Cisco

Network Admission Control

Cisco Systems, Inc.
11, rue Camille Desmoulins
92310 Issy Les Moulineaux Cedex

Tél. **01.58.04.60.00** Télécopie **01.58.04.61.00**

Pourquoi Cisco NAC ?

L'entreprise est fréquemment confrontée à des serveurs et des ordinateurs de bureau qui ne respectent pas les politiques de sécurité internes. De telles 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 de l'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 de nets progrès 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.

Présentation de Cisco Network Admission Control

Les dégâts générés par les virus et les vers montrent l'inadéquation des dispositifs actuels de sécurité à la réalité des menaces. Cisco Network Admission Control offre une nouvelle approche qui permet aux entreprises d'appliquer de façon directive des politiques de correctifs logiciels sur les postes de travail et qui permet d'isoler les systèmes non conformes et potentiellement vulnérables dans des zones de quarantaine disposant de peu, voire d'aucun accès au réseau. En associant les informations sur l'état de la sécurité des postes avec les conditions d'admission au réseau, Cisco Network Admission Control permet aux entreprises d'améliorer de manière considérable la sécurité de leurs systèmes d'informations.

Cisco Network Admission Control tire le meilleur profit des investissements existants en matière d'infrastructures de réseau et de technologie de protection des postes 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 Network Admission Control 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.

Remarque :

Cisco NAC existe sous deux formes :

- NAC *Appliance* : plus connue sous le nom Cisco Clean Access. C'est une architecture centralisée qui s'appuie sur un boîtier (CCA server) qui s'ajoute à l'infrastructure.
- NAC *Framework* : architecture distribuée qui fait intervenir tous les équipements du réseau.

Cisco Network Admission Control accorde un accès au réseau aux systèmes d'extrémité – PC, serveurs ou PDA, par exemple – conformes et de confiance et le refuse aux systèmes non conformes.
La décision d'accorder cet accès peut reposer sur des informations comme l'état du logiciel anti-virus du point d'extrémité, la version du système d'exploitation ou encore la version du correctif de son système d'exploitation etc.

Détails des composants requis

- **Cisco Trust Agent (CTA) –** Il s'agit d'un logiciel à installer sur les systèmes d'extrémités (postes clients, serveurs…) et s'interface avec d'autres logiciels de sécurité pour collecter les informations relatives à l'état du poste : présence ou non d'antivirus, version des signatures anti-virus et prochainement version des correctifs du système d'exploitation. Ces informations sont envoyées au serveur de politique de sécurité (ACS Access Control Server) qui décide ensuite de l'accès au ou non du poste au réseau. Plusieurs éditeurs d'agents antivirus (Trend Micro, Mcafee, Symantec,…) supportent aujourd'hui NAC et proposent des pluggins à copier sur les postes clients, qui vont permettre à l'agent CTA de collecter sur le poste les informations relatives à l'agent anti-virus en question.

  D'autres scripts de pluggins peuvent être ajoutés pour n'importe quelle application tournant sur le client.

  CTA informe le client de la posture qu'il prend par le biais de popups affichés sur le poste en fonction du contrôle de conformité. Le contenu du popup est défini sur le serveur ACS de politiques de sécurité.
- **Network Access Device (NAD)** - Il s'agit des équipements d'accès au réseau (routeur, commutateur, borne wireless, concentrateur VPN…) qui appliquent les actions envoyées par le serveur de politique de sécurité après analyse de l'état du poste. En fonction des politiques de sécurité appliquées pour un poste, le NAD autorise, interdit ou isole un poste qui tente de se connecter au réseau d'entreprise. Le serveur ACS va télécharger des règles de filtrage réseau (access-list) sur les ports d'un routeur, forcer une redirection d'URL, affecter un port d'un switch à un VLAN particulier en fonction du résultat du contrôle…
- **Serveur de politique de sécurité Cisco Secure ACS** – Il s'agit du « l'intelligence » de la solution NAC dans la mesure où il centralise l'ensemble des politiques de sécurité définies, ainsi que les mesures à appliquer en fonction des informations reportées par l'agent CTA. Comme on l'a vu précédemment, ces mesures de sécurité (affecter un port à un VLAN, pousser une access-list sur un port,…) sont ensuite appliquées au niveau du Network Acces Device. Le serveur Cisco Secure ACS peut

également communiquer avec un serveur de politique antivirus externe par le biais du protocole HCAP (Host Credential Authorization Protocol). Grâce à un autre protocole, le protocole GAME, il peut aussi relayer le contrôle d'un poste client à un serveur externe (cas typique d'un poste client sans agent CTA).

- **Serveur de politique antivirus :** Une dizaine d'éditeurs d'antivirus participent au programme Network Admission Control. Ceci signifie qu'ils fournissent au minimum les pluggins qui permettent à l'agent CTA de récupérer les informations essentielles qui concernent l'agent antivirus du poste. Toutefois à ce jour, seul Trend Micro propose un serveur de politique antivirus supportant le protocole de communication HCAP. L'intérêt d'un tel dialogue est l'automatisation de l'information du serveur ACS sur les versions de mises à jour antivirus du poste utilisateur, surtout lorsque l'on sait que les mise à jour de signatures d'antivirus se fait plusieurs fois par jour.

