux ressources réseau dont ils ont besoin pour travailler tandis que les systèmes et les processus critiques pour l’activité de l’entreprise sont protégés contre tout abus et compromis.

L’approche architecturale d’Enterasys intègre la sécurité à l’infrastructure réseau et administre l’environnement réseau hétérogène de manière centralisée. Grâce à une interopérabilité normalisée, la Direction Informatique peut optimiser ses investissements existants et étendre le cycle de vie des produits et des technologies. Les solutions Secure Networks d’Enterasys administrent de manière proactive aussi bien un utilisateur de confiance, un invité ou un équipement pour vérifier s’il peut se connecter à un réseau et ce qu’il est autorisé à y faire une fois connecté. Cette vérification s’appuie sur des critères de politique tels que l’identité de l’équipement et de l’utilisateur, son rôle dans l’entreprise, l’heure et l’emplacement de la connexion ainsi que l’état du système d’extrémité.

Une solution NAC efficace doit faire partie intégrante d’une stratégie globale de sécurité réseau pour intégrer :

• Des services d’identité et d’authentification pour les équipements et les utilisateurs

• Une évaluation avant et après la connexion de l’état du système d’extrémité

• L’administration automatisée de l’isolement, de la mise en quarantaine et des menaces

• L’utilisation du réseau et l’accès aux services régis par des politiques, notamment la remédiation automatique

• L’analyse, la prévention et le contrôle permanents des menaces

• Un audit complet de la conformité

Les offres NAC qui gèrent uniquement les problèmes avant la connexion, sans tenir compte de l’importance des règles d’utilisation et de sécurité réseau lorsque le système d’extrémité y est connecté, sont nombreuses. Si un utilisateur ou un équipement est rejeté pendant son évaluation et son authentification lors de sa connexion à l’équipement réseau Enterasys, il ne peut pas utiliser des services critiques et il est seulement autorisé à accéder à des services prédéfinis de remédiation ou réservés aux invités. Lorsqu’elle est connectée à l’équipement réseau d’un autre fournisseur, la solution NAC d’Enterasys peut mettre en quarantaine le système d’extrémité au sein d’un réseau local virtuel (VLAN) à l’aide de méthodes normalisées (RFC3580).

La solution NAC d’Enterasys prend en charge des services d’évaluation des systèmes d’extrémité basés ou non sur des agents. Par conséquent, les systèmes d’extrémité fonctionnant avec des systèmes d’exploitation tels que Windows, Solaris, Linux et MacOS ainsi qu’avec des systèmes d’extrémité de tout type peuvent faire l’objet d’une évaluation de leurs vulnérabilités et des menaces qu’ils représentent. S’appuyant sur son interopérabilité avec les technologies avancées d’évaluation des vulnérabilités de Check Point, Lockdown Networks, Microsoft, Tenable Network Security et Symantec, la solution NAC d’Enterasys est une solution de sécurité réseau complète et proactive qui détermine si un système d’extrémité est conforme aux exigences de sécurité des communications réseau de l’entreprise.

Cette solution fournit un accès réservé aux invités, et sécurisé, afin que la Direction Informatique puisse autoriser, sans aucun risque et de manière fiable, des visiteurs administrés ou non à se connecter à Internet sans que cela constitue pour autant une menace pour les ressources informatiques critiques. Grâce à de nombreuses méthodes d’authentification telles que 802.1X, MAC et Web, ainsi qu’à une évaluation à base d’agent ou sans agent, un quelconque système d’extrémité ou utilisateur peut être évalué et authentifié afin de pouvoir se connecter au réseau et accéder en toute sécurité aux services indispensables à sa mission dans l’entreprise.

Une fois qu’un système d’extrémité accède en toute sécurité au réseau, les menaces qu’il peut représenter sont analysées en permanence et les politiques sont appliquées en continu grâce à une intégration intelligente de la solution NAC d’Enterasys, de la solution de détection d’événements Enterasys Dragon® et de l’application Enterasys NetSight® Automated Security Manager. Enterasys Dragon intègre des technologies de détection d’intrusions (IDS), de prévention des intrusions (IPS), de détection des anomalies de comportement sur le réseau (NBAD) et d’administration des informations de sécurité (SIM). Quant à Enterasys NetSight Automated Security Manager, cette solution offre une infrastructure automatisée pour aligner la détection des événements sur l’emplacement de la source et la réduction des menaces. Cette approche totalement intégrée garantit une sécurité avant et après la connexion, une réponse dynamique aux intrusions ainsi que la prévention proactive contre des attaques Zero Day.

La solution Secure Networks d'Enterasys pour le contrôle d'accès au réseau (NAC) fournit des fonctionnalités complètes de sécurité à la fois pratiques et concrètes et garantit une rentabilité rapide tout en répondant aux questions majeures suivantes :

- Le réseau peut-il procéder de manière stricte à l'authentification d'un quelconque utilisateur ou équipement sans exiger une mise à niveau majeure ?
- Le réseau peut-il avoir la garantie qu'un système d'extrémité est bien fiable et sécurisé avant d'autoriser ce dernier à accéder à des services informatiques ?
- Des politiques d'utilisation du réseau appropriées peuvent-elles être automatiquement déterminées en fonction du type de système d'extrémité et de ses utilisateurs ? Le réseau peut-il garantir l'application granulaire de politiques réseau là où le système d'extrémité se connecte ?
- Le réseau peut-il réagir en temps réel à une menace provenant d'un système d'extrémité précédemment autorisé dans l'environnement ?
- Le réseau peut-il conserver la trace de l'emplacement et du moment où tous les types de systèmes d'extrémité sont en train de communiquer et des ressources informatiques qu'ils utilisent ?
- Le réseau prend-il en charge une interopérabilité d'architecture ouverte et multifournisseur ?
- Existe-t-il un logiciel d'administration capable de fournir la visibilité et le contrôle centralisés nécessaires à l'administration de politiques de contrôle d'accès dans l'entreprise ?

À nous de vous démontrer comment nos solutions et technologies novatrices peuvent vous permettre de contrôler efficacement l'accès à vos applications réseau et métier et de protéger de manière proactive la confidentialité, l'intégrité et la disponibilité de vos ressources informatiques. Des entreprises de premier ordre à travers le monde ont déployé des solutions Secure Networks d'Enterasys pour contrôler l'accès à leur réseau. Nous sommes à votre disposition pour vous démontrer que notre approche unique peut améliorer votre stratégie de sécurité globale tout en optimisant vos investissements existants. Appelez le + 33 (0)1 40 84 61 80 ou rendez-vous sur enterasys.com/securenetworks**.**

Introduction

Le présent livre blanc traite des défis auxquels la Direction Informatique est confrontée lors de la conception et du déploiement d'une solution de contrôle d'accès au réseau (NAC). Il propose une approche architecturale unique pour répondre aux besoins de performances, de disponibilité et de sécurité d'une infrastructure réseau qui prend en charge des communications régies par des politiques.

Le contrôle d'accès au réseau est un terme métier utilisé depuis longtemps par les fournisseurs d'infrastructure réseau, de systèmes d'exploitation et de logiciels de sécurité. Les fournisseurs d'infrastructure réseau ont commencé par introduire des technologies de contrôle d'accès sous la forme de solutions d'authentification et d'autorisation afin de contrôler les communications réseau de base des utilisateurs et des équipements. Des systèmes de certificats à la fois au niveau de l'utilisateur et de l'équipement ont permis à la Direction Informatique d'administrer de manière centralisée qui et ce qui a été autorisé à communiquer sur le réseau. Au fur et à mesure, ce concept de contrôle d'accès au réseau a évolué vers l'intégration d'un ensemble complexe d'informations contextuelles, capable de déterminer qui et quoi est autorisé à communiquer sur le réseau depuis un emplacement particulier et à un moment donné. Les fournisseurs de systèmes d'exploitation et de logiciels de sécurité pouvaient fournir des informations sur le système d'extrémité en plus des certificats sur les processus d'authentification. L'évaluation de la « santé » d'un système d'extrémité, notamment de la menace que le système d'extrémité pourrait poser à l'environnement en réseau et de la vulnérabilité de ce système à une infection par un ver ou un virus, peut faire partie du contexte utilisé lors du processus d'authentification et d'autorisation.

