MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE

DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention
du Diplôme de Master Académique en
Electronique

Option : Réseaux Et Télécommunications

Thème :

La mise en place de la protection d'accès au réseau NAP associe au serveur DHCP.

Proposé et dirigé par :
Mr. OUALLOUCHE .F.
Mr. KIBOUH .M

Présenté par :
Mr. TALIOUINE BOUSSAD

Année universitaire 2011/2012

Remerciement

Remerciement

Je remercié tout d'abord, Allah qui m'a donné la force et le courage pour terminer mes études et élaborer ce modeste travail.

Je tiens à exprimer mes plus sincères remerciements à mon promoteur Mr.OUALLOUCHE, qui m'a aidé pour terminer le travail.

Un grand merci aussi à Mr.KIBOUH (2INT Drugstore) pour ses encouragements et ses orientations qui mon ont beaucoup aidé au cours de mon projet.

Je tiens à remercier également mes amis (es) et ma famille pour leurs aides considérables.

« Louange à Dieu, le seul et unique »

Je dédie ce modeste travail à tous ceux que j’aime ainsi que ceux qui m’aiment.

SOMMAIRE

Introduction sur le NAP

Architecture de NAP

LA mise en œuvre de nap avec serveur DHCP

Préambule

Par leur nature, les réseaux peuvent permettre à des ordinateurs en excellente santé de communiquer avec des ordinateurs contaminés et des outils malveillants qui s'attaquent à des applications légitimes. Cela peut aboutir à de coûteuses conséquences sécuritaires, comme un ver qui se répand rapidement sur un réseau interne ou un assaillant sophistiqué qui dérobe des données confidentielles sur le réseau.

Afin de mieux répondre aux problématiques introduites par les ordinateurs mal saints et contaminés. En se connectent directement sur le réseau sans respecter les exigences de sécurité. La protection de l'accès au réseau ou « NAP » Network Access Protection peut améliorer la sécurité de ces ordinateurs en veillant à ce que les utilisateurs conservent à jour leur ordinateurs, il impose aux ordinateurs d'effectuer un contrôle d'intégrité avant de leur accorder un accès complet au réseau et facilite la résolution des problèmes avec les ordinateurs qui ne répondant pas aux exigences d'intégrité.

Ce travail permettra de décrire le NAP et comment le déployer sur un réseau.

L'application choisie sera la mise en œuvre de NAP avec la Méthode d'enfoncement DHCP Cette Méthode s'impose d'elle-même vue l'importance de DHCP dans le domaine des réseaux informatique et sa facilité de mise on place.

Introduction générale

Introduction générale

Depuis plusieurs années maintenant, la question de la sécurité informatique a pris une place considérable dans les décisions des entreprises. La majorité d'entre elles n'hésitent plus à investir de manière conséquente dans du matériel et des solutions de plus en plus pointues destinées à garantir l'intégrité de leur infrastructure. La plupart du temps, les solutions misent en place (pare-feu, antivirus, anti spam…etc.) visent à protéger le réseau des menaces extérieures ce qui, bien qu'être une nécessité absolue peut s'avérer de nos jours insuffisante.

La sécurité n'est pas un produit- c'est un processus qui nous impose de penser de manière stratégique aux moyens d'appliquer des solutions techniques destinées à remplir les objectifs de notre stratégie de sécurité d'entreprise. Prenons comme exemple ce scénario classique : une entreprise possède des milliers d'ordinateurs sur un réseau privé. Des par feu périmétriques protègent le réseau des menaces Internet dont les attaques de ver. Soudain, quelqu'un crée un ver capable d'exploiter une vulnérabilité des ordinateurs dépourvus des derniers correctifs de sécurité. Le ver se multiplie rapidement sur Internet, mais les par feu périmétriques du réseau privé protègent les ordinateurs vulnérables du réseau interne. Un commercial revient alors de voyage avec son ordinateur portable infecte par le ver pendant qu'il était connecté au réseau Internet dès qu'il se connecte au réseau privé, le ver commence immédiatement à contaminer les ordinateurs vulnérables, En quelques heures, la plupart des ordinateurs du réseau interne sont infectés

