Serveur dédié Cisco NAC

Le serveur Cisco® NAC, précédemment appelé Cisco Clean Access, est un Serveur de Contrôle d'Admission Réseau (Network Admission Control) facile à déployer 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 les équipements en réseau – ordinateurs portables ou fixes etc. – sont conformes aux politiques de sécurité de l'entreprise et « répare » les éventuelles vulnérabilités avant de leur permettre l'accès au réseau.

Description du Produit

Le serveur Cisco® NAC est une solution de bout en bout pour l'enregistrement des équipements informatiques et l'application des politiques du réseau qui permet à l'administrateur réseau d'authentifier, d'autoriser, d'évaluer et de corriger les machines avant de donner à leurs utilisateurs un accès au réseau. Ce produit évolué de sécurité de réseau :

- reconnaît les utilisateurs, leurs appareils et leurs rôles sur le réseau. Cette première étape intervient au point d'authentification, avant que d'éventuels codes malveillants puissent endommager le réseau.
- évalue si les machines sont en conformité avec les politiques de sécurité. Ces politiques peuvent varier en fonction du type d'utilisateur, du type d'équipement ou du système d'exploitation.
- applique les politiques de sécurité en bloquant, en isolant et en « réparant » les équipements non conformes. Ceux-ci sont redirigés vers une zone de quarantaine où une remédiation peut être effectuée selon les modalités définies par l'administrateur.

Le serveur dédié Cisco NAC peut effectuer une évaluation de posture de sécurité et une remédiation sur tous les équipements, quels que soient :

- le type d'appareil. Le serveur dédié Cisco NAC peut appliquer les politiques de sécurité sur tous les équipements en réseau, y compris sur les machines Windows, Mac ou Linux, les ordinateurs portables ou fixe, les ordinateurs de poche (PDA) et les équipements de l'entreprise comme les imprimantes et les téléphones IP.
- le propriétaire de l'appareil. Le serveur dédié Cisco NAC peut appliquer des politiques de sécurité aux systèmes appartenant à l'entreprise, à ses employés, à ses fournisseurs et ses invités.
- la méthode d'accès au réseau. Le serveur dédié Cisco NAC applique le contrôle d'admission aux appareils qui se connectent par les réseaux LAN, WLAN, WAN ou VPN.

La particularité du serveur dédié Cisco NAC est sa capacité à appliquer les politiques dans tous les scénarios opérationnels sans avoir besoin de produit spécifique ni de modules supplémentaires

Caractéristiques et avantages

Essentiellement, les réseaux protégés par le serveur dédié Cisco NAC bénéficient des avantages suivants :

- ils restent sains car la conformité est une condition d'accès.
- ils sont protégés de manière proactive contre les virus, les vers, les logiciels espions et les autres applications malveillantes.
- les vulnérabilités des équipements utilisateurs qui y accèdent sont minimales grâce à l'évaluation périodique et aux outils de remédiation.
- ils sont nettement moins coûteux à gérer car les processus de « réparation » et de mise à jour des équipements utilisateurs sont automatisés.

Intégration de l'authentification avec ouverture de session unique

Le serveur dédié 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, le serveur dédié 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.

Evaluation des vulnérabilités

Le serveur dédié Cisco NAC supporte l'analyse de toutes les machines et systèmes d'exploitation Windows, Mac OS et 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. Le serveur dédié Cisco NAC peut vérifier n'importe quelle application identifiée par ses clés de registres, les services exécutés ou les fichiers systèmes.

Mise en quarantaine

Le serveur Cisco NAC peut placer les machines non conformes en quarantaine pour éviter la propagation des infections tout en leur proposant 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 serveur Cisco NAC permet à l'administrateur de définir les types d'analyse exigibles pour chaque rôle ainsi que les outils de remédiation nécessaires aux « réparations ». Une même console de gestion peut administrer plusieurs serveurs.

Remédiation et réparation

La quarantaine donne 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 permettre la remédiation automatique grâce à un agent en option, ou définir une série d'instructions de remédiation.