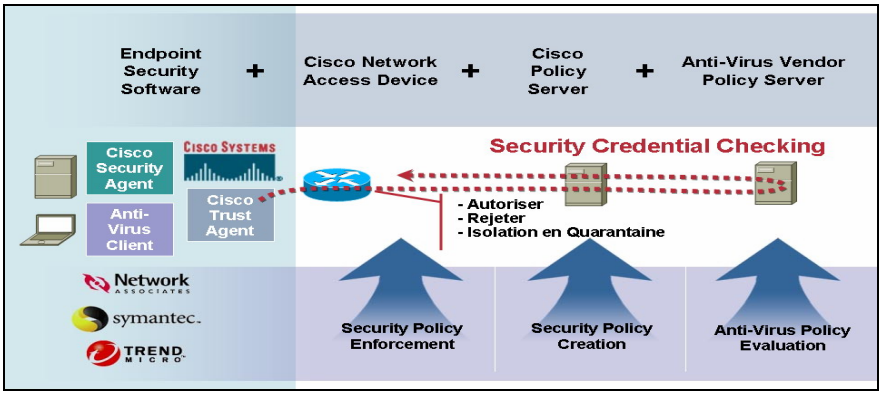


Figure 1 composants d'une solution Cisco NAC

Exemples d'applications de Cisco Network Admission Control

- Contrôle de conformité pour les succursales d'entreprise – Cisco NAC permet de garantir la conformité des systèmes d'extrémité 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 des virus et des vers se propagent au sein de l'entreprise en élargissant le contrôle d'admission aux commutateurs de niveau 2.

- Conformité extranet – Cisco NAC peut servir à 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 les systèmes des sous-traitant 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 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.

- 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.

Modes de fonctionnement de Cisco NAC

Cisco NAC fonctionne suivant trois modes :
- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x

Les différences entre ces trois modes sont résumées sur le tableau ci-dessous.

Tableau 1 Comparaison entre les trois modes de fonctionnement NAC

	NAC L2 802.1x	NAC L2 IP	NAC L3 IP
Déclenchement du mécanisme NAC	**Dès que le lien physique "monte"**	**Requite DHCP ou ARP**	**Paquet IP**
Identification Machine	**X**		
Identification Utilisateur	**X**		
Posture	**X**	**X**	**X**
Assignement de VLAN	**X**		
URL-Redirection		**X**	**X**
Downloadable ACLs	**Seulement sur les 6500-**	**X**	**X**
Posture Status Queries		**X**	**X**
802.1x Posture Change	**X**		

NAC L3 IP

Fonctionnement de NAC L3 IP

Le premier mode de fonctionnement de Cisco NAC est NAC L3 IP. Il s'agit d'une architecture fonctionnant uniquement avec des NADs routeurs ou des concentrateurs VPN. Ce mode de fonctionnement est le premier des modes lancés par Cisco Systems dès 2004, connu aussi sous le nom de « NAC phase 1 ». Il est très utile pour des architectures avec plusieurs nœuds de niveau 3.

Le principe de NAC L3 IP est le suivant :

1- Un client essaie d'atteindre un réseau derrière un routeur.

2- Le serveur ACS effectue un contrôle sur le client et télécharge des listes de contrôle d'accès (access lists) et/ou des redirections URL, sur le port du routeur, en fonction du résultat du contrôle effectué.

Ci-dessous la liste des routeurs Cisco supportant NAC L3 IP :

Tableau 2 Gammes de routeurs supportant NAC L3 IP

Cisco 18xx, 28xx, 38xx	Yes
Cisco 72xx, 75xx	Yes
Cisco 37xx	Yes
Cisco 3640, 3660-ENT Series	Yes
Cisco 2600XM, 2691	Yes
Cisco 1701,1711, 1712, 1721, 1751, 1751-V, 1760	Yes
Cisco 83x	Yes
Cisco 4500	No
Cisco 3660-CO Series	No
Cisco 3620	No
Cisco 2600 non-XM Models	No
Cisco 1750, 1720, 1710	No

Le shéma ci-dessous montre le fonctionnement de NAC L3 IP.

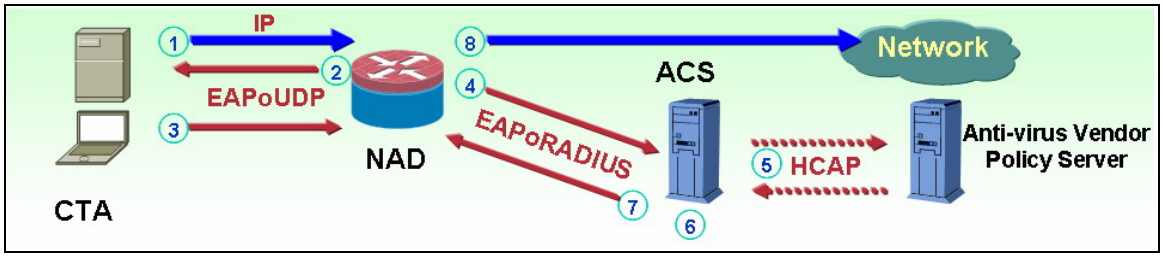


Figure 2 Schéma détaillé du fonctionnement de NAC L3 IP

1. Le client tente envoie une première trame IP vers le port configuré en NAC du NAD.
2. Le NAD intercepte le paquet IP et envoie une requête de validation de « l'état de sécurité » du poste client (protocole EAP over UDP)
3. Le poste client (avec CTA) renvoie au NAD ses *credentials*, c'est à dire les informations relatives à son état de sécurité (protocole d'échange : EAP o UDP)
4. Le NAD transmet les informations du poste client au serveur Cisco Secure ACS (protocole EAP over RADIUS)
5. Le serveur ACS retransmet éventuellement les informations du poste client à un serveur de politique antivirus externe via le protocole Host Credential Authorization Protocol (protocole HCAP), ou encore vers un serveur d'audit externe (protocole GAME)
6. Le serveur ACS valide l'état du poste et lui associe une politique de sécurité (conforme, quarantaine, mise à jour…)
7. Le serveur ACS transmet au NAD la politique de sécurité associée au poste utilisateur sous forme de droits d'accès : access-list, redirection URL

8. le poste client Accède au réseau, est interdit d'accès ou est confiné en zone de quarantaine selon la politique décidée par ACS.

