

Cisco NAC

La mise au point du réseau capable de se défendre tout seul

Description générale

Cisco® Network Admission Control (NAC) exploite au maximum l'infrastructure réseau pour limiter les dégâts occasionnés par les virus et les « vers ».

Grâce à Cisco NAC, l'entreprise peut fournir aux unités d'extrémité comme les PC, les PDA et les serveurs, un accès réseau qui respecte scrupuleusement les politiques de sécurité en place. Cisco NAC permet de refuser l'accès aux unités non conformes, de les placer en quarantaine ou de restreindre leur accès aux ressources informatiques.

Cisco NAC est la première étape du projet Cisco de réseau capable de se défendre tout seul – Cisco® Self-Defending Network – un système capable d'identifier et de prévenir les menaces de sécurité et de s'y adapter.

Introduction – Comment répondre à l'évolution des menaces de sécurité

Les virus et les vers qui interrompent la bonne marche des systèmes continuent de désorganiser les entreprises en faisant baisser leur productivité et en les contraignant à corriger en continu les failles de leurs systèmes de sécurité. La nature autoreproductible des attaques les plus récentes les rend particulièrement virulentes et dangereuses. Les solutions anti-virus existantes, qui reposent sur la reconnaissance de la signature de l'attaque, sont incapables de détecter et de neutraliser les virus inconnus et les attaques par déni de service qu'ils génèrent.

L'entreprise est fréquemment confrontée à des serveurs et des ordinateurs de bureau qui ne respectent pas sa politique de sécurité. Ces unités sont difficiles à détecter, à isoler et à nettoyer. La localisation et la mise en quarantaine de ces systèmes consomment beaucoup de temps et de ressources, et même lorsque les infections qu'ils propagent semblent avoir disparu du réseau d'entreprise, elles sont

susceptibles de réapparaître par la suite. Le problème est encore multiplié par la complexité des environnements de réseau modernes qui comprennent des types très variés :

- d'utilisateurs finaux – employés, constructeurs et sous-traitants
- de points d'extrémité – ordinateur de bureau dans l'entreprise ou à domicile, serveurs
- d'accès – filaire, sans fil, réseau privé virtuel (VPN) ou accès commuté

Cisco NAC s'interpose entre ces menaces évoluées et le réseau, en gérant la complexité de l'environnement et en offrant des progrès très nets par rapport aux technologies de sécurité ponctuelles qui se concentrent sur un serveur ou une station de travail plutôt que sur la disponibilité et la robustesse globale du réseau.

Description générale de Cisco NAC

Les dégâts générés par les virus et les vers ont montré dans toute sa réalité l'inadéquation des dispositifs actuels de sécurité. Cisco NAC offre une nouvelle solution complète qui permet aux organisations d'appliquer des politiques de correctifs logiciels sur les hôtes et de rediriger les systèmes non conformes et potentiellement vulnérables vers des environnements de quarantaine disposant de peu, voire d'aucun, accès au réseau. En associant les informations sur l'état de la sécurité des points d'extrémité avec les conditions d'admission au réseau, Cisco NAC permet aux organisations d'améliorer de manière considérable la sécurité de leurs infrastructures informatiques.

Cisco NAC accorde un accès au réseau aux unités d'extrémité – PC, serveurs ou PDA, par exemple – conformes et de confiance et le refuse aux unités non conformes.



La décision d'accorder cet accès peut reposer sur des informations comme l'état du logiciel anti-virus du point d'extrémité ou la version du correctif de son système d'exploitation.

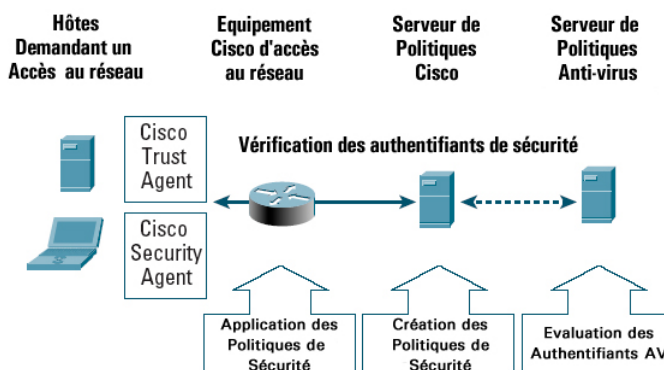


Figure 1 Cisco NAC

Cisco NAC dispose des composants suivants :