C'est à partir de cette stratégie multifacette destinée à déterminer qui et quoi doit être autorisé sur le réseau et où et quand un système d'extrémité doit être autorisé à y accéder que s'est développée l'utilisation du terme désormais commun de contrôle d'accès au réseau ou NAC. Les solutions NAC actuelles peuvent aider à protéger une entreprise contre une utilisation indésirable des ressources réseau, contre des menaces de sécurité involontaires ou délibérées ainsi que contre des attaques par déni de service diffusées par des vers et des virus et qui se propagent via des systèmes d'extrémité vulnérables. Les solutions NAC peuvent également aider à appliquer des politiques de communication pour une meilleure allocation des ressources réseau et rendre les processus métier aussi efficaces que possibles. L'avantage du déploiement d'une solution NAC pour l'entreprise est un environnement métier plus sécurisé et plus efficace. Le défi consiste à maîtriser les nombreuses technologies associées aux différentes solutions NAC disponibles. Il s'agit aussi de trouver une véritable approche architecturale capable de fournir les fonctionnalités critiques suivantes :

- L'administration de la visibilité et des identités des divers systèmes d'extrémité qui se connectent à un réseau
- L'évaluation des systèmes d'extrémité, avant et après qu'ils soient autorisés à se connecter au réseau
- La capacité d'appliquer avec précision des politiques appropriées d'utilisation du réseau et des applications sur tous les systèmes d'extrémité, partout où ils connectent
- Une assistance pour la remédiation des systèmes d'extrémité et/ou des utilisateurs qui ne sont pas conformes aux politiques de sécurité et d'utilisation du réseau
- Un reporting de conformité qui renseigne sur l'emplacement actuel et passé des systèmes d'extrémité sur le réseau et sur ce qu'ils y faisaient

De nos jours, le réseau revêt un caractère critique pour l'activité de l'entreprise. Parallèlement à l'augmentation massive des menaces de sécurité pouvant affecter l'entreprise, les solutions qui intègrent des technologies à la fois proactives et réactives pour garantir la continuité de l'activité offrent un retour sur investissement important. Le contrôle d'accès au réseau est un élément essentiel d'une architecture de sécurité réseau globale afin de protéger la confidentialité, l'intégrité et la disponibilité du capital information.

Contrôle d’accès au réseau - Définition

Le contrôle d’accès au réseau ou NAC est un terme qui décrit diverses technologies développées pour contrôler/restreindre l’accès au réseau par les systèmes d’extrémité en fonction de leur « état de santé ». L’idée de base est que les systèmes d’extrémité dangereux ou vulnérables (« en mauvaise santé ») ne doivent pas communiquer sur le réseau de l’entreprise dans la mesure où ils pourraient introduire un risque de sécurité pour les processus et les services critiques. Une solution NAC empêchera un système d’extrémité en mauvaise santé d’accéder normalement au réseau jusqu’à ce que la santé de ce système soit déterminée.

Le bilan de santé d’un équipement connecté au réseau est également appelé « évaluation » du système d’extrémité. Les systèmes d’extrémité peuvent être notamment des PC, des imprimantes, des téléphones IP, des caméras de sécurité IP traditionnels. Cette évaluation doit permettre de découvrir le niveau de vulnérabilité et de menace acceptable d’un système d’extrémité. Des éléments tels que le niveau de patch de sécurité, la présence de solutions antivirus/anticodes malveillants, les mises à jour de signatures antivirales/anticodes malveillants, les applications en cours d’exécution, les ports ouverts, etc. peuvent tous être analysés afin de déterminer l’état de santé global du système d’extrémité.

Une approche NAC souhaitable doit permettre d’évaluer n’importe quel type de système d’extrémité connecté au réseau. Ce critère est d’une importance capitale en raison de la diversité croissante des systèmes d’extrémité connectés aux réseaux traditionnels. C’est la mission de la solution NAC que d’appliquer une stratégie complète et proactive pour la sécurité du réseau et de chaque système d’extrémité qui se connecte au réseau, et ce quel que soit le type d’équipement. L’évaluation réelle peut être fournie par diverses applications et exiger qu’un agent soit placé sur le système d’extrémité lui-même ou qu’il fonctionne complètement indépendamment du système d’extrémité sans agent.

Actuellement, les solutions NAC de nombreux fournisseurs ne recourent pas à une authentification du système d’extrémité dans le cadre du processus de contrôle d’accès. L’authentification doit être au cœur de toute solution NAC. Elle est impérative pour garantir l’évolutivité, la souplesse, la visibilité et l’application avec force des politiques de sécurité et d’utilisation du réseau. Une fois un utilisateur identifié ou une machine authentifiée, c’est-à-dire après vérification des certificats, le processus d’autorisation modifie la configuration du port physique réseau source ou le flux virtuel pour autoriser des communications régies par un ensemble de règles de politiques. Une puissante technologie d’autorisation s’appuie sur des niveaux de contexte supplémentaires tels que l’emplacement, l’heure de la journée, une autorisation MAC ou utilisateur explicite (MAC/User Overrides, capacité à « écraser » les résultats du processus d’autorisation), ce qui garantit une solution puissante plus facile à aligner sur les processus métier. La souplesse de l’authentification multiutilisateur et multiméthode d’une solution NAC vous évite de devoir remplacer vos commutateurs de périphérie pour bénéficier d’une visibilité et d’un contrôle supérieurs des utilisateurs et des équipements connectés.

Après exécution du processus d’évaluation et d’autorisation du système d’extrémité, si ce dernier est déterminé comme non conforme aux politiques de sécurité du réseau, il est mis en quarantaine réseau. Le processus d’application des politiques de mise en quarantaine fait intervenir des politiques de communication réseau très granulaires, c’est-à-dire à base de flux, et non pas une simple affectation à un VLAN. En effet, regrouper tous les systèmes d’extrémité « en mauvaise santé » au sein du même VLAN de quarantaine revient à les laisser s’infecter mutuellement avec de nouvelles vulnérabilités. Les politiques réseau décrivent la manière dont le trafic entrant sur des ports de commutation doit être traité au niveau du filtrage, de la prioritisation et du balisage.

La remédiation consiste à résoudre un problème à des fins de conformité avec certaines politiques prédéfinies. Dans le cadre d’une solution NAC, le processus de remédiation permet à l’utilisateur mis en quarantaine réseau de recouvrer sa conformité. Il est important que ce dernier soit impliqué dans le processus de remédiation afin d’optimiser les performances des processus métier. Lorsqu’un utilisateur ou son système d’extrémité pose un problème, ce dernier doit être résolu sans solliciter le service informatique, ce qui évitera au Help Desk informatique d’être saturé par des problèmes de configuration/conformité des systèmes d’extrémité. Cependant, afin que ce processus soit efficace, la solution NAC doit informer l’utilisateur du moment où un système d’extrémité est mis en quarantaine réseau. Des politiques de communication doivent être appliquées dans le cadre de la mise en quarantaine pour garantir une communication sécurisée vers les services requis afin que le système d’extrémité recouvre sa conformité.

L’authentification, l’évaluation, l’autorisation, l’application des politiques ainsi que la remédiation sont toutes des composantes critiques d’une solution NAC exhaustive. De très nombreux produits et technologies sont disponibles auprès d’une multitude de fournisseurs qui n’offrent que certains de ces composants. Une solution NAC d’architecture ouverte et intégrée assurera le bon fonctionnement de tous ces composants critiques, et de manière totalement intégrée, afin de fournir une sécurité efficace.

Besoins liés à une solution NAC complète

Pour le déploiement efficace d’une solution NAC, plusieurs conditions doivent être remplies :

• Architecture ouverte – Support d’environnements multifournisseur

• Inclusion de systèmes d’extrémité – Support de tout type de système d’extrémité

• Autorisation multicontexte - Attributs divers

• Application des politiques – À base de profil et mise en quarantaine

• Notification et remédiation – Auto-assistance utilisateur

• Reporting de conformité – Informations d’historique et en temps réel

Pour être efficace, une solution NAC doit être déployable en tant qu’architecture ouverte. Cette solution doit pouvoir évaluer tout type d’équipement susceptible de se connecter au réseau. Elle doit aussi fournir une sécurité renforcée dans des environnements sur lesquels des équipements de plusieurs fournisseurs d’infrastructure réseau ont été déployés. L’évaluation et l’authentification des ordinateurs qui n’exécutent que certains systèmes d’exploitation ou logiciels à base d’agent ne constituent pas une solution satisfaisante pour protéger les environnements d’entreprise d’aujourd’hui qui sont fortement hétérogènes. Afin que la solution NAC puisse sécuriser efficacement un environnement réseau réel contre les menaces et vulnérabilités liées à l’éventail de systèmes d’extrémité connectés, il est nécessaire d’intégrer des technologies d’évaluation de

différents fournisseurs. Une technologie d'évaluation uniquement destinée à certains systèmes d'extrémité laisse le réseau et les services associés vulnérables aux attaques en provenance de systèmes d'extrémité non intégrés à la stratégie de sécurité. De nombreuses technologies d'évaluation de différents fournisseurs de logiciels doivent pouvoir être intégrées à la solution NAC qui pourra ainsi évaluer n'importe quel type de système d'extrémité qui se connecte au réseau.