Un temporisateur de revalidation paramétrable oblige une revalidation permanente de l'état de conformité pour un poste déjà connecté au réseau. Deux cas peuvent se présenter :

1- Le client garde la même posture : Le NAD et le CTA communiquent avec un processus « *L3 EAP Status Query* » pour vérifier que :

1) l'agent CTA est toujours actif

2) il s'agit toujours de la même machine validée

3) la posture est restée inchangée

2- Le client change de posture : l'agent CTA ne répond pas dans ce cas au *Status Query*, provoquant ainsi un processus de revalidation.

NAC L2 IP

Fonctionnement de NAC L2 IP

Le mode NAC L2 IP permet aujourd'hui les mêmes possibilités offertes par NAC L3 IP (renvoi d'access lists, redirection URL) sur des switchs niveau 3. Contrairement à NAC L3 IP, le mode L2 IP est plus récent et n'est disponible que depuis Novembre 2005.

Ci-dessous une liste récapitulant le support de NAC L2 IP sur les différentes gammes de switchs Cisco :

Tableau 3 Gammes de switchs supportant NAC L2 IP

Platform, Supervisor	OS	NAC L2 IP
6500—Sup32, 720	Native IOS	Yes
6500—Sup2	Native IOS	Yes
6500—Sup32, 720	Hybrid	Yes
6500—Sup2	Hybrid	Yes
6500—Sup2,32, 720	CATOS	Yes
4500Series— SupII+, II+TS, IV, V, V-10GE	IOS	Yes
4900	IOS	Yes
3550,3560, 3750	IOS	Yes
2950,2940, 2955, 2960,	IOS	No

2970		
6500—Sup1A	All	No
5000	All	No
4000 Sup I, II, III (IOS)	CATOS	No
3500XL, 2900XM, 1900	All	No

Le principe est globalement le même que dans NAC L3 IP, sauf que le processus L2 IP est déclenché par simple interception par le switch d'une requête DHCP ou ARP.

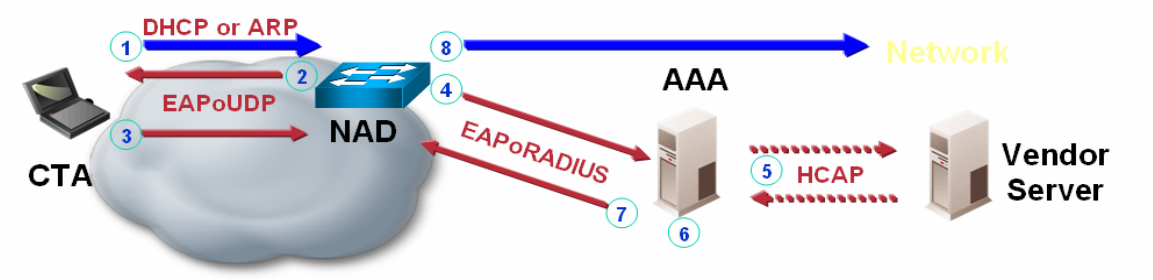


Figure 3 Schéma détaillé du fonctionnement de NAC L3 IP

1. Le client envoie une requête DHCP (ou requête ARP) vers le port configuré en NAC du NAD.
2. Le NAD déclenche une communication EAP avec le client et envoie une requête de validation de « l'état de sécurité » du poste (protocole EAP over UDP)
3. Le poste client (avec CTA) renvoie au NAD ses *credentials* (protocole d'échange : EAP o UDP)
4. Le NAD transmet les informations du poste client au serveur Cisco Secure ACS (protocole EAP over RADIUS)
5. Le serveur ACS retransmet éventuellement les informations du poste client à un serveur de politique antivirus externe via le protocole Host Credential Authorization Protocol (protocole HCAP), ou encore vers un serveur d'audit externe (protocole GAME)
6. Le serveur ACS valide l'état du poste et lui associe une politique de sécurité (conforme, quarantaine, mise à jour…)
7. Le serveur ACS transmet au NAD la politique de sécurité associée au poste utilisateur sous forme de droits d'accès : access-list, redirection URL
8. le poste client accède au réseau, est interdit d'accès ou est confiné en zone de quarantaine selon la politique décidée par ACS.

Comme dans le cas L3 IP, un temporisateur de revalidation permet une revalidation permanente de l'état de conformité.

Description du scénario NAC L2 IP avec intégration de l'antivirus TrendMicro Office Scan

Le contrôle d'intégrité du client au niveau du serveur ACS se fait sur les critères suivants :

1- A partir d'une base « interne » d'ACS en vérifiant la version de patch et la version de système d'exploitation.

2- A partir d'une base « externe », en vérifiant si le client dispose bien d'un agent anti-virus Trend Micro, actif, de version récente et disposant de signatures anti-virus mises à jour.

