École Supérieure de Gestion d'Informatique et des Sciences

Bd de l'Ouémé Jéricho, Cotonou - BENIN

école supérieure de génie informatique

28 rue du plateau, 75019 Paris - FRANCE

MEMOIRE DE FIN D'ETUDE

Filière : INGENIERIE INFORMATIQUE ET RESEAUX

(Option Systèmes Réseaux et Sécurité)

THEME

LE CONTRÔLE ET LA SÉCURITÉ D'ACCÈS AUX RÉSEAUX D'ENTREPRISES

Présenté par :

HOUNGBO Mathias
LAHAMY Armand

Sous la direction de :

AÏNA Alain
Ingénieur réseaux

Année académique 2011-2012

TABLE DES MATIERES

DEDICACES

Je dédie ce travail à

Mon père, mon professeur de toujours

Benjamin LAHAMY.

Ma très chère mère Jeanne BOKO, pour tout son amour, ses sacrifices et tout son soutien.

Ma très précieuse mère, mon soutien

Anastasie NASCIMENTO.

Ma très chère épouse auprès de laquelle j'ai trouvé la joie dans les moments difficiles et dont le soutien m'a toujours été très précieux.

A ces uniques personnes …

Qui me sont chères.

Recevez mes reconnaissances sincères.

A tous ceux qui m'ont soutenu durant mon cursus scolaire, recevez ici l'expression de ma profonde gratitude.

Armand LAHAMY

Mathias HOUNGBO

REMERCIEMENTS

« Et quelque chose que vous fassiez, soit par parole ou par œuvre, faites tout au Nom du Seigneur Jésus, rendant grâces par lui à notre Dieu et Père. » (Bible édition Martin 1744, Colossiens 3:17)

Nous adressons tous nos remerciements à l'Éternel qui nous a donné la santé, la force et la détermination de réaliser ce document.

Nous voudrions aussi adresser notre profonde gratitude à notre maitre de mémoire Mr Alain AÏNA, pour ses remarques pertinentes et ses précieuses recommandations.

Aussi est-ce le moment pour nous, d'adresser tous nos vifs remerciements à tout le personnel de l'ESGIS pour l'encadrement et les divers efforts qu'ils ont consentis pour que notre formation puisse se dérouler convenablement jusqu'à son terme. Nous pensons particulièrement au Directeur Général Mr Macy AKAKPO, à notre chef de département Mr Béthel ATOHOUN, à tous nos formateurs particulièrement à M. Alain AINA, M. Farell FOLLY, M. Alain GBAGUIDI, M. Kamal HENNOU et M. Hervé TYPAMM pour leur grand professionnalisme.

Pour finir, nous remercions toutes nos familles, nos promotionnaires, nos ami(e)s et toutes autres personnes ayant de près ou de loin contribué à la réussite de ce travail.

Que Dieu vous les rende au centuple.

RÉSUMÉ

La sécurité informatique est un sujet ancien et abondamment traité, qu'elle concerne l'accès à Internet, avec l'étude des flux (pare-feu, détection d'intrusions, ...), ou la sécurisation des postes de travail et des serveurs. Depuis quelques années, un nouveau concept est apparu : « contrôle d'accès au réseau ».

Le contrôle d'accès au réseau est censé mettre en œuvre la politique de sécurité d'une entreprise concernant aussi bien l'identification et l'authentification des usagers (humain ou matériel), que l'évaluation du niveau de sécurité de ses usagers (avant et après connexion), ces informations étant utilisées pour accorder ou non l'accès aux ressources informatiques de l'entreprise.

Dans un premier temps, le contrôle d'accès sera présenté sous l'ensemble de ces aspects. Les solutions et approches suivront et seront exposées. Nous vous ferons ensuite part des limites et des points forts des différents protocoles à la base du contrôle d'accès ainsi que les critères devant guidé une entreprise dans le choix d'une solution de contrôle d'accès au réseau. Et enfin nous implémenterons une solution de test.

Mots-clés : Contrôle d'accès, Sécurité informatique, Réseau, Politique de sécurité.

ABSTRACT

Information system security regarding internet access, study of streams (firewall, intrusion detection, …) or servers and workstations security, is an old subject and widely handled. These last years, a new concept appeared : « network access control ».

Network access control is supposed to implement the safety policy in a company whether it deals with identification, users authentication (human or equipment), or security level evaluation on users (before and after connection). Those information are processed to grant or deny access to network resources.

At first, Network Access Control will be presented in its entirety. Next, approaches and solutions will be exposed. We shall then state the limits and the key points of network access underlying protocols as well as criteria on which an enterprise must choose its solution. We'll finish by implementing a standard test solution.

Keywords : Network Access Control, Information system security, Network, Safety policy.

INTRODUCTION

Les efforts en matière de sécurité des réseaux se focalisent souvent sur le périmètre entre réseau privé et internet avec un pare-feu et la sécurité des postes de travail se limite souvent au seul antivirus. Cette approche considère que le risque majeur de sécurité provient exclusivement de l'extérieur, d'où la tendance à durcir les défenses de périmètre, alors que les utilisateurs internes ont plein accès aux ressources du réseau.

Les statistiques[1] [2] montrent que 60 % des incidents d'attaques et d'intrusions viennent de l'intérieur du réseau (dont 20 % non volontaires et 40 % volontaires) et 40 % de l'extérieur. Cela dit, la protection contre les attaques informatiques doit englober la totalité du réseau.

Pour une entreprise, ceci n'est plus suffisant dans un monde d'ordinateurs portables, de smartphones, de connexions au réseau dans des zones non sécurisées, avec un nombre croissant de visiteurs, de partenaires externes, de réorganisations, etc.

L'accès au réseau interne devrait être restreints aux seuls PCs et autres équipements autorisés. Comment peut-on alors autoriser ou bloquer l'accès au réseau à un hôte ? Comment imposer le respect de sa politique de sécurité comme condition préalable lors de l'accès au réseau?

C'est dans ce cadre qu'intervient le contrôle d'accès au réseau afin de n'autoriser que les entités (personnes ou matériels) validées à accéder aux données auxquelles elles ont droit et seulement à celles-ci, afin de préserver la qualité et la sécurité du système d'information.

1 B. Morin. Corrélation d'alertes issues d'outils de détection d'intrusions avec prise en compte d'informations sur le système surveillé. Thèse de doctorat en informatique de l'Institut National des Sciences Appliquées de Rennes, février 2004.

2 La Sécurité informatique vue par Deloitte, http://www.mag-securs.com/News/tabid/62/id/16014/La-Securite-informatique-vue-par-Deloitte.aspx

1

PARTIE 1 : LE CONTRÔLE D'ACCÈS AU RÉSEAU

1.1 Les principes

Un contrôleur d'accès au réseau (Network Access Control ou NAC) est une méthode informatique permettant de soumettre l'accès à un réseau d'entreprise à un protocole d'identification de l'utilisateur et au respect par la machine de cet utilisateur des restrictions d'usage définies pour ce réseau.

Il est censé répondre à la mise en œuvre de certaines parties de la politique de sécurité concernant l'accès au réseau local d'une entreprise (filaire, sans-fil ou VPN[3]), dont principalement :

- l'identification et l'authentification des utilisateurs,
- l'évaluation du niveau de sécurité des systèmes se connectant,
- la gestion des « invités »,
- le contrôle de l'activité,
- et parfois la détection d'intrusion.

L'ensemble de ces informations sera utilisé pour positionner l'équipement demandant un accès dans un certain environnement réseau. Cet environnement sera choisi en fonction de la politique de sécurité en vigueur. D'autres éléments peuvent entrer en jeu pour le choix du contexte réseau à mettre en place, le lieu, le moment, et le moyen utilisé pour la connexion par exemple. La possibilité de modifier le contexte d'accès réseau tout au long de la connexion d'un système, basée sur de nouvelles évaluations et authentifications, doit permettre au contrôle d'accès au réseau de maintenir un bon niveau de sécurité.

3 VPN : réseau privé virtuel en anglais, une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

Le rôle joué par le NAC lui confère aussi la possibilité d'être un élément important dans un système d'inventaire puisqu'il est censé connaître l'ensemble du parc informatique d'une entreprise.

1.1.1 Identification et authentification

L'identification et l'authentification sont à la base du contrôle d'accès réseau. Connaître l'identité des entités qui souhaitent accéder aux ressources et pouvoir les vérifier, permet la mise en place des règles d'accès décidées lors de l'élaboration de la politique de sécurité. Ces deux mécanismes peuvent être employés, pour des systèmes physiques (ordinateurs, imprimantes, téléphones ip, etc...), pour des utilisateurs, ou bien pour les deux quand les règles d'accès à appliquer à un utilisateur dépendent du système utilisé et inversement.

1.1.2 Évaluation et conformité

Le besoin d'évaluer les systèmes qui souhaitent accéder à des ressources s'est accru avec l'augmentation de leur mobilité et de leur diversité. Ces systèmes peuvent être aussi bien à l'origine d'attaque utilisant le réseau que les cibles de ces attaques. Il est donc apparu essentiel de récupérer un maximum d'informations sur ces systèmes pour décider de la politique à leur appliquer.

1.1.3 Isolement et mise en conformité

Lorsque le choix d'interdire l'accès à une ressource réseau demandée a été fait, il est nécessaire de mettre en place un dispositif permettant d'appliquer cette interdiction mais aussi de permettre la mise en conformité du système par rapport aux règles. Cela implique une capacité à communiquer avec l'utilisateur (ou le système directement) pour l'informer des raisons de sa mise à l'écart et des actions qu'il doit mener pour respecter la politique de sécurité.

1.1.4 Contrôle des activités

Un contrôle permanent des activités du système connecté est utile pour pouvoir s'assurer du respect de la politique de sécurité. En cas d'infraction aux règles, il est intéressant de pouvoir réagir en modifiant les accès aux ressources et en informer l'utilisateur du système.

1.1.5 Inventaire

L'inventaire est un rôle connexe au contrôle d'accès réseau, puisque c'est en s'appuyant sur les informations collectées qu'il est possible d'établir un état des lieux du parc informatique. Cet inventaire peut être effectué sur les matériels physiques mais peut aussi s'étendre aux logiciels utilisés.

1.2 Les composants

On peut distinguer différents éléments composant une architecture de contrôle d'accès réseau:
Tout d'abord l'élément de base qui est constitué par l'équipement physique qui souhaite accéder à des ressources, appelé ici « système d'extrémité » ; Le deuxième élément fondamental appelé ici « système d'évaluation » va être en charge de décider du contexte dans lequel va être placé le système d'extrémité à partir des informations recueillies sur ce dernier ; Le troisième élément, le « système de contrainte », est en charge d'appliquer les modifications de contexte décidées par le « système d'évaluation » ; Le dernier élément est le « système de mise en conformité », c'est un lieu de quarantaine où les systèmes d'extrémité auront la possibilité de devenir conformes à la politique de sécurité.

L'ensemble de ces composants devra être capable de fournir les informations permettant de suivre en temps réel les différents événements d'un accès au réseau et de construire un historique.

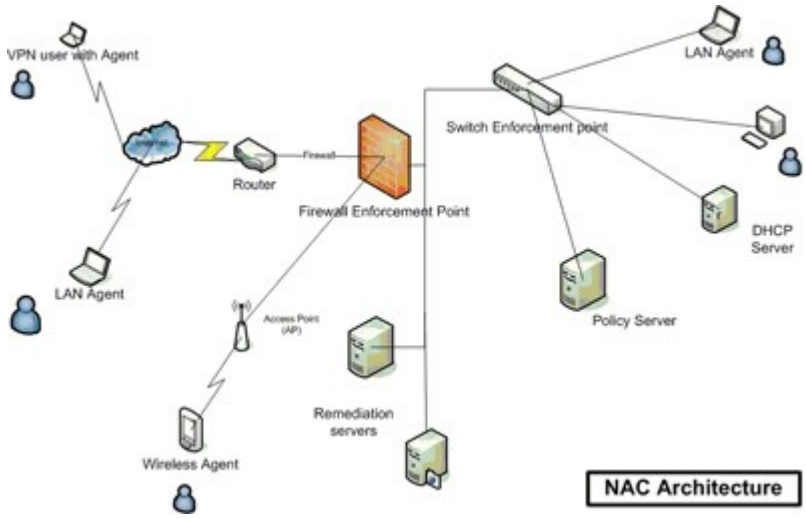

Figure 1: Architecture générale d'un NAC

1.2.1 Le système d'extrémité

C'est à partir de ce composant (poste de travail, imprimante, téléphone ip, etc) que les informations relatives à l'authentification et à la conformité doivent être récupérées, aussi bien à la demande de connexion que de manière régulière durant la connexion.

1.2.1.1 Identification et authentification

Afin de connaître l'identité d'une entité (personne, ordinateur …) et dans certains cas, de valider l'authenticité de cette identification, plusieurs méthodes sont disponibles.

Utilisation de l'adresse MAC[4]

Ici, seule l'adresse MAC du système d'extrémité est utilisée pour l'identification. C'est un moyen facile à mettre en œuvre, par exemple avec l'utilisation des requêtes DHCP. Il nécessite néanmoins la mise en place d'une base renseignée de toutes les adresses MAC autorisées à se connecter sur le réseau. Cette technique ne protège pas de l'usurpation d'identité. En usurpant son adresse MAC, un utilisateur pourrait se faire passer pour une imprimante. Mais des techniques de prise d'empreinte du système d'exploitation peuvent

4 Adresse MAC : Une adresse MAC (Media Access Control) est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisé pour attribuer mondialement une adresse unique au niveau de la couche de liaison (couche 2 du modèle OSI)

limiter ce problème en associant et en vérifiant les informations liées aux adresses MAC de la base.

Portail Web

L'authentification à l'aide d'une page web sécurisée (https[5]), tels les portails captifs, a l'avantage d'être accessible à tous les utilisateurs possédant un navigateur Web. En revanche, cette solution n'est pas envisageable pour les autres systèmes d'extrémité tels les imprimantes.

802.1X[6]

Le standard 802.1X (Port Based Network Access Control) est un mécanisme d'authentification utilisé au moment de l'accès au réseau. Basé sur EAP[7], son principe repose sur des échanges sécurisés entre le « supplicant » (l'utilisateur et sa machine), l' « authenticator » (le point d'accès sans-fil, le commutateur, ...) et l' « authentication server » (un serveur RADIUS[8] par exemple). Si l'identité de l'utilisateur (ou de la machine) est validée, le commutateur ouvrira l'accès au réseau (le VLAN[9] de l'utilisateur peut être transmis par le serveur d'authentification).

1.2 1.2 Conformité

Le but est de récupérer des informations sur l'état du système d'extrémité. Deux possibilités sont envisageables :

- avec un agent embarqué sur le poste utilisateur, il faudra prendre en compte le temps d'exécution, la charge processeur, le niveau de sécurité des échanges agent/serveur et la méthode de déploiement de ces agents.

5 HTTPS: L'HyperText Transfer Protocol Secure est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS.
6 802.1X : est un standard lié à la sécurité des réseaux informatiques, mis au point en 2001 par l'IEEE (famille de la norme IEEE 802). Il permet de contrôler l'accès aux équipements d'infrastructures réseau.
7 EAP : Extensible Authentication Protocol est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil et les liaisons point à point.
8 RADIUS : Remote Authentication Dial-In User Service est un protocole client-serveur permettant de centraliser des données d'authentification.
9 VLAN : pour Virtual LAN, est un réseau informatique logique indépendant.

- Sans agent, le temps d'exécution peut être long (scanner de vulnérabilités), ce qui peut contraindre à évaluer la conformité après la connexion.

Agent permanent

L'agent permanent est pré-installé ou chargé à la première connexion. Cet agent a pour rôle de récupérer des informations sur l'état du système d'extrémité (version système, correctifs de sécurité, logiciels installés, présence d'antivirus, de pare-feu, processus actifs, état des services, etc...). Il doit fournir ces informations au système d'évaluation au moment de la connexion mais aussi sur demande (permettant une réévaluation régulière). En général ces agents sont dit « lourds » car les processus démarrés pour récupérer les informations du système d'extrémité ont un coût processeur non négligeable. L'installation de ces agents nécessite des droits administrateur sur la machine.

