

Symantec™ Network Access Control

Conformité totale des terminaux

Présentation

Symantec Network Access Control est une solution de contrôle d'accès complète et globale qui permet de contrôler de manière efficace et sûre l'accès aux réseaux de l'entreprise tout en s'intégrant aux infrastructures de réseau existantes. Quel que soit le mode de connexion des terminaux au réseau, Symantec Network Access Control détecte et évalue le statut de conformité de chaque terminal, octroie les droits d'accès appropriés, offre des fonctionnalités permettant de résoudre les problèmes si nécessaire, et surveille en permanence les changements d'état de conformité des terminaux. Les entreprises bénéficient ainsi d'une réduction considérable des coûts liés aux incidents informatiques et de meilleurs niveaux de conformité aux politiques internes de sécurité.

Avec Symantec Network Access Control, le déploiement et la gestion du contrôle d'accès au réseau deviennent un objectif réalisable sur le plan technique aussi bien que sur le plan économique.

Autorisation au niveau des terminaux, et pas seulement à celui des utilisateurs

Dans les environnements informatiques d'aujourd'hui, les entreprises et les administrateurs réseau doivent relever un défi de taille : fournir l'accès aux ressources d'entreprise à des utilisateurs toujours plus nombreux. Et cette population se diversifie. Aujourd'hui, employés sur site et à distance, invités, sous-traitants et autres employés temporaires doivent tous accéder au réseau. Jamais encore le maintien de l'intégrité des environnements réseau n'avait semblé tâche aussi ardue. En effet, à l'heure actuelle, il n'est plus acceptable de fournir un accès réseau sans vérification. Compte tenu de l'explosion du nombre des terminaux et de leur diversification, les entreprises

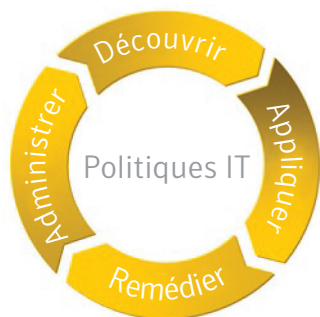
doivent pouvoir vérifier leur état et leur évolution, avant la connexion aux ressources, puis en continu après la connexion. Symantec Network Access Control permet de s'assurer que les terminaux sont en conformité avec la politique informatique en vigueur avant de les autoriser à se connecter aux réseaux LAN, WAN, WLAN ou VPN de l'entreprise.

Avantages clés

Les entreprises qui déploient Symantec Network Access Control en retirent des avantages concrets à plusieurs niveaux :

- Diminution de la propagation de codes malveillants, tels que virus, vers, logiciels espions et autres formes de logiciels criminels
- Profil de risque réduit grâce au contrôle accru des terminaux gérés et non gérés qui accèdent au réseau de l'entreprise
- Plus grande disponibilité du réseau et réduction des interruptions de service pour les utilisateurs finaux
- Information sur la conformité organisationnelle vérifiable grâce aux données de conformité des terminaux obtenues en temps réel
- Réduction du coût total de possession grâce à une architecture de gestion centralisée
- Vérification du bon fonctionnement des investissements de sécurité, tels qu'antivirus et pare-feu clients
- Intégration transparente avec Symantec™ AntiVirus™ Advanced Endpoint Protection

Principales fonctionnalités



Processus de Symantec Network Access Control

Processus de contrôle des accès réseau

Le contrôle des accès réseau est un processus qui impose la nécessité de couvrir tous les types de terminaux et tous les types de réseaux. Il débute avant la connexion au réseau et se poursuit pendant toute la durée de la connexion. Comme tous les processus de l'entreprise, il fonde ses évaluations et ses actions sur des politiques.

Le processus de contrôle des accès réseau comprend quatre étapes :

- 1. Détecter et évaluer les terminaux.** Cette étape intervient dès la demande de connexion des terminaux au réseau, avant leur accès aux ressources. Grâce à l'intégration à l'infrastructure réseau existante et à l'utilisation d'un logiciel agent intelligent, les administrateurs réseau ont la certitude que les nouveaux périphériques qui se connectent au réseau sont évalués selon des exigences minima en matière de politique informatique.
- 2. Octroyer l'accès au réseau.** L'accès total au réseau n'est accordé qu'une fois que les systèmes ont été évalués et qu'il est établi qu'ils sont en conformité avec la politique informatique. Les systèmes qui ne sont pas conformes ou qui ne répondent pas aux exigences minimales de l'entreprise sont mis en quarantaine avec un accès limité au réseau, ou pas d'accès du tout.