- *Cisco Trust Agent (CTA)* – Ce logiciel, qui réside sur un système d'extrémité, collecte les informations sur l'état de l'unité provenant de nombreux clients logiciels de sécurité – clients anti-virus, par exemple – et communique ces informations aux unités Cisco d'accès réseau chargées d'appliquer les contrôles d'admission. Cisco a fourni des licences de sa technologie CTA à ses partenaires anti-virus afin qu'ils puissent l'intégrer dans leurs produits clients logiciels de sécurité. La technologie CTA sera également intégrée à Cisco Security Agent pour faire appliquer les privilèges d'accès en fonction de la version du correctif du système d'exploitation du point d'extrémité. Cisco Security Agent (CSA), solution logicielle de protection de l'hôte dès le premier jour, évaluera la version, les correctifs et les informations de dépannage à chaud du système d'exploitation avant de les communiquer à Cisco trust agent. Les hôtes qui ne disposent pas des correctifs requis peuvent ne recevoir qu'un accès limité au réseau, et même en être exclus.
- *Unités d'accès réseau* – Les routeurs, les commutateurs, les points d'accès sans fil et les serveurs de sécurité dédiés appliquent la politique de contrôle d'admission au réseau. Ces unités exigent des « authentifiants » de sécurité hôte et relaient l'information aux serveurs de politique qui prennent les décisions de contrôle d'admission au réseau. Selon la politique définie par l'utilisateur, le réseau applique la décision appropriée de contrôle d'admission – autorisation, refus, quarantaine ou accès restreint.
- *Serveur de politiques* – Ce serveur évalue les informations de sécurité du point d'extrémité provenant des unités d'accès au réseau et détermine la politique d'accès qu'il convient de lui appliquer. Cisco Secure Access Control Server (ACS), serveur AAA (authentification, autorisation et administration) de type RADIUS, est le cœur du système de serveur de politiques. Il travaille en association avec les serveurs d'application de nos partenaires Cisco NAC qui fournissent des fonctionnalités plus puissantes de validation des authentifiants comme les serveurs de politiques anti-virus.
- *Système d'administration* – CiscoWorks VPN/Security Management Solution (VMS) dimensionne les éléments Cisco NAC tandis que CiscoWorks Security Information Manager Solution (SIMS) fournit les outils de contrôle et de reporting. Les partenaires Cisco NAC fournissent les solutions d'administration pour leurs logiciels de sécurité pour points d'extrémité.

Essentiellement, Cisco NAC tire le meilleur parti des investissements existants en matière d'infrastructure de réseau et de technologie de protection des hôtes en associant les deux fonctionnalités pour réaliser un système de contrôle d'admission au réseau. L'entreprise peut, par exemple, s'assurer que les éléments du réseau Cisco – routeurs, commutateurs, équipements sans fil ou serveurs de sécurité dédiés – contrôlent l'usage d'un logiciel anti-virus. De la sorte, Cisco NAC complète plus qu'il ne remplace les technologies classiques de sécurité déjà couramment utilisées – passerelle pare-feu, systèmes de protection contre les intrusions, authentification d'identité et sécurité des communications.



Cisco NAC en action

Cisco NAC est une solution souple et omniprésente capable d'assurer la protection de tous les systèmes informatiques connectés. Cisco NAC opère sur toutes les méthodes d'accès utilisées par les hôtes pour se connecter au réseau, y compris la commutation campus, les connexions filaires et sans fil, les liaisons de réseau WAN et LAN par routeur, les connexions IPSec (IP Security), l'accès à distance et les liaisons commutées.

Voici quelques exemples de déploiement de Cisco NAC :