Le déploiement généralisé sur les postes peuvent se faire par différentes techniques : Microsoft Systems Management Server (SMS), Web, etc.

- Avantages : granularité fine des informations, différents mécanismes d'authentification possibles.
- Difficultés : le déploiement, variété des systèmes d'extrémité, interopérabilité si les agents sont différents, le coût financier éventuel, le coût processeur, l'accès possible à des informations privées.
- Risques : Quelle confiance peut-on accorder à l'agent si le poste est corrompu?

Agent temporaire

L'agent temporaire est chargé sur le système d'extrémité à chaque tentative de connexion. Techniquement cela se fait soit à partir d'applet Java, d'ActiveX[10] ou bien par le téléchargement d'un exécutable (ne nécessitant pas de droits administrateur). Son utilisation se fait, la plupart du temps, dans le cadre d'accès de type portail captif ou d'accès de type VPN. Le positionnement du système d'évaluation fournissant l'agent est important. En coupure sur le réseau, les systèmes d'extrémité ont déjà accès à un réseau

10 ACTIVEX : désigne l'une des technologies du Component Object Model de Microsoft avec COM+ et Distributed COM utilisées en programmation pour permettre le dialogue entre programmes.

et peuvent communiquer entre eux contrairement à un positionnement au niveau du port physique de la connexion (port du commutateur de bordure).

- Avantages : le déploiement est facile, le coût financier faible, ne nécessite en général qu'un navigateur Web.
- Difficultés : nécessite l'ouverture d'un navigateur Web (impossible pour une imprimante), le temps passé à l'analyse peut être long.
- Risques : Quelle confiance peut accorder l'utilisateur à l'agent qui va être installé sur son équipement? L'utilisateur risque d'accepter n'importe quelle application pour avoir sa connexion.

Sans agent

Dans ce cas de figure, il existe deux méthodes potentiellement complémentaires :

-l'utilisation d'outils réseaux spécifiques (scanner de vulnérabilité, prise d'empreinte)

- Avantages : Pas d'intervention sur le système d'extrémité, transparent pour l'utilisateur.
- Difficultés : peut être lent, qualité et précision de l'information faibles, présence de pare-feu sur le système d'extrémité.
- Risques : existence d'outils de contournement (IpMorph[11]).

- l'utilisation d'appel de procédure à distance (RPC[12],WMI[13]), permettant la récupération d'information sur le poste par l'exécution de programmes spécifiques.

- Avantage : transparent pour l'utilisateur.
- Difficultés : nécessité d'un compte administrateur sur toutes les machines.
- Risques : une porte est ouverte sur le système d'extrémité.

11 IpMorph : outil de dissimulation et la mystification d'empreinte http://blog.hynesim.org/fr/ipmorph/

12 RPC : Remote Procedure Call est un protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications.

13 WMI : est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressource système via un ensemble d'interfaces.

Solutions		Avantages	Difficultés	Risques
Agent permanent		Granularité fine des informations, différents mécanismes d'authentification possibles	Le déploiement, variété des systèmes d'extrémité, interopérabilité si les agents sont différents, le coût financier éventuel, le coût processeur, l'accès possible à des informations privées	Quelle confiance peut-on accorder à l'agent si le poste est corrompu?
Agent temporaire		Le déploiement est facile, le coût financier faible, ne nécessite en général qu'un navigateur Web	Nécessite l'ouverture d'un navigateur Web (impossible pour une imprimante), le temps passé à l'analyse peut être long	Quelle confiance peut accorder l'utilisateur à l'agent qui va être installé sur son équipement? L'utilisateur risque d'accepter n'importe quelle application pour avoir sa connexion
Sans agent	**outils réseaux spécifiques**	Pas d'intervention sur le système d'extrémité, transparent pour l'utilisateur	Peut être lent, qualité et précision de l'information faibles, présence de pare-feu sur le système d'extrémité	Existence d'outils de conto urnement
	appel de procédure à distance	Transparent pour l'utilisateur	nécessité d'un compte administrateur sur toutes les machines	Une porte est ouverte sur le système d'extrémité

1.2.2 Le système d'évaluation

Cet élément de l'infrastructure est crucial pour la politique de sécurité de l'entreprise. À partir des informations recueillies sur le système d'extrémité, des informations sur la méthode d'accès (réseau filaire, sans-fil, VPN), mais aussi à l'aide d'informations sur le lieu ou le moment de la demande d'accès, le système d'évaluation va décider d'un contexte de connexion en accord avec la politique de sécurité.

Un exemple simple de système d'évaluation serait l'utilisation des adresses MAC des systèmes d'extrémité pour déterminer leur VLAN d'appartenance, le choix de la mise en quarantaine serait fait si l'adresse MAC est inconnue. La complexité du système d'évaluation dépendra de la quantité d'informations obtenue sur les systèmes d'extrémité et de la complexité de la politique d'accès à mettre en place.

Et ce système doit être capable de rejouer l'évaluation de manière régulière, tout le temps de la connexion, permettant ainsi de se prémunir contre un changement d'état du système d'extrémité.

1.2.3 Le système de contrainte

1.2.3.1 Rôle du système de contrainte

C'est l'ensemble des éléments de l'infrastructure réseau permettant de détecter la demande d'accès au réseau et d'appliquer les décisions du système d'évaluation.

Dans le cas d'un NAC basé sur un matériel dédié (dit « appliance ») positionné en coupure sur le réseau, c'est généralement lui qui gérera la connexion du système d'extrémité dans son ensemble et mettra en œuvre la politique décidée par le système d'évaluation.

Si le système NAC n'est pas positionné en coupure (« out-of-band »), le système de contrainte doit s'appuyer sur l'infrastructure existante.

Les actions mises en œuvre par le système de contrainte sont les suivantes :

- positionner le système d'extrémité dans un VLAN particulier.
- mettre en place des contrôles d'accès aux niveaux 2, 3 ou 4 sur les équipements de bordure (commutateurs d'extrémité) ou plus près du cœur du réseau (routeurs, pare-feu, proxy).
- gérer la qualité de service, la bande passante.

1.2.3.2 Différents systèmes de contrainte

Utilisation d'un serveur dédié

Positionné en coupure, le serveur dédié capture l'ensemble des paquets.

- Avantages : facilité de déploiement, gestion centralisée.
- Difficultés : cela peut créer un Single Point Of Failure (SPOF), adaptation à la montée en charge difficile.
- Risque : les systèmes d'extrémité ont déjà un accès au réseau (ils se voient entre eux).

Utilisation du protocole 802.1X

Protocole d'accès au réseau, le 802.1X utilise EAP pour transporter les informations d'authentification entre le client et le serveur. Il est implanté aujourd'hui dans la plupart des équipements réseau, commutateurs et points d'accès sans-fil. Si l'authentification est valide, il est possible de modifier la configuration des ports du matériel réseau au travers d'attributs, le VLAN par exemple.

- Avantage : isolation au plus près de la demande d'accès.
- Difficultés : capacité des matériels existants, il faut un client sur le système d'extrémité, choisir la méthode d'authentification (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, etc).
- Risque : Dépendant de l'authentification utilisée (ex: EAP-MD5 est à éviter).

Utilisation du mécanisme VMPS (VLAN Management Policy Server)

C'est une technique utilisée sur les commutateurs Cisco permettant d'attribuer un VLAN à un port en fonction de l'adresse MAC de la machine connectée sur ce port. Nécessite un serveur où sont enregistrées les correspondances entre adresses MAC et numéro ou nom de VLAN.

- Avantage : la simplicité.
- Difficultés : maintenance de la base de données (adresses MAC/VLAN), gestion impossible de plusieurs adresses MAC par port, commutateurs Cisco seulement et en cours d'abandon par le constructeur.
- Risque : usurpation d'adresse MAC.

Utilisation du DHCP

pour envoyer le bon profil IP (adresse, routeur, masque) au système d'extrémité:

- Avantage: simplicité.
- Difficulté : aucune.
- Risque : le système d'extrémité doit jouer le jeu (ne pas utiliser d'adresse IP fixe).

-Utilisation de trap SNMP

émis par les matériels réseau, permettant de détecter la connexion physique d'un système d'extrémité.

- Avantage : adaptable à une grande partie des matériels réseau.
- Difficulté : aucune
- Risques : risque de déni de service avec des instabilités de liens, usurpation d'adresse MAC, les traps utilisent le protocole UDP ce qui n'assure pas la délivrance de l'information, besoin de maintenir un état de l'ensemble des ports.

1.2.4 Le système de mise en conformité

Dans le cas où le système d'extrémité n'a pas été jugé compatible avec la politique d'accès (manque de correctifs de sécurité, pas d'antivirus, échec de l'authentification, etc) il est

nécessaire de prévoir un contexte réseau où le système pourra se mettre en conformité (mise à jour système, possibilité de télécharger un antivirus, une base de signature à jour, demande de compte d'accès). Cette action de mise en conformité est parfois appelée « remédiation ».

La technique la plus communément employée est l'utilisation d'un VLAN spécifique redirigeant le trafic vers un portail captif Web qui doit guider l'utilisateur dans sa mise en conformité. Quelques difficultés apparaissent alors :

- gérer les matériels sans navigateur Web (imprimante);
- habituer l'utilisateur à ouvrir son navigateur en cas de soucis, même s' il ne souhaitait qu'utiliser son client de messagerie par exemple;
- personnaliser la page web en fonction du problème spécifique;

En plus de ces difficultés, un problème de sécurité est généré en positionnant dans le même réseau des machines potentiellement fragiles. Premièrement, il y a un risque de contamination mutuelle, deuxièmement, ce réseau peut être utilisé par un attaquant pour trouver des machines vulnérables.

Une autre technique est basée sur les capacités de l'agent, résidant sur le poste, à communiquer avec le système hôte ou à communiquer avec l'utilisateur. Sur instruction du système d'évaluation l'agent pourrait forcer une mise à jour logiciel ou donner les instructions adéquates à l'utilisateur.

1.2.5 Contrôle des activités

Après avoir subi l'ensemble des contrôles et avoir été positionné dans le contexte désiré, un système peut avoir un comportement ne répondant plus à la politique de sécurité. En observant par exemple la bande passante monopolisée par un utilisateur, il peut être utile d'utiliser les techniques de mise en conformité pour isoler et informer l'utilisateur du non respect de la charte qu'il a acceptée.

La mise en place de système de détection d'intrusions (IDS[14]), comportemental ou par signatures, peut aussi permettre de décider de la mise à l'écart d'un système d'extrémité de manière dynamique. Dans ce cas, la réactivité de l'infrastructure à se protéger est bonne mais le risque d'erreur est aussi important.

14 IDS : Intrusion Detection System – Un équipement ou une application qui contrôle le réseau ou les activités d'un système dans le but de détecter les activités suspectes ou des violations de politique de sécurité.

2

PARTIE 2 : LES SOLUTIONS EXISTANTES

2.1 Différentes approches

Les composants fondamentaux d'une solution NAC sont :

- Le système d'extrémité
- Le système de contrainte
- Le système de mise en conformité

Les offres des fournisseurs comprennent une combinaison de ces éléments. La compréhension de ces éléments permettra de différencier les offres de solutions d'un fournisseur à l'autre. Il existe sur le marché de nombreuses solutions et ce marché n'est pas encore mature.

2.2 Solutions commerciales

Les trois principaux acteurs commerciaux du NAC sont actuellement Microsoft, Cisco et Juniper.

2.2.1 Microsoft Network Access Protection

Quatre fonctionnalités:

- conformité à la politique de sécurité,
- mise en quarantaine (optionnelle),
- mise à niveau automatique (auto-remédiation),
- suivi en continu.

Le client/agent NAP[15] est disponible sur :

- Windows xp sp3, Vista, 7,
- Windows server 2008 , 2008R2, (client et serveur de la solution NAC),
- Il existe des agents pour Redhat, OpenSuse, Suse, Centos, Ubuntu, Fedora, Mac OS,
- Pas sur Windows mobile pour l'instant.

15 NAP : Network Access Protection

La politique de sécurité est définie sur un serveur (Policy Decision Point), vérifiée par des mesures faites sur la machine qui se connecte et qui possède l'agent NAP (Network Access Protection). L'agent NAP doit fournir un bilan de santé de la machine.
À l'agent NAP, sont ajoutés différents plugins SHA (System Health Agent) qui regardent chacun un aspect spécifique du système d'extrémité (anti-virus, pare-feu, registre, etc).

Du coté serveur sont installés un NPS (Network Policy Server) qui est un serveur RADIUS (toutes les demandes d'accès passent par lui), un serveur d'administration NAP et des SHV (System Health Validator) chargés de communiquer avec les SHA pour évaluer le système d'extrémité. Les SHV peuvent communiquer avec des serveurs de politique (exemple: serveur de correctifs). Le résultat de l'évaluation va conditionner le futur accès donné au système d'extrémité. Les échanges SHA – SHV respectent le protocole IF-TNCCS-SOH du TCG/TNC. Les SHA et SHV sont créés par les vendeurs de logiciels pour être intégrés à l'agent NAP.

Cinq méthodes de contraintes sont possibles:

- 802.1X : Le bilan de santé est fourni au moment de l'authentification qui n'est possible qu'en PEAP. En fonction du bilan de santé, le système d'extrémité est positionné dans un VLAN. Pour l'authentification trois processus doivent être lancés sur le poste (dot3svc, EapHost et l'agent NAP),
- IPSec : La connexion est acceptée si la machine présente un certificat de bonne santé. La PKI qui délivre le certificat de santé est mise en œuvre par le serveur NAP HRA (Health Registration Authority) en relation avec le serveur PDP (Policy Decision Point),
- DHCP : Le bilan de santé est donné au moment de la requête DHCP, le serveur DHCP fournit, soit une adresse valide, soit l'adresse ip=0.0.0.0, le masque=255.255.255.255 et une route vers des serveurs de remédiation. Il n'y a pas d'authentification, ce sont les options 220 MS Vendor du DHCP qui sont utilisés,
- VPN : Le bilan de santé est fourni au moment de l'authentification. C'est l'utilisation de filtres IP qui permet de délimiter l'environnement pour le système d'extrémité. L'authentification est faite en PEAP over PPP. C'est le serveur VPN qui gère

l'ensemble de la connexion en relation avec le serveur (Policy Decision Point),

- Terminal Server : RDP over HTTPS, donne accès à une station de travail, un serveur de terminaux ou à rien, en fonction du bilan de santé.

Au niveau de l'agent NAP, sont positionnés des EC (Enforcement Client) qui vont échanger avec des ES (Enforcement Server) que sont les serveurs VPN, IPSec, etc. La partie auto-remédiation est assurée en donnant un accès aux SHA à des serveurs WSUS (Windows Server Update Services) ou au site Web de Windows Update par exemple. Le suivi en continu est assuré par la capacité du serveur de conformité à être à l'initiative d'une nouvelle évaluation.

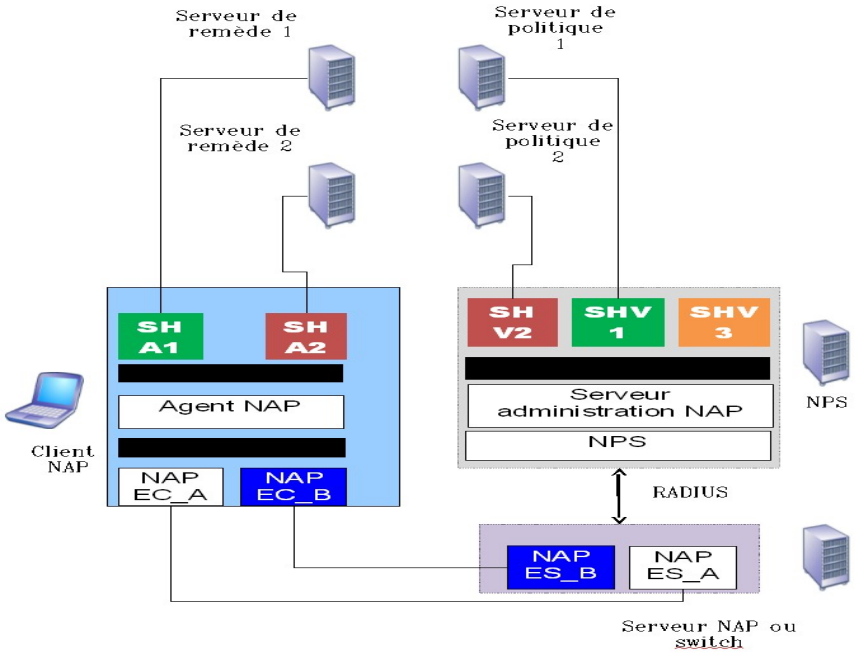

Figure 2: Schéma Microsoft NAP

2.2.2 Cisco NAC

La solution NAC proposée par Cisco est constituée de différents composants.