En plus de pouvoir tirer parti de nombreuses technologies d'évaluation pour une approche complète de la protection proactive, la solution NAC doit être opérationnelle dans un environnement basé sur une infrastructure multifournisseur. Plusieurs produits d'infrastructure de différents fournisseurs peuvent être déployés dans les environnements réseau. Une solution NAC doit pouvoir gérer des systèmes d'extrémité connectés à divers types de commutateurs réseau de différents fournisseurs. Une mise à jour majeure des produits d'infrastructure de communication réseau n'est pas une solution économiquement envisageable pour déployer une solution NAC complète. Les technologies normalisées d'authentification et d'application de politiques telles qu'IEEE 802.1X et RFC3580 doivent permettre le déploiement d'une solution NAC bien conçue dans un environnement réseau composé de plusieurs produits d'infrastructure de différents fournisseurs.

Les solutions de sécurité réseau éprouvées sont celles qui sont souples, qui s'adaptent et qui garantissent la continuité de l'activité pour les réseaux complexes. Grâce à une approche ouverte du déploiement NAC, l'entreprise peut sécuriser correctement son environnement réseau contre les vulnérabilités et les menaces de tout système d'extrémité connecté à un quelconque produit d'infrastructure réseau. Elle pourra ainsi déployer des systèmes d'extrémité, des applications et des logiciels pour répondre à ses besoins métiers, sans compromission au niveau de la sécurité du réseau ni éventuels coûts indirects.

La variété des systèmes d'extrémité connectés au réseau augmente sensiblement sur les réseaux d'entreprise modernes. Avec l'avènement des réseaux convergents qui hébergent un large éventail d'applications métier, les types de système d'extrémité connectés continuent d'évoluer. Un réseau d'entreprise accueille aussi bien des systèmes d'extrémité comme des téléphones IP, des caméras de surveillance et des distributeurs automatiques que les traditionnels postes de travail, ordinateurs portables et imprimantes. Avec une telle diversité de systèmes d'extrémité connectés, il est impératif qu'une solution NAC bien architecturée intègre tous ces systèmes. Sur un réseau hébergeant différents types de systèmes d'extrémité, les processus de sécurité ne doivent pas être enfermés dans des types d'équipement, de systèmes d'exploitation ou de logiciels spécifiques. Une imprimante, un copieur, un téléphone IP ou une caméra de sécurité peut être facilement infecté et constituer également un point d'infection et de propagation d'une menace de sécurité lors de la connexion d'un poste de travail ou d'un ordinateur portable au réseau. Une solution NAC doit pouvoir fournir une sécurité proactive et réactive pour tout système d'extrémité. Cette solution intègre des technologies pour évaluer, authentifier et autoriser un quelconque système d'extrémité, quel que soit le type d'équipement et le système d'exploitation ou les applications qui fonctionnent sur l'équipement.

Une solution NAC efficace doit pouvoir prendre en compte de nombreux attributs différents pour déterminer l'état de santé, de la sécurité et du rôle d'un système d'extrémité et, le cas échéant, son utilisateur. Une autorisation multicontextuelle des systèmes d'extrémité permet de déployer des mesures de sécurité plus spécifiques ainsi qu'une utilisation plus fine du réseau et des applications. À elle seule, une évaluation des systèmes d'extrémité n'est pas suffisante pour déterminer si un équipement et un utilisateur sont autorisés à accéder au réseau et à des applications et des services spécifiques. La solution NAC doit pouvoir intégrer des attributs contextuels supplémentaires tels que le type d'équipement, le lieu et l'heure de la connexion, les certificats de l'utilisateur et de la machine ainsi que le rôle de l'équipement et de l'utilisateur dans l'entreprise. La prise en compte de ces nombreux attributs contextuels permet d'appliquer une politique de communication réseau sur le système d'extrémité et de fournir des règles de communication réseau et de sécurité très spécifiques. Il est possible d'empêcher les systèmes d'extrémité de communiquer avec des applications inappropriées pour le type d'équipement ou le profil de l'utilisateur. Des règles de mise en quarantaine spécifiques peuvent être appliquées pour une communication sécurisée avec les services critiques requis pour procéder à la remédiation d'un équipement, mais sans que ces règles puissent avoir un impact négatif sur les systèmes d'extrémité ou les communications métier. Plus le contexte sera riche pour le processus d'autorisation d'une solution NAC, plus précises et efficaces seront les communications et la sécurité réseau.

Le processus d'application de politiques est un aspect fondamental d'une solution NAC. Appliquer des règles de politiques de communication et de sécurité réseau directement sur le point de connexion au réseau d'un système d'extrémité est le meilleur moyen pour que les équipements et les utilisateurs communiquent avec la bonne application métier au bon moment. Ceci garantit également une connexion fiable et sécurisée qui ne compromet pas d'autres équipements, personnes et applications présentes sur le réseau. Les règles de politiques doivent être de nature granulaire afin de contrôler de manière spécifique les communications dangereuses ainsi que l'utilisation des applications en un quelconque point du réseau. Si un système d'extrémité est considéré comme dangereux ou vulnérable, il est possible d'appliquer des règles de politiques pour mettre ce système en quarantaine afin qu'il ne mette pas en danger le reste de l'environnement métier. Les règles de la politique de mise en quarantaine ne doivent pas se limiter à placer le système d'extrémité dans un VLAN où d'autres systèmes d'extrémité également non conformes pourront communiquer. En effet, ce processus peut augmenter les risques pour les autres systèmes d'extrémité et constituer un point de distribution et d'échange d'infections favorisant des communications dangereuses. La politique de mise en quarantaine granulaire appliquée ne doit avoir aucune dépendance topologique spécifique (notamment l'affectation de VLAN). Il doit être possible d'appliquer des règles de politiques spécifiques pour une communication réseau de niveau 2 à 4 afin qu'un système d'extrémité puisse être complètement isolé du reste du réseau, sauf des services applicatifs nécessaires à la notification ou éventuellement à la remédiation. Cette application de politiques doit être dynamique et entièrement distribuée sur l'infrastructure du réseau. De plus, des règles de politiques doivent être appliquées par l'infrastructure réseau elle-même, directement sur la connexion du point d'extrémité, qui garantit une infrastructure de politiques évolutive et complète dans le cadre d'une solution NAC.

Si un système d'extrémité est déterminé comme menaçant ou vulnérable, la notification et la remédiation deviennent une phase critique du processus. Appliquer une politique de mise en quarantaine sur un système d'extrémité non conforme à la politique permet d'empêcher ce dernier d'endommager le réseau d'entreprise. Cependant, si l'utilisateur de ce système ne sait pas qu'il a été mis en quarantaine (ni pourquoi), il pensera probablement qu'il s'agit d'un problème lié au réseau de communication ou à des services applicatifs.

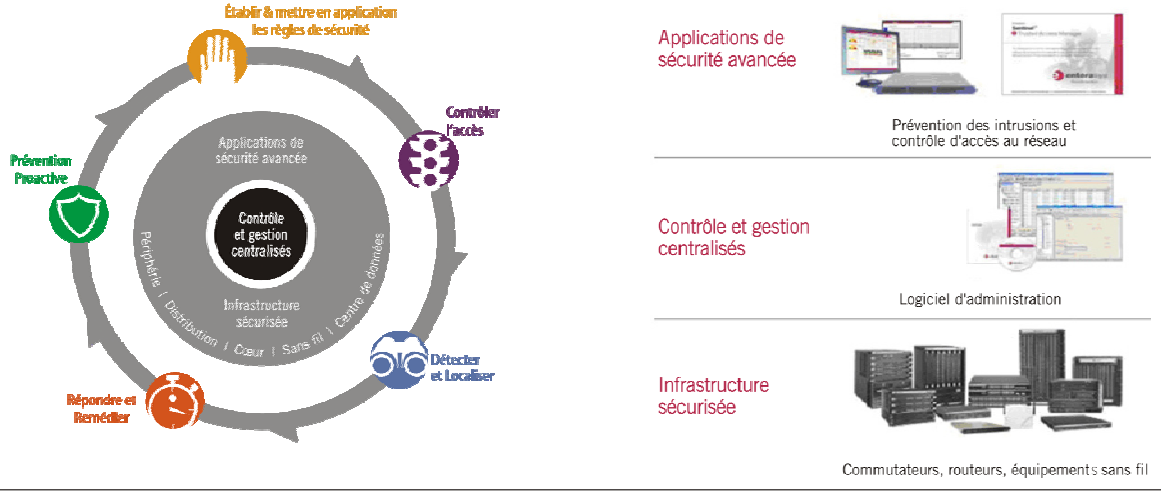
Avertir un utilisateur de la mise en quarantaine de son système d'extrémité évite donc d'inonder le Help Desk d'appels et renseigne l'utilisateur sur un problème concernant son système d'extrémité ou sa tentative de communication. Une solution NAC bien architecturée intégrera un processus de notification système destiné à l'utilisateur du système d'extrémité. Généralement fournie par un navigateur Web classique, cette notification peut également être transmise par d'autres services