3. Corriger les terminaux non conformes. La fonction de remédiation automatique des terminaux non conformes permet aux administrateurs de les mettre rapidement en conformité et de modifier en conséquence l'accès au réseau. Les administrateurs ont deux possibilités : soit automatiser totalement le processus de correction, qui est alors entièrement transparent pour l'utilisateur final, soit fournir des informations à l'utilisateur pour qu'il réalise lui-même l'opération manuellement.

4. Surveiller la conformité de manière proactive. Le respect des politiques est l'affaire de tous les instants. C'est pour cela que Symantec Network Access Control surveille activement, selon une périodicité définie par l'administrateur, l'évolution de tous les terminaux en matière de conformité. Ainsi, si le statut de conformité d'un terminal vient à changer, les privilèges d'accès réseau du terminal changent eux aussi.

Couverture omniprésente des terminaux

Les réseaux regroupent les systèmes d'entreprise nouveaux et originaux, les systèmes de sous-traitants, les systèmes invités, les kiosques publics, les systèmes de partenaires commerciaux et d'autres systèmes inconnus. Les administrateurs n'exercent souvent que peu de contrôle, sur la gestion de beaucoup de ces terminaux, alors qu'ils doivent absolument garantir la sécurité et la disponibilité du réseau. Symantec Network Access Control permet aux entreprises d'appliquer des processus de contrôle d'accès réseau aux terminaux, que ces derniers soient administrés ou non, originaux ou nouveaux, connus ou inconnus.

Déployable sur n'importe quel réseau

L'utilisateur type se connecte au réseau d'entreprise par des méthodes d'accès multiples. De ce fait, les administrateurs doivent avoir la possibilité d'appliquer de façon homogène des contrôles et des évaluations quel que soit le type de connexion. Solution de contrôle d'accès réseau

Fiche technique : Sécurité des terminaux Symantec Network Access Control

parmi les plus matures du marché, Symantec Network Access Control permet aux administrateurs réseau d'appliquer la conformité aux infrastructures réseaux existantes sans que des mises à niveau de l'équipement réseau soient nécessaires.

Qu'elles utilisent l'un des Symantec Network Access Control Enforcers (qui s'intègrent directement au réseau), l'option de mise en quarantaine spécifique à l'hôte (ne nécessitant aucune intégration réseau), ou un agent temporaire intégré dans votre environnement d'application Web, les entreprises ont les moyens de s'assurer que les utilisateurs aussi bien que les terminaux sont conformes, au point d'accès, avec le réseau de l'entreprise.

Architecture de Symantec Network Access Control

L'architecture de Symantec Network Access Control inclut trois composants principaux : la gestion des politiques, l'évaluation des terminaux et la mise en quarantaine sur le réseau. Ces trois composants collaborent comme une solution unique sans que leur fonctionnement dépende d'éléments externes.

Gestion et reporting centralisés des politiques

Pour qu'une solution, quelle qu'elle soit, fonctionne bien, une console d'administration est absolument nécessaire. Symantec Endpoint Protection Manager offre une console basée sur la technologie Java™ pour créer, déployer, gérer et analyser l'activité de l'agent et de l'Enforcer. Suffisamment évolutif pour s'adapter aux environnements les plus exigeants au monde, le gestionnaire de politiques assure le contrôle granulaire de toutes les tâches administratives au sein d'une architecture hautement disponible.

Evaluation des terminaux

Le contrôle des accès réseau protège le réseau contre les codes malveillants et contre les menaces liées aux terminaux inconnus ou non autorisés, mais il vérifie également que les terminaux qui se connectent au réseau sont configurés de manière à être protégés des attaques perpétrées en ligne. Quel que soit l'objectif, le processus commence par une évaluation du terminal. Bien que la présence d'antivirus, d'antispyware et l'installation de correctifs soient quelques-unes des exigences minimales pour autoriser l'accès réseau, la plupart des entreprises vont rapidement au-delà de ces minima après le déploiement initial du contrôle d'accès réseau.