- Le « NAC Manager » est une interface Web permettant de créer les politiques de sécurité et de gérer les connexions en cours. Les différents profils utilisateurs associés aux vérifications de conformité, ainsi que les actions de remédiation, sont configurés sur ce serveur. Le Nac Manager communique et gère le NAC Server.
- Le « NAC Server » est un serveur qui va accorder ou non l'accès au réseau en fonction des informations recueillies sur les systèmes d'extrémité. C'est sur ce serveur que sont situés les profils de sécurité, les actions de remédiation etc... Ce serveur peut fonctionner en coupure ou « out of band » au niveau 2 ou 3.
- Le « NAC Agent » est un agent léger installé sur les postes, chargé de collecter des informations sur le poste et de les transmettre à l'ACS (serveur Radius Cisco) au moment de la demande de connexion.

Des composants additionnels sont aussi proposés.

- Le « NAC Profiler » est chargé d'évaluer les systèmes d'extrémité spécifiques comme les téléphones IP, les imprimantes, etc … Ce module permet aussi de localiser physiquement les matériels connectés et d'appliquer des profils en fonction d'informations récupérées.
- Le « NAC Guest Server » permet d'offrir et de gérer les accès pour les visiteurs.
- Le « Secure Access Control System » (ACS) est un serveur jouant le rôls de serveur Radius ou Tacacs[16] qui va accorder ou non l'accès au réseau aux utilisateurs. C'est lui qui communique avec les équipements réseaux sur lesquels les connexions sont faites en jouant le rôle d' « authenticator » lors de connexion 802.1X.

Le concept développé par Cisco est l'utilisation de l'ensemble des composants du réseau (commutateurs, routeurs, pare-feu, détecteurs d'intrusions...) pour collecter des informations ou pour appliquer la politique de sécurité décidée.

16 Tacacs : Terminal Access Controller Access-Control System – Protocole d'authentification distante utilisé généralement dans les réseaux UNIX pour communiquer avec un serveur d'authentification.

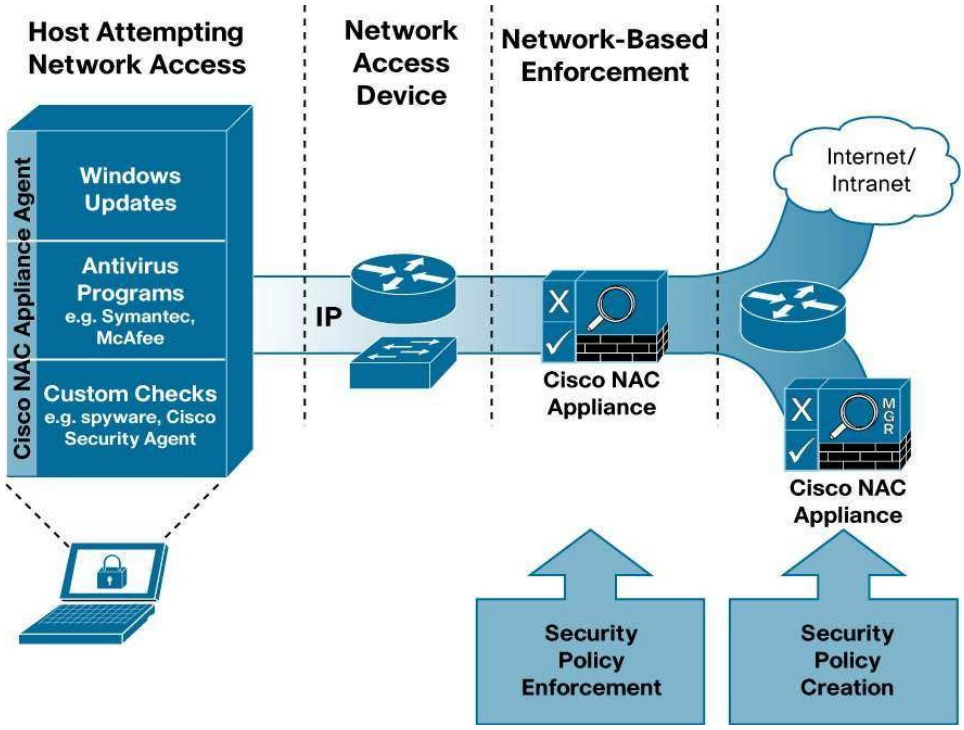

Figure 3: Architecture en ligne pour un serveur Cisco NAC

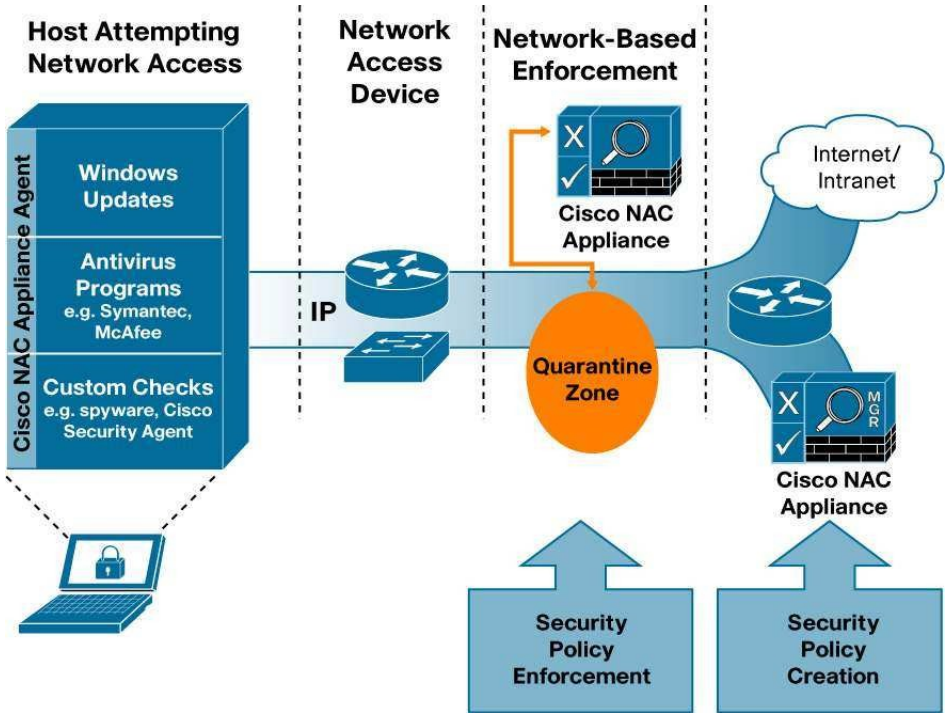

Figure 4: Architecture hors bande pour un serveur Cisco NAC

2.2.3 Juniper Networks UAC

La solution Juniper s'appuie sur les protocoles 802.1X, RADIUS, IPSec et sur les standards du TCG/TNC.

Les composants de la solution sont :

- Un agent UAC qui sert de client 802.1X et récupère les informations sur la machine (antivirus, pare-feu, niveau système …); toutes ces informations sont envoyées dans des attributs RADIUS,
- Un portail captif pour les accès « invité »,
- Authentification sur adresse MAC pour les imprimantes, etc,
- Une appliance, IC Series UAC; c'est un RADIUS pour la partie « Authenticator » du protocole 802.1X, qui prend les décisions du devenir de la connexion et agit sur le système de contrainte,
- Suivant l'infrastructure réseau, le système de contrainte peut être réduit aux capacités des commutateurs compatibles 802.1X et ne s'applique alors qu'au niveau 2. Avec des équipements Juniper (commutateurs, pare-feu, IPS15, VPN ..), il est possible d'exercer des contraintes de niveau 2 à 7. Avec les commutateurs Juniper, des contraintes sont possibles sur la bande passante, la QoS et d'autres fonctionnalités.

Les phases d'authentification et d'évaluation peuvent être répétées régulièrement.

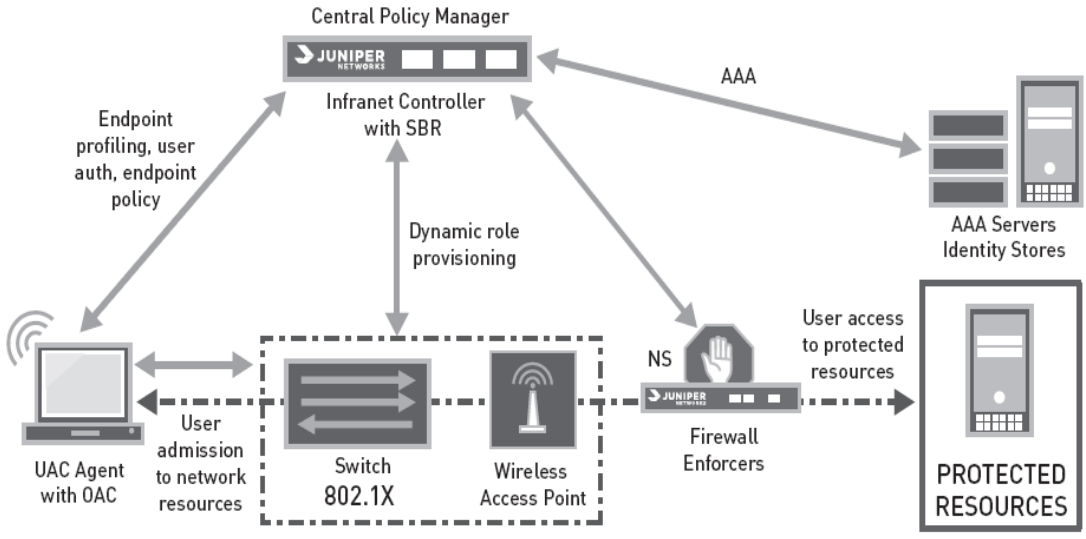

Figure 5: Schéma Juniper UAC

2.2.4 Enterasys

C'est une solution axée multi-constructeurs, Enterasys coopère avec Microsoft et siège au TCG/TNC.

Pour la solution Out-Of-Band:

- une appliance NAC, c'est un proxy RADIUS qui s'appuie sur les méthodes d'authentification classiques.
- des logiciels (et briques logiciels) sur appliance ou sur serveur (Netsight/NAC Manager).

Quatre briques fonctionnelles principales:

- Visibilité des informations :
  associations UserName/MAC/OS/IP/DNS/Commutateur/Port/... en temps réel et conservation de l'historique. La détermination des systèmes d'exploitation est basée sur un mécanisme de prise d'empreinte DHCP,
- Accès :
  Utilisation du protocole 802.1X et de l'authentification sur adresse MAC (dans ce cas c'est l'appliance qui termine la session EAP), une autre fonctionnalité : le « AAA MAC Locking » qui permet de verrouiller la position d'une adresse MAC sur un port de commutateur,
- Réseau invité :
  c'est un portail Web, l'enregistrement de l'adresse MAC peut être sponsorisée par une personne tiers, sinon l'obtention d'un compte suffit aux visiteurs pour valider leurs adresses MAC sur le portail.

La partie évaluation est composée de trois possibilités:

- agent enterasys, il peut être temporaire (Code Java) ou bien permanent (nécessite un accès administrateur sur le poste). Les OS supportés sont Windows, Mac OSX (bientôt...) mais pas Linux,

- Le NAP de Microsoft est supporté, le serveur NAP Microsoft est nécessaire,
- Sans agent : des « connecteurs » existe avec les logiciels Nessus[17] et eEye[18], il est aussi possible développer d'autres connecteurs au travers d'API XML.

Pour la partie post-connexion :

- répétition possible des phases d'authentification et de vérification,
- action sur événement (logiciel spécifique en plus) sur messages SNMP (générés par IDS,pare-feu,....), action et notification au NAC ce qui évite les problèmes de changement de prise de l'utilisateur fuyant les restrictions.

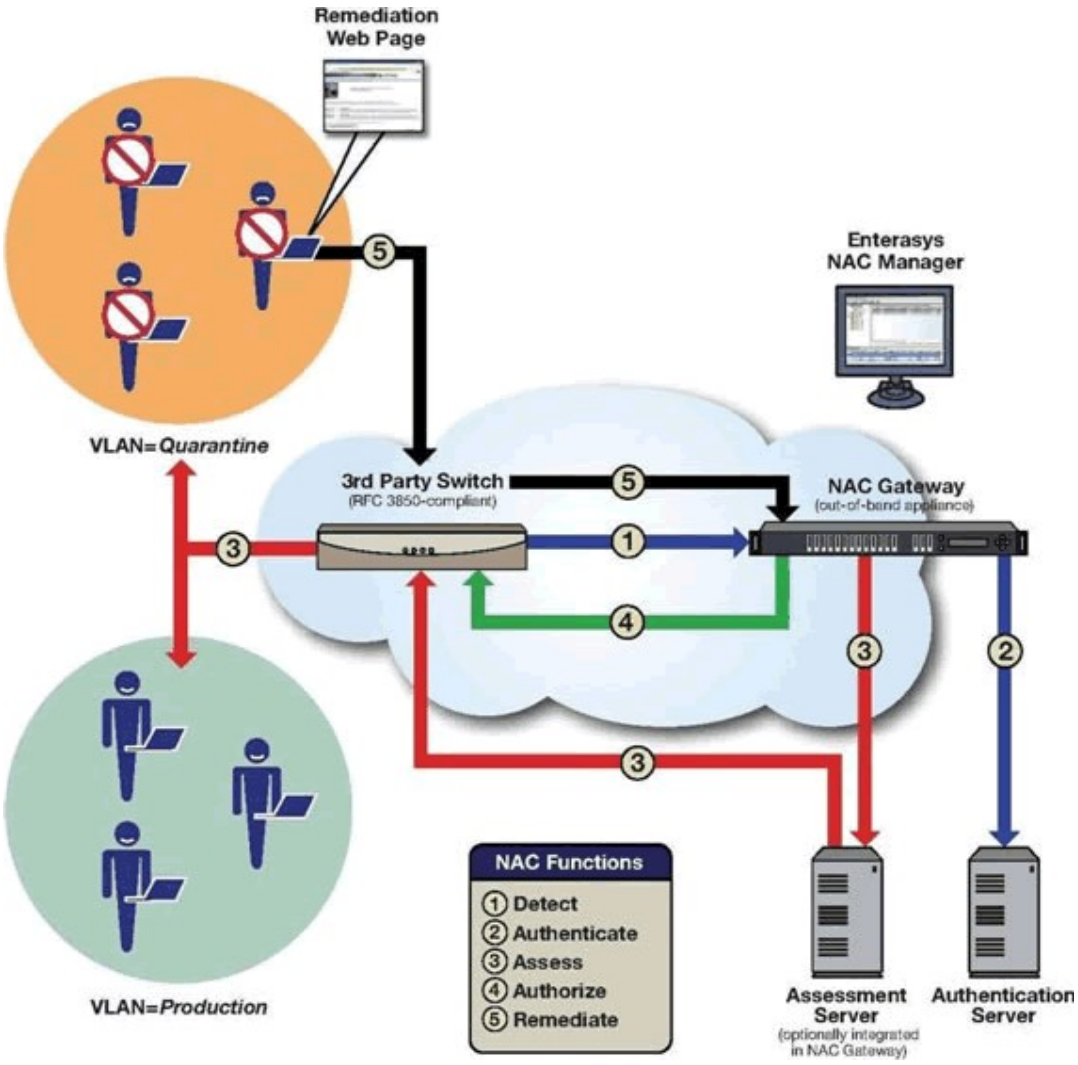

Figure 6: Schéma Enterasys NAC

17 Nessus : Application propriétaire permettant de scanner un système pour détecter des vulnérabilités et les corriger.
18 eEye : Application propriétaire permettant de scanner un système pour détecter des vulnérabilités et les corriger.

