CHAPITRE 3 :

ETUDE TECHNIQUE DES SOLUTIONS

Notre projet consiste à implémenter une solution NAC (Network Access Control). Nous allons donc énumérer quelques solutions visant à contrôler l'accès et mettre l'accent particulièrement sur la solution ISE dans le but de mieux comprendre la partie de déploiement qui sera traitée ultérieurement.

I. LE VLAN PAR PORT

1. Définition d'un VLAN

Un réseau local virtuel, communément appelé VLAN, est un réseau informatique logique indépendant. En d'autres termes, c'est un réseau local regroupant un ensemble de machines de façon logique et non physique.

2. Fonctionnement du VLAN basé sur les ports

Les VLAN par port associent un port d'un switch à un numéro de Vlan. On dit alors que le port est tagué suivant le Vlan donné. Le switch entretien ensuite une table qui lie chaque Vlan au port associé. Le taggage des ports peut se faire de manière statique ou de manière dynamique

La figure suivante illustre les écrits.

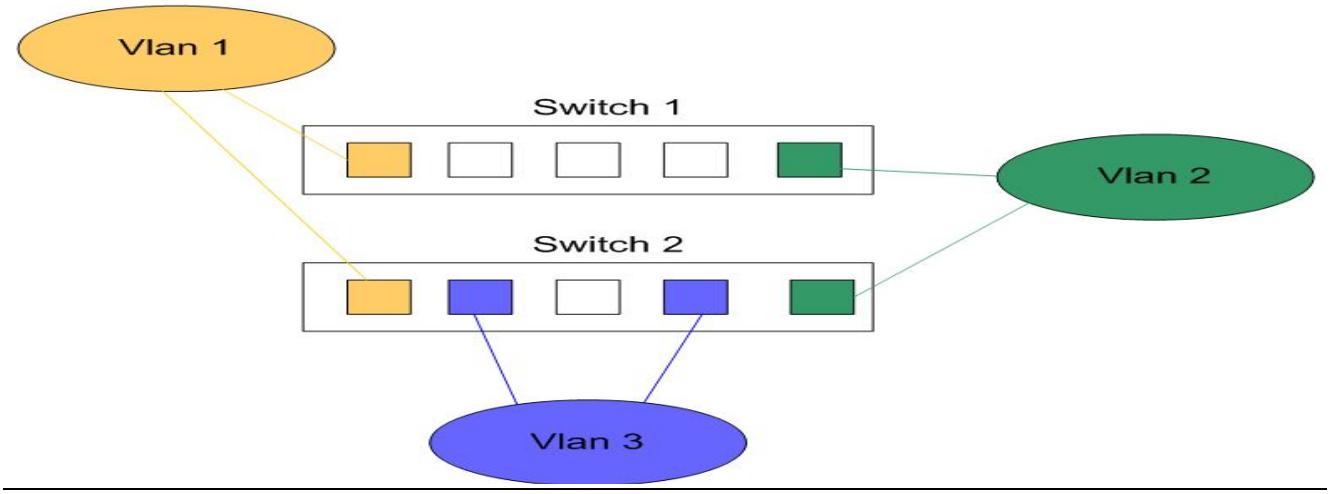

Figure 2 : Taggage de ports

3. Avantages

L'avantage principale du Vlan par port est qu'il permet une étanchéité maximale des Vlan. Une attaque extérieure ne pourra se faire qu'en branchant le PC pirate sur un port taggué. Le pirate a donc besoin d'avoir accès à la machine physique pour s'introduire au Vlan.

Le Vlan par port offre une facilité de configuration. L'administrateur peut sans difficulté choisir les ports à taguer sans avoir d'information de la part des machines auxquelles sont reliés les ports.

4. Inconvénients

Le principal inconvénient du Vlan par port est qu'il nécessite une configuration lourde et contraignante sur chaque switch. A chaque déplacement de poste, il faut modifier les switches correspondant pour maintenir une qualité de service. Ce système peut être atténuer par la mise en place d'une solution de carte client 802.1q couplée à une authentification en 802.1x et à une solution de transport des Vlan.

Le mécanisme de Vlan par port ne possède pas d'architecture centralisée qui pourrait permettre d'éviter la lourdeur de la configuration. Chaque switch possède sa table de correspondance indépendamment du contenu des autres switches.

II. LE NAC (NETWORK ACCESS CONTROL)

1. Définition

Un contrôleur d'accès au réseau (Network Access Control ou NAC) est une méthode informatique permettant de soumettre l'accès au réseau de l'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.