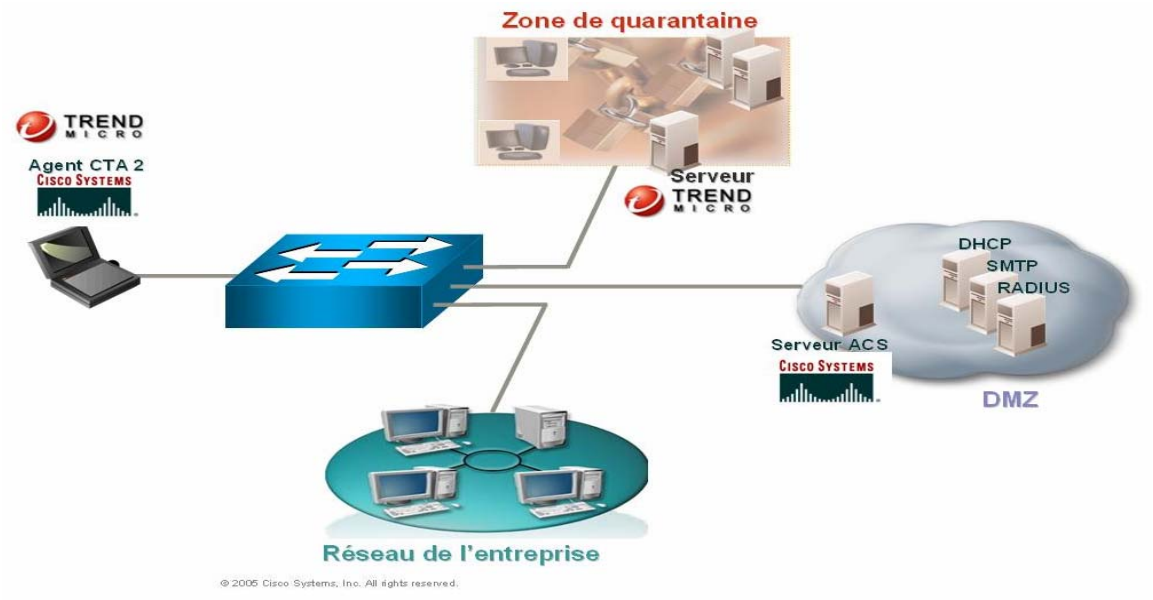


Figure 4 Maquette NAC L2 IP

On définit donc tout d'abord sur le serveur ACS les règles de sécurité suivantes :

- Le client doit avoir une version de CTA supérieure où égale à la version 2.0.0.25.
- Le système d'exploitation du client doit être :
  - Soit un Windows 2000 avec un service pack 4.
  - Soit un Windows XP avec un service pack 2.
- Le client doit disposer d'un client antivirus Trend-Micro récent et actif. Cette règle est définie sur l'ACS en tant que règle externe que l'ACS doit aller vérifier sur la base de données externe du serveur Trend.

Si une machine cliente vérifie tous ces critères, elle est considérée comme conforme et a accès au réseau d'entreprise.

Autrement, le client est aiguillé vers une zone de quarantaine. Dans le cas précis où le client ne vérifie pas la troisième condition, une mise à jour à distance est effectuée par le serveur Trend.

Le scénario se déroule en trois étapes :

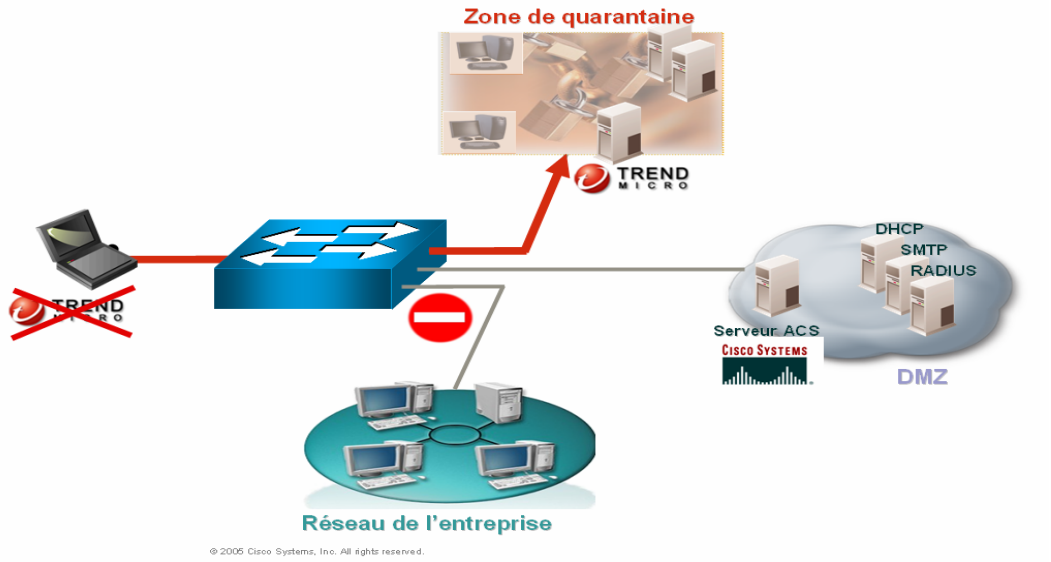
1- Nous nous connectons sur le port 1 du switch configuré en NAC L2IP avec un client Windows XP avec un service pack 2, sur lequel on a installé une version 2.0.0.30 de CTA. Le client a été préalablement défini dans la base du serveur Trend. De ce fait, le client dispose donc déjà d'une version récente d'antivirus qui lui a été installé à distance par le serveur Trend-Micro.

   Le client est donc conforme, et on peut le vérifier en se connectant sur le switch et en observant un popup « healthy » sur le client. A ce stade on peut aussi accéder à une page web « healthy » qui se situe sur le réseau de l'entreprise.