2.3 Solutions libres ou open source

2.3.1 PacketFence

PacketFence est une solution de conformité réseau entièrement libre et opensource. Il possède un grand nombre de fonctionnalités. Parmi celles-ci :

- L'enregistrement des composantes réseau grâce à un portail captif,
- Le blocage automatique, si souhaité, des appareils indésirables tels les iPod, Iphone, PlayStation, bornes sans fil etc ... ,
- La vérification de la conformité des postes présents sur le réseau (logiciels installés, configurations particulières, etc.),
- Une gestion des invités sur le réseau,
- Plusieurs mécanismes de contrôle d'accès incluant à base de rôles (RBAC[19]),
- L'intégration avec divers détecteurs de vulnérabilités et d'intrusions,
- La comptabilisation de l'utilisation de la base passante de tous les équipements.

19 RBAC : contrôle d'accès à base de rôles est un modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est attaché.

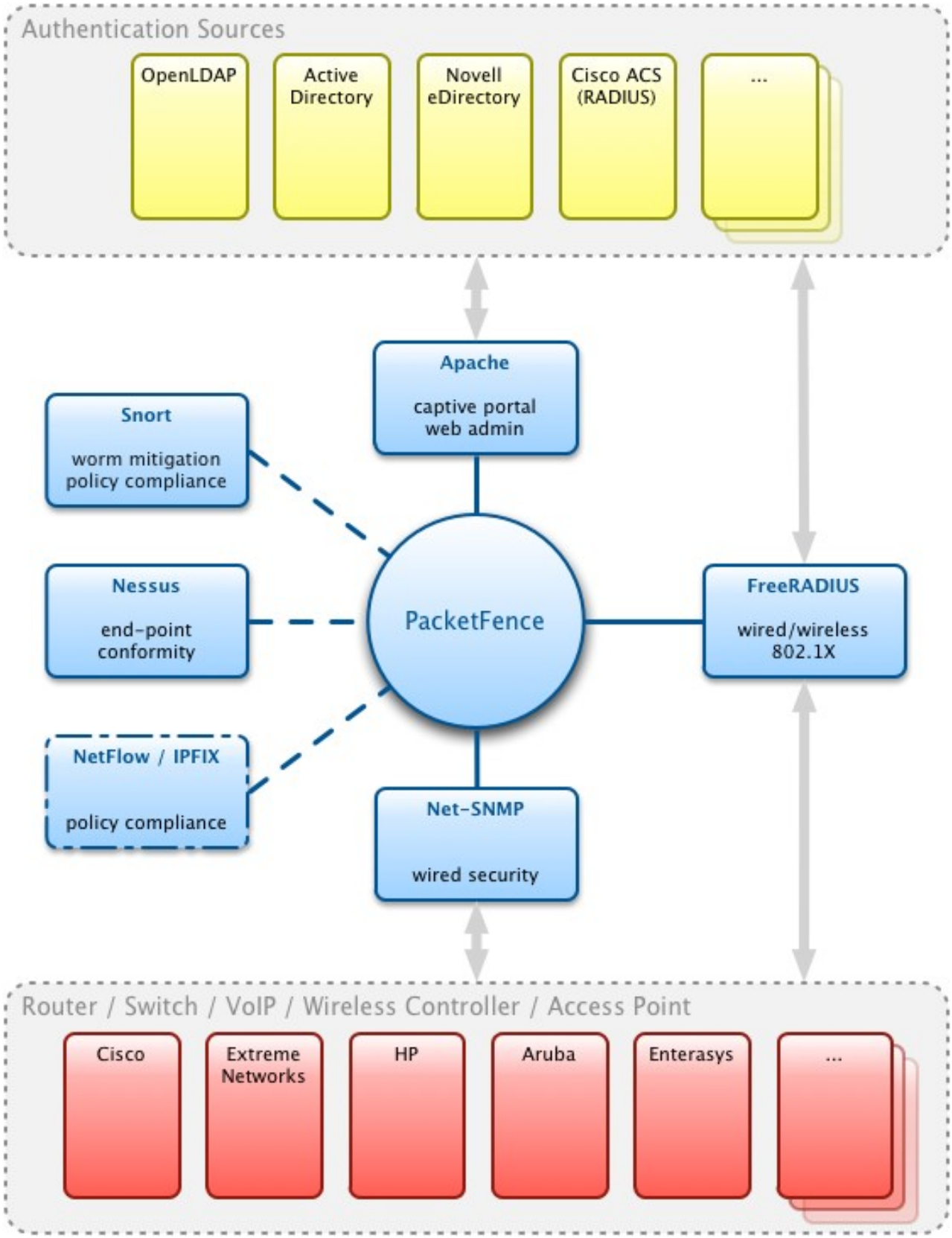

Figure 7: Les composants de PacketFence

2.3.2 KU RINGS Security Analyzer

Créé à l'Université du Kansas, c'est un portail Web qui utilise une applet java pour évaluer (système, logiciel anti-virus, etc) les machines cherchant à accéder au réseau (autorisation valide pendant sept jours). En cas d'échec, les accès sont réduits aux sites de mises à jour de logiciels, d'anti-virus, ...

La solution KU RINGS Security Analyzer effectue les vérifications suivantes :

- Présence d'antivirus installé (recherche des programmes Sophos, Microsoft Security Essentials, MacAfee 2007, McAfee Enterprise 8.5 Antivirus, Zone Alarm Antivirus, Norton, Avast, AVG, PC Cillin, V-Com, Clam AV, ClamX AV, NOD32 or Symantec antivirus).
- Pour Macintosh – il ne peut tourner que sur Mac OS X 10.4 ou plus récent.
- Pour Windows, les versions antérieures Windows 95/98/ME ne sont pas supportées. Il fonctionne cependant sur Windows XP SP2, Windows 2000 SP4, Vista ou Seven.
- La mise à jour automatique doit être configurée sur Windows pour le téléchargement et l'installation.
- le pare-feu doit être fonctionnel. Une vérification est faite pour s'assurer de l'installation et de l'activation du pare-feu de Windows ou de Mac OSX. Le pare-feu Windows est le seul autorisé sur les machines Windows. Pour les distributions linux, IP Tables doit être activé.

2.3.3 FreeNAC

Présenté comme offrant une gestion simplifiée des VLANs, un contrôle d'accès au réseau et un outil d'inventaire, FreeNAC est basé principalement sur le protocole VMPS (authentification sur adresse MAC). Il permet aussi l'utilisation du 802.1X en interaction avec un serveur RADIUS. La partie évaluation n'est pas prise en compte.

En mode VMPS, quand un switch compatible détecte un nouvel ordinateur, il crée une requête VMPS demandant l'autorisation de FreeNAC. Celui-ci vérifie sa base de données et en réponse refuse ou permet l'accès au réseau, basé sur l'adresse MAC du PC. Le switch applique la décision prise par FreeNAC et refuse l'accès ou, en cas de succès, envoie dynamiquement l'ordinateur dans un VLAN prédéterminé.

En mode 802.1X, FreeNAC vérifie les autorisations des utilisateurs (grâce à l'utilisation d'un serveur d'authentification tierce partie) et utilise l'adresse MAC de l'équipement se connectant pour lui attribuer un VLAN. Cela crée une combinaison nom d'utilisateur / mot de passe qui est unique pour chaque client qui se connecte.

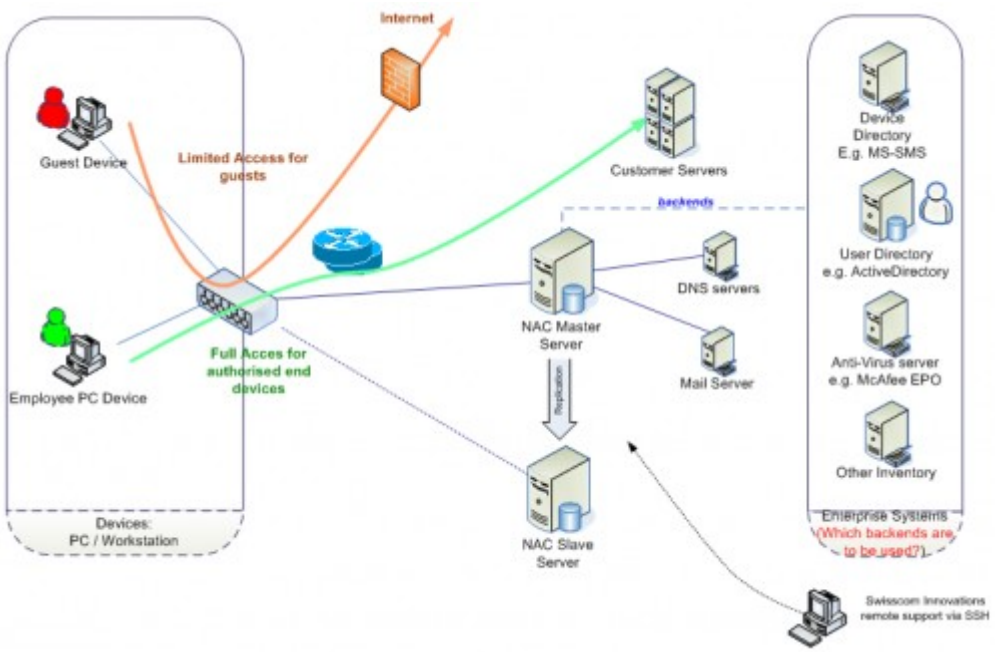

Figure 8: Architecture FreeNAC

3

PARTIE 3 : DU NAC A LA REALITE

L'absence initiale de normalisation et les différents enjeux auxquels se confronte le NAC ont généré une multitude de réponses. Les solutions émanent aussi bien des constructeurs de matériel réseau, de concepteurs de logiciel ou de sociétés de service, l'offre est pléthorique et diversifiée. Mais toutes les offres se basent sur des principes et des technologies communes. Au moment de choisir une solution, il faudra faire le tri entre ces différentes technologies et les besoins de l'entreprise.

3.1 Normalisation de l'agent

3.1.1 IETF

L'Internet Engineering Task Force (IETF) a constitué un groupe de travail, le Network Endpoint Assessment (NEA). Ce groupe de travail, reconnaissant qu'un certain nombre de protocoles existaient déjà dans le domaine du NAC, a décidé de publier un ensemble d'exigences concernant l'aspect client/serveur avec la RFC[20] 5209.

Le principe retenu côté client NEA est constitué d'échanges entre des « collecteurs de posture » (Posture Collectors) qui sont chargés de récolter des informations sur le client.
Ces « collecteurs de posture » transmettent les informations à un « broker » au travers d'une API qui va, à son tour, les transmettre à un ou plusieurs « demandeurs d'accès réseau » (Posture Transport) qui sont chargés d'effectuer la partie authentification de l'accès au réseau et d'envoyer ces informations au serveur NEA.

Du coté serveur, on retrouve les trois niveaux avec une différence au niveau « collecteurs de posture » puisque dénommé ici « vérificateurs de posture » (Posture Validators).

20 RFC : requests for comments, littéralement « demande de commentaires », sont une série numérotée de documents officiels décrivant les aspects techniques d'Internet, ou de différent matériel informatique (routeurs, serveur DHCP).

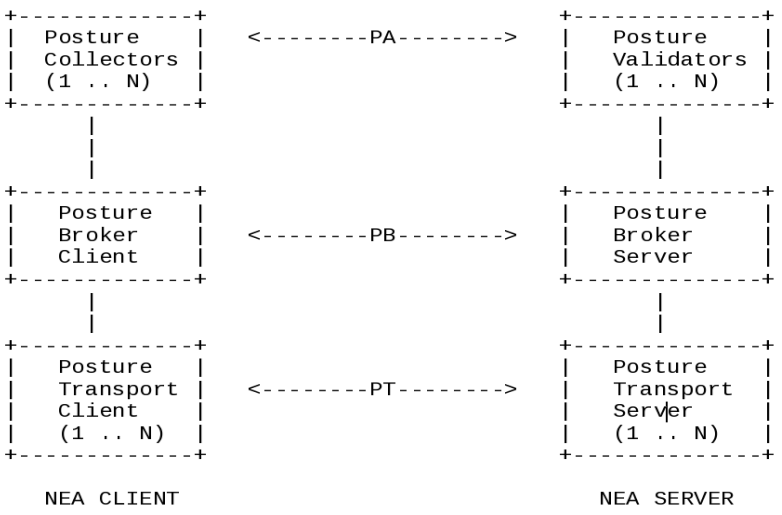

Figure 9: NEA Reference Model

La priorité du travail de l'IETF a été positionnée sur l'interopérabilité entre clients et serveurs. Suite à cette publication, un appel a été lancé pour recueillir des propositions de spécifications de protocoles répondant aux exigences de la RFC 5209. Une seule proposition a été faite à l'IETF avec les protocoles « nea-pa-tnc » et « nea-pb-tnc » qui décrivent respectivement les protocoles IF-M 1.0 et IF-TNCCS 2.0 développés par le Trusted Computing Group (TCG). Une analyse de compatibilité de ces deux protocoles avec la RFC 5209 est positionnée en annexe à ces deux drafts.

3.1.2 Trusted Computing Group (TCG) et Trusted Network Connect (TNC)

Le TCG est un regroupement d'industriels ayant pour but, à l'origine, le développement de ce que l'on appelle « une informatique de confiance ». Créateur du Trusted Platform Module (TPM[21]), le groupement propose une architecture ouverte et un ensemble de standards concernant le NAC, le Trusted Network Connect (TNC).

21 TPM : Trusted Platform Module est un composant cryptographique matériel, sur lequel s'appuie l'implémentation au niveau matériel du système Next-Generation Secure Computing Base (NGSCB).

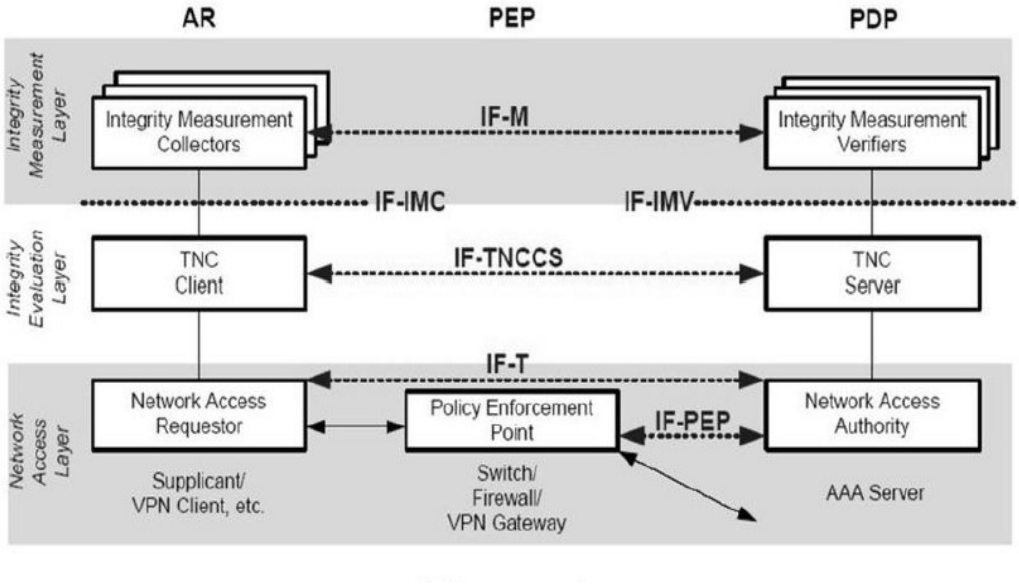

Figure 10: Modèle TCG/TNC

3.2 Technologies utilisées

Le concept NAC se base sur un certain nombre de technologies qui sont combinées suivant les constructeurs et leur approche de solution.