Plusieurs solutions de contrôle d'accès au réseau existent. Parmi celle-ci, on peut citer.

- JUNIPER Unified Access Control (UAC),
- MICROSOFT Network Access Protection (NAP),
- FreeNAC
- PacketFence, etc…

La solution qui retient notre attention est celle proposée par CISCO Systems, à savoir la plate-forme ISE car celui utilisé par l'entreprise de télécommunication MTN CI.

Identity Services Engine (ISE) est une solution NAC qui est l'une des dernières générations des plates-formes de contrôle d'accès au réseau proposées par Cisco et qui permet aux entreprises d'imposer leurs politiques de sécurité lors de l'accès, de renforcer la sécurité de leurs infrastructures et de rationaliser leurs opérations de services.

Pour mieux assimiler la suite, il est utile d'une part, de rappeler le principe de fonctionnement, les avantages et les inconvénients de la solution ISE

2. Architecture

L'implémentation d'une solution de contrôle d'accès nécessite l'existence d'un ensemble de composants. L'architecture ci-dessous montre l'ensemble de ces éléments et le flux de communication échangé.

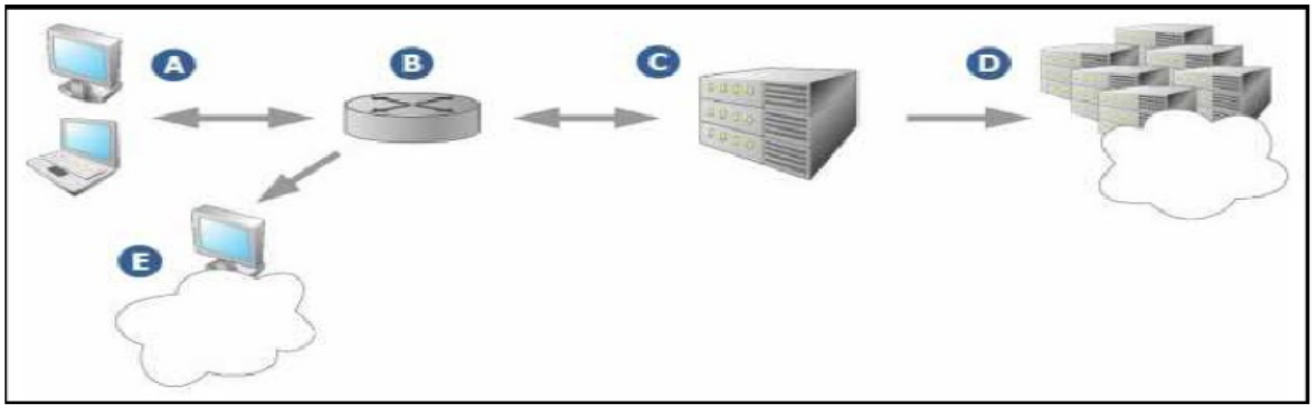

Figure 3 : Architecture globale d'une solution NAC

- **Périphériques essayant d'accéder au réseau ou "Agents" (A)** : inclut les ordinateurs portables mobiles ou qui ne se connectent que rarement, les utilisateurs invités ou les visiteurs ainsi que les utilisateurs de réseau habituels qui tentent d'accéder au réseau d'entreprise.

- **Périphérique de contrôle d'accès au réseau (B) :** du point de vue du périphérique demandeur, le périphérique d'accès réseau fonctionne en tant que périphérique réseau de « premier saut » qui lance le traitement Posture Validation et le processus d'authentification.

- **Posture Validation Server (point de décision d'accès réseau) (C) :** serveur en arrière-plan dédié, également appelé "Posture Validation Server", qui évalue les références d'authentification Posture (statut des périphériques qui requièrent un accès) en fonction des règles de conformité.

- **Serveurs d'entreprise (D) :** zone critique du réseau et que la solution NAC protège des périphériques malsains, infectés ou vulnérables.

- **VLAN de quarantaine (E) :** zone de réseau protégée virtuelle dans laquelle les périphériques peuvent être sécurisés et corrigés, ré-analysés, puis ils obtiennent un accès complet au réseau d'entreprise, ou restent conservés avec un accès restreint aux ressources de réseau telle que l'Internet.