Symantec Network Access Control propose trois technologies d'évaluation distinctes pour déterminer la conformité des terminaux.

- **Agents permanents.** Les systèmes appartenant à l'entreprise et les autres systèmes gérés font appel à un agent installé par l'administrateur pour déterminer le statut de conformité. Cet agent vérifie la présence d'antivirus, d'antispyware et l'installation de correctifs, ainsi que des caractéristiques complexes du statut système telles que les entrées de registre, les processus en cours d'exécution et les attributs de fichiers. Les agents permanents fournissent les informations de conformité système les plus approfondies, les plus précises et les plus fiables, tout en offrant les fonctionnalités de correction et de réparation les plus flexibles.
- **Agents temporaires.** Pour les périphériques ou systèmes n'appartenant pas à l'entreprise et qui ne sont pas gérés par les administrateurs, des agents Java sont délivrés à la demande et sans privilèges administratifs afin d'évaluer la conformité des terminaux. A la fin de la session, ces agents s'effacent automatiquement du système.

- **Analyse de vulnérabilité à distance.** Cette technologie fournit aux équipements de mise en quarantaine Symantec Network Access Control des informations de conformité d'un poste à partir du résultat d'analyse de vulnérabilité effectuée à distance sans privilège du Symantec Network Access Control Scanner. L'analyse à distance étend les fonctionnalités de collecte des informations aux systèmes pour lesquels aucune technologie agent n'est installée (postes non gérés).

Mise en quarantaine

L'évolution de l'environnement réseau de chaque entreprise étant unique, aucune méthode de mise en quarantaine n'est en mesure de contrôler efficacement à elle seule l'accès à tous les points du réseau. Les solutions de contrôle d'accès réseau doivent être suffisamment flexibles pour pouvoir intégrer plusieurs méthodes de mise en quarantaine dans l'environnement existant sans augmenter la charge de gestion et de maintenance. Symantec Network Access Control vous permet de choisir la méthode de mise en quarantaine la mieux adaptée à chaque partie de votre réseau sans augmenter la complexité opérationnelle ni le coût. Chaque méthode de mise en quarantaine est disponible sous forme logicielle ou en tant que composant intégré dans un boîtier.

- **LAN Enforcer 802.1X** est une solution de proxy RADIUS 802.1X qui fonctionne avec les commutateurs des principaux fournisseurs prenant en charge la norme 802.1X. Le LAN Enforcer peut s'intégrer dans une architecture de gestion d'identité AAA existante authentifiant les utilisateurs et terminaux, ou agir en tant que solution RADIUS indépendante pour les environnements ne nécessitant que la validation de la conformité des terminaux. Le LAN Enforcer octroie l'accès aux ports des commutateurs en fonction des résultats de l'authentification des terminaux connectés.

- **DHCP Enforcer** est déployé en ligne entre les terminaux et l'infrastructure de service DHCP existante, et joue le rôle de proxy DHCP. Des baux DHCP restrictifs sont assignés à tous les terminaux assujettis jusqu'à ce que la conformité aux politiques soit vérifiée. Un nouveau bail DHCP est alors assigné au terminal. L'intégration de DHCP Enforcer au plug-in Microsoft® DHCP Server permet le déploiement rapide du contrôle d'accès réseau sans avoir à déployer des périphériques supplémentaires.
- **Gateway Enforcer** est un dispositif de mise en quarantaine en ligne utilisé aux points de congestion du réseau. Il contrôle les flux du trafic en se basant sur la conformité aux politiques des terminaux distants. Que le point de congestion se situe en périphérie, comme les liaisons WAN ou les VPN, ou sur des segments internes accédant à des systèmes d'entreprise critiques, Gateway Enforcer assure un contrôle efficace de l'accès aux ressources et fournit des services de remédiation.
- La **mise en quarantaine automatique** s'appuie sur les capacités de pare-feu personnel intégrées à Symantec Protection Agent pour ajuster les politiques locales des agents suivant le statut de conformité des terminaux. Cela permet aux administrateurs de contrôler les accès à n'importe quel réseau, à l'intérieur comme à l'extérieur du réseau de l'entreprise, pour des périphériques tels que les ordinateurs portables qui se connectent régulièrement à plusieurs réseaux différents.