3.2.1 802.1x

EAP & 802.1x

802.1x est un standard IEEE qui permet l'authentification basé sur les ports dans un LAN. Une connexion est initiée avec demande d'identifiant et de mot de passe pour prévenir les accès des dispositifs non autorisés. Il est efficient aussi bien pour l'authentification et le contrôle du trafic des utilisateurs que par les clés cryptées. Il attache le protocole EAP dans des paquets Ethernet et supporte plusieurs méthodes d'authentification comme les certificats, les clés publiques …

EAP a vu le jour pour répondre aux besoins de sécurité des entreprises. Il présente une structure générale pour plusieurs mécanismes d'authentification et refreine ainsi l'évolution des mécanismes propriétaires. EAP permet une opération souple pour presque tout, que ce soit les mots de passe, les mécanismes de défis/réponses ou les certificats numériques. Le standard 802.1x fait passer le protocole EAP à travers des connexions LAN filaires ou wi-fi sans le protocole PPP d'où EAP est extrait. Il permet donc l'utilisation de l'EAP dans les paquets Ethernet sans les autres fonctionnalités de PPP.

802.1x a été développé pour certains besoins clés à savoir : le contrôle du réseau au niveau des ports, l'utilisation du protocole AAA pour fournir ses fonctionnalités aux clients 802.1x, la sécurité des réseaux étendus aux aires publiques (universités, place publiques …) et la distribution de clés cryptées de façon dynamique.

Avantages du standard 802.1x

On peut retenir les points ci-dessous comme étant les principaux avantages du 802.1x

• Standards ouverts : 802.1x utilise des normes existantes : EAP (RFC 2284), RADIUS (RFC 2138, 2139) et permet une interopérabilité dans l'identification d'utilisateurs, une authentification centralisée et une gestion des clés.

• Identification d'utilisateur : L'identification basée sur Network Access Identifier (RFC 2486) supporte l'accès en itinérance sur les aires publiques (RFC 2607).

• Gestion de clé dynamique.

• Administration centrale des utilisateurs : L'utilisation du RADIUS (RFC 2138, 2139) permet une gestion centralisée de l'authentification, de l'autorisation et la comptabilité (AAA - Authentication Autorisation and Accounting). RADIUS peut aussi encapsuler les paquets EAP.

• Authentification extensible : EAP est conçu pour fournir de nouvelles méthodes d'authentification sans aucun changement sur le point d'accès. La RFC 2284 permet l'authentification par mot de passe (EAP-MD5) ou par One-Time Passwords (OTP).

Composition d’un système 802.1x

Les principaux éléments d’un système 802.1x sont :

- le demandeur : c’est le dispositif client qui demande l’accès aux ressources offertes par le système,
- le port : l’endroit où le dispositif client se raccorde au LAN. C’est soit directement au switch soit par un point d’accès wi-fi,
- l’authentificateur : il s’agit de l’élément qui lance un défi au demandeur avant de l’autoriser à trafiquer via le port. L’authentificateur communique avec le dispositif client et soumets l’information reçue de lui au serveur approprié. Ceci permet à déterminer le contexte du port connecté. La fonction de l’authentificateur est indépendante de la méthode d’authentification,
- le protocole EAP (Extensible Authentication Protocol) : le standard 802.1x utilise ce protocole comme un moyen d’authentification. EAP transporte les messages d’authentification entre le demandeur et le serveur d’authentification. Aucun autre élément (point d’accès, proxy ou autre) ne participe à cet échange,
- le protocole EAPOL (Extensible Authentication Protocol Over LAN) : le protocole EAPOL capture les messages EAP pour l’implémentation du service de gérance MAC dans un LAN. Il fournit les fonctions comme start ou log off de port ou encore la distribution de clé,
- le serveur RADIUS (Remote Access Dial In User Service) : le serveur RADIUS gère la base de données des utilisateurs, fournit l’authentification par vérification d’identifiant et de mot de passe et de façon optionnelle, fournit l’attribution dynamique de VLAN ou d’informations de comptabilité (durée de connexion, volume de transfert de données d’un utilisateur).

Processus d'authentification

Dans le processus d'authentification, les dispositifs connectés utilisent les paquets EAP pour effectuer l'authentification des ports. Aucun demandeur ne peut accéder à des ressources autres que l'authentificateur tant que le processus d'authentification n'a réussi. Le port reste alors dans un état non autorisé jusqu'à la fin où il passe à un nouvel état autorisé. Les étapes suivantes décrivent le processus d'authentification et d'autorisation.

- Étape 1 : Soit l'authentificateur, soit le demandeur initie un échange de messages d'authentification. L'authentificateur envoie le message EAP-Request/Identity quand c'est lui qui initie l'échange. Le demandeur envoie le message EAPOL-Start lorsque c'est lui qui initie. C'est à cette requête que l'authentificateur répond en envoyant son message EAP-Request/Identity.
- Étape 2 : Le demandeur envoie le message EAP-Response/Identity via le l'authentificateur au serveur d'authentification qui confirme son identité.
- Étape 3 : Le serveur d'authentification choisit un algorithme pour vérifier l'identité du demandeur. Cet algorithme peut être : EAP-MD5 (Message Digest 5) ou EAP-OTP (OneTime Password). Le serveur envoie alors au demandeur un message EAP-Request correspondant.
- Étape 4 : Le demandeur fournit ses références d'identité via un message de réponse EAP-Response approprié.
- Étape 5 : Le serveur d'authentification envoie soit un message de succès EAP-Success soit un message d'échec EAP-Failure.
- Étape 6 : Suite à une réussite d'authentification, le port sous le contrôle 802.1x prend l'état autorisé et le dispositif demandeur à un accès total aux ressources offertes via ce port.
- Étape 7 : A l'envoi du message EAPOL-Logoff à l'authentificateur, le port sous contrôle 802.1x passe à l'état non autorisé.

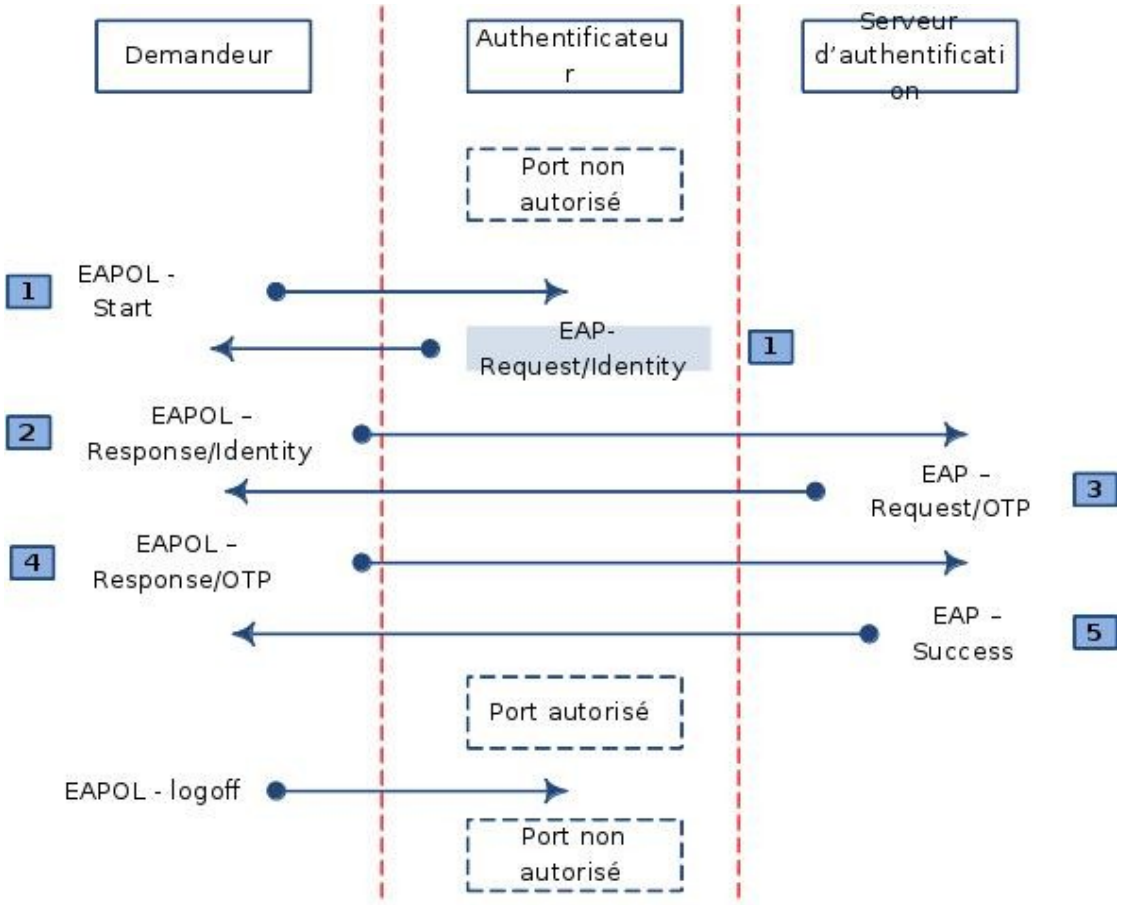

Figure 11: Requêtes 802.1X

Types d'EAP

Différents types du protocole EAP ont été conçu pour supporter les authentificateurs et leur politiques de sécurité dans le réseau correspondant. Les plus utilisés de ces types sont décrits ci-dessous.

- EAP-MD5 (Message Digest)

  EAP-MD5 est un algorithme de sécurité EAP qui constitue le niveau de base. EAP-MD5 utilise un message de 128 bits (hash du challenge du serveur et du mot de passe de l'utilisateur) pour vérifier l'authenticité du demandeur. Il est parfait pour les réseaux locaux de confiance où le risque sécuritaire est faible. Il n'est pas recommandé pour les réseaux publics ou les réseaux wi-fi puisqu'il fournit une authentification dans un seul sens. Sans une authentification mutuelle, des individus externes aux réseaux peuvent facilement sniffer l'identité et le hash d'une station ou se faire passer pour un

point d'accès et collecter les infos de stations se connectant.

- EAP-OTP

  EAP-OTP est similaire à EAP-MD5 à l'exception qu'il utilise One-Time Password comme réponse. La requête contient un message affichable. Le mécanisme OTP définit par la RFC 2289 est employé abondamment dans les scénarios VPN et PPP mais pas dans le monde sans fil.

- Lightweight EAP (LEAP)

  LEAP supporte l'authentification mutuelle et utilise les clés WEP pour chiffrer les données transmises. L'authentification mutuelle réduit les risques de point d'accès déguisé qui est un type d'attaque d'homme du milieu. Cependant, les identités des stations et les mots de passe restent vulnérables aux attaques de dictionnaire ou avec des outils de sniff. LEAP est souvent utilisé par des entreprises qui souhaitent modestement élever le niveau de sécurité dans leur réseau.

- EAP with Transport Layer Security (EAP-TLS)

  EAP-TLS est basé sur SSL (Secure Sockets Layer) qui est utilisé pour sécuriser la majorité des transactions web aujourd'hui. Il requiert une authentification mutuelle du client et du réseau à base de certificat. Le serveur RADIUS et le client doivent prouver leur identité avec des clés publiques sous forme de certificat numérique. Appliqué aux solutions sans fil, les clés WEP d'utilisateurs ou de sessions peuvent être générées de façon dynamique pour sécuriser la communication future entre le client WLAN et le point d'accès. Un tunnel TLS très résistant aux attaques de dictionnaire et d'homme du milieu, sécurise cet échange. EAP-TLS a également des inconvénients. On peut toujours sniffer l'identité d'une station (nom donné au certificat). Aussi, les certificats doivent être gérés du côté serveur comme du côté client.

- EAP avec Tunneled TLS (EAP-TTLS) et Protected EAP (PEAP)

  EAP-TTLS et PEAP ont tous deux été conçus pour simplifier l'application du 802.1x. EAP-TTLS utilise l'authentification mutuelle entre client et réseau, à base de certificats au travers d'un tunnel sécurisé par clé WEP d'utilisateur ou de session. Contrairement à EAP-TLS, EAP-TTLS nécessite seulement les certificats du côté serveur. Comme EAP-TLS, PEAP authentifie les clients d'un LAN sans fil en utilisant

seulement les certificats du coté serveur. Ceci permet l'implémentation et l'administration d'un réseau LAN sans fil sécurisé. EAP-TTLS et PEAP présentent la même efficacité qu'EAP-TLS à propos des écoutes de réseaux.

	Serveur d'authentification	Méthodes d'authentification	Délivrance de clé dynamique	Risques sécuritaires
EAP-MD5	NON	Hash de mot de passe	NON	Attaque: l'homme du milieu Détournement de session
LEAP	Hash de mot de passe	Hash de mot de passe	OUI	Identité exposée Attaque par dictionnaire
EAP-TLS	Clé publique (certificat)	Clé publique (certificat ou SMART Card)	OUI	Identité exposée
EAP-TTLS	Clé publique (certificat)	CHAP, PAP, MS-CHAP (v2), EAP	OUI	Attaque: l'homme du milieu
PEAP	Clé publique (certificat)	Tout ERings Security AnalyserAP comme EAP-MS-CHAPv2 ou Clé publique	OUI	Attaque: l'homme du milieu Identité caché en phase 2 mais potentiellement exposée en phase 1

Figure 12: Différents types d'EAP

Caractéristiques avancées

- Allocation de VLAN

  Dans un environnement contenant d multiples VLANs, il peut être bénéfique d'assigner le même VLAN aux utilisateurs itinérants quel que soit l'endroit d'où ils se connectent au réseau. Par exemple, les utilisateurs travaillant dans plusieurs bureaux à la fois, ou ayant besoin des mêmes droits d'accès dans les salles de conférence que dans leur bureau ont soit besoin d'un accès total au réseau soit besoin d'un accès restreint suivant les exigences de leur travail. C'est aussi la même idée lorsqu'il s'agit de différencier les accès suivant qu'un individu est manager, employé ou invité dans une entreprise.

- VLAN Invités

  En offrant un accès internet aux invités dans une entreprise pour leur permettre de joindre le réseau de leur entreprise, il faut s'assurer que leur accès au réseau local est suffisamment restreint. Avec un VLAN invité, un utilisateur qui tente de se connecter sans avoir un client 802.1x sera automatiquement migré dans ce VLAN dont les accès sont réduits uniquement à internet par exemple. Par contre, tout échec d'authentification doit également empêcher l'utilisateur d'accéder à quoi que ce soit y compris ce VLAN.

- Contrôle d'accès

  Le contrôle d'accès est une caractéristique qui permet de créer des « access list » basés sur des filtres, de façon dynamique sur un port. Suivant l'utilisateur qui s'authentifie, ces liste d'accès peuvent primer sur l'appartenance à un VLAN. Ceci permet une répartition du réseau en zones dans lesquelles on retrouve des utilisateurs ayant des droits d'accès similaires. Par exemple, la limitation de bande passante peut être appliquée à tous les ports configurés dans le VLAN invité de façon à ce que ces invités ne puissent monopoliser la connexion internet de l'entreprise hôte.

3.2.2 Radius

Origine & Principes généraux

RADIUS avait tout d'abord pour objet de répondre aux problèmes d'authentification pour des accès distants, par liaison téléphonique, vers les réseaux des fournisseurs d'accès ou des entreprises. C'est de là qu'il tient son nom qui signifie Remote Access Dial In User Service. Au fil du temps, il a été enrichi et on peut envisager aujourd'hui de l'utiliser pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil.

RADIUS est donc un protocole d'authentification qui a été initialement mis au point par un projet de la société Livingston. Sa première version en Janvier 1997 est définie par les RFC 2058 et 2059. La deuxième version en Avril 1997 est fixée par les RFC 2138 et 2139. Enfin la troisième et dernière version est élaborée en Juin 2000 et défini par les RFC 2865 (authentication) et 2866 (accounting).

Principes de fonctionnement

Le protocole RADIUS repose essentiellement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Il n'y a jamais de communication directe entre cet utilisateur et le serveur.

L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré. Le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS. Le serveur traite les demandes d'authentification en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateurs, de machines ou de domaines. Pour cela, RADIUS dispose pour cela d'un certain nombre d'interfaces ou de méthodes.

Le protocole répond au modèle AAA. Ces initiales résument les trois fonctions du protocole :

- A = Authentication : authentifier l'identité du client ;
- A = Authorisation : accorder des droits au client ;
- A = Accounting : enregistrer les données de comptabilité de l'usage du réseau par le client.