tels que la messagerie instantanée ou électronique. Une véritable notification doit non seulement expliquer la politique de mise en quarantaine appliquée au système d'extrémité, mais aussi décrire la (les) raison(s) de cette quarantaine et indiquer la procédure pour remédier efficacement au problème. Il peut s'agir d'une simple instruction concernant la procédure d'accès à un serveur de correctifs ou à un serveur de mises à jour de signatures. Cette notification peut également comprendre des instructions sur la marche à suivre pour désactiver des services ou des applications non conformes à des politiques spécifiques. Une fois qu'il a procédé à la remédiation de son système extrémité, l'utilisateur peut à nouveau le soumettre à une évaluation pour le sortir de son état de quarantaine et redevenir ainsi productif car conforme à un profil de politique spécifique.

Une solution NAC bien architecturée permet de collecter et d'utiliser beaucoup d'informations sur les systèmes d'extrémité connectés, sur les utilisateurs ainsi que sur les communications réseau. Une grande partie de ces informations peut être vitale pour faciliter le reporting de conformité. Dans la mesure où la solution NAC participe à la validation de chaque système d'extrémité connecté au réseau, les données disponibles fournissent, d'une part, une visibilité en temps réel des éléments connectés au réseau et des points de connexion et, d'autre part, des vues sous forme d'historiques des systèmes d'extrémité connectés. Ce qui peut s'avérer extrêmement utile pour gérer un problème de conformité lorsqu'un enregistrement d'historique est nécessaire pour spécifier le point de connexion d'un système d'extrémité à un réseau ainsi que les services qu'il a utilisés. En outre, parce qu'une solution NAC appropriée intègre l'authentification des systèmes d'extrémité et des utilisateurs qui les utilisent, il est possible d'établir une corrélation entre les utilisateurs présents sur le réseau à un moment particulier et leur point de connexion. Les solutions NAC qui permettent d'appliquer des politiques granulaires peuvent également établir un rapport sur l'utilisation réelle du réseau et de ses ressources par un système d'extrémité et/ou un utilisateur particulier. Les solutions NAC complètes doivent non seulement évaluer et autoriser les systèmes d'extrémité et les utilisateurs, mais aussi établir un rapport sur les paramètres de conformité importants.

Une approche architecturale

Enterasys Networks propose une approche architecturale au travers de la solution Secure Networks. Contrairement à la stratégie d'autres fournisseurs, Enterasys intègre pleinement une infrastructure dédiée à la sécurité, des applications avancées de sécurité ainsi qu'une visibilité et un contrôle centralisés qui permettent à la Direction Informatique de déployer des réseaux qui atténueront les risques de manière proactive et réactive pour fournir un environnement de communication métier hautement disponible et sécurisé.



Cette approche architecturale de la solution Secure Networks offre des fonctionnalités importantes. L'architecture permet d'établir 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, la Direction informatique peut garantir l'intégrité globale des communications de données et limiter et isoler les communications des systèmes d'extrémité et des utilisateurs suspects et dangereux. Les politiques sont applicables à la communication depuis un quelconque type de système d'extrémité qui se connecte au réseau.

L'architecture applique le contrôle d'accès des utilisateurs et des équipements qui tentent de communiquer sur le réseau convergent et avec des services spécifiques. Il est possible de détecter et d'identifier des systèmes d'extrémité de différents types qui se connectent au réseau. Une fois un système d'extrémité identifié, il est possible de contrôler l'accès de ce dernier au réseau ainsi qu'à des services spécifiques en fonction de différents critères : le type de système, le rôle dans l'entreprise de ce même système et/ou de la personne susceptible de l'utiliser, le lieu et l'heure de connexion ainsi que l'évaluation de l'état et de la vulnérabilité du système d'extrémité. Ainsi, il est possible d'identifier les différents types de point d'extrémité qui se présentent sur le réseau et de contrôler leurs communications sur ce dernier afin de garantir un accès sécurisé et fiable aux services appropriés.

L'architecture détectera les menaces et les anomalies en un quelconque point du réseau et en localisera la source exacte. En raison de l'importance croissante de l'infrastructure réseau convergente pour l'activité de l'entreprise, il est vital que les menaces à l'encontre des services critiques soient détectées et atténuées en temps réel. Enterasys s'appuie sur une technologie brevetée pour fournir une fonctionnalité unique qui détecte un problème dès qu'il se produit sur le réseau et qui en

localise la source exacte. Ainsi, sur un réseau composé de milliers de systèmes d'extrémité, il est possible de déterminer en quelques secondes seulement la source exacte d'une menace ou d'un problème.

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 d'une menace pour l'environnement permet de mettre en place une réponse appropriée. La réaction 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 règles de politiques de communication, ainsi que la notification et la mise en quarantaine d'un utilisateur spécifique ou d'un flux de communication. 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 le problème afin de pouvoir rapidement retravailler de manière productive.

Cette architecture protégera de manière proactive le réseau contre les systèmes d'extrémité vulnérables et dangereux. Elle empêchera ainsi ces systèmes de compromettre des services métier critiques, ainsi que d'autres utilisateurs et 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 des systèmes d'extrémité de tout type 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 crucial que l'architecture puisse protéger de manière proactive l'environnement réseau contre tout système d'extrémité dangereux.

En s'appuyant sur l'approche architecturale de Secure Networks, la Direction Informatique peut déployer une solution Enterasys qui garantit un environnement de réseau métier efficace et rentable.

Principes de la solution NAC d'Enterasys

La solution NAC d'Enterasys répond à tous les besoins vitaux pour garantir une puissante stratégie de sécurité et protéger les processus métier critiques. Des technologies clés sont déployées afin de fournir une architecture ouverte, évolutive et complète pour évaluer, authentifier, autoriser et appliquer des règles sur un système d'extrémité qui se connecte au réseau de communication de l'entreprise. Le schéma ci-dessous illustre les fonctionnalités de la solution Secure Networks d'Enterasys ainsi que leur relation avec la solution NAC d'Enterasys.

Enterasys Secure Networks™ et NAC

Avec l'architecture Secure Networks, Enterasys offre une solution NAC complète qui répond à tous les besoins critiques.

Architecture ouverte

S'appuyant depuis longtemps sur des technologies normalisées et des systèmes d'architecture ouverte, la solution NAC d'Enterasys intègre et complète différentes infrastructures NAC et technologies d'évaluation. Partenaire technologique de Microsoft, Enterasys s'engage à prendre en charge et à enrichir la stratégie Microsoft Network Access Protection (MNAP) en utilisant la norme 802.1X comme méthode d'authentification réseau. Orientée Windows, Microsoft NAP se concentre sur les clients administrés et exige la présence d'un agent NAP. Microsoft NAP s'appuie sur des technologies normalisées telles que DHCP, VPN, 802.1X et IPsec. Enterasys est membre du Trusted Computing Group/Trusted Network Connect (TCG/TNC), un groupe de normalisation industrielle qui se consacre à l'interopérabilité et à l'intégration de technologies associées au contrôle d'accès au réseau. La mission du groupe de travail TCG/TNC consiste à définir des interfaces de programmation d'application (API) pour faciliter l'intégration de technologies d'évaluation de différents fournisseurs ainsi que l'authentification et l'autorisation réseau. Enterasys a certifié ses gammes de commutateurs Enterasys Matrix™ et SecureStack™ comme points d'applications de politiques (PEP – Policy Enforcement Point) conformes avec les exigences du groupe de travail TCG/TNC. En plus de travailler étroitement avec des groupes industriels dédiés à l'interopérabilité de technologies NAC, Enterasys

entretient des partenariats avec plusieurs fournisseurs qui proposent des technologies de premier ordre pour évaluer les systèmes d'extrémité. Des fournisseurs comme Tenable Network Security, Lockdown Networks, Check Point Software et Symantec offrent d'importantes technologies qui s'intègrent à la solution NAC d'Enterasys.