Souplesse du déploiement

Le serveur dédié 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 ligne ou hors bande par rapport au trafic réseau.

Modes de déploiement

Le serveur dédié Cisco NAC peut être déployé de plusieurs manières pour s'adapter au réseau de l'utilisateur. Le Tableau 1 décrit les différentes options de déploiement :

Tableau 1. Options de déploiement du serveur dédié Cisco NAC

Modèle de déploiement	Options
Mode Trafic passant	• Passerelle virtuelle (mode ponté) • Passerelle IP réelle / passerelle NAT (mode routé)
Modèle de déploiement physique	• Périphérie • Central
Mode d'accès client	• Couche 2 (client est adjacent au serveur Cisco Clean Access) • Couche 3 (client est à plusieurs sauts du serveur Cisco Clean Access)
Modèle flux de trafic	• Hors bande (le serveur Cisco Clean Access est toujours en ligne avec le trafic utilisateur) • Hors bande (le serveur Cisco Clean Access n'est en ligne que pendant les procédures d'authentification, d'évaluation de posture de sécurité et de remédiation)

Architecture produit

Le serveur dédié Cisco NAC comprend les composantes suivantes :

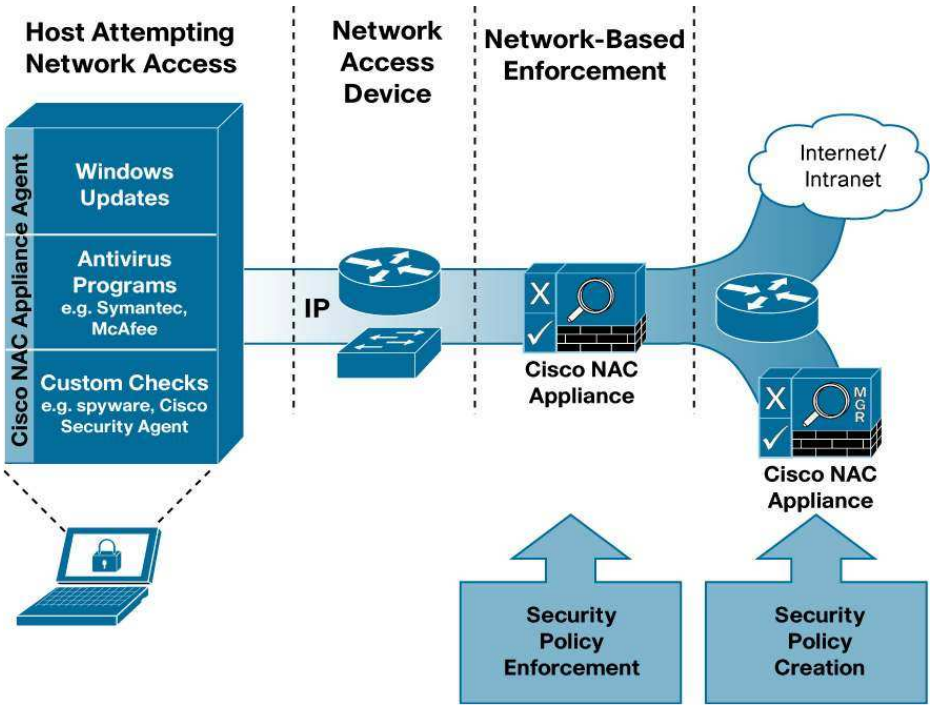
Le serveur Cisco Clean Access – le serveur qui procède à l'évaluation des points d'extrémité et leur attribue des privilèges d'accès en fonction de leur conformité à la politique. L'utilisateur est bloqué au niveau de la couche de port et ne peut pas accéder au réseau sécurisé tant qu'il n'a pas passé l'inspection avec succès. Le serveur Cisco Clean Access est disponible en cinq tailles selon le nombre d'utilisateurs simultanément en ligne : 100, 250, 500, 1500 et 2500 utilisateurs. Une même entreprise peut exploiter des serveurs de tailles différentes – par exemple, le siège social aura besoin d'un serveur Cisco Clean Access de 1500 utilisateurs tandis qu'une agence de la même société pourra se contenter d'un serveur de 100 utilisateurs.