Le protocole établit une couche applicative au-dessus de la couche de transport UDP. Les ports utilisés sont : 1812 pour recevoir les requêtes d'authentification et d'autorisation et 1813 pour recevoir les requêtes de comptabilité. Le choix est porté sur UDP parce que RADIUS est un protocole sans état et n'exige pas une détection "sensible" de la perte de données. Aussi, l'idée de permettre à un serveur secondaire de répondre à une demande d'authentification (lorsque le principal ne répond pas) confère à UDP une simplification de la mise en œuvre du serveur.

Le scénario de fonctionnement peut être décrit à travers les étapes ci-dessous :

- Envoie d'une requête au NAS pour autorisation d'une connexion à distance
- Acheminement de la demande du NAS au serveur RADIUS : Access-Request
- Consultation de la base de données au niveau du serveur pour déterminer le type de scénario d'identification demandé
- Si le scénario actuel ne convient pas, une autre méthode d'identification est demandée à l'utilisateur. Au point de convenance des deux parties sur la méthode, le serveur retourne l'une des trois réponses suivantes : Access-Accept, Access-Reject ou Access-Challenge. Access-Accept est envoyé par le serveur pour autorisé la connexion si la vérification des informations est correcte. En cas d'échec, Access-Reject est envoyé. Le serveur envoie Access-Challenge pour demander la réémission d'un access-request ou des informations complémentaires.
- Une autre réponse est possible : CHANGE PASSWORD où le serveur RADIUS demande à l'utilisateur un nouveau mot de passe
- Après cette phase d'authentification est suivie une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

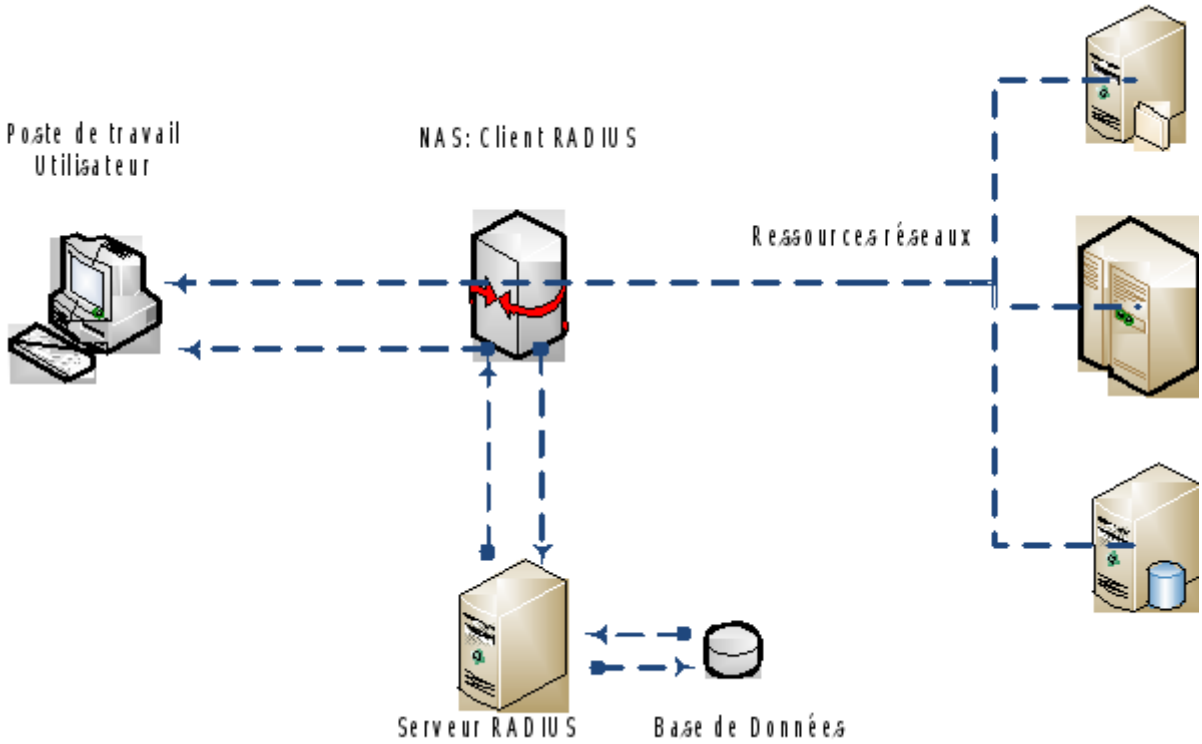

Figure 13: Architecture RADIUS

De façon native, RADIUS utilise les protocoles PAP et CHAP pour l'échange des mots de passe. Avec PAP, les données sont échangées en clair. Pour CHAP, l'échange est basé sur des hash de part de d'autre et seul le challenge est envoyé. Le protocole RADIUS prévoit deux attributs séparés pour gérer ceci : User-Password et CHAP-Password. Par la suite, les variations Microsoft s'y sont greffées et l'on a aujourd'hui MS-CHAP et MS-CHAP-V2.

Limitations

RADIUS a été conçu pour des identifications par modem, sur des liaisons lentes et peu sûres

- c'est la raison du choix du protocole UDP (discuté plus haut)
- ce choix technique d'un protocole non agressif conduit à des échanges laborieux basés sur des temporisations de réémission, des échanges d'accusés-réceptions.
- DIAMETER[22] (qui vient remplacer RADIUS) utilise TCP ou STCP.

22 DIAMETER : est un protocole d'authentification, successeur du protocole RADIUS.

RADIUS base son identification sur le seul principe du couple nom/mot de passe :

- parfaitement adapté à l'époque (1996),
- cette notion a dû être adaptée.

RADIUS assure un transport en clair, seul le mot de passe est chiffré par hachage :

- la sécurité toute relative du protocole repose sur le seul "shared secret" et impose la sécurisation des échanges entre le client et le serveur par sécurité physique ou VPN
- DIAMETER peut utiliser IPSec ou TLS.

RADIUS limite les attributs :

- gérés sous forme de chaîne "Pascal" avec un octet en entête donnant la longueur, à 255 octets, ce qui était cohérent avec la notion de nom/mot de passe,
- mais inadapté à toute tentative d'introduction de la biométrie (fond d'œil, empreinte digitale) de cryptographie (certificat),
- DIAMETER utilise des attributs sur 32 bits au lieu de 8 (déjà présents dans certaines extensions EAP de RADIUS, notamment TTLS).

RADIUS est strictement client-serveur :

- d'où des discussions et bagarres de protocoles propriétaires quand un serveur doit légitimement tuer une session pirate sur un client,
- DIAMETER possède des mécanismes d'appel du client par le serveur.

RADIUS n'assure pas de mécanismes d'identification du serveur :

- se faire passer pour un serveur est un excellent moyen de récolter des noms et mots de passe,
- EAP assure une identification mutuelle du client et du serveur.

3.2.3 VMPS

Objectifs et contraintes

Les solutions d'authentification locale comme 802.1x fonctionnent bien. Cependant, pour les ordinateurs plus anciens, de l'ère d'avant Windows XP, il n'est pas possible d'effectuer une authentification de l'utilisateur de manière fiable. Pour ces cas, une autre mesure d'authentification a été mise en place : il s'agit de VMPS (VLAN Membership Policy Server). VMPS est un protocole propriétaire Cisco qui permet de forcer le VLAN d'un port d'un commutateur en fonction de l'adresse MAC de la machine qui est connectée dessus. Ce n'est pas une authentification de l'utilisateur mais, une identification de la machine connectée. Cette mesure est un palliatif en attendant la compatibilité de tous les équipements à 802.1x.

Parmi les configurations à faire du VMPS, une table est construite pour faire correspondre les adresses MAC à des VLANs valides du réseau connecté. Cette base de données VMPS est placée sur un switch dans le réseau de façon à ce qu'il se comporte comme un serveur VMPS vers lequel des requêtes seront envoyées. Un ordinateur au démarrage et après activation de sa carte réseau accède au switch qui dans son environnement utilise le protocole VQP VLAN Query Protocol pour déterminer le VLAN à assigner à ce port. La base de données VMPS est maintenue manuellement et suivant la taille de l'entreprise peut être mise à jour dix fois ou plus en une journée. Le serveur hébergeant le fichier de configuration vmps.cfg est un switch Cisco. Ce fichier se transmet aux serveurs VMPS via le protocole TFTP. Il est aussi possible d'avoir un serveur primaire et un autre secondaire pour assurer la disponibilité.

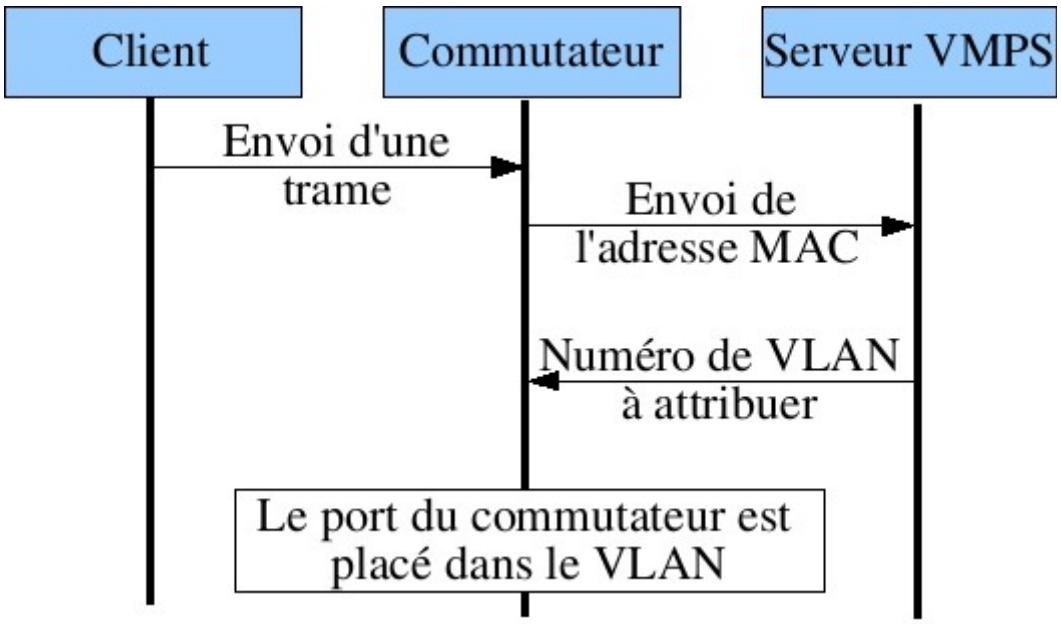

Figure 14: Fonctionnement de VMPS

VQP utilise le port UDP 1589 pour l'échange entre les switchs. Le protocole UDP ne supportant aucune forme d'authentification, l'utilisation du VQP dans un environnement sensible parlant de sécurité n'est pas conseillée. Une attaque par spoofing peut facilement s'opérer pour empêcher des connexions au réseau ou accéder à des VLANs non autorisés.
VQP et VMPS sont rarement utilisés pour l'attribution de VLAN base sur les adresses MAC principalement à cause du maintien manuel de la table de correspondance MAC – VLAN.

Inconvénients avec VMPS

Il existe un certain nombre d'imperfections au sujet du VMPS. Un attaquant qui sait ce qu'il fait peut octroyer une adresse IP statique au système et le corrompre en gérant localement les adresses MAC. L'historique des adresses MAC maintenue est donc mis en cause et devrait être soumis à un audit régulièrement. Un autre souci au niveau des serveurs VMPS est la consommation élevée des cycles du processeur suivant le nombre d'utilisateurs et la taille de la base de données. Le manque de maintenance régulière peut facilement entrainer des milliers d'entrées dans la base pour une entreprise moyenne. Dans ces cas de figures, les logs montrent des messages abondants relatifs au VQP ou des erreurs du genre :

- UDP socket overflow from Source IP: x.x.x.x, Destination port: 1589

D’autres inconvénients du VMPS concernent le fichier de configuration vmps.txt qui prend beaucoup de place sur le système de fichier du serveur VMPS. Le problème survient en effet parce que pour utiliser VMPS, il faut utiliser CatOS. VMPS n’étant pas supporté dans Cat IOS, les entreprises ayant choisis cette technologie se sont vues empêchées d’accéder aux nouvelles caractéristiques de Cat IOS. De plus, Cisco déconseille l’utilisation du VMPS. L’agence de la défense des systèmes d’information aux Etas Unis a publié dans son document de sécurité, des paragraphes pour également déconseiller le même fait.

Les alternatives au VMPS sont multiples et s’insèrent bien dans les solutions du NAC. Les différentes techniques de mise en vigueur de la politique de sécurité sont entre autres :

- VLAN Steering: Cette technique assigne un port d’utilisateur à un VLAN spécifique (invite, de mise en conformité, intanet, …). La fonction de contôle et de commande du système NAC doit interagir avec le switch.
- DHCP Lease Management: Le système NAC contrôle l’adresse IP que recoit un utilisateur à travers le DHCP.
- ARP Poisoning: utilise ARP pour controller quel hôte peut communiquer en modifiant le couplage adresse IP et adresse MAC
- DNS Redirection: redirige toutes les requêtes vers un portail web pour guider l’utilisateur dans une authentification sur le système
- Inline Blocking: un système NAC en coupure de bande entre le poste de travail de l’utilisateur et le cœur du réseau peut stopper un client spécifique de communiquer avec le reste du réseau. Plus le système NAC se trouve proche de l’utilisateur final, plus le contôle est fin.
- DHCP et ARP poisoning sont deux techniques utiliser pour contrôler quel utilisateur accède au réseau. Le système NAC mets d’abord l’utilisateur dans un réseau privé puis change l’adresse IP à convenance. Le contrôle DHCP ne demande pas beaucoup de changement et est moins invasif que la manipulation des ports, dans le VLAN steering ou pour la mise à jour dynamique des ACLs de routeur. ARP poisoning utilise ARP to gérer la correspondance adresse MAC – adresse IP utilisé par les postes pour communiquer dans un même sous réseau.

L'un ou l'autre de ces méthodes peuvent être facilement contourné par des attaques. En utilisant une adresse IP statique, on peut contourner le serveur DHCP. Pour l'ARP Poisining, c'est un peu plus compliqué. Cependant, sur les postes Windows, en utilisant la commande arp –a on peut faire un mappage ARP statique. La partie la plus difficile est de faire connaitre aux autres nœuds (un routeur par exemple) sa réelle adresse MAC. L'envoi constant de réponses tronquées niveau ARP pourrait être une échappatoire.

Les switchs Cisco de couche 3 ont des fonctionnalités pour prévenir ce genre d'attaques de réseau.

3.3 Critères de choix d'une solution NAC

Pour le choix efficace d'une solution NAC pour une entreprise, plusieurs conditions doivent être remplies :

- Architecture ouverte;
- Inclusion de systèmes d'extrémité;
- Autorisation multicontexte;
- Application des politiques;
- Notification et remédiation;
- Reporting de conformité.

3.3.1 Architecture ouverte

Pour être efficace, une solution NAC doit être déployable en tant qu'architecture ouverte. Cette solution doit pouvoir évaluer tout type d'équipement susceptible de se connecter au réseau. Elle doit aussi fournir une sécurité renforcée dans des environnements sur lesquels des équipements de plusieurs fournisseurs d'infrastructure réseau ont été déployés. L'évaluation et l'authentification des ordinateurs qui n'exécutent que certains systèmes d'exploitation ou logiciels à base d'agent ne constituent pas une solution satisfaisante pour protéger les

environnements d'entreprise d'aujourd'hui qui sont fortement hétérogènes. Afin que la solution NAC puisse sécuriser efficacement un environnement réseau réel contre les menaces et vulnérabilités liées à l'éventail de systèmes d'extrémité connectés, il est nécessaire d'intégrer des technologies d'évaluation de différents fournisseurs. Une technologie d'évaluation uniquement destinée à certains systèmes d'extrémité laisse le réseau et les services associés vulnérables aux attaques en provenance de systèmes d'extrémité non intégrés à la stratégie de sécurité.