Figure 5 Le client est conforme. Il est autorisé à accéder au réseau de l'entreprise

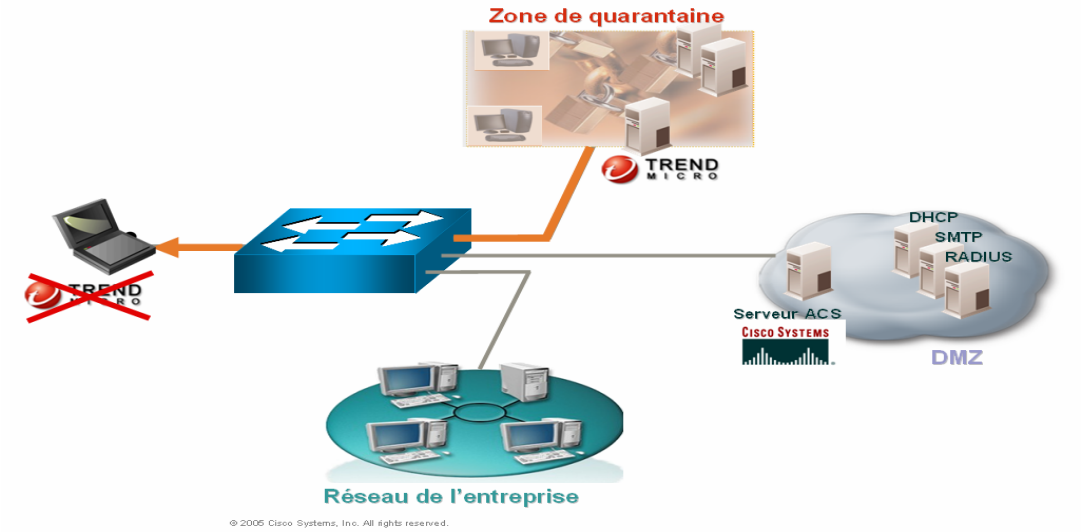
2- Dans un deuxième temps, on désactive l'antivirus du client en désactivant un des process Trend-Micro. Le client prend aussitôt la posture « quarantaine » qu'on peut observer avec l'apparition d'un popup « quarantine ».

   En tentant d'accéder à la page web « healthy », on se rend compte qu'on est redirigé vers une autre page de mise à jour.



L'utilisateur désactive son antivirus. Le client n'est plus conforme.
Il est aiguillé en zone de quarantaine

3- Après un certain délai d'attente, le serveur Trend réactive l'antivirus client à distance. Ceci est visible sur l'écran du client et un nouveau popup « healthy » apparaît ce qui signifie que le client a de nouveau une posture « conforme».



Le serveur Trend Micro réactive à distance l'antivirus

NAC L2 802.1x

NAC L2 802.1x permet une authentification 802.1x couplée d'un contrôle de conformité NAC.

Contrairement à NAC L2 IP et NAC L3 IP, le serveur ACS ne télécharge ni des access lists ni des redirections URL sur les ports du NAD. ACS assigne dans NAC L2 802.1x le port du NAD où le client est connecté à un VLAN en fonction du résultat du contrôle de conformité NAC sur le client.

NAC 802.1x n'est supporté que sur les switchs et les bornes WiFi.

Ci-dessous une liste récapitulant le support de NAC NAC 802.1x sur les différentes gammes de switchs Cisco :

Tableau 4 Gammes de switchs supportant NAC L2 802.1x

Platform, Supervisor	OS	NAC L2 802.1x
6500—Sup32, 720	Native IOS	Future
6500—Sup2	Native IOS	Future
6500—Sup32, 720	Hybrid	Yes
6500—Sup2	Hybrid	Yes
6500—Sup2, 32, 720	CATOS	Yes
4500 Series— SupII+, II+TS, IV, V, V-10GE	IOS	Yes
4900	IOS	Yes
3550,3560, 3750	IOS	Yes
2950,2940, 2955, 2960, 2970	IOS	Yes
6500—Sup1A	All	No
5000	All	No
4000 Sup I, II, III (IOS)	CATOS	No
3500XL, 2900XM, 1900	All	No

Avant de décrire le fonctionnement du mode NAC 802.1x, il est nécessaire de présenter tout d'abord le protocole 802.1x.

Le protocole 802.1x

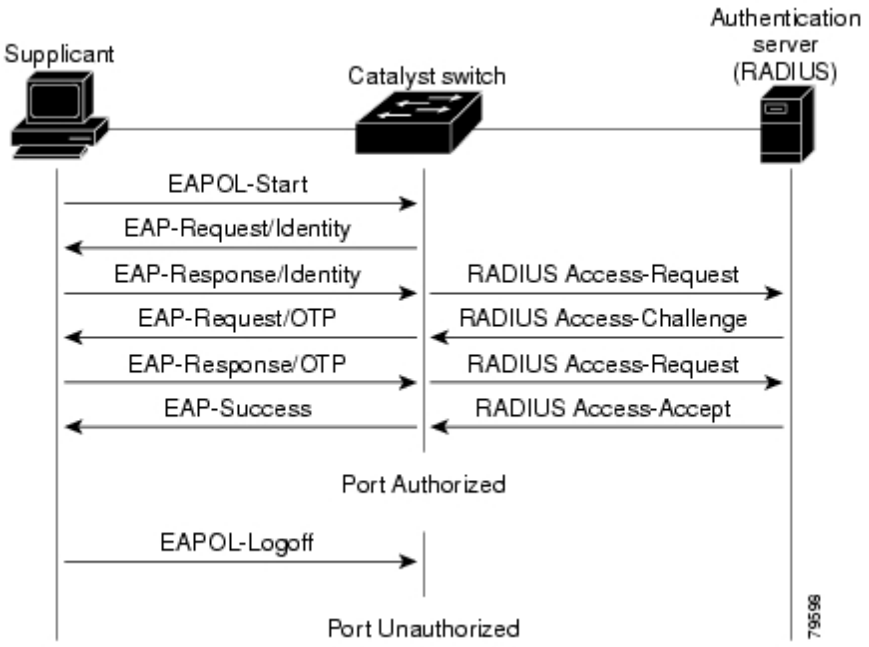
Le protocole 802.1x a pour but de définir un «contrôle d'accès réseau par port ». Un port peut tout aussi bien être physique (port d'un équipement de commutation) ou virtuel (port sur une borne d'accès WiFi).