La protection de l'accès au réseau ou NAP (Network Access Protection) peut éviter ce scénario. Lorsque les ordinateurs se connectent au réseau local (LAN) ils doivent respecter des exigences d'intégrité spécifiques, comme posséder les derniers correctifs installés S'il ne peuvent remplir ces exigences d'intégrité, ils peuvent être mis en quarantaine vers un réseau ou ils peuvent télécharger les mises

à jour, installer des logiciels antivirus et obtenir plus d'informations sur la façon de satisfaire les exigences du LAN.

L'objectif de ce projet de fin d'étude est de décrire l'architecture de NAP avec ses différentes entités, son fonctionnement et ainsi que la mise en place de la méthode d'enfoncement NAP avec serveur DHCP

Le chapitre 1 présente des généralités sur les réseaux, les notions de bases sur la sécurité des réseaux sont décrites dans le chapitre 2, le chapitre3 présente une introduction sur le NAP et son architecture et enfin nous terminons par implémenter le NAP via serveur DHCP on configurant les différentes entités qui le constituant

Chapitre 1

Généralité sur les réseaux informatiques

I.1.Introduction

L'installation d'un réseau de point de vue matériel est un processus assez linéaire; il est impératif de faire les choses dans un certain ordre, afin de s'assurer le bon fonctionnement futur de l'ensemble, Dans ce chapitre, nous allons se familiarisé avec les différents éléments de réseau et ces caractéristiques.

I.2.Que signifie un réseau ?

Un réseau en général est le résultat de connexion de plusieurs machines entre elles afin que les utilisateurs puissent échanges des informations et des applications qui fonctionne sur ces dernières. Le terme réseau en fonction de son contexte peut designer plusieurs choses :

- désigner l'ensemble des machines ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés. Ce qu'est le cas lorsqu'on parle de l'Intranet.
- décrire la façon dont les machines d'un site sont interconnectées.
- spécifier les protocoles qui sont utilisés pour que les machines communiquent on peut parler de réseau TCP/IP.

I.3.classification des réseaux

On distingue différents types de réseaux selon leur taille leur vitesse de transfert des données ainsi que leurs étendues Généralement on a trois classifications:

I.3.1.Classification selon la taille

- **Réseau locaux :** LAN (Local Area Network) : Destinés pour de courtes distances avec des débits de quelques dizaines de Mbits / seconde jusqu'à quelques centaines.

- **Réseaux métropolitains :** MAN (Métropolitaine Area Network) : Destinés à courir de très grands périmètres qui sont fédérateurs de réseaux locaux.
- **Réseaux étendue :** WAN (Wide Area Network) : Réseaux terrestres à travers des câbles posés qui interconnectent plusieurs réseaux locaux à travers de grandes distances géographiques.

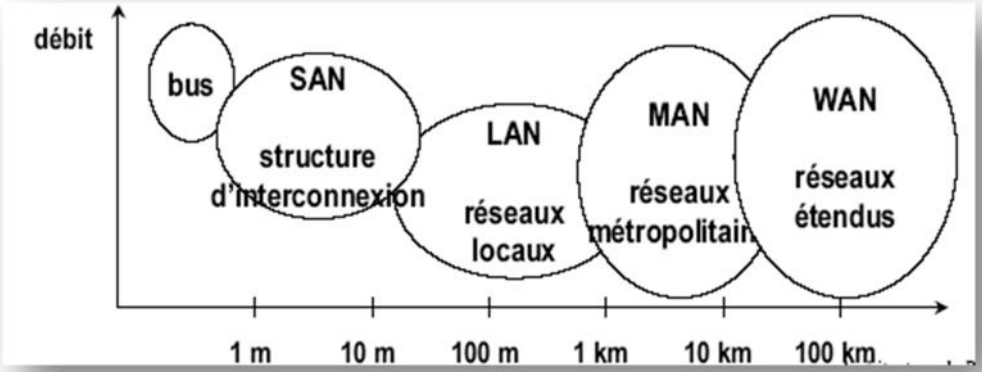


Figure I.1: types des réseaux classés selon la taille.

