Description de la gamme Cisco NAC

La fiabilité du réseau nécessite l'application de politiques de sécurité

Les utilisateurs qui accèdent au réseau avec des équipements mal protégés – vulnérabilités systèmes, précautions de sécurité obsolètes, etc. – sont à l'origine d'un grand nombre des problèmes qui pénalisent les systèmes informatiques de l'entreprise. L'application de politiques de sécurité au point d'ouverture de session est un bon moyen de s'assurer que ces équipements, quels que soient leur origine, leur type ou leur propriétaire, ne compromettent pas la sécurité du réseau.

Le Contrôle d'Admission au Réseau Cisco NAC (Net work Admission Control) est une solution qui s'appuie sur l'infrastructure réseau pour appliquer les politiques de sécurité sur la totalité des appareils qui cherchent à accéder aux ressources informatiques. En minimisant les risques associés aux équipements non conformes, Cisco NAC contribue à rendre votre réseau plus robuste et plus sûr.

De plus, Cisco NAC peut réaliser l'authentification utilisateur au niveau du réseau afin que seules les personnes qui disposent d'authentifiants valides puissent y accéder.

Qu'est-ce qu'une solution efficace dans ce domaine ?

L'application de politiques dépasse de loin la recherche d'éventuelles infections actives sur les équipements entrants. C'est un moyen pour l'entreprise d'appliquer de manière homogène des critères de sécurité à ses utilisateurs et leurs appareils, sans réduire la productivité. Pour être efficace, l'application de politiques doit pouvoir :

- identifier et authentifier : reconnaître de manière univoque l'utilisateur et son appareil et les associer l'un à l'autre ;
- analyser et faire respecter les postures de sécurité : évaluer les équipements et appliquer une politique homogène à l'échelle du réseau ;
- mettre en quarantaine et corriger : agir en fonction des résultats des évaluations de postures de sécurité afin d'isoler les équipements non conformes et les mettre en conformité ;
- gérer et configurer : créer facilement des politiques exhaustives et aussi fines que possible, capables d'associer rapidement l'utilisateur entrant à un groupe ou à un rôle

Le Contrôle d'Admission Réseau NAC dans un serveur dédié

Cisco® NAC, précédemment appelé Cisco Clean Access, est un serveur autonome dédié à l'application des politiques qui permet à l'administrateur réseau d'authentifier, d'autoriser, d'évaluer et de corriger les équipements filaires, sans fil et distants avant de donner à leurs utilisateurs un accès au réseau. Il détermine si l'équipement est en conformité avec les politiques de sécurité et « répare » les vulnérabilités éventuelles avant de l'autoriser à se connecter.

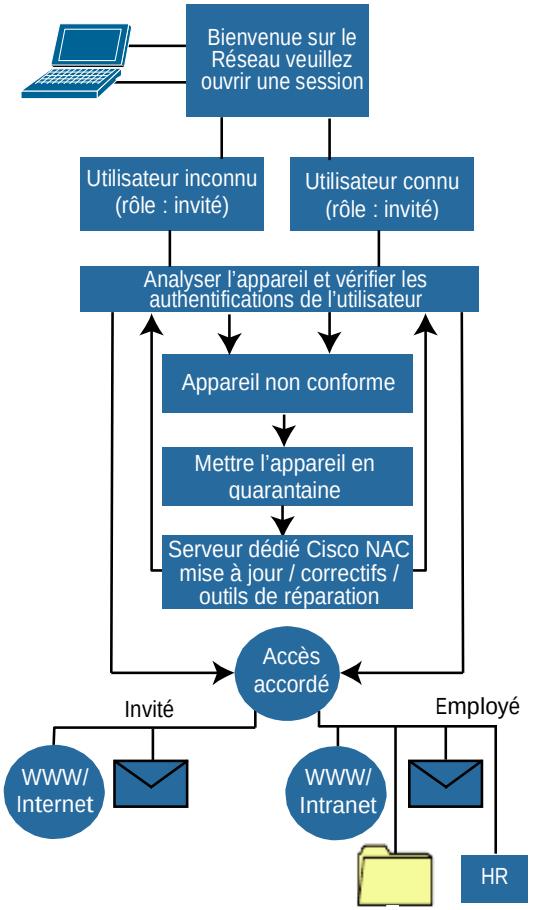
Les avantages du serveur dédié Cisco NAC

Avec plus de 600 clients dans des organisations de toutes tailles, le Contrôle d'Admission Réseau Cisco NAC est aujourd'hui la solution la plus déployée sur le marché. Contrairement à de nombreuses autres solutions, qui exigent des produits différents en fonction des divers scénarios, un même serveur dédié Cisco NAC répond à tous les cas possibles – que la mise en conformité aux politiques concerne les utilisateurs du réseau LAN, de l'accès distant ou des VPN, de l'accès sans fil, des agences de l'entreprise ou de l'extranet.
Plus qu'un outil proactif pour renforcer la sécurité du réseau, le Contrôle d'Admission Réseau Cisco NAC :