- *Contrôle de conformité pour les succursales d'entreprise* – Cisco NAC permet de garantir la conformité des hôtes des succursales distantes ou des bureaux à domicile qui cherchent à se connecter aux ressources centralisées de l'entreprise, que ce soit par l'intermédiaire d'un réseau WAN privé ou d'un canal sécurisé sur le Web. Il effectue notamment des vérifications de conformité au niveau du routeur Cisco de la succursale ou sur celui du siège social de l'entreprise.
- *Protection des accès distants* – Cisco NAC permet de garantir que les ordinateurs des travailleurs distants ou mobiles disposent des versions les plus récentes du logiciel anti-virus et des correctifs du système d'exploitation avant de leur donner accès aux ressources de l'entreprise par l'intermédiaire de liaisons commutées, IPSec ou autres types d'accès VPN.
- *Protection du campus sans fil* – Cisco NAC vérifie les hôtes qui se connectent au réseau par une liaison sans fil afin de s'assurer qu'ils disposent des bons correctifs. Pour cette validation, il utilise le protocole 802.1x et procède à l'authentification de la station comme de l'utilisateur.
- *Accès au réseau campus et protection des centres de calcul* – Cisco NAC contrôle les ordinateurs et les serveurs du bureau et permet de s'assurer que ces unités sont conformes aux politiques de l'entreprise en matière d'anti-virus et de correctifs de système d'exploitation avant de leur accorder l'accès au réseau LAN. Il réduit ainsi le risque que les virus et les vers se propagent au sein de l'entreprise en élargissant le contrôle d'admission aux commutateurs de la couche 2.
- *Conformité extranet* – Cisco NAC peut servir à vérifier la conformité de chaque système qui tente d'obtenir un accès au réseau et pas uniquement ceux qui sont gérés par le service informatique. Cisco NAC permet de vérifier la conformité à la politique en matière d'anti-virus et de systèmes d'exploitation des hôtes, qu'ils soient gérés ou non par l'entreprise, y compris des systèmes des sous-traitants et des partenaires. Si le logiciel Cisco Trust Agent n'est pas présent sur l'hôte interrogé, une politique d'accès par défaut peut-être appliquée.

Les avantages de Cisco NAC

- *Amélioration considérable de la sécurité* – Cisco NAC permet de s'assurer que chaque hôte se conforme aux politiques les plus récentes de l'entreprise en matière d'anti-virus et de correctifs du système d'exploitation avant de lui accorder l'accès normal au réseau. Il peut isoler les hôtes vulnérables ou non conformes et leur accorder un accès restreint jusqu'à ce qu'ils exécutent le bon correctif ou qu'ils soient correctement protégés : il évite ainsi qu'ils deviennent la cible ou la source d'infections par virus ou par vers.
- *Rentabilisation de l'investissement de réseau et anti-virus* – Cisco NAC intègre et consolide la valeur des investissements dans l'infrastructure de réseau Cisco, la sécurité des points d'extrémité Cisco et la technologie anti-virus.
- *Evolutivité du déploiement* – Cisco NAC assure un contrôle d'accès complet sur toutes les méthodes d'accès utilisées par les hôtes pour se connecter au réseau et supporte également les scénarios multiconstructeurs. Si, par exemple, un employé dispose d'une solution anti-virus avec un logiciel Cisco Trust Agent, et qu'un sous-traitant utilise une autre solution anti-virus avec un logiciel Cisco Trust Agent, Cisco NAC permet de vérifier la conformité des deux systèmes et d'appliquer des politiques différentes en fonction de l'identité de l'utilisateur et de l'état de sécurité du point d'extrémité. Enfin, Cisco NAC peut définir des politiques d'accès différentes selon que l'hôte répond – autrement dit qu'il exécute Cisco Trust Agent – ou non.
- *Amélioration de la robustesse et de la disponibilité* – En associant les informations sur l'état de la sécurité des points d'extrémité avec les conditions d'admission au réseau, Cisco NAC permet à ses utilisateurs d'améliorer de manière considérable la sécurité de leurs infrastructures informatiques.



Disponibilité et utilisation

Cisco NAC sera disponible au cours du premier semestre 2004. A partir de sa commercialisation, tous les routeur Cisco communiqueront avec le logiciel Cisco Trust Agent pour fournir le contrôle d'admission au réseau. Les listes de contrôle d'accès (ACL) sur le routeur permettront de limiter les communications entre les hôtes non conformes et les autres systèmes du réseau – par exemple en ne permettant que les communications vers un serveur anti-virus pour permettre le téléchargement d'un fichier de mise à jour. Dès son lancement, Cisco NAC supportera les points d'extrémité sous Microsoft® Windows NT, XP et 2000.