Cisco Network Admission Control et Microsoft Network Access Protection

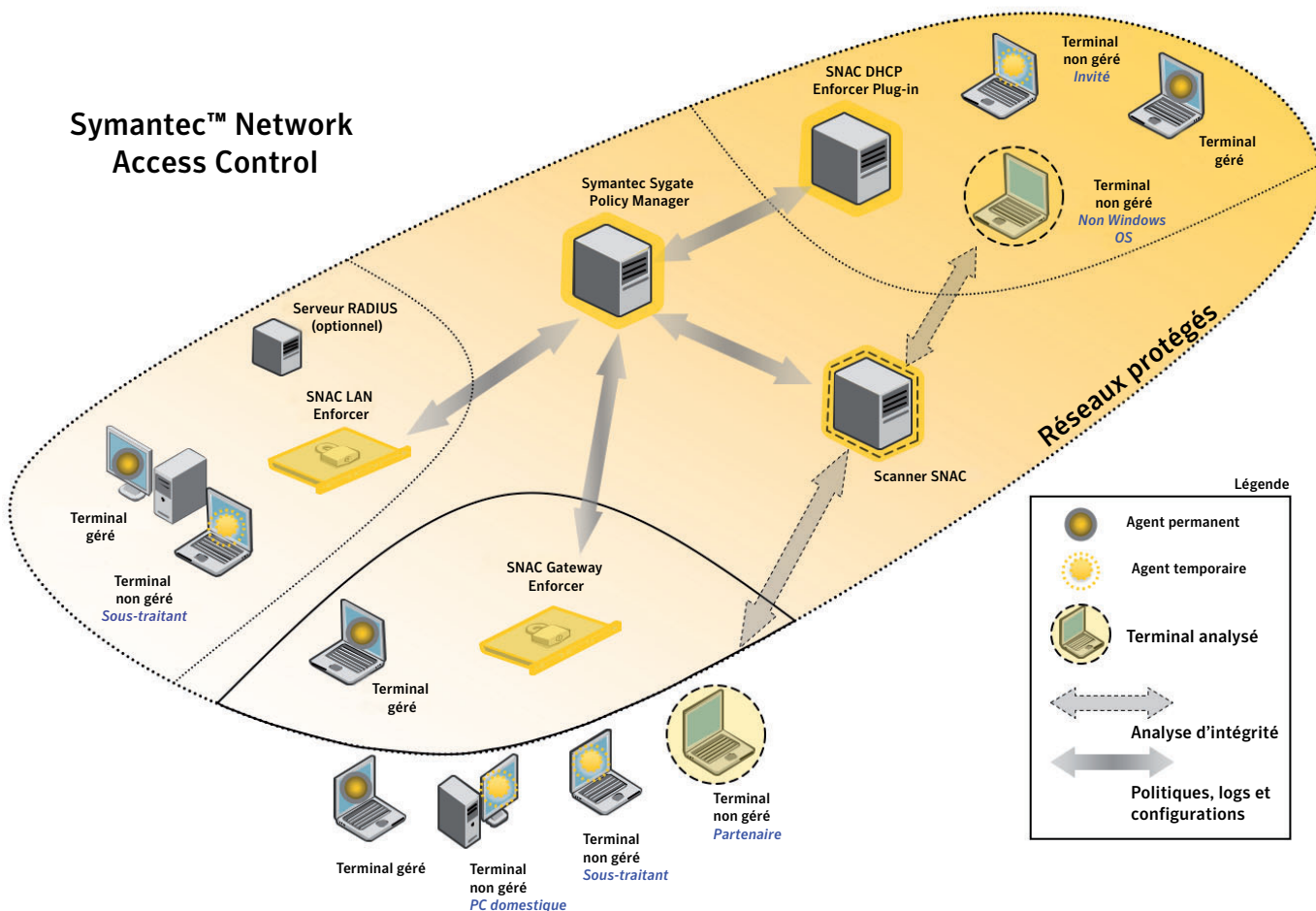
Symantec Network Access Control fournit des fonctionnalités de contrôle de bout en bout sans nécessiter de solutions externes, et s'intègre avec d'autres technologies de contrôle d'accès réseau dont il contribue à renforcer l'efficacité. Les administrateurs sécurité sont ainsi assurés de disposer d'une couverture et d'un contrôle complets quel que soit la méthodologie de mise en quarantaine.