Une approche ouverte de l'infrastructure réseau est également au cœur de la solution NAC d'Enterasys. Chez Enterasys, nous sommes conscients que les réseaux peuvent être composés de produits d'infrastructure de différents fournisseurs. Remplacer des produits d'infrastructure dans le simple but d'avoir une solution NAC opérationnelle n'est pas une démarche rentable. Les commutateurs de distribution Matrix N-Series prennent en charge des fonctionnalités d'authentification multiméthode et multiutilisateur. Ainsi, un commutateur d'accès semi-intelligent ou non intelligent qui ne supporte pas l'authentification de systèmes d'extrémité nécessaire à une solution NAC peut être connectée en amont à un commutateur Enterasys. Les flux de trafic de chaque utilisateur et équipement peuvent être authentifiés au sein de ce commutateur à l'aide de technologies normalisées. En outre, des politiques simples telles que l'affectation de VLAN peuvent être appliquées sur le commutateur d'un quelconque fournisseur à l'aide d'une technologie d'affectation de VLAN dynamique et normalisée, notamment RFC3580. Ainsi, les systèmes d'extrémité qui se connectent aux commutateurs d'accès d'un quelconque fournisseur peuvent s'intégrer à la solution NAC d'Enterasys.

Grâce à cette architecture ouverte, le service informatique peut appliquer les meilleures technologies d'évaluation disponibles avec intégration complète de l'authentification, de l'autorisation et de l'application de politiques de sécurité et de communication. Concernant la solution NAC d'Enterasys, il n'existe aucune restriction au niveau du déploiement de technologies d'évaluation ou des systèmes d'extrémité associés pouvant faire l'objet d'une évaluation. Ainsi, la Direction Informatique peut déployer une solution NAC d'Enterasys sans surcoût indirect lié au remplacement de l'infrastructure afin d'améliorer la stratégie de sécurité d'un réseau.

Prise en compte des systèmes d'extrémité

Pour qu'elle soit efficace, une solution NAC doit inclure tous les systèmes d'extrémité présents dans l'environnement réseau. La solution NAC d'Enterasys prend en charge un environnement de systèmes d'extrémité hétérogène et fournit une sécurité et une administration intégrées quel que soit le type d'équipements connectés au réseau de l'entreprise.

Enterasys s'appuie sur deux modèles d'évaluation pour faciliter le contrôle NAC dans un environnement réseau. Une évaluation à base d'agent et une évaluation sans agent sont toutes les deux critiques pour inclure tout système d'extrémité d'un quelconque type dans le processus NAC. Plusieurs raisons font que les deux modèles d'évaluation sont indispensables pour bénéficier d'une solution NAC complète. Les agents déployés sur les systèmes d'extrémité administrés offrent des fonctionnalités d'évaluation complètes, mais il faut aussi tenir compte de certains types de système d'extrémité qui ne sont peut-être pas en mesure de charger un agent logiciel sur un réseau. Et quid des systèmes d'extrémité tels que les téléphones, caméras et imprimantes IP ? Si un agent n'est pas disponible pour un équipement (ou pour les systèmes d'exploitation qui permettent à ce même équipement de fonctionner), une approche sans agent est le seul moyen d'évaluer le système d'extrémité. Il faut également tenir compte des systèmes d'extrémité qui pourraient normalement intégrer un agent, mais qui échappent au contrôle de la Direction Informatique. Dans le cas d'un accès réseau pour des invités (prestataires, fournisseurs, public, etc.), il peut être souhaitable de prendre en charge un minimum de services réseau ou des services réseau spécifiques, tout en garantissant la sécurité du réseau et des personnes qui l'utilisent. Une simple politique d'utilisation du réseau ne suffit pas pour limiter les services auxquels un « utilisateur invité » peut accéder. En effet, dans la mesure où l'invité profite de la même infrastructure réseau que les utilisateurs clés de l'entreprise, il est important que des mesures de sécurité proactives s'appliquent à l'invité, au même titre qu'un utilisateur « administré ». Il s'agit d'un autre cas de stratégie d'évaluation des systèmes d'extrémité sans agent vitale pour garantir une stratégie NAC complète. Les modèles d'évaluation avec et sans agent peuvent être déployés et intégrés ensemble à la solution NAC d'Enterasys.

Le modèle sans agent d'évaluation des systèmes d'extrémité n'exige l'installation d'aucun agent logiciel sur le système. Ce modèle supporte divers types de systèmes d'extrémité tels que des PC, des téléphones IP, des caméras et des imprimantes IP, etc., ainsi que de nombreux systèmes d'exploitation.

Il existe deux variantes du modèle sans agent :

- Le modèle « network-based » : s'appuyant sur des moteurs d'évaluation des vulnérabilités basés sur le réseau comme Nessus de Tenable Network Security et sur la technologie d'évaluation intégrée de Lockdown Networks, la solution NAC d'Enterasys offre un support intégré pour l'authentification, l'autorisation et l'application des politiques. Ce modèle s'applique aux traditionnels systèmes d'extrémité de type PC, mais il est plus particulièrement utile pour prendre en charge les environnements les plus hétérogènes qui hébergent des systèmes d'extrémité qui ne dépendent pas de l'utilisateur ainsi que des systèmes d'extrémité fonctionnant avec des systèmes d'exploitation non traditionnels. Cette évaluation n'exige aucune connaissance particulière du système d'extrémité et elle s'exécute à distance. À noter que les technologies d'évaluation basées sur le réseau exigent de désactiver des fonctionnalités de firewall sur les systèmes d'extrémité.
- Le modèle « applet-based »ou « basé sur un agent temporaire » : en forçant le système d'extrémité à télécharger une applet Java, un contrôle ActiveX ou un agent logiciel temporaire (valide le temps de la session), il est possible de procéder à une évaluation locale lorsque le système d'extrémité accède à une page Web. Enterasys s'appuie sur les technologies de Symantec, Check Point et Lockdown Networks pour évaluer un système d'extrémité à partir d'un agent logiciel installé sur ce système via le réseau.

Le modèle d'évaluation du système d'extrémité basé sur un agent exige l'installation d'un agent logiciel sur ce système. Cet agent fournit un « point de présence » sur le système d'extrémité pour communiquer avec le serveur d'évaluation. L'agent logiciel contrôle la présence et la configuration des ressources antivirus, antispyware, de firewall personnel et effectue également des analyses système approfondies.

Il existe deux variantes du modèle à base d'agent :

- Le modèle à base d'agent « léger » : l'agent « léger » n'exige qu'un minimum de ressources et aucune configuration du côté client. Les agents sont préconfigurés, installés et mis à jour au moyen du serveur d'évaluation. Le modèle à base d'agent « léger » est déployable dans des environnements de système d'exploitation spécifiques en fonction des systèmes d'extrémité pris en charge par les fournisseurs de solutions d'évaluation. Enterasys NAC s'intègre à la technologie d'évaluation à base d'agent fin de Lockdown Networks.

• Le modèle à base d'agent « lourd » : l'agent « lourd » fournit une solution de sécurité personnelle intégrée telle qu'un firewall personnel ou un système IDS hôte. Ce modèle est généralement utilisé pour les systèmes d'exploitation Microsoft. Il peut également exiger d'importantes ressources (mémoire, processeur, etc.) du côté client. L'offre NAC d'Enterasys s'intègre à plusieurs technologies pour agents « lourd » :

— Symantec avec le produit Sygate Enterprise Protection. Enterasys a certifié Sygate Enterprise Protection pour sa gamme de produits (s'appuyant sur 802.1X/EAP).

— Check Point avec son produit Integrity. Enterasys a certifié Integrity pour sa gamme de produits (s'appuyant sur 802.1X/EAP).

— Microsoft avec la technologie NAP (Network Access Protection). Enterasys est en train de tester activement NAP sur les produits Windows Vista et Windows Server 2008 qui intègre les méthodes d'« enforcement » 802.1X, DHCP et IPSec.

S'appuyant sur des technologies l'évaluation à la pointe du marché, la solution NAC d'Enterasys intègre tout type de systèmes d'extrémité connectés au réseau d'entreprise.