I.3.2.Classification selon l'organisation

- **Architecture Égal à égal :** Dans un réseau d'architecture égal à égal (Peer-to-Peer) tous les ordinateurs connectés ont le même statut et se partagent toute l'information et tous les services sans l'aide d'un serveur.
- **Architecture Client/serveur :** Un réseau d'architecture client/serveur est celui où des ordinateurs (clients) sont reliés à un serveur dédié.

I.3.3.Classification selon les topologies

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à du matériel (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique.

- **Topologie en bus :**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau. L'avantage du bus est sa simplicité de mise en œuvre et sa bonne immunité aux perturbations électromagnétiques. Par contre, si le câble est interrompu, toute communication sur le réseau est impossible.

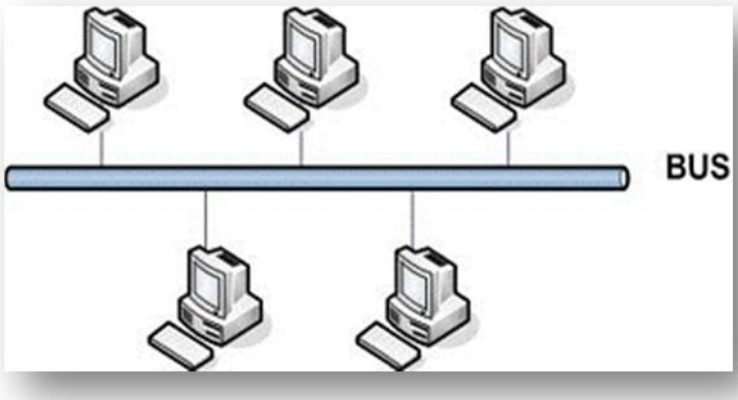


Figure I.2 topologie en bus

Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui est affecté.

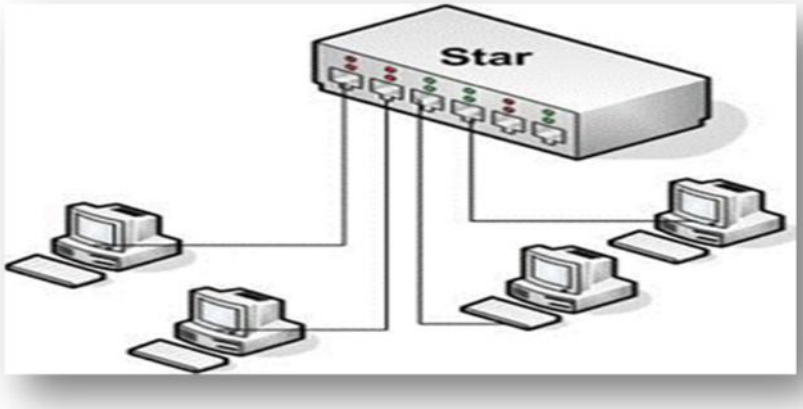
- **Topologie en étoile :**

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un matériel appelé hub ou concentrateur.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérable car on peut aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau.

En revanche un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub).

Figure I.3 topologie en étoile



- **Topologie en anneau :**

Dans un réseau en topologie en anneau, les ordinateurs communiquent chacun à leur tour, on a donc une boucle d'ordinateurs sur laquelle chacun d'entre eux va "avoir la parole successivement.