Services de support

Symantec fournit toute une panoplie de services de consulting, de formations techniques et de support pour guider les entreprises dans les phases de migration, de déploiement et de gestion de Symantec Network Access Control, et pour les aider à tirer le meilleur profit de leur investissement. Pour les entreprises qui souhaitent externaliser la surveillance et la gestion de la sécurité, Symantec propose également, avec Managed Security Services, des services de supervision de la sécurité qui garantissent une protection en temps réel.

Famille de produits Symantec Network Access Control

	Symantec Network Access Control	Symantec Network Access Control Starter Edition
Mise en quarantaine		
LAN 802.1x	X	
DHCP	X	
Passerelle	X	X
Mise en quarantaine automatique	X	X
Evaluation des terminaux		
Agent permanent	X	X
Agent temporaire	X	
Analyse de la vulnérabilité à distance	X	



Configuration système requise

Plates-formes prises en charge

Symantec Endpoint Protection Manager

- Microsoft® Windows® 2003 (32 bits et 64 bits)
- Microsoft Windows XP (32 bits)
- Microsoft Windows 2000—SP3 et ultérieur (32 bits)

Symantec Endpoint Protection Manager Console

- Microsoft Vista® (32 bits et 64 bits)
- Microsoft Windows 2003 (32 bits et 64 bits)
- Microsoft Windows XP (32 bits et 64 bits)
- Microsoft Windows 2000—SP3 et ultérieur (32 bits)

Symantec Network Access Control client

Système d'exploitation :

- Windows 2000 Professionnel
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows XP Edition familiale ou Professionnel
- Windows XP Tablet Edition
- Windows Server 2003 Standard ou Enterprise
- Mac OS X 10.4 ou version ultérieure

Symantec Network Access Control Scanner

Système d'exploitation :

- Windows 2000 Server SP4
- Windows 2003 Server SP1

Processeur nécessaire (minimum) : Intel® Pentium® 4 à 1,8 GHz

1 Go de RAM minimum

1 Go d'espace disque libre

Internet Explorer® 5.5 ou ultérieur - Windows 2000 Professional

Symantec Network Access Control Enforcer 6100 Series

Options du boîtier de base (Passerelle, LAN et DHCP)

Nombre de châssis	1
Dimensions	1.68" x 17.60" x 21.5"
Processeur	1 2.8-Ghz Intel Pentium 4 processor
Mémoire	1 GB
Stockage	1 160-GB (SATA)

Options du boîtier Fail Open (Passerelle, LAN et DHCP)

Nombre de châssis	1
Dimensions	1.68" x 17.60" x 21.5"
Processeur	1 2.8-Ghz Intel Pentium 4 processor
Mémoire	1 GB
Stockage	1 160-GB (SATA)

Option de plug-in Microsoft DHCP Server (s'installe directement sur les serveurs Microsoft DHCP, éliminant la nécessité d'un DHCP Enforcer externe)

Fiche technique : Sécurité des terminaux Symantec Network Access Control

Pour plus d'informations

Rendez-vous sur notre site Web :

www.symantec.com/endpoint

Contactez un spécialiste produit en dehors des Etats-Unis

Pour connaître les coordonnées des bureaux dans un pays spécifique, visitez notre site Web.

A propos de Symantec

Leader mondial dans le domaine des solutions logicielles d'infrastructure, Symantec permet aux entreprises et aux particuliers d'avoir confiance dans le monde connecté. Symantec aide ses clients à protéger leurs infrastructures, informations et interactions en proposant des solutions logicielles et des services ayant pour but de réduire les risques en matière de sécurité, disponibilité, conformité et performances. L'entreprise Symantec est présente dans plus de 40 pays à travers le monde.

Des informations supplémentaires sont disponibles à l'adresse www.symantec.com/fr

Symantec Dublin

Ballycoolin Business Park

Blanchardstown

Dublin 15

Ireland

Phone: +353 1 803 5400

Fax: +353 1 820 4055