La gestion des contrôles d'accès au niveau port permet donc de spécifier les modalités d'accès à un réseau au niveau de l'interfaçage « physique » entre le client et l'équipement d'accueil.

Dans le fonctionnement du protocole, les trois entités qui interagissent sont :

- le système à authentifier (*supplicant*),
- le système authentificateur (*authenticator system*)
- un serveur d'authentification (*authentication server*).

Ci-dessous, le diagramme de flux :



Cinématique des flux 802.1x

Deux cas de figure peuvent se présenter :

1. Si le supplicant est authentifié avec succès (reçoit une trame d'accord du serveur d'authentification), le port change en état autorisé, et toutes les trames du supplicant authentifié sont permises par le port.
2. Si l'authentification échoue, le port est dans l'état non autorisé, mais l'authentification peut être réessayée. Si aucune réponse n'est reçue du serveur après le nombre spécifique de tentatives, l'authentification échoue, et l'accès au réseau n'est pas accordé.

Quand un supplicant se déconnecte, il envoie un message d'EAPOL-logoff (EAPOL : EAP over Lan), obligeant le port du commutateur à se mettre dans l'état non autorisé.

Comme on peut le voir, le serveur d'authentification et le client ne communiquent à aucun moment directement. Toute la communication est arrêtée et transmise par relais

par l'authentificateur. Une fois qu'un client est authentifié, seulement alors il peut accéder aux ressources du réseau.

Fonctionnement de NAC L2 802.1x

Pour avoir un fonctionnement NAC L2 802.1x il est nécessaire d'installer sur le client une version de CTA 2 avec supplicant. Une version a été prévue à cet effet incluant un supplicant Meeting House en version limitée.

Ainsi CTA se chargera non seulement de relayer les informations relatives à NAC mais aussi d'envoyer des credentials 802.1x au NAD qui les relayera au serveur ACS. Celui-ci peut aussi relayer la partie authentification 802.1x à une base externe d'utilisateurs et/ou de machines, comme par exemple une base Windows Active Directory.

Le schéma ci-dessous résume le fonctionnement de NAC 802.1x :

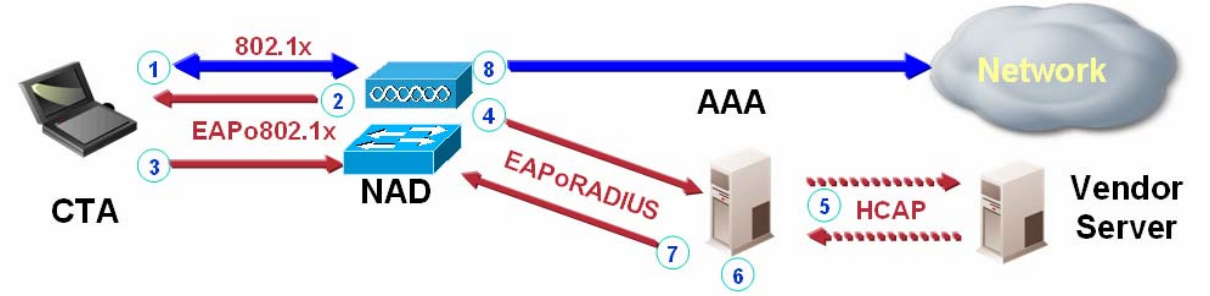


Figure 6 Schéma détaillé du fonctionnement de NAC L2 802.1x

1. Etablissement d'un dialogue 802.1x entre le NAD et le client (CTA avec supplicant)
2. Le NAD réclame des credentials du client. Ces credentials peuvent concerner la posture du poste en plus de l'identité de l'utilisateur et/ou de la machine. (EAP o 802.1x)
3. Le poste client (avec CTA) renvoie au NAD ses *credentials* (EAP o 802.1x)
4. Le NAD transmet les informations du poste client au serveur Cisco Secure ACS (EAP o RADIUS)
5. Le serveur ACS retransmet éventuellement les informations du poste client à un serveur externe (Vendor Server sur la figure) pour l'authentification 802.1x, un cas typique c'est d'avoir une base Active Directory ou LDAP préexistantes et il est alors plus simple de leurs relayer la partie authentification. (protocole HCAP)
6. Le serveur ACS valide l'état du poste et définit les autorisations d'accès du poste (exemple : un poste invité aura un accès « guest », un poste non-conforme aura un accès « quarantaine », …)
7. Le serveur ACS transmet au NAD la politique de sécurité associée au poste utilisateur: Le port du NAD où le client est connectée est assigné à un VLAN.

8. le poste client accède au VLAN auquel il a été aiguillé et dispose des droits ou des restrictions relatives à ce VLAN.

Description du scénario NAC L2 802.1x avec intégration d'Active Directory.

Ce scénario permet de mettre en évidence l'interaction du serveur ACS avec un autre composant externe qu'est Active Directory de Microsoft.