De nombreuses technologies d'évaluation de différents fournisseurs de logiciels doivent pouvoir être intégrées à la solution NAC qui pourra ainsi évaluer n'importe quel type de système d'extrémité qui se connecte au réseau.

En plus de pouvoir tirer parti de nombreuses technologies d'évaluation pour une approche complète de la protection proactive, la solution NAC doit être opérationnelle dans un environnement basé sur une infrastructure multifournisseur. Plusieurs produits d'infrastructure de différents fournisseurs peuvent être déployés dans les environnements réseau. Une solution NAC doit pouvoir gérer des systèmes d'extrémité connectés à divers types de commutateurs réseau de différents fournisseurs. Une mise à jour majeure des produits d'infrastructure de communication réseau n'est pas une solution économiquement envisageable pour déployer une solution NAC complète. Les technologies normalisées d'authentification et d'application de politiques telles qu'IEEE 802.1X et RFC 3580 doivent permettre le déploiement d'une solution NAC bien conçue dans un environnement réseau composé de plusieurs produits d'infrastructure de différents fournisseurs.

3.3.2 Inclusion de systèmes d'extrémité

La variété des systèmes d'extrémité connectés au réseau augmente sensiblement sur les réseaux d'entreprise modernes. Avec l'avènement des réseaux convergents qui hébergent un large éventail d'applications métier, les types de système d'extrémité connectés continuent d'évoluer. Un réseau d'entreprise accueille aussi bien des systèmes d'extrémité comme des téléphones IP, des caméras de surveillance et des distributeurs automatiques que les traditionnels postes de travail, ordinateurs portables, smartphones et imprimantes. Avec une

telle diversité de systèmes d'extrémité connectés, il est impératif qu'une solution NAC bien architecturée intègre tous ces systèmes. Sur un réseau hébergeant différents types de systèmes d'extrémité, les processus de sécurité ne doivent pas être enfermés dans des types d'équipement, de systèmes d'exploitation ou de logiciels spécifiques. Une imprimante, un copieur, un téléphone IP ou une caméra de sécurité peut être facilement infecté et constituer également un point d'infection et de propagation d'une menace de sécurité lors de la connexion d'un poste de travail ou d'un ordinateur portable au réseau. Une solution NAC doit pouvoir fournir une sécurité proactive et réactive pour tout système d'extrémité.

3.3.3 Autorisation multicontexte

Une solution NAC efficace doit pouvoir prendre en compte de nombreux attributs différents pour déterminer l'état de santé, de la sécurité et du rôle d'un système d'extrémité et, le cas échéant, son utilisateur. Une autorisation multicontextuelle des systèmes d'extrémité permet de déployer des mesures de sécurité plus spécifiques ainsi qu'une utilisation plus fine du réseau et des applications. À elle seule, une évaluation des systèmes d'extrémité n'est pas suffisante pour déterminer si un équipement et un utilisateur sont autorisés à accéder au réseau et à des applications et des services spécifiques. La solution NAC doit pouvoir intégrer des attributs contextuels supplémentaires tels que le type d'équipement, le lieu et l'heure de la connexion, les certificats de l'utilisateur et de la machine ainsi que le rôle de l'équipement et de l'utilisateur dans l'entreprise.

La prise en compte de ces nombreux attributs contextuels permet d'appliquer une politique de communication réseau sur le système d'extrémité et de fournir des règles de communication réseau et de sécurité très spécifiques. Il est possible d'empêcher les systèmes d'extrémité de communiquer avec des applications inappropriées pour le type d'équipement ou le profil de l'utilisateur. Des règles de mise en quarantaine spécifiques peuvent être appliquées pour une communication sécurisée avec les services critiques requis pour procéder à la remédiation d'un équipement, mais sans que ces règles puissent avoir un impact négatif sur les systèmes d'extrémité ou les communications métier. Plus le contexte sera riche pour le processus d'autorisation d'une solution NAC, plus précises et efficaces seront les communications et la sécurité réseau.

3.3.4 Application des politiques

Le processus d'application de politiques est un aspect fondamental d'une solution NAC. Appliquer des règles de politiques de sécurité réseau directement sur le point de connexion au réseau d'un système d'extrémité est le meilleur moyen pour que les équipements et les utilisateurs communiquent avec la bonne application métier au bon moment. Ceci garantit également une connexion fiable et sécurisée qui ne compromet pas d'autres équipements, personnes et applications présentes sur le réseau. Les règles de politiques doivent être de nature granulaire afin de contrôler de manière spécifique les communications dangereuses ainsi que l'utilisation des applications en un quelconque point du réseau. Si un système d'extrémité est considéré comme dangereux ou vulnérable, il est possible d'appliquer des règles de politiques pour mettre ce système en quarantaine afin qu'il ne mette pas en danger le reste de l'environnement métier. Les règles de la politique de mise en quarantaine ne doivent pas se limiter à placer le système d'extrémité dans un VLAN où d'autres systèmes d'extrémité également non conformes pourront communiquer. En effet, ce processus peut augmenter les risques pour les autres systèmes d'extrémité et constituer un point de distribution et d'échange d'infections favorisant des communications dangereuses. La politique de mise en quarantaine granulaire appliquée ne doit avoir aucune dépendance topologique spécifique (notamment l'affectation de VLAN). Il doit être possible d'appliquer des règles de politiques spécifiques pour une communication réseau de niveau 2 à 4 afin qu'un système d'extrémité puisse être complètement isolé du reste du réseau, sauf des services applicatifs nécessaires à la notification ou éventuellement à la remédiation. Cette application de politiques doit être dynamique et entièrement distribuée sur l'infrastructure du réseau. De plus, des règles de politiques doivent être appliquées par l'infrastructure réseau elle-même, directement sur la connexion du point d'extrémité, qui garantit une infrastructure de politiques évolutive et complète dans le cadre d'une solution NAC.

3.3.5 Notification et remédiation

Si un système d'extrémité est déterminé comme menaçant ou vulnérable, la notification et la remédiation deviennent une phase critique du processus. Appliquer une politique de mise en quarantaine sur un système d'extrémité non conforme à la politique permet d'empêcher ce dernier d'endommager le réseau d'entreprise. Cependant, si l'utilisateur de ce système ne sait pas qu'il a été mis en quarantaine (ni pourquoi), il pensera probablement qu'il s'agit d'un problème lié au réseau de communication ou à des services applicatifs.

Avertir un utilisateur de la mise en quarantaine de son système d'extrémité évite donc d'inonder le Help Desk d'appels et renseigne l'utilisateur sur un problème concernant son système d'extrémité ou sa tentative de communication.

Une solution NAC bien architecturée intégrera un processus de notification système destiné à l'utilisateur du système d'extrémité.

Généralement fournie par un navigateur Web classique, cette notification peut également être transmise par d'autres services tels que la messagerie instantanée ou électronique. Une véritable notification doit non seulement expliquer la politique de mise en quarantaine appliquée au système d'extrémité, mais aussi décrire la (les) raison(s) de cette quarantaine et indiquer la procédure pour remédier efficacement au problème. Il peut s'agir d'une simple instruction concernant la procédure d'accès à un serveur de correctifs ou à un serveur de mises à jour de signatures. Cette notification peut également comprendre des instructions sur la marche à suivre pour désactiver des services ou des applications non conformes à des politiques spécifiques. Une fois qu'il a procédé à la remédiation de son système extrémité, l'utilisateur peut à nouveau le soumettre à une évaluation pour le sortir de son état de quarantaine et redevenir ainsi productif car conforme à un profil de politique spécifique.

3.3.6 Reporting de conformité

Une solution NAC bien architecturée permet de collecter et d'utiliser beaucoup d'informations sur les systèmes d'extrémité connectés, sur les utilisateurs ainsi que sur les communications réseau. Une grande partie de ces informations peut être vitale pour faciliter le reporting de

conformité. Dans la mesure où la solution NAC participe à la validation de chaque système d'extrémité connecté au réseau, les données disponibles fournissent, d'une part, une visibilité en temps réel des éléments connectés au réseau et des points de connexion et, d'autre part, des vues sous forme d'historiques des systèmes d'extrémité connectés. Ce qui peut s'avérer extrêmement utile pour gérer un problème de conformité lorsqu'un enregistrement d'historique est nécessaire pour spécifier le point de connexion d'un système d'extrémité à un réseau ainsi que les services qu'il a utilisés.

En outre, parce qu'une solution NAC appropriée intègre l'authentification des systèmes d'extrémité et des utilisateurs qui les utilisent, il est possible d'établir une corrélation entre les utilisateurs présents sur le réseau à un moment particulier et leur point de connexion. Les solutions NAC qui permettent d'appliquer des politiques granulaires peuvent également établir un rapport sur l'utilisation réelle du réseau et de ses ressources par un système d'extrémité et/ou un utilisateur particulier.

4

PARTIE 4 : UNE SOLUTION NAC BASEE SUR VMPS

4.1 Qu'est ce que VMPS

VMPS est un protocole créé par Cisco. Il est chargé de faire correspondre un Vlan à une ou plusieurs adresses MAC.

VMPS est basé sur une architecture client / serveur pour gérer des Vlan de façon dynamique en utilisant les adresses MAC des systèmes d'extrémité.

Le fonctionnement de la gestion dynamique des Vlan nécessite la compréhension du protocole VTP (Vlan Trunking Protocol) et du protocole VQP (Vlan Query Protocol) qui sont utilisés par VMPS.

4.1.1 Le protocole VTP (Vlan Trunking Protocol)

Le protocole VTP permet à un administrateur réseau d'effectuer des modifications sur un commutateur qui est configuré comme serveur VTP. Ce serveur VTP est chargé de distribuer et de synchroniser les informations Vlan aux commutateurs compatibles VTP sur le réseau. Cette méthode permet de minimiser les problèmes de configuration incorrecte ou inhérente.

Le protocole VTP doit obligatoirement être configuré sur les commutateurs de l'architecture réseau sur laquelle sera déployer la solution VMPS. En effet, le nom de domaine VTP sera utilisé lors de l'échange de paquet entre le serveur VMPS et les commutateurs clients.

4.1.2 Le protocole VQP (Vlan Query Protocol)

Le protocole VQP est utilisé pour transporter les données VMPS. Il utilise le protocole de transport UDP (User Datagram Protocol) et le port 1589.

Le protocole VQP permet à un commutateur client d'interroger un serveur VMPS, qui dispose d'une base de données contenant les adresses MAC des périphériques réseau et les Vlan qui leurs sont associés.

4.1.3 Fonctionnement de VMPS

L'architecture VMPS est composée d'un serveur VMPS principale, de 0 à 3 serveurs secondaires et de plusieurs commutateurs clients.

Si un périphérique réseau se connecte sur un port dynamique, le commutateur n'acheminera aucun trafic à partir ou à destination de ce port, tant qu'il n'a pas reçu le Vlan associé à ce périphérique.

Nous allons voir comment un client est affecté dynamiquement à un Vlan en se basant sur son adresse MAC. Le schéma ci-dessous montre les différentes étapes de ce processus :

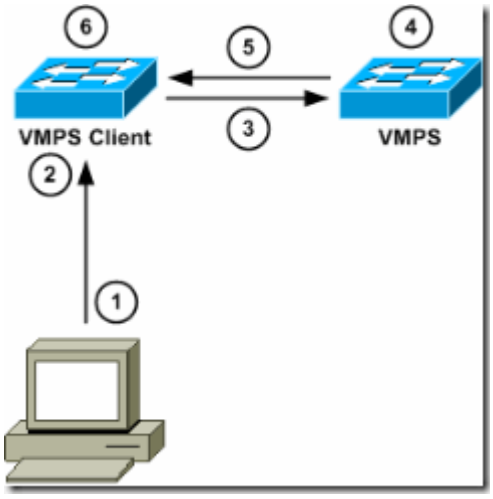

Figure 15: Fonctionnement de VMPS

- Étape 1 : L'ordinateur envoie une trame vers le commutateur VMPS client.
- Étape 2 : Le client VMPS apprend l'adresse MAC du PC qui est connecté sur le port dynamique.
- Étape 3 : Le client VMPS envoie une requête VQP vers le serveur VMPS. La requête contient l'adresse IP du client VMPS, l'adresse MAC de l'ordinateur, le numéro de port du commutateur sur lequel est connecté le PC et le nom de domaine VTP.
- Étape 4 : Le serveur VMPS parcourt la base de données afin de trouver une

correspondance entre l'adresse MAC du PC et le Vlan auquel il doit être associé.

- Étape 5 : Le serveur VMPS envoie une réponse VQP au client VMPS.
- Étape 6 : Si la réponse VQP contient une affectation de Vlan, le client VMPS associe la station de travail à ce Vlan. Sinon, le client VMPS refuse l'accès à cet ordinateur.

4.1.4 Le serveur VMPS

Le serveur VMPS utilise une base de données contenant les correspondances entre les adresses MAC et les Vlan, ainsi que des règles qui permettent d'autoriser ou non un utilisateur à se connecter sur certains ports des commutateurs.

Réponse du serveur VMPS :

Si l'adresse MAC du périphérique réseau est dans la base de données VMPS, alors le serveur VMPS répond positivement à la requête du commutateur client en envoyant le numéro de Vlan à affecter au périphérique.

Si l'adresse MAC du périphérique réseau n'est pas dans la base de données, le serveur VMPS répond négativement à la requête du commutateur client, en fonction de son mode de sécurité :

- Si le serveur VMPS est configuré dans le mode « open » (non sécurisé), il envoie une réponse « access-denied » (accès refusé) au commutateur client. Par conséquent, tout le trafic sera bloqué pour le port du commutateur sur lequel le périphérique est connecté.
- Si le serveur VMPS est configuré dans le mode « secure » (sécurisé), il envoie une réponse « port-shutdown » au commutateur client. Le port du commutateur sur lequel le périphérique est connecté, sera fermé. Un administrateur réseau devra réactiver manuellement ce port au moyen de la commande *no shutdown* dans le mode de configuration d'interface.

Les options supplémentaires :

Il existe une option permettant de configurer un Vlan par défaut appelé Vlan Fallback. Lorsqu'un serveur VMPS reçoit une requête d'un commutateur client contenant une adresse MAC qui ne figure pas dans la base de données, le serveur VMPS renvoie le nom de ce Vlan par défaut au commutateur client. Ce commutateur ouvre l'accès au réseau pour le port sur lequel est connecté le périphérique.

Une option permet de filtrer les adresses MAC. Nous pouvons ainsi refuser l'accès au réseau pour ces adresses MAC en indiquant l'option NONE à l'endroit ou doit se trouver usuellement le nom du Vlan.

Selon le mode de configuration du serveur VMPS, le port sera fermé (mode secure) ou un message de refus de connexion sera envoyé au commutateur client.

La dernière option permet de créer des groupes de ports associés à un Vlan. Lorsqu'un périphérique se connecte sur l'un de ces ports, le serveur VMPS récupère le nom du Vlan dans la base de données qui correspond à l'adresse MAC de celui-ci. Le serveur VMPS compare le nom du Vlan à celui associé aux ports. Si les deux noms de Vlan sont identiques, le port du commutateur client est ouvert et placé dans le Vlan approprié. Sinon, le serveur VMPS envoie un message annonçant que l'accès est refusé ou referme le port s'il y est dans le mode secure.

Un port configuré dans le mode dynamique ne peut être associé qu'à un seul Vlan. Les connexions multiples sur un port via un doubleur ou un hub ne sont possible que si toutes les adresses MAC des machines appartiennent au même Vlan.