Cisco Clean Access Manager – console Web centralisée pour l'établissement des rôles, des contrôles, des règles et des politiques. La console Cisco Clean Access Manager est disponible en trois tailles : Cisco Clean Access Lite Manager gère jusqu'à trois serveurs Cisco Clean Access, Cisco Clean Access Standard Manager jusqu'à 20 serveurs Cisco Clean Access et Cisco Clean Access Super Manager jusqu'à 40 serveurs Cisco Clean Access.

Cisco Clean Access Agent – client léger à lecture seule qui améliore les fonctions d'évaluation de la posture de sécurité et accélère le processus de remédiation. Les agents Cisco Clean Access sont des options fournies gratuitement.

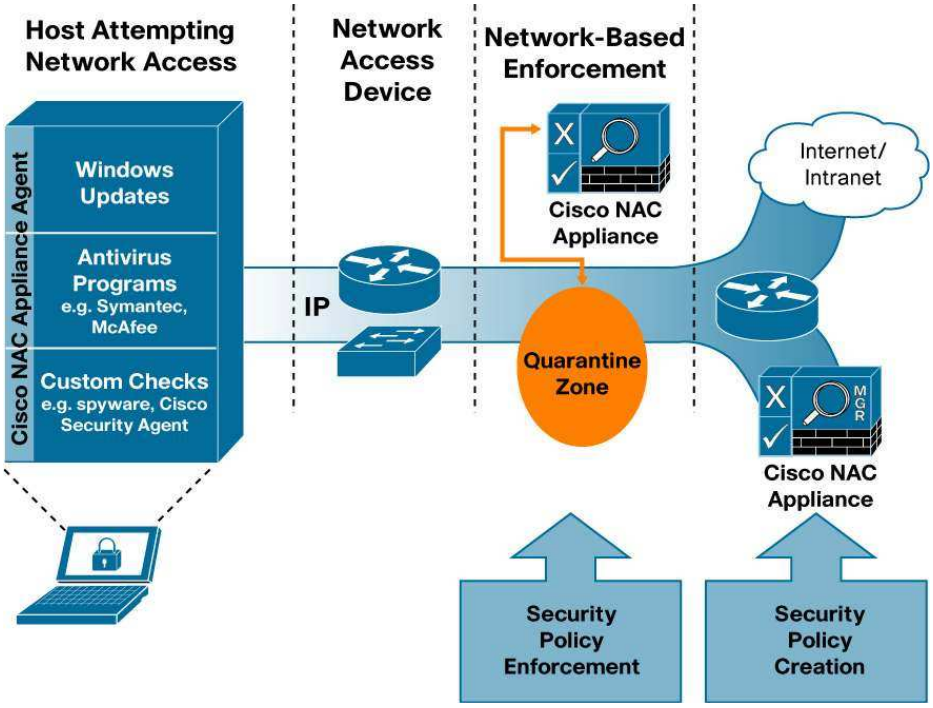
La Figure 1 présente un diagramme logique pour le déploiement en ligne d'un serveur dédié Cisco NAC. Cette configuration accepte n'importe quel point d'accès sans fil 802.11 ainsi que les points d'accès Cisco Aironet®. Le mode en ligne est également indiqué pour le trafic VPN.

Figure 1. Architecture en ligne pour un serveur Cisco NAC



La Figure 2 présente un diagramme logique pour le déploiement hors bande d'un serveur dédié Cisco NAC. Dans ce mode, le serveur Cisco Clean Access n'est en ligne que pendant les procédures d'authentification, d'évaluation de posture de sécurité et de remédiation Une fois que l'appareil utilisateur a réussi à ouvrir une session, son trafic traverse directement le port de commutation.