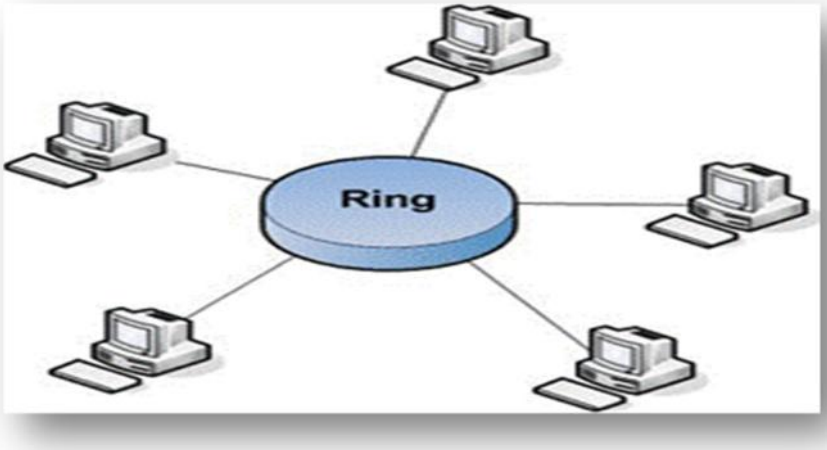


Figure I.4 topologie en anneau

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multi station Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en impartissant à chacun d'entre eux un temps de parole. Les deux principales topologies logiques utilisant cette topologie physique sont TOKEN RING (anneau à jeton) et FDDI.

I.4.Les équipements d'interconnexion

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelles, Routeurs, Ponts …) qui assurent le transfert des données :

- **Les Hubs** (concentrateurs)

Le Hub est également appelé concentrateur ou répétiteur. C'est un boîtier électronique assurant la liaison des postes et des périphériques du réseau. Le répétiteur se contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau (dont le destinataire).

- **Les Switches**

Egalement appelé Commutateur, Boîtier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le switch permet ainsi de libérer la bande passante en évitant ainsi le transfert de données inutiles sur le réseau.

- **Les Ponts**

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. Le pont filtre les données et ne laisse passer que les données destinées aux ordinateurs situés de l'autre côté du pont.

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet de données sur l'une de ses interfaces, il analyse l'adresse physique (MAC) du destinataire et de l'émetteur. Si jamais le pont ne connaît pas l'émetteur, il stocke son adresse dans une table afin de se "souvenir" de quel côté du réseau se trouve l'émetteur.

Ainsi le pont est capable de savoir si émetteur et destinataire sont situés du même côté ou bien de part et d'autre du pont. Dans le premier cas le pont ignore le message, dans le second le pont transmet la trame sur l'autre réseau.

- **Les Retour**

Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagrammes) afin de pouvoir assurer le passage d'un type de réseau à un autre (contrairement aux ponts).

Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en termes de taille de paquets de données. Les routeurs ont donc la possibilité de fragmenter les paquets de données pour permettre leur circulation.

Ils fonctionnent grâce à des tables de routage et des protocoles de routage. Les routeurs intègrent souvent une fonction de passerelle leurs permettant d'acheminer les paquets quel que soit l'architecture.

- **Les Passerelles**

Ce sont des systèmes matériels et/ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents, l'information est codée et transportée différemment sur chacun des réseaux.
Elles permettent aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre. Les réseaux ne peuvent pas faire circuler la même quantité de données simultanément en termes de taille de paquet de données, mais la passerelle réalise cette transition en convertissant les protocoles de communication de l'un vers l'autre. Cette opération ralentie le transfert de données.

I.5 Le Modèle OSI

OSI signifie (Open System Interconnections), Ce modèle a été mis en place par l'ISO (**I**nternational **S**tandard **O**rganisation) afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Le modèle OSI est un modèle qui comporte 7 couches :

- **Couche physique:** S'occupe de la connexion physique d'une machine avec le réseau.
- **Couche liaison :** S'occupe de l'acheminement de trames de données entre deux équipements voisins.
- **Couche réseau :** Définit l'unité de données de base transférée sur le réseau entre deux sites extrêmes et inclut les concepts d'adressage et de routage.
- **Couche transport :** Assure un contrôle de bout en bout en permettant à un processus destinataire de communiquer directement avec le processus source.
- **Couche session** : Définit la manière dont les protocoles peuvent être organisées pour fournir toutes les fonctionnalités dont les programmes d'applications se servent.
- **Couche présentation :** destinée à supporter les fonctions dont beaucoup de programme ont besoin comme la compression de texte ou la conversion d'image graphique.
- **Couche application :** Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.