3. Principe de fonctionnement de l'ISE

Lors de la phase d'authentification et pour communiquer avec le client ou sa machine, la plate-forme ISE fait appel à un ensemble de normes et de protocoles. Ce sont principalement : 802.1X, EAP et RADIUS

a. 802.1X

802.1X est un standard qui définit un mécanisme d'authentification pour l'accès au réseau. 802.1X peut être comparé au protocole PPP (Point-to-Point Protocol) qui est un est un protocole de transmission pour l'internet, largement diffusé et nécessaire pour un accès à Internet utilisant un modem. Le protocole PPP s'appuie sur un mécanisme embarqué, chargé de l'authentification et pour lequel deux sous-protocoles étaient proposés au choix : PAP et CHAP. Schématiquement, nous pourrions écrire : Accès Internet = modem + PPP + (PAP ou CHAP) + TCP/IP. Au cas où 802.1X est utilisé sur un équipement tel que le commutateur (Switch), l'utilisateur connectant son ordinateur au réseau (filaire ou sans fil) est obligé à s'authentifier avant d'entamer toute activité. A l'issue du processus d'authentification et en cas de succès, le client reçoit un profil réseau (TCP/IP et VLAN) ainsi qu'un assortiment de règles de sécurité.

Le standard 802.1X fait intervenir trois entités :

- Le client ou "supplicant" qui est typiquement un PC
- L'authentificateur (Switch, WLC)
- Le serveur d'authentification ou "authentication server" qui est un serveur RADIUS.

802.1x s'appuie sur EAP (Extensible Authentication Protocol) qui présente un moyen pour transporter un protocole d'authentification.

b. EAP (Extensible Authentication Protocol)

Le besoin de compatibilité avec des infrastructures d'authentification diversifiées et la nécessité de disposer de secrets partagés dans des environnements multiples ont conduit à la genèse du protocole EAP, capable de transporter des méthodes d'authentification indépendamment de leurs particularités. Le protocole EAP fournit un cadre peu complexe pour le transport de protocoles d'authentification. Un message comporte un en-tête de 5 octets et des données optionnelles, comme illustré dans la figure qui suit.

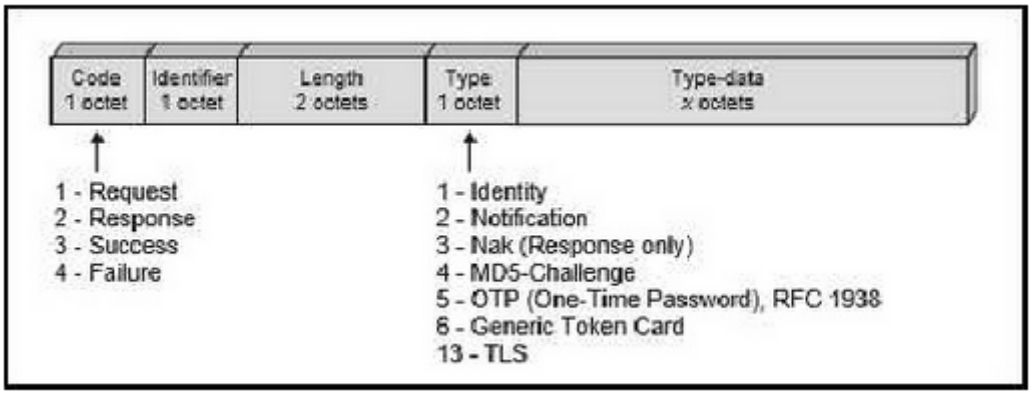

Figure 4 : Datagramme EAP

Le protocole EAP est extensible puisque tout mécanisme d'authentification peut être encapsulé à l'intérieur des messages EAP. Au niveau supérieur se trouvent les méthodes d'authentification, comme TLS, MSChap, SIM, etc. La trame EAP elle-même est encapsulée dans une trame de transport. Cette encapsulation peut s'effectuer soit dans une trame EAP over Radius, c'est-à-dire dans une trame RADIUS, soit dans une trame EAPoL (EAP over LAN) qui est utilisée dans les réseaux locaux, en particulier les réseaux locaux sans fil de type Wi-Fi.

c. RADIUS (Remote Authentication Dial-In User Server)

Quel que soit le choix du mécanisme d'authentification entre le point d'accès et le serveur d'authentification, les paquets EAP sont généralement acheminés grâce au protocole RADIUS. RADIUS est depuis longtemps le protocole AAA (Authentication, Authorization, Accounting) le plus largement adopté. Utilisé par les ISP pour authentifier les utilisateurs, il est principalement conçu pour transporter des données d'authentification, d'autorisation et de facturation entre des NAS (Network Access Server) distribués, qui désirent authentifier leurs utilisateurs et un serveur d'authentification partagé.