Figure 2. Architecture hors bande pour un serveur Cisco NAC



Caractéristiques techniques

Cisco NAC est désormais disponible en tant que « véritable » serveur dédié, ce qui signifie qu'il n'est plus nécessaire de commander séparément les composantes logicielles et matérielles. A l'appui de cette évolution, Cisco présente trois nouvelles options matérielles qui forment les bases du serveur Clean Access et de Clean Access Manager. Le Tableau 2 donne la liste des caractéristiques techniques des versions matérielles du serveur dédié Cisco NAC.

Tableau 2. Caractéristiques matérielles du serveur dédié Cisco

	Serveur dédié Cisco NAC 3310	Serveur dédié Cisco NAC 3350	Serveur dédié Cisco NAC 3390
Produits	• Serveur Cisco Clean Access pour 100, 250 et 500 utilisateurs • Cisco Clean Access Lite Manager	• Serveur Cisco Clean Access pour 1500, 2500 et 3500 utilisateurs • Cisco Clean Access Standard Manager	Cisco Clean Access Super Manager
Processeur	Intel Xeon Dual-core 2,33 GHz	Intel Xeon Dual-core 3,0 GHz	Double Intel Xeon Dual-core 3,0 GHz
Mémoire	1 Go PC2-4200 (2 x 512 Mo)	2 Go PC2-5300 (2 x 1Go)	4 Go PC2-5300
Bus mémoire	1333 MHz FSB	1333 MHz FSB	1333 MHz FSB
Contrôleur	Contrôleur RAID SATA intégré	Contrôleur Smart Array E200i	Contrôleur Smart Array E200i
Disque dur	80 Go NPH SATA	2 x 72 Go RAID SFF SAS	4 x 72 Go RAID SFF SAS
Supports amovibles	Lecteur CD/DVD-ROM	Lecteur CD/DVD-ROM	Lecteur CD/DVD-ROM
Connectivité réseau			
Carte NIC (Network Interface Card) Ethernet	• 2 x NIC 5708 10/100/1000 Broadcom intégrées • 2 x NIC Intel e1000 Gigabit (PCI-X)	• 2 x NIC 5721 10/100/1000 Broadcom intégrées • 2 x NIC Intel e1000 Gigabit (PCI-X)	• 2 x NIC 5721 10/100/1000 Broadcom intégrées • 2 x NIC Intel e 1000 Gigabit (PCI-X)
Support de câble 10BASE-T	Paire torsadée non blindée de catégorie (Cat) 3, 4 ou 5 jusqu'à 100 m	Paire torsadée non blindée de Cat 3, 4 ou 5 jusqu'à 100 m	Paire torsadée non blindée de Cat 3, 4 ou 5 jusqu'à 100 m
Support de câble 10/100/1000BASE-TX	Paire torsadée non blindée de Cat 5 jusqu'à 100 m	Paire torsadée non blindée de Cat 5 jusqu'à 100 m	Paire torsadée non blindée de Cat 5 jusqu'à 100 m
Carte accélératrice SSL (Secure Sockets Layer)	Aucune	Cavium CN1120-NHB-E	Cavium CN1120-NHB-E
Interfaces			
Ports séries	1	1	1
Ports USB 2.0	4 (deux à l'avant, deux à l'arrière)	4 (un à l'avant, un interne, deux à l'arrière)	4 (un à l'avant, un interne, deux à l'arrière)
Port clavier	1	1	1
Port vidéo	1	1	1
Port souris	1	1	1
Port SCSI externe	Aucun	Aucun	Aucun
Unité système			
Compacité	Montage sur rack 1 RU	Montage sur rack 1 RU	Montage sur rack 1 RU
Poids	15,87 kg à pleine configuration	15,87 kg à pleine configuration	15,87 kg à pleine configuration
Dimensions	4,32 x 42,62 x 70,49 cm	4,32 x 42,62 x 70,49 cm	4,32 x 42,62 x 70,49 cm
Alimentation	650 W autocommutée, PFC	700 W double (redondante)	700 W double (redondante)
Ventilateurs	6, non remplaçables à chaud,	9, redondants	9, redondants
Emissions thermiques	742 kcal/h (2910 BTU/h) à 120 VAC; 732 kcal /h (2870 BTU/h) à 240 VAC	742 kcal/h (2910 BTU/h) à 120 VAC; 732 kcal /h (2870 BTU/h) à 240 VAC	742 kcal/h (2910 BTU/h) à 120 VAC; 732 kcal /h (2870 BTU/h) à 240 VAC