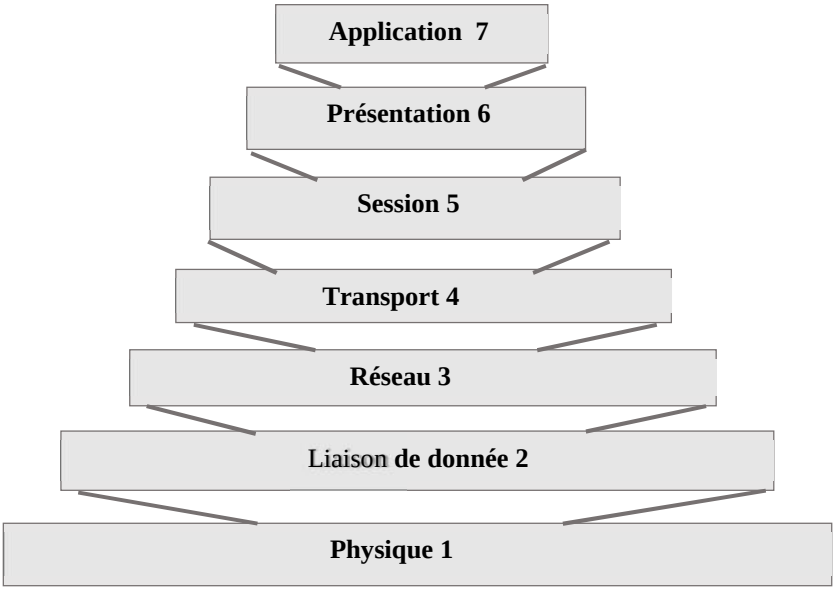


Figure I.9: Standard de modèle OSI

I.6 Architecture TCP/IP

I.6.1 Définition

Fournit un protocole standard pour résoudre le problème de connexion entre différents réseaux, TCP (Transfert Contrôle Protocole) se charge du transport de bout en bout pour toute application alors que IP (Internet Protocole) est responsable de routage à travers le réseau. D'autres protocoles sont aussi inclus comme ARP (Adresse Résolution Protocole), FTP (File Transfert Protocole), SMTP (Simple Mail Transfert Protocole),…..

TCP/IP est structuré en quatre niveaux :

- L'interface réseau (1 et 2 du modèle OSI).
- Le routage (3 du modèle OSI).
- Le transport (4 et 5 du modèle OSI).
- L'application (5,6et7 du modèle OSI).

I.6.2.Description du modèle :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches

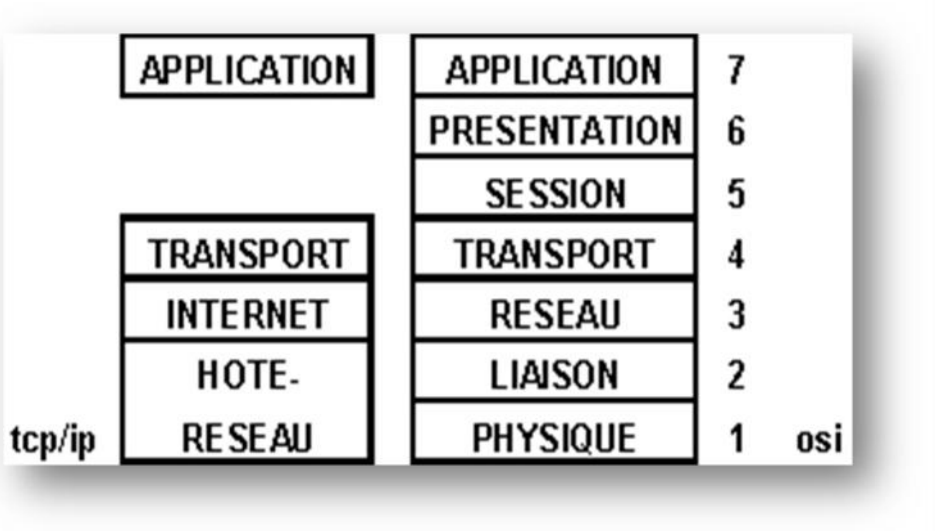


Figure I.6 : Analogie de modèle OSI avec le model TCP/IP

- **La couche application :**

C'est la couche située au sommet des couches du protocole TCP/IP .Elle contient les applications réseau permettant de communiquer grâce aux couches inférieure

La couche transport :

Elle permet à des applications tournant sur des machines distantes de communiquer.

La couche transport contient deux protocoles permettant à deux applications d'échanger des données indépendamment du type du réseau emprunté (c'est-à-dire indépendamment des couches inférieures …), il s'agit des protocoles suivants :

- **TCP :** un protocole orienté connexion qui assure le contrôle des erreurs.
- **UDP** : un protocole non orienté connexion dont le contrôle d'erreur est archaïque.

- **La couche internet**

C'est la couche la plus importante, car c'est elle qui définit les datagrammes (paquets de données), et qui gère la notion d'adressage IP.

Elle permet l'acheminement des datagrammes vers des machines distantes ainsi que la gestion de leur fragmentation et de leur assemblage à la réception.

La couche internet contient cinq protocoles : IP, ARP, ICMP, RARP et IGMP.

- **La couche accès réseau**

C'est la première couche de la pile TCP/IP, elle offre les capacités à accéder à un réseau physique quel qu'il soit, c'est-à-dire les moyens à mettre en œuvre afin de transmettre des données via un réseau.

Cette couche contient toutes les spécifications concernant la transmission de données sur un réseau physique, qu'il s'agisse de réseau local (Token Ring, Ethernet, FDDI), de connexion à une ligne téléphonique ou n'importe quel type de liaison à un réseau. Elle prend en charge les notions suivantes :

- Acheminement des données sur la liaison.
- Coordination de la transmission de données (synchronisation).
- Format des données.

- Conversion des signaux (analogique /numérique).
- Contrôle des erreurs à l'arrivée.

I.7 Encapsulations des données

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'un en-tête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original.

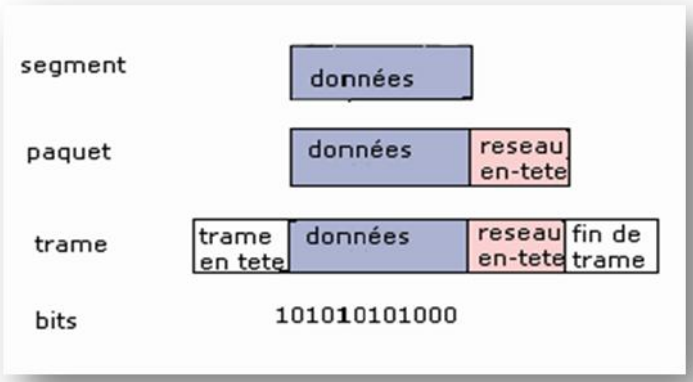


Figure I.7 : principe d'encapsulation.

I.8 Les protocoles réseaux

I.8.1 Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre deux machines c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

I.8.2 Différents type de protocoles

Il en existe plusieurs selon que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (protocole ICMP). Sur Internet par exemple les protocoles utilisés font partie d'une suite de protocoles, c'est-à dire un ensemble de protocoles reliés entre eux. Cette suite de protocole s'appelle TCP/IP.

- **Le Protocole TCP**

Protocole sécurisé d'échange de données créé dans but d'établir une communication de haute fiabilité entre deux tâches exécutées sur deux ordinateurs autonomes et raccordés à un réseau (protocole orienté connexion).