- protège les intérêts de l'entreprise en sécurisant l'infrastructure du réseau, les informations sensibles et la propriété intellectuelle.Il permet au service informatique de protéger les informations confidentielles de l'entreprise en contrant les menaces engendrées par la disparition des frontières de sécurité, l'accès non autorisé et les attaques internes ;
- entretient la crédibilité, la réputation et l'image publique d'une organisation en évitant que les activités malveillantes et les attaques puissent paralyser son réseau ;
- améliore la productivité des employés en réduisant et en éliminant les tentatives d'exploitation des vulnérabilités et les attaques. Grâce à ce type de contrôle, l'utilisateur évite les pannes d'infrastructure à grande échelle, la baisse de productivité et les pertes financières directes ;
- aide l'entreprise à se mettre en règle avec les réglementations en matière de confidentialité et de protection des informations comme Sarbanes-Oxley et la loi Informatique et Libertés. Les entreprises incapables de respecter les exigences de conformité de ces législations mettent en danger leurs relations avec leurs clients et s'exposent à des sanctions de la part des autorités compétentes.

Les composantes du Contrôle d'Admission Réseau Cisco NAC

- Clean Access Server – serveur qui procède à l'évaluation des points d'extrémité et leur attribue des privilèges d'accès en fonction de leur conformité à la politique.
- Clean Access Manager – console Web centralisée pour l'établissement des rôles, des contrôles, des règles et des politiques.
- Clean Access Agent (en option) – client léger à lecture seule qui améliore les fonctions d'évaluation des vulnérabilités et accélère le processus de remédiation.



Les caractéristiques du serveur dédié Cisco NAC

Intégration de l'authentification avec ouverture de session unique

Cisco NAC joue le rôle de proxy d'authentification pour la plupart des formes d'authentification puisqu'il intègre de manière native Kerberos, LDAP (Lightweight Directory Access Protocol), RADIUS, Active Directory, S/Ident et bien d'autres solutions encore. Afin de minimiser la gêne pour les utilisateurs finaux, Cisco NAC supporte l'ouverture de session unique pour les clients VPN, les clients sans fil et les domaines Windows Active Directory. Le contrôle d'accès à base de rôles permet à l'administrateur de gérer de multiples profils utilisateurs avec des niveaux de permission différents.

Description de la gamme Cisco NAC

Evaluation des vulnérabilités

Cisco NAC supporte l'analyse de tous les systèmes d'exploitation Windows, de Mac OS, des machines Linux et des équipements de réseau autres que les PC – consoles de jeu, PDA, imprimantes, téléphones IP, etc. Il effectue une analyse réseau et peut, si nécessaire, utiliser des outils d'analyse personnalisés. Cisco NAC peut vérifier n'importe quelle application identifiée par ses clés de registres, les services exécutés ou les fichiers systèmes.

Mise en quarantaine

Cisco NAC peut placer les machines non conformes en quarantaine pour éviter la propagation des infections tout en lui ouvrant un accès à des ressources de remédiation. La quarantaine peut s'effectuer sur un sous réseau de petite taille (type /30) ou sur un VLAN de quarantaine.

Mises à jour automatisées des politiques de sécurité

Les mises à jour automatiques des politiques de sécurité fournies par Cisco dans le cadre du service de maintenance logicielle standard permettent d'obtenir des politiques prédéfinies pour les critères d'accès réseau les plus courants, notamment les politiques qui vérifient les mises à jour critiques du système d'exploitation comme des signatures antivirus et antilogiciels espions des principaux produits du marché. Cette fonction réduit les frais de gestion pour l'administrateur réseau qui peut laisser au serveur Cisco NAC le soin de veiller à la mise à jour permanente des politiques de sécurité.

Gestion centralisée

La console de gestion Web du Cisco NAC permet à l'administrateur de définir les types d'analyse exigibles pour chaque rôle ainsi que les outils de remédiation nécessaire aux « réparations ». Une même console de gestion peut administrer plusieurs serveurs.

Remédiation et réparation

Les fonctionnalités de quarantaine du serveur dédié Cisco NAC donnent aux appareils un accès à des serveurs de remédiation qui peuvent leur fournir des correctifs et des mises à jour de système d'exploitation, des fichiers de définition de virus ou des solutions de sécurité pour points d'extrémité comme Cisco Security Agent. L'administrateur peut autoriser les remédiations automatiques grâce à l'option Cisco NAC Agent, initier le lancement automatique des mises à jour Windows ou fournir une liste de page Web contenant les instructions de remédiation.

Souplesse du déploiement

Cisco NAC offre le plus large éventail de modes de déploiement pour s'insérer aussi simplement que possible dans n'importe quel réseau. Il peut être installé en tant que passerelle IP virtuelle ou réelle, en périphérie ou au cœur du réseau, avec un accès client en couche 2 ou 3, et en bande ou hors bande par rapport au trafic réseau.

POUR PLUS D'INFORMATION

Pour toute information complémentaire, contactez votre représentant commercial ou visitez http://www.cisco.com/go/cca.

C45-350989-00 05/06