4.2 Implémentation de VMPS sur une architecture composée de commutateur

4.2.1 Installation du serveur VMPS sous linux

Le schéma suivant décrit l'architecture sur laquelle est implémentée la solution VMPS :

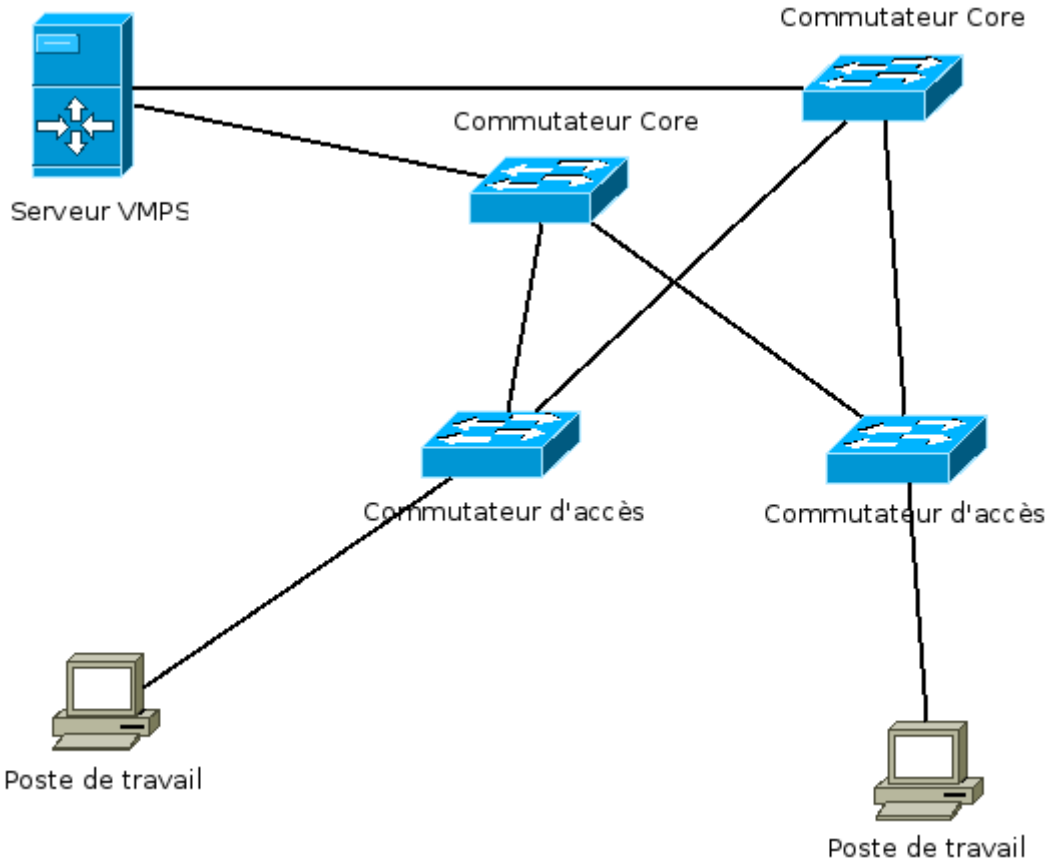

Figure 16: Architecture comportant un serveur VMPS et deux clients VMPS.

Installation du serveur OpenVMPS[23] sous Fedora Linux

```
# yum install vmpsd
```

23 OpenVMPS : est une implémentation opensource de VMPS http://vmps.sourceforge.net/

Le fichier de configuration du serveur VMPS se trouve dans /etc/vlan.db

```
! --- Init ---                          Bloc d'initialisation des options
!Choix du mode secure ou open
vmps mode open

!Nom du domaine VTP
vmps domain ESGIS

!Action par défaut lorsqu'une requête sans nom de domaine arrive au serveur,
!ici on refuse le traitement
vmps no-domain-req deny

!Vlan par défaut si l'adresse MAC n'est pas trouvée
vmps fallback VMPSRogue

! --- Mac Address Section ---          Bloc équivalent à la base de données
vmps-mac-addrs                        !Début de liste des adresses MAC

! --- VLAN Admin ---                   !Nom du Vlan concerné
!Cette ligne contient le mot clé address suivi de l'adresse MAC de la machine concernée,
!puis le mot clé vlan-name suivi du nom du Vlan dans laquelle cette machine doit être placée.
!En fin de ligne on trouve un commentaire avec le nom de la machine.
address 0000.0000.0001 vlan-name Admin ! machine1

! --- VLAN Compta ---
address  0000.0000.0002 vlan-name Compta ! machine2

! --- VLAN Serveur ---
address 0000.0000.0003 vlan-name Serveur ! machine3

! --- VLAN Poubelle ---
!Une section pour le Vlan par défaut peut être créée afin d'y placer volontairement des machines
```

4.2.2 Configuration des commutateurs

Configuration du protocole VTP :

Le protocole VTP a été activé afin que les informations sur les Vlan soit transmissent automatiquement vers les commutateurs. La commande *vtp domain ESGIS* exécuter dans le mode de configuration globale permet d'activer le protocole VTP.

Paramétrage de l'adresse IP et de la default gateway :

Les commandes suivantes permettent de paramétrer l'adresse IP et la default gateway sur un commutateur cisco 2950 :

```
Switch # configure terminal
Switch (config) # interface vlan 1
Switch (config-if) # ip address 192.168.255.1 255.255.255.0
Switch (config-if) # no shutdown
Switch (config-if) # exit
Switch (config) # ip default-gateway 192.168.255.254
Switch (config) # end
```

Création de lien Trunk 802.1Q[24] :

Nous devons ensuite créer des liens trunk[25] entre les liaisons reliant les commutateurs composant l'architecture comme suit :

```
Switch # configure terminal
Switch (config) # interface range fastEthernet 0/23 - 24
Switch (config-if-range) # switchport trunk encapsulation dot1q
Switch (config-if-range) # switchport mode trunk
Switch (config-if-range) # switchport trunk native vlan 1
Switch (config-if-range) # end
```

24 802.1q : est un mécanisme d'encapsulation de trame permettant d'effectuer un marquage identifiant le VLAN d'appartenance de cette trame.

25 TRUNK : Lien sur lequel est établit un mécanisme de transport ethernet (ISL ou IEEE 802.1Q) sur les switchs Cisco

Ajout de l'adresse IP des serveurs VMPS :

Nous devons indiquer l'adresse IP du serveur VMPS primaire et des serveurs secondaires au niveau des commutateurs comme suit :

```
Switch # configure terminal
Switch (config) # vmps server 172.16.1.1 primary
Switch (config) # vmps server X.Y.Z.W
Switch (config) # end
```

Configuration des ports dans le mode d'accès dynamique :

Les ports des commutateurs sur lesquelles les périphériques réseaux vont se connecter doivent être configurés dans le mode d'accès dynamique. Les commandes ci-dessous montrent comment le faire :

```
Switch # configure terminal
Switch (config) # interface range fastEthernet 0/1 - 22
Switch (config-if-range) # switchport mode access
Switch (config-if-range) # switchport access vlan dynamique
Switch (config-if-range) # end
```

N.B : Le serveur VMPS peut être implémenté sur un commutateur serveur, mais il n'est disponible qu'à partir des commutateurs Catalyst 4000.

CONCLUSION

Le contrôle d’accès au réseau est un composant clé d’une solution de sécurité réseau. S’informer sur l’identité et l’état d’un système d’extrémité avant qu’il se connecte au réseau est critique pour garantir la continuité de l’activité et la sécurité globale de l’entreprise.

La maîtrise des accès au réseau est donc indispensable pour assurer un niveau de sécurité satisfaisant du système d'information. L'étude menée ici montre que dans un environnement complexe, il est difficile de mettre en place un concept comme le NAC qui s'appuie sur des technologies nouvelles et des matériels relativement récents. Il est toutefois possible de mettre en place, dès aujourd'hui, les éléments nécessaires au contrôle d'accès au réseau afin, dans un premier temps, de familiariser les utilisateurs et les administrateurs à ce contrôle, ce qui est déjà le cas pour les accès sans-fil mais beaucoup moins pour les accès filaires, et, dans un deuxième temps, de développer peu à peu tous les éléments d'un NAC. Le recueil d'informations pertinentes sur les systèmes d'extrémité est nécessaire à l'application de la politique de sécurité et se développe actuellement au niveau des postes informatiques avec la mise en place d'agents spécialisés. Il sera en revanche toujours utile de corréler ces informations avec des outils réseau indépendants et de mettre en place une analyse des flux afin de ne pas faire reposer la sécurité sur une source d'information unique. La mise en place d'un NAC ne pourra garantir une protection totale face aux menaces liées aux accès réseau, cependant, il contribuera certainement à augmenter la protection des systèmes d'information.

Pour terminer, nous tenons à souligner que nous n'avons nullement pas la prétention d'avoir présenté un travail parfait, car aucun travail scientifique ne peut l'être, ainsi nous laissons le soin à tous ceux qui nous lirons et qui sont du domaine de nous faire parvenir leurs remarques et suggestions pour l'enrichir et l'améliorer.

LISTE DES FIGURES

ANNEXES

LISTE DES SOLUTIONS NAC DU MARCHE

Produit	Vendeur	Licence
Alcatel-Lucent SafeNAC	Alcatel-Lucent	Commercial
Apani EpiForce	Apani Networks	Commercial
Auconet Network Access Control (NAC)	Auconet	Commercial
Avenda OnGuard Health Agents	Aruba Networks	Commercial
BRADFORD.cloud	Bradford Networks	Commercial
BSA Guest Network Access Overview	Insightix	Commercial
BSA Network Access Control	Insightix	Commercial
Cisco Identity Services Engine	Cisco Systems Inc	Commercial
Cisco NAC Appliance	Cisco Systems Inc	Commercial
Cisco NAC Guest Server	Cisco Systems Inc	Commercial
Cisco NAC Profiler	Cisco Systems Inc	Commercial
CyberGatekeeper Remote	InfoExpress Inc	Commercial
CyberGatekeeper Server	InfoExpress Inc	Commercial
Enterasys Network Access Control	Enterasys Networks	Commercial
Fiberlink MaaS360 Laptop Management	Fiberlink	Commercial
FreeNAC	Swisscom Innovations	Open source
ForeScout CounterACT	ForeScout Technologies	Commercial
Impulse Point Safe Connect	Impulse Point	Commercial
iNetSec Inspection Center®	PFU Systems, Inc.	Commercial
InfoExpress Dynamic NAC Suite	InfoExpress Inc	Commercial
Juniper Unified Access Control	Juniper Networks	Commercial
LANenforcer 2024/2124 Security Appliance	Nevis Networks	Commercial
Lan-Secure Switch Protector	Lan-Secure	Commercial
Mancala Network Controller	Mancala Networks	Commercial
McAfee Network Access Control	McAfee, Inc	Commercial
NetClarity NACwall	NetClarity, Inc	Commercial
Network Sentry Solutions	Bradford Networks	Commercial
PacketFence	Inverse inc.	Open source
Portnox™	Access Layers	Commercial
SkyRecon StormShield	SkyRecon Systems, Inc.	Commercial
Sophos Network Access Control (NAC) Advanced	Sophos, Inc.	Commercial
StillSecure Safe Access®	StillSecure	Commercial

SWAT	Wise-Mon Ltd	Commercial
Symantec Network Access Control	Symantec Corporation	Commercial
Symantec Network Access Control Mobile Edition	Symantec Corporation	Commercial
Symantec Network Access Control Starter Edition	Symantec Corporation	Commercial
Trustwave Enterprise Network Access Control	Trustwave	Commercial
Trustwave Managed Network Access Control	Trustwave	Commercial
Trustwave Plug-and-Play Network Access Control	Trustwave	Commercial
Veri-NAC™	Black Box Corporation	Commercial

RFC

- RFC 2284, PPP Extensible Authentication Protocol (EAP), https://tools.ietf.org/html/rfc2284
- RFC 2138, Remote Authentication Dial In User Service (RADIUS), https://tools.ietf.org/html/rfc2138
- RFC 2139, RADIUS Accounting, https://tools.ietf.org/html/rfc2139
- RFC 2486, The Network Access Identifier, https://tools.ietf.org/html/rfc2486
- RFC 2607, Proxy Chaining and Policy Implementation in Roaming, https://tools.ietf.org/html/rfc2607
- RFC 2289, A One-Time Password System, https://tools.ietf.org/html/rfc2289
- RFC 2058, Remote Authentication Dial In User Service (RADIUS), https://tools.ietf.org/html/rfc2058
- RFC 2059, RADIUS Accounting, https://tools.ietf.org/html/rfc2059
- RFC 2865, Remote Authentication Dial In User Service (RADIUS), https://tools.ietf.org/html/rfc2865
- RFC 2866, RADIUS Accounting, https://tools.ietf.org/html/rfc2866
- RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, https://tools.ietf.org/html/rfc3580
- RFC 5209, Network Endpoint Assessment (NEA): Overview and Requirements, https://tools.ietf.org/html/rfc5209

SIGLES ET DEFINITIONS

VPN (Virtual Private Network) est un réseau privé vituel permettant un accès au réseau local depuis un réseau extérieur.

L'adresse MAC (Media Access Control) est un identifiant physique d'une interface réseau.

DHCP (Dynamic Host Configuration Protocol) est un protocole réseau permettant d'attribuer les paramètres réseau d'une interface.

EAP (Extensible Authentication Protocol) est un mécanisme d'authentification.

RADIUS (Remote Authentication Dial-In User Service) est un protocole réseau d'authentification centralisé.

VLAN (Virtual Local Area Network) Réseau local virtuel.

ActiveX : Composant logiciel réutilisable pour Microsoft Windows

VMPS (VLAN Management Policy Server)

TRAP : Paquet SNMP émis par un matériel réseau lorsqu'un événement se produit.

SNMP (Simple Network Management Protocol) est un protocole de communication permettant d'administrer les matériels réseau.

API (Application Programming Interface) est un ensemble de programmes permettant une interopérabilité entre composants logiciel.

PLUGIN est un logiciel venant en compléter un autre.

PEAP (Protected Extensible Authentication Protocol) est une méthode d'authentification

IPSec (Internet Protocol Security) permet de sécuriser une communication par l'utilisation de moyen cryptographique.

IPS (Intrusion Prevention System) est un système de détection d'intrusion capable de réagir en temps réel pour bloquer un trafic indésirable.

DNS (Domain Name Server) est un système de nom de domaine permettant de faire le lien entre un nom de domaine et une adresse IP.

NESSUS: logiciel de détection de vulnérabilités.

XML (Extensible Markup Language) successeur du html, c'est un langage de balisage extensible.

LDAP (Lightweight Directory Access Protocol) est un protocole d'échange pour un service d'annuaire.

SIP (Session Initiation Protocol) est un protocole de gestion de session multimédia, principalement de voix sur IP.

Active Directory: Service d'annuaire mis en œuvre par Microsoft

802.1q est un mécanisme d'encapsulation de trame permettant d'effectuer un marquage identifiant le VLAN d'appartenance de cette trame.

EAP-TTLS (EAP-Tunneled Transport Layer Security) méthode d'authentification utilisant des certificats X-509.

BIBLIOGRAPHIE

[1] B. Morin. Corrélation d'alertes issues d'outils de détection d'intrusions avec prise en compte d'informations sur le système surveillé. Thèse de doctorat en informatique de l'institut national des sciences appliquées de Rennes, février 2004.

[2] Stephen Northcutt et Judy Novak. Détection des intrusions réseaux. CampusPress, 2001.

WEBLIOGRAPHIE

[1] Frédéric Boivent et Pierre-Antoine Angelini, Centre de Ressources Informatiques Université Rennes1, Du NAC … à la réalité, déc 2009 - https://2009.jres.org/planning_files/article/pdf/90.pdf

[2] Yves DROTHIER, JDN Solutions, Le Network Access Control en 5 questions, Article du 19/04/2006 - http://www.journaldunet.com/solutions/0604/060419-qr-nac.shtml

[3] Naveen Sharma – CISSP, Network Access Control, Article du 26/11/2007 - https://www.net-security.org/article.php?id=1096

[4] Claude Duvallet, Le protocole RADIUS - Remote Authentication Dial-In User Service, Université du Havre, UFR des Sciences et Techniques - http://litis.univ-lehavre.fr/~duvallet/enseignements/Cours/CNAM/CNAM-Cours-ServeurRadius.pdf

[5] Allied Telesis | White Paper, 802.1x White Paper - http://www.alliedtelesyn.com/media/pdf/8021x_wp.pdf

[6] Benny Czarny, OPSWAT White Paper October 2008, Network Access Control Technologies - http://www.opswat.com/sites/default/files/Network_Access_Control_Technologies.pdf

Les sources sont disponibles sur https://github.com/mhoungbo/memoire-esgis-2012

N’hésitez pas à le corriger, le compléter ou l’actualiser.