Les équipements mis en jeu sont :

- un switch Catalyst 3750.
- Un poste client Windows XP service pack 2.
- Un serveur ACS Windows 2000.
- Sur la même machine où l'on a installé ACS on installe *Active Directory*.

Nous définissons sur Active Directory deux utilisateurs :

- Un utilisateur « administrateur » faisant partie notamment du groupe d'utilisateurs « users »,
- Un utilisateur « invité » faisant partie uniquement du groupe « guests ».

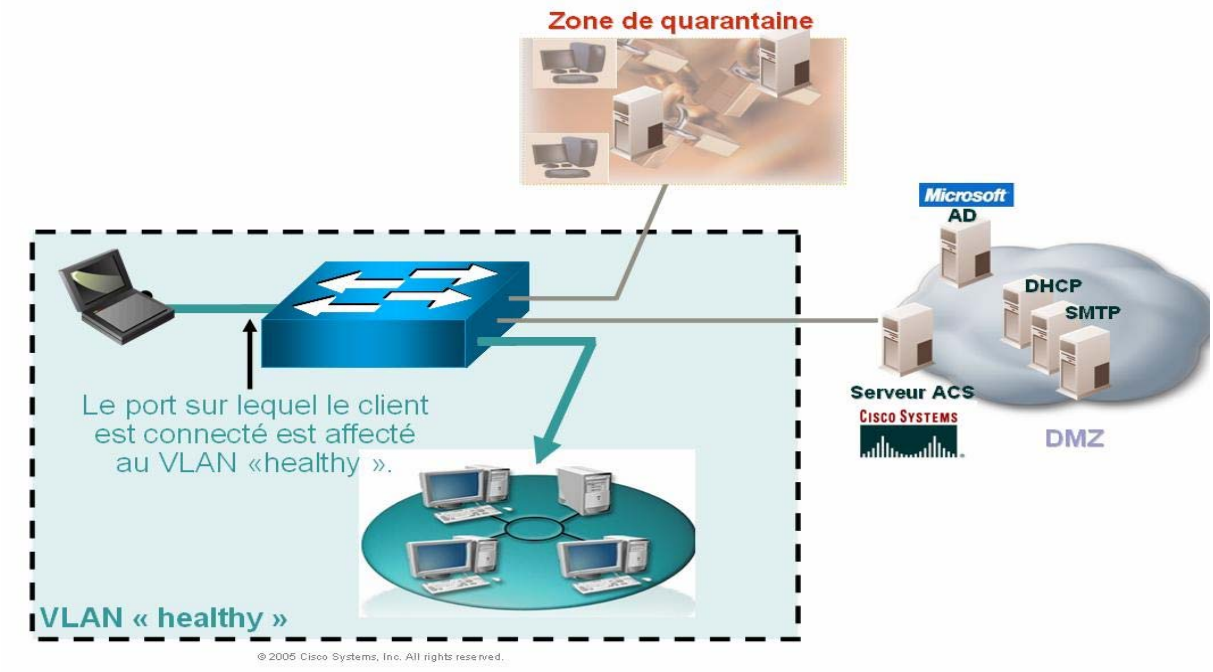
Pour qu'un poste soit considéré comme conforme il faut qu'il vérifie :

- une version de CTA supérieure ou égale à 2.0.0.25.
- un système d'exploitation Windows XP avec un service pack 2.

Nous disposons de deux machines clientes, toutes deux enregistrées dans la base d'Active Directory. L'une dispose du service pack 2, l'autre non.

La démonstration se déroule en trois phases :

1- On se connecte tout d'abord sur le réseau avec la première machine (disposant du service pack 2) et avec comme nom d'utilisateur « administrateur ». La machine est conforme, un popup de CTA avec la mention « conforme » apparaît et on remarque en se connectant sur le switch que le port surlequel on est connecté (le port Fa1/0/3), initialement affecté au VLAN par défaut (c'est-à-dire le VLAN 1) est désormais affecté au VLAN 50, défini comme VLAN Healthy.