Autorisation multicontextuelle

L'authentification et l'autorisation réseau sont des composants essentiels de la solution NAC d'Enterasys. Enterasys déploie des mécanismes tels que l'authentification/l'autorisation multiutilisateur et multiméthode. Pouvoir authentifier de nombreux utilisateurs (ou équipements) sur un seul port de commutation physique est important afin d'autoriser divers services pour des utilisateurs et des équipements différents. Un port de commutation réseau auquel un téléphone IP et un PC sont tous les deux connectés est un bon exemple. L'authentification distincte des deux équipements différents permet d'autoriser des politiques d'utilisation du réseau spécifiques à l'équipement et à l'utilisateur. Les commutateurs Enterasys Matrix et SecureStack prennent en charge une authentification multiutilisateur.

En outre, cette authentification permet d'inclure des commutateurs sans fonctionnalités d'authentification à l'infrastructure. Connecter des commutateurs dépourvus de fonctionnalités d'authentification à un commutateur de distribution Enterasys Matrix doté d'une fonction d'authentification multiutilisateur permet d'authentifier des flux de trafic de différents utilisateurs au niveau Distribution. Il en résulte un type d'authentification de « port virtuel » au niveau Distribution du réseau.

La souplesse des méthodes d'authentification utilisées par les commutateurs Enterasys garantit une authentification réseau totalement intégrée dans tous les environnements, notamment pour les systèmes d'extrémité orientés machine et utilisateur. Les commutateurs Enterasys prennent en charge les méthodes d'authentification basées sur IEEE 802.1X, MAC et Web.

Il est possible de détecter automatiquement des systèmes d'extrémité spécifiques tels que des téléphones IP ou des caméras IP sur le réseau et de les placer dans un environnement de communication particulier. D'autres systèmes d'extrémité, par exemple des imprimantes, peuvent être authentifiés et autorisés en fonction de champs de codes fournisseur et d'équipement (dans l'adresse MAC) en s'appuyant sur une fonctionnalité de « masking » OUI.

Lorsqu'un système d'extrémité se connecte au réseau, l'authentification réseau est appliquée et détectée par le contrôleur NAC d'Enterasys. Avec la solution NAC d'Enterasys, le système d'extrémité est autorisé de façon temporaire dans un environnement d'« évaluation » (policy ou VLAN). Cet environnement permet de déterminer l'état et la menace que peut représenter le système d'extrémité en cours d'évaluation sans risquer de compromettre l'intégrité des autres systèmes d'extrémité. Une fois qu'il a fini d'évaluer le système d'extrémité, le serveur d'évaluation communique les résultats au processus d'autorisation. Ce dernier décide alors de la mise en quarantaine du système d'extrémité s'il n'est pas conforme ou bien force une nouvelle authentification ainsi qu'une autorisation pour le système d'extrémité afin de lui permettre de communiquer sur le réseau en fonction de son profil dans l'entreprise. Le processus d'autorisation comprend de nombreuses variables telles que l'emplacement, l'heure, une autorisation MAC ou utilisateur explicite (MAC/User Overrides, capacité à « écraser » les résultats du processus d'autorisation), la présence de verrous d'emplacement MAC (MAC Locks) préconfigurés, etc.

Application de politiques

Lorsqu'un système d'extrémité est mis en quarantaine suite à une évaluation qui conclut à sa non conformité, le profil de la politique de mise en quarantaine est appliqué au niveau du réseau en modifiant la configuration du port du commutation. L'environnement de mise en quarantaine est configuré de manière à ce que le trafic réseau soit contenu conformément à des règles de sécurité préalablement définies. La solution NAC d'Enterasys s'appuie sur plusieurs fonctionnalités majeures d'application de politiques basées sur l'architecture Secure Networks.

• Politique par défaut pour un accès de base : application d'une politique par défaut sur des ports réseau auxquels se connectent des systèmes d'extrémité. Cette politique par défaut fournit un accès de base au réseau et sera contournée après authentification pour les utilisateurs et systèmes d'extrémité connus.

• Politique d'évaluation des systèmes d'extrémité : à l'aide d'un profil de politique d'« évaluation », des règles de politique granulaires sont appliquées sur les systèmes d'extrémité pour restreindre les communications réseau aux seules applications nécessaires à l'évaluation. Il est indispensable de contrôler l'environnement dans lequel les systèmes d'extrémité sont placés lors du processus d'évaluation. Les règles de communication sont déterminées par les politiques de l'environnement métier et par les besoins de sécurité. Un profil de politique d'évaluation peut fournir un accès Internet et email lors du processus d'évaluation tout en empêchant l'accès aux serveurs et aux applications critiques. Dans d'autres cas, le profil de la politique d'évaluation peut complètement restreindre l'accès aux ressources réseau jusqu'à ce que le système d'extrémité soit évalué comme étant sain et sécurisé et qu'il soit autorisé à communiquer sur le réseau.

• Politique de mise en quarantaine/sécurité intégrée pour les systèmes d'extrémité non conformes : application de règles de politique granulaires pour mettre en quarantaine des systèmes d'extrémité via un profil de politique de mise en quarantaine (« Quarantine »). Une fois déterminé comme non conforme, le système d'extrémité est mis en quarantaine. Les règles de communication spécifiques de l'environnement de quarantaine sont déterminées par les politiques de sécurité de l'entreprise. La politique « Failsafe » est utilisée lorsque l'« état » d'un système d'extrémité ne peut pas être déterminé (lorsqu'il ne peut pas faire l'objet d'une analyse de vulnérabilités ou que le processus d'authentification/autorisation n'est pas disponible).

• Politique en fonction du profil dans l'entreprise pour les systèmes d'extrémité/utilisateurs autorisés : une fois qu'un système d'extrémité et un utilisateur sont déterminés comme étant fiables et sécurisés à l'issue du processus d'évaluation), des règles de politiques de communication basées sur leur rôle dans l'entreprise sont appliquées sur le point de connexion au réseau. Ces règles de politique imposent la manière dont un système d'extrémité peut utiliser le réseau ainsi que les applications et les services auxquels il peut accéder. Des règles de sécurité spécifiques sont également appliquées pour garantir en permanence une analyse des menaces et une sécurité basée sur le contrôle après la connexion au réseau.

Notification/Remédiation

Avec la solution NAC d'Enterasys, il est possible d'intégrer une notification et une remédiation qui s'appuient sur le réseau. La notification est un aspect critique d'une solution NAC et permet de placer un système d'extrémité dans un type de configuration de politique réseau de mise en quarantaine. Si le PC d'un utilisateur est soudainement mis en quarantaine et incapable d'accéder aux types de services auxquels son utilisateur a généralement accès, il est important que les informations sur cet événement soient fournies à la Direction Informatique, mais aussi que l'utilisateur soit directement avisé de la raison de l'interruption de service. Si son système d'extrémité est mis en quarantaine, l'utilisateur pensera certainement qu'il s'agit d'un problème de communication réseau s'il n'a pas été avisé de la mesure qui a été prise. Cependant, déployer une solution NAC pouvant mettre en quarantaine un système sans en informer son utilisateur peut augmenter le nombre d'appels au Help Desk de la part d'utilisateurs qui ne peuvent plus accéder aux services dont ils besoin et qui ne comprennent pas pourquoi. La solution NAC d'Enterasys intègre une fonctionnalité de notification de l'utilisateur en cas de mise en quarantaine déclenchée par le système NAC lui-même. Ainsi, une fois qu'un système d'extrémité est mis en quarantaine, il est possible de déclencher une notification en redirigeant le trafic Web du système d'extrémité non conforme vers une page Web de remédiation. Cette page Web peut être mise à jour par la Direction Informatique et comporter des informations détaillées sur les raisons de la mise en quarantaine du système d'extrémité ainsi que sur la manière dont un utilisateur peut résoudre les problèmes qui sont à l'origine de cet état de non conformité. Même si le système d'extrémité peut accéder au réseau et à la page Web de remédiation, la communication est spécifiquement configurée au moyen d'un ensemble de règles de politiques qui garantit l'absence de danger pour le reste du réseau lors de la notification à l'utilisateur.