« Les récentes infections virales et par vers ont rendu encore plus cruciale la nécessité d'empêcher les nœuds mal sécurisés de contaminer le réseau, et en ont fait une priorité absolue pour les entreprises modernes », déclare Mark Bouchard, directeur principal de la programmation chez META Group. « De nombreuses organisations ont montré leur capacité à bloquer les récentes attaques par vers aux frontières Internet de leur réseau. Elles sont toutefois encore victimes des « exploits » des pirates dès que leurs utilisateurs mobiles ou non-résidents connectent leurs PC infectés directement aux réseaux locaux internes. L'élimination de ce type de menaces passe par l'association du renforcement des politiques et de la technologie du contrôle d'admission au réseau. »

La première version de Cisco NAC satisfait aux exigences des deux tests de conformité les plus urgents – l'état du logiciel anti-virus et les informations relatives au système d'exploitation. Ceci englobe la version du logiciel anti-virus du constructeur, la version du moteur et les niveaux des fichiers de signature ainsi que le type, les correctifs et les dépannages à chaud du système d'exploitation. Dans un premier temps, Cisco NAC sera probablement utilisé en mode de contrôle : la conformité de l'hôte sera évaluée sans essayer de limiter l'accès réseau. Au cours de cette période, les systèmes non conformes pourront être, si nécessaire, mis à jour afin d'atteindre les niveaux de conformité requis.

Pour les versions suivantes de Cisco NAC, les commutateurs et les points d'accès sans fil Cisco seront en mesure de rediriger les hôtes non conformes vers des segments de réseau VLAN de quarantaine sur lesquels ne résideront que des serveurs de remédiation. Les versions suivantes élargiront le support de Cisco NAC aux serveurs de sécurité dédiés Cisco comme les pare-feu et les concentrateurs VPN.

Dans ses phases ultérieures, Cisco NAC assurera le contrôle dynamique des infections. Les points d'extrémité ainsi que les autres éléments systèmes conformes pourront alors signaler les utilisations abusives provenant des systèmes illégaux ou infectés au cours d'une attaque. Cette intelligence permettra d'isoler de manière dynamique les systèmes infectés du reste du réseau et de réduire de manière considérable la propagation des menaces dues aux virus, aux vers et à toute combinaison de ces méthodes.

Conclusion – un réseau capable de se défendre lui-même

Cisco NAC est une étape cruciale dans la mise au point du réseau capable de se défendre tout seul – Cisco® Self-Defending Network – initiative innovante de sécurité qui améliore de manière spectaculaire la capacité des réseaux à identifier et prévenir les menaces de sécurité et à s'y adapter. Le projet Cisco Self-Defending Network renforce considérablement la stratégie de Cisco pour l'intégration des services de sécurité sur l'ensemble des réseaux IP en fournissant de nouvelles méthodes de défense au niveau système contre les menaces de sécurité.

Pour plus d'informations

Pour plus d'informations, visitez

<http://www.cisco.com/go/selfdefend>



Siège social
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
États-Unis
www.cisco.com
Tél. : 408 526-4000
800 553-NETS (6387)
Fax : 408 526-4100

Siège Europe
Cisco Systems Europe
11, rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www.cisco.com
Tél. : 33 1 58 04 60 00
Fax : 33 1 58 04 61 00

Siège Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
États-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-883

Siège Asie/Pacifique
Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060, Australie
www.cisco.com
Tél. : +61 2 8448 7100
Fax : +61 2 9957 4350

Cisco Systems compte plus de 200 bureaux dans les pays suivants. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web Cisco.com à l'adresse www.cisco.com/go/offices.

Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • République populaire de Chine • Colombie • Costa Rica
Croatie • République tchèque • Danemark • Dubaï • Finlande • France • Allemagne • Grèce • Hong-Kong • Hongrie • Inde • Indonésie
Irlande • Israël • Italie • Japon • Corée • Luxembourg • Malaisie • Mexique • Pays-Bas • Nouvelle-Zélande • Norvège • Pérou • Philippines
Pologne • Portugal • Porto Rico • Roumanie • Russie • Arabie saoudite • Écosse • Singapour • Slovaquie • Slovénie • Afrique du Sud
Espagne • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Royaume-Uni • États-Unis • Venezuela • Vietnam • Zimbabwe

Copyright © 2001 Cisco Systems, Inc. Tous droits réservés. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems et le logo de Cisco Systems sont des marques déposées de Cisco Systems, Inc. ou de ses filiales aux États-Unis et dans certains autres pays. Tous les autres noms ou marques de fabrique mentionnés dans ce document ou site Web appartiennent à leurs propriétaires respectifs. L'utilisation du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société (0012R) 12/00 BW6904