Si un équipement mobile a besoin d'accéder au réseau en utilisant RADIUS pour l'authentification, il doit présenter au NAS des crédits d'authentification (identifiant utilisateur, mot de passe, etc.). Ce dernier les transmet au serveur RADIUS en lui envoyant un ACCESS-REQUEST. Le NAS et les proxys RADIUS ne peuvent interpréter ces crédits d'authentification car ces derniers sont chiffrés entre l'utilisateur et le serveur RADIUS destinataire. À la réception de cette requête, le serveur RADUIS vérifie l'identifiant du NAS puis les crédits d'authentification de l'utilisateur dans une basa de données LADP (Lightweight Directory Access Protocol) ou autre.

Les données d'autorisation échangées entre le client (le NAS) et le serveur RADUIS sont toujours accompagnées d'un secret partagé. Ce secret est utilisé pour vérifier l'authenticité et l'intégrité de chaque paquet entre le NAS et le serveur.

d. 802.1X-EAP-RADIUS

Les messages EAP transportent les échanges d'authentification entre le client et le serveur d'authentification. Le switch ne fait que les relayer, toutefois de part et d'autres de switch, les messages EAP ne sont pas transportés de la même façon. Entre le client et le switch, EAP est directement dans la charge utile des trames Ethernet. Entre le switch et le RADUIS, EAP est transporté dans les messages RADUIS. La figure suivante explique les deux encapsulations :

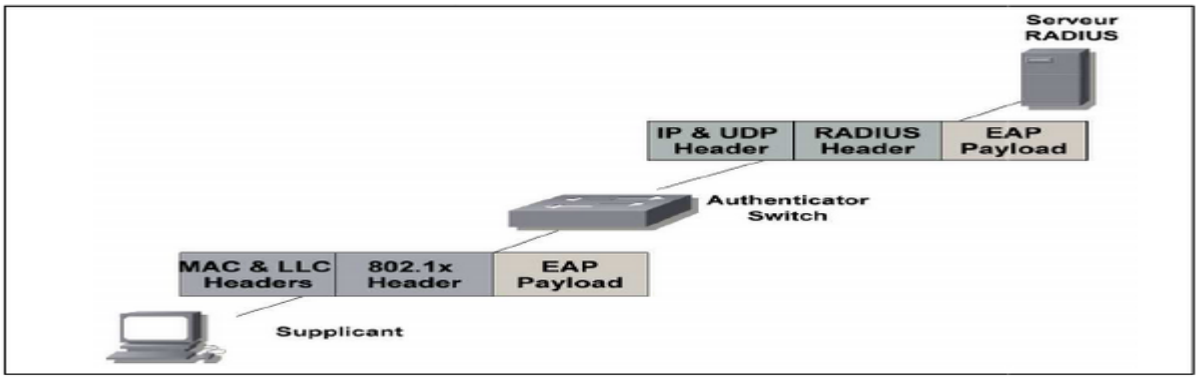

Figure 5 : Encapsulation des message EAP

4. Les licences de l'ISE

La stratégie des licences suivie par CISCO vise à minimiser le nombre de licences à commander en combinant les différents services. Actuellement, quatre paquets de licences ISE CISCO sont disponibles : Base, Advanced, Plus et Wireless. La licence d'évaluation est incluse dans la plate-forme ISE, offrant tous les services pour une durée de trois mois. La licence à commander reste valide durant un, trois ou cinq ans. Le tableau qui suit expose les différents services correspondants.

Services de ISE CISCO	Licences
Services RADIUS incluant dot1x et MAB	Base - Wireless
Authentification WEB	Base - Wireless
MACsec	Base - Wireless
Portail "Guest" & services du sponsor	Base - Wireless
Posture	Advanced - Wireless
Security Group Access	Plus - Advanced - Wireless
Services de protection des terminaux	Plus - Advanced - Wireless
Mobile Device Management(MDM)	Advanced - Wireless
Enregistrement des périphériques via portail	Plus - Advanced - Wireless
Profilage	Plus - Advanced - Wireless
Profiler feed service	Plus - Advanced - Wireless
Services RESTful externes	Base - Wireless

Tableau 1 : Les services de l'ISE et les services correspondants

5. Avantages

La plate-forme ISE peut être considérée comme étant un système de contrôle d'accès consolidé, à base de règles et intégrant un sur-ensemble de fonctionnalités disponibles dans les plates-formes existantes.