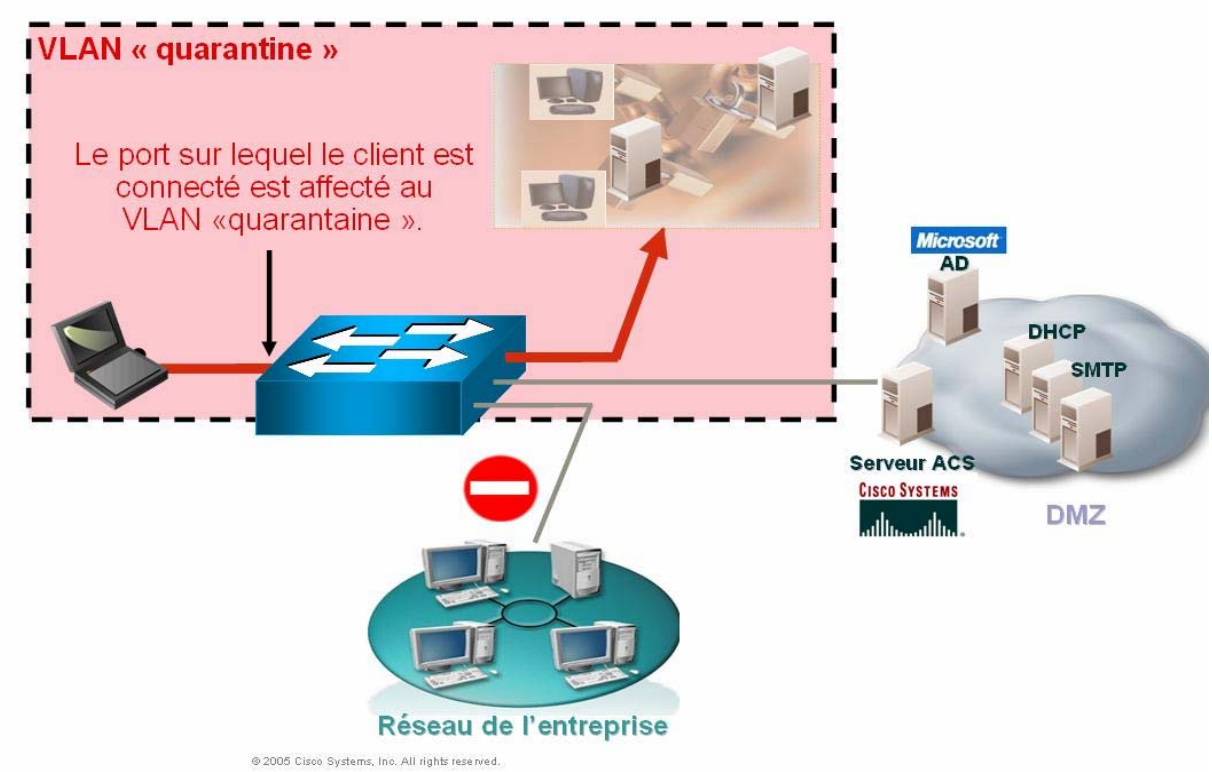
Le poste client est un utilisateur interne et est conforme. Ila accès au VLAN "healthy"

Ci-dessous un aperçu d'un « show VLAN brief » sur le switch montrant que le port Fa 1/0/3 change de VLAN.

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa1/0/4, Fa1/0/13, Fa1/0/14
                                                   Fa1/0/15, Fa1/0/16, Fa1/0/17
                                                   Fa1/0/18, Gi1/0/1, Gi1/0/2
2    NAC_L2_IP                           active    Fa1/0/1, Fa1/0/2
3    LAN                                 active    Fa1/0/5, Fa1/0/6, Fa1/0/7
                                                   Fa1/0/8, Fa1/0/9
4    WIRELESS                            active    Fa1/0/10
5    WAN                                 active    Fa1/0/11, Fa1/0/12
15   DECISION/REMEDIATION                active    Fa1/0/20, Fa1/0/21, Fa1/0/22
25   CORPORATE                           active    Fa1/0/23, Fa1/0/24
40   guests                              active
50   healthy                             active    Fa1/0/3
60   checkup                             active
70   transition                          active
80   quarantine                          active
90   infected                            active
100  unknown                             active
110  voice                               active
200  servers                             active
300  Gateway_ASA_Network                 active    Fa1/0/19
 --More--
```

Capture d'écran du switch. Cas "conforme"

2- Dans une deuxième phase, on se connecte avec la deuxième machine (sans service pack 2). On est cette fois jugé non-conforme par le serveur ACS. Un popup « quarantaine » apparaît donc sur le poste client et on est aiguillé vers le VLAN 80, défini dans la configuration comme VLAN de quarantaine.



Le poste client est non conforme. Il est aiguillé dans le VLAN "quarantine"

Ci-dessous une capture d'écran sur le switch montrant l'aiguillage du port Fa1/0/3 vers le VLAN 80.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/0/4, Fa1/0/13, Fa1/0/14
                                                 Fa1/0/15, Fa1/0/16, Fa1/0/17
                                                 Fa1/0/18, Gi1/0/1, Gi1/0/2
2    NAC_L2_IP                         active    Fa1/0/1, Fa1/0/2
3    LAN                               active    Fa1/0/5, Fa1/0/6, Fa1/0/7
                                                 Fa1/0/8, Fa1/0/9
4    WIRELESS                          active    Fa1/0/10
5    WAN                               active    Fa1/0/11, Fa1/0/12
15   DECISION/REMEDIATION              active    Fa1/0/20, Fa1/0/21, Fa1/0/22
25   CORPORATE                         active    Fa1/0/23, Fa1/0/24
40   guests                            active
50   healthy                           active
60   checkup                           active
70   transition                        active
80   quarantine                        active    Fa1/0/3
90   infected                          active
100  unknown                           active
110  voice                             active
200  servers                           active
300  Gateway_ASA_Network               active    Fa1/0/19
 --More--
```

Capture d'écran du switch. Cas "non conforme"

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa1/0/4, Fa1/0/13, Fa1/0/14
                                                 Fa1/0/15, Fa1/0/16, Fa1/0/17
                                                 Fa1/0/18, Gi1/0/1, Gi1/0/2
2    NAC_L2_IP                         active    Fa1/0/1, Fa1/0/2
3    LAN                               active    Fa1/0/5, Fa1/0/6, Fa1/0/7
                                                 Fa1/0/8, Fa1/0/9
4    WIRELESS                          active    Fa1/0/10
5    WAN                               active    Fa1/0/11, Fa1/0/12
15   DECISION/REMEDIATION              active    Fa1/0/20, Fa1/0/21, Fa1/0/22
25   CORPORATE                         active    Fa1/0/23, Fa1/0/24
40   guests                            active    Fa1/0/3
50   healthy                           active
60   checkup                           active
70   transition                        active
80   quarantine                        active
90   infected                          active
100  unknown                           active
110  voice                             active
200  servers                           active
300  Gateway_ASA_Network               active    Fa1/0/19
 --More--
```

Capture d'écran du switch. Cas "invité conforme"