Afin qu'un utilisateur dont le système d'extrémité a été mis en quarantaine puisse recouvrer l'accès à l'ensemble des services réseau nécessaires, il doit tout d'abord résoudre le problème à l'origine de la mise en quarantaine. Ceci n'est pas toujours possible pour l'utilisateur. En effet, prenons le cas d'un utilisateur qui agit avec malveillance et qui menace le réseau et ses services. La remédiation peut ne pas être souhaitable et, à la place, une politique de mise en quarantaine persistante sera appliquée pour empêcher l'utilisateur d'endommager l'environnement informatique. Dans d'autres cas, lorsqu'un utilisateur ou un système d'extrémité viole involontairement une politique de sécurité prédéterminée, il est souhaitable d'en informer son utilisateur puis de l'autoriser à résoudre le problème lui-même. Il est fondamental que le réseau puisse appliquer une politique d'utilisation qui protège complètement toutes les ressources critiques et les autres utilisateurs, tout en autorisant l'accès aux ressources de remédiation clés telles que les serveurs Web fournissant des patches de sécurité. Grâce à la solution NAC d'Enterasys, une politique de mise en quarantaine peut être établie avec un ensemble très spécifique de règles de politique pour filtrer et contrôler le trafic réseau à l'aide de caractéristiques source et de destination spécifiques et d'identifiants applicatifs particuliers (par exemple, des « ports » UDP/TCP). En outre, la solution NAC d'Enterasys prendra en charge un nombre illimité de profils de politique de mise en quarantaine différents et donc divers degrés de restriction d'utilisation du réseau en fonction de la gravité de la non conformité ou de l'infraction à la sécurité. Cette approche est différente de celles de nombreuses solutions NAC qui offrent uniquement un « placement » dans un VLAN pour les systèmes d'extrémité qui doivent être mis en quarantaine. À l'aide des fonctionnalités de politique granulaires des commutateurs Enterasys, il est possible d'appliquer un ensemble spécifique de règles de politiques pour autoriser un accès limité en débit à une application spécifique ou à un service Web spécifique tout en filtrant tous les autres trafics du réseau. Ainsi, une quelconque menace en temps réel pour l'environnement réseau peut être contrôlée pendant que l'utilisateur applique la bonne mesure de remédiation pour rendre son système d'extrémité conforme à une utilisation sans risque sur le réseau. Lorsque l'utilisateur estime avoir terminé la remédiation, il demande à la solution NAC d'Enterasys de réévaluer le système d'extrémité pour vérifier sa conformité. Si le problème est réglé, une politique d'utilisation du réseau lui accorde un accès aux services métier.

Grâce à cette technologie intégrée, la solution NAC d'Enterasys peut déployer la remédiation pour les environnements de systèmes d'extrémité avec et sans agent. En outre, des mécanismes d'enregistrement peuvent être déployés afin que les utilisateurs non authentifiés puissent enregistrer l'adresse (MAC) physique de leur système d'extrémité. L'accès au réseau est accordé aux utilisateurs enregistrés après évaluation du système d'extrémité et autorisation de l'administrateur réseau.

Reporting de conformité

Autre aspect important d'une solution NAC, sa capacité à visualiser rapidement l'état de l'environnement réseau. Les administrateurs informatiques ont besoin d'informations sur qui et ce qui se connecte au réseau. Et aussi sur l'endroit et le moment où les équipements se connectent, sur la fiabilité et la sécurité des équipements ainsi que sur les utilisateurs des équipements qui représentent une menace pour l'environnement réseau. Des informations en temps réel et d'historique complètes sur les systèmes d'extrémité et sur les utilisateurs qui communiquent sur le réseau sont essentielles pour connaître l'état de conformité à une politique prédéterminée.

La solution NAC d'Enterasys maintient un ensemble complet de données importantes qui peuvent être optimisées pour déterminer rapidement l'utilisation du réseau ainsi que les menaces et vulnérabilités que posent les systèmes d'extrémité de tout type. Autre aspect important de la solution NAC d'Enterasys : sa capacité à consulter les données d'historique sur n'importe quel système d'extrémité. Cette solution peut établir des rapports non seulement sur l'endroit depuis lequel un système d'extrémité est actuellement connecté, mais aussi sur ses points de connexion précédents, ainsi que sur les personnes qui utilisent le système d'extrémité et si ce dernier était conforme à ce moment. Les données collectées à partir de la solution NAC d'Enterasys comprennent :

• L'adresse MAC : *L'adresse physique du système d'extrémité*

• L'adresse IP de commutation : *Le commutateur du réseau auquel le système d'extrémité est connecté*

• L'index du port de commutation : *L'index du port du commutateur auquel le système d'extrémité est connecté*

• Le port de commutation : *Le « nom » du port de commutation auquel le système d'extrémité est connecté*

• L'adresse IP : *La dernière adresse IP connue du système d'extrémité*

• Le type d'authentification : *La méthode utilisée pour authentifier le système d'extrémité*

• L'état : *L'état du système d'extrémité en matière d'autorisation*

• Le motif : *Le motif pour lequel le système d'extrémité se trouve dans tel état d'autorisation*

• Le nom d'utilisateur : *Le nom d'utilisateur de toute personne qui utilise le système d'extrémité*

• La première fois : *La première fois que le système d'extrémité a été détecté sur le réseau*

• La dernière fois : *La détection la plus récente du système d'extrémité sur le réseau*

• La dernière analyse : *La dernière fois que le système d'extrémité a été évalué*

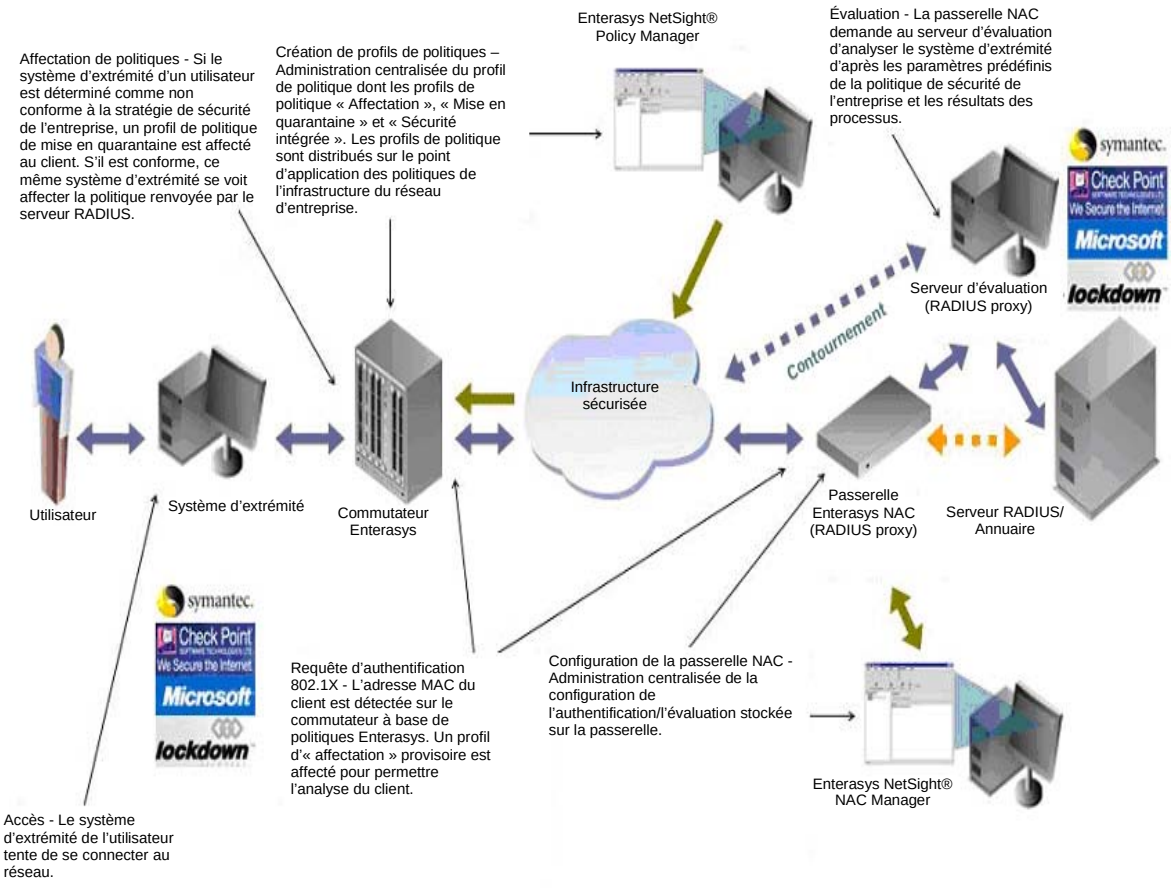
À partir des données collectées par la solution NAC d'Enterasys, les administrateurs informatiques peuvent connaître la conformité du système d'extrémité en temps réel de même que son historique. Grâce aux fonctionnalités de reporting de la solution NAC d'Enterasys, la Direction Informatique peut établir des rapports sur la conformité du système d'extrémité, justifier les dépenses technologiques et fournir, le cas échéant, des informations de conformité aux normes en vigueur.