Bien que, en mode en bande, le serveur dédié Cisco NAC supporte toutes les infrastructures de réseau, le mode hors bande communique avec les commutateurs à l'aide du protocole SNMP (Simple Network Management Protocol).

Pour connaître la liste la plus récente des commutateurs supportés, visitez HYPERLINK "http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008075fff6.html" http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008075fff6.html. Cette liste est fréquemment mise à jour.

Configuration système nécessaire

L'option Cisco Clean Access Agent est compatible avec les systèmes dont les caractéristiques sont données dans le Tableau 3.

Tableau 3. Configuration système minimale pour Cisco Clean Access Agent

Fonctionnalité	Configuration minimale
Système d'exploitation supporté	Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows ME, Mac OS X (authentification seulement)
Espace disque	10 Mo minimum d'espace libre sur le disque dur
Matériel	Pas de configuration matérielle minimale (compatible avec différentes machines clientes)

Le serveur dédié Cisco NAC supporte également l'ouverture de session unique pour les utilisateurs sans fil et distants qui utilisent certains clients Ipsec (IP Security) VPN et WebVPN. La liste de ces clients est donnée dans le Tableau 4 :

Tableau 4. Composants VPN et Sans fil compatibles avec l'ouverture de session unique

Fonctionnalité	Configuration minimale
Contrôleurs WLAN CISCO	–
Serveurs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500	• VPN SSL Cisco (Tunnel) • Client VPN Cisco IPsec
Modules de services Cisco WebVPN pour les commutateurs de la gamme Cisco Catalyst® 6500 et les routeurs de la gamme Cisco 7600	
Concentrateurs de la gamme Cisco VPN 3000	
Serveurs de sécurité dédiés Cisco PIX ®	

Le serveur Cisco est préconfiguré pour effectuer des contrôles de politiques sur plus de 300 applications de 50 constructeurs. Cette liste est constamment actualisée. Pour connaître la liste la plus récente des applications supportées (sous « Cisco NAC Appliance Supported AV/AS Product List »), visitez HYPERLINK http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

Note : Les différents types de contrôles ne sont pas supportés pour tous les produits et certains constructeurs ne supportent pas Windows 9x. En plus des contrôles préconfigurés, le client dispose d'un accès intégral au moteur de règles du serveur Cisco NAC et peut créer ses propres contrôles ou ses propres règles pour n'importe quelle application tierce.

Maintenance et assistance technique

Cisco Systems propose une large gamme de programmes de services pour que ses clients puissent réussir plus vite. Le succès de ces programmes de services innovants est assuré grâce à une combinaison unique de personnes, de processus, d'outils et de partenaires qui maximisent la satisfaction de nos clients. Cisco Services vous aide à protéger votre investissement de réseau, à optimiser son exploitation et à le préparer aux nouvelles applications afin d'en étendre l'intelligence et d'accroître le succès de votre activité. Pour plus d'informations sur Cisco Services, consultez HYPERLINK "http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html" Cisco Technical Support Services ou Cisco Advanced Services. Pour consulter les informations relatives à la garantie, visitez http://www.cisco.com/en/US/products/prod_warranties_item09186a00805f005b.html.

Pour consulter les informations relatives aux licences, visitez http://www.cisco.com/en/US/products/ps6128/prod_pre_installation_guide09186a008073136b.html.

Pour plus d'informations

Pour plus d'informations sur le serveur dédié Cisco NAC, http://www.cisco.com/go/nac/appliance ou contactez votre Responsable de compte local.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

Printed in USA C78-348585-04 5/07