Elle permet entre autre de :

- D'augmenter la visibilité, contrôler l'accès et maîtriser les risques. En d'autres termes, bénéficiez d'une plate-forme de gestion des politiques de sécurité qui automatise et met en place un accès sécurisé et sensible au contexte aux ressources du réseau.
- D'offrir une plus grande visibilité sur les utilisateurs et les terminaux pour favoriser les expériences de mobilité dans l'entreprise et contrôler les accès.
- D'envoyer des données aux solutions partenaires intégrées afin d'accélérer l'identification, la réduction et l'élimination des risques.
- De fournir un support pour la découverte, le profilage "profiling", le placement à base de règles et le suivi des périphériques d'extrémité sur le réseau.
- De combiner l'authentification, l'autorisation, la traçabilité (AAA : Authentication, Authorization, Accounting), l'évaluation de posture et le profilage en une seule application.
- De prendre en charge l'évolutivité nécessaire pour soutenir un certain nombre de scénarios de déploiement, du petit bureau aux grands environnements d'entreprise.
  - ❖ *Remarque : notons que ACS pour Access Control System est le prédécesseur de l'ISE*

6. Inconvénients

La plate-forme ISE peut être considérée comme la meilleur en solution de contrôle d'accès. Mais comme tous systèmes, il faut retenir qu'elle présente également des inconvénients. Nous pouvons citer :

- Un peu de lenteur lors de la première connexion au réseau due au chargement de l'agent NAC et à l'authentification. Il faut que les utilisateurs soient sensibilisés pour ce changement
- La mise à jour d'un Switch requiert le redémarrage de celui-ci. Pendant le redémarrage, les utilisateurs connectés à ce Switch n'auront donc pas accès au réseau. Et cette déconnection pourra durer jusqu'à quinze (15) minutes maximum

III. ETUDE COMPARATIVE ET CHOIX DE LA SOLUTION

1. Etude comparative

	VLAN PAR PORT	CISCO ISE
Niveau de sécurité	Moindre	Elévé
Services invité (GUEST) intégré	NON	OUI
Méthodes d'authentification	802.1X	802.1X MAC authentification bypass (MAB) L'authentification WEB via un portail captif

Tableau 2 : Tableau de comparaison des différentes solutions

2. Choix de la solution

Nous avons présenté quelques solutions permettant de mettre en œuvre un système de contrôle d'accès réseaux. Certaines sont l'apanage de grandes firmes et s'intègreraient mieux dans un environnement où les autres composants (tant logiciels que matériels) proviendraient de la même maison mère. D'autres outils sont proposés par des acteurs du marché et s'intègrent facilement dans la plupart des systèmes sur le marché, nous pouvons citer la solution proposée par JUNIPER. D'autres encore sont des outils libres.

L'entreprise ayant une ligne de conduite basée sur l'implémentation d'une solution CISCO, notre choix ne pouvait se porter que dans ceux appartenant à cette catégorie. Le désir de pouvoir maîtriser la solution à proposer et de ne pas fournir une solution à la base trop complexe et les besoins exprimés plus hauts nous ont amenés à mettre en place la plate-forme CISCO ISE.

Les raisons qui militent en faveur de ce choix sont diverses. A savoir :

- L'entreprise fonctionne déjà dans un environnement full Cisco,
- Les équipements sont soumis à un contrat de maintenance,
- CISCO-ISE est une solution adaptée à l'environnement réseaux de MTN CI,
- Les raisons financières dans le but de réduire les réduire le cout de la réalisation,
- La solution CISCO-ISE est facile à déployé,
- Une compatibilité avec les switches d'accès.

L'architecture unique de Cisco ISE permet aux entreprises de recueillir les informations concernant les utilisateurs et les périphériques, en temps réel à partir du réseau. L'administrateur peut ensuite utiliser ces informations pour prendre des décisions de gouvernance proactive en liant l'identité à divers éléments du réseau, y compris les commutateurs, les contrôleurs de réseau local sans fil (WLC) et les passerelles des réseaux privés virtuels (VPN).

Dans ce présent chapitre, nous avons essayé de mettre en relief le principe de fonctionnement de toute solution NAC, son architecture globale ainsi que les différentes solutions disponibles ; néanmoins, nous nous sommes attardés sur une solution particulière proposée par CISCO Systems, à savoir la plate-forme ISE. Dans la suite nous verrons comment effectuez le déploiement de la solution retenue.