Enterasys NAC en action

La solution NAC d'Enterasys met en scène plusieurs technologies et produits qui coopèrent de manière complètement intégrée pour garantir une stratégie complète de protection proactive dans le cadre d'une architecture de sécurité globale.

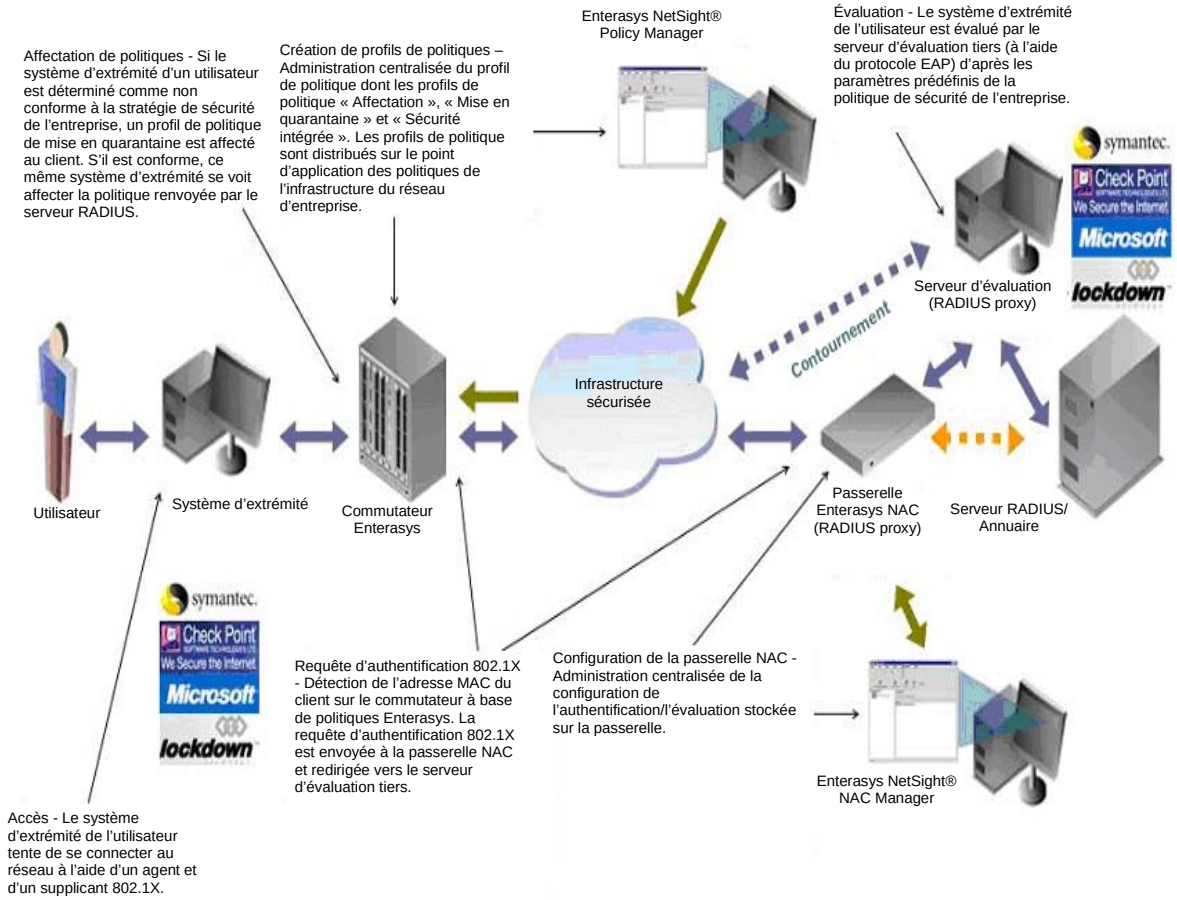
Le schéma suivant décrit la solution NAC d'Enterasys dans un environnement d'évaluation sans agent.

Enterasys NAC en action — Sans agent (« Network-based »)



Le schéma suivant décrit la solution NAC d'Enterasys dans un environnement d'évaluation à base d'agent.

Enterasys NAC en action — Avec agent (léger et lourd) « Agent-based »



Enterasys offre un ensemble complet de technologies pour le déploiement d'une solution réseau NAC exhaustive. Le tableau ci-dessous indique les technologies nécessaires à une solution NAC ainsi que les produits Enterasys qui les fournissent.

Contrôle d'accès au réseau - Besoins	Technologies/Fonctionnalités		Produits Enterasys
Architecture ouverte	•IEEE •IETF • Microsoft NAP • TCG/TNC	• Authentification multiutilisateur • Politique de niveau Distribution • API logicielles • Évaluation tierce	• Commutateurs Matrix/SecureStack • Logiciel d'administration NetSight • Passerelle NAC Enterasys • NetSight NAC Manager
Prise en compte des systèmes d'extrémité	• IEEE 802.1X • Authentification basée MAC • Authentification basée Web • Détection des points CEP	• Évaluation basée sur un agent • Évaluation sans agent	• Commutateurs Matrix/SecureStack • Passerelle NAC Enterasys • NetSight Policy Manager
Autorisation multicontextuelle	• Authentification IEEE 802.1X • Authentification basée MAC • Authentification basée Web • Détection des points CEP	• Masquage/Authentification OUI • Authentification multiutilisateur • Configuration des politiques en fonction du profil	• Commutateurs Matrix/SecureStack • NetSight Policy Manager • Passerelle NAC Enterasys
Application de politiques	• Filtres de trafic • Limitation du débit • Isolement de flux • Application dynamique de politiques	• Détection d'intrusions • Isolement de flux • Atténuation des menaces	• Commutateurs Matrix/SecureStack • NetSight Policy Manager • Passerelle NAC Enterasys
Notification et remédiation	• Règles de politique de niveau 4 • Redirection Web • Filtrage applicatif • Application dynamique de politiques	• Enregistrement des systèmes d'extrémité • Réévaluation initiée par l'utilisateur	• Commutateurs Matrix/SecureStack • NetSight Policy Manager • Passerelle NAC Enterasys
Reporting de conformité	• Emplacement des systèmes d'extrémité • État de l'évaluation des systèmes d'extrémité • Identité des utilisateurs	• Historique – Emplacement/État de l'évaluation • Historique des analyses	• Passerelle NAC Enterasys • NetSight NAC Manager

En résumé

Le contrôle d'accès au réseau est un composant clé d'une solution de sécurité réseau. S'informer sur l'identité et l'état d'un système d'extrémité avant qu'il se connecte au réseau est critique pour garantir la continuité de l'activité et la sécurité globale de l'entreprise. Enterasys offre une approche basée sur une architecture ouverture et normalisée du contrôle d'accès au réseau. Cette solution répond aux besoins les plus critiques de sécurité de n'importe quelle entreprise.

Grâce à l'architecture ouverte de la solution NAC d'Enterasys, les meilleures technologies d'évaluation de fournisseurs de premier ordre s'intègrent pleinement aux fonctionnalités d'authentification, d'autorisation et à l'application de politiques des solutions Secure Networks.

Déployer la solution NAC d'Enterasys garantit la visibilité et le contrôle de qui et de ce qui est autorisé à se connecter au réseau. Les systèmes d'extrémité dangereux et non conformes sont isolés et ne peuvent donc pas nuire aux processus métier pris en charge par le réseau. La solution NAC d'Enterasys offre une stratégie complète pour répondre aux besoins d'évaluation d'un quelconque système d'extrémité. Cette approche s'appuie sur l'utilisation du réseau en fonction d'un large éventail de contextes, sur l'application de politiques de sécurité et de communication métier, sur la notification des utilisateurs concernant leur état de non conformité, sur une assistance pour une remédiation fiable et sécurisée ainsi que sur la fourniture de données de conformité importantes.

Avec la solution NAC d'Enterasys, il n'est pas nécessaire de remplacer les produits d'infrastructure installés. S'appuyant sur une authentification multiméthode et multiutilisateur novatrice ainsi que sur l'application de politiques à base de VLAN (RFC3580), Enterasys vous permet de déployer une solution NAC complète au sein de votre environnement réseau actuel. L'engagement d'Enterasys en matière d'architecture ouverte et normalisée garantit le déploiement NAC le plus économique et le plus complet actuellement disponible sur le marché.

Et parce que la solution NAC d'Enterasys fait partie intégrante de l'approche architecturale de l'offre Secure Networks en matière de sécurité du réseau, vous bénéficiez d'une sécurité avant et après la connexion ainsi que de technologies réactives, toutes intégrées à une architecture facile à administrer.

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

9014192 4/07

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