- **Le protocole IP**

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, Mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP.

- **Protocole UDP**

Le protocole UDP (User Data gram Protocol) a été créé dans le but d'établir comme le TCP une communication entre deux ordinateurs mais il ne fournit pas de contrôle d'erreur (il n'est pas orienté connexion).

- **Le protocole RIP**

L'un des protocoles de routage les plus populaires est RIP (Routing Information Protocol) qui est un protocole de type vecteur de distance. C'est-à-dire que les messages échangés par des routeurs voisins contiennent un ensemble de distances entre routeur et destinations qui permet de réactualiser les tables de routage. Ce protocole utilise une métrique simple : la distance entre une source et une destination est égale au nombre de sauts qui les séparent. Elle est comprise entre 1 et 15, la valeur 16 représentant l'«infini». Ceci implique que RIP ne peut être utilisé

qu'à l'intérieur de réseaux qui ne sont pas trop étendus.

- **Le protocole OSPF**

Est un nouveau type de protocole de routage dynamique qui élimine les limitations de RIP. C'est un protocole d'état de liens, c'est-à-dire qu'ici un routeur n'envoie pas des distances à ses voisins, mais il teste l'état de la connectivité qui le relie à chacun de ses voisins. Il envoie cette information à tous ses voisins, qui ensuite le propagent dans le réseau. Ainsi, chaque routeur peut posséder une carte de la topologie du réseau qui se met à jour très rapidement lui permettant de calculer des routes aussi précises qu'avec un algorithme centralisé.

En fait, RIP et OSPF, sont des protocoles de type IGP (Interior Gateway Protocol) permettant d'établir les tables des routeurs internes des systèmes autonomes. Un système autonome peut être défini par un ensemble de routeurs et de réseaux sous une administration unique.

Cela peut donc aller d'un seul routeur connectant un réseau local à Internet, jusqu'à l'ensemble des réseaux locaux d'une multinationale. La règle de base étant qu'un système autonome assure la connexité totale de tous les points qui le composent en utilisant notamment un protocole de routage unique

- **Le protocole DNS**

Le DNS est le mécanisme qui permet de convertir le symbolique en adresse IP, Lorsque les machines communiquent sur un réseau informatique, c'est toujours par l'utilisation d'une adresse (IP ou autre) source ou destination. Mais ces adresses bien que nécessaires, sont difficiles à mémoriser et ne permettent pas de souplesse dans les configurations des stations.

Pour quelqu'un de normalement constitué, il est difficile de se souvenir de 192.168.1.56 alors que www.ummto.dz sera assez aisé à mémoriser, C'est le but du protocole DNS : fournir une association (adresse IP, nom FQDN) et inversement.

Le service DNS est donc utilisé pour la « résolution de noms », Cette opération consiste à fournir aux clients DNS qui en font la demande une association adresse IP, un nom symbolique et vice-versa.

- **Le protocole DHCP**

Le protocole DHCP (Dynamics Host Configuration Protocol) attribue automatiquement des adresses IP aux équipements branchés au réseau. Lorsqu'un client essaie de se brancher au réseau, une demande de paramètres de configuration est envoyée au serveur DHCP. Une fois que le serveur a reçu le message, le serveur DHCP envoie une réponse au client, qui comprend les informations de configuration, puis enregistre en mémoire les adresses qui ont été attribuées.

DHCP utilise le protocole *BOOTP* pour communiquer avec les clients. Les clients doivent renouveler leur adresse IP à 50 % de la période d'utilisation, puis de nouveau à 87,5 %, en envoyant un message *DHCPREQUEST*. Les hôtes clients conservent leur adresse IP jusqu'à l'expiration de leur période d'utilisation, ou lorsqu'ils envoient une commande *DHCPRELEASE*. *IPCONFIG* et *WINIPCFG* sont des utilitaires exécutés à partir de la ligne de commande et qui permettent de vérifier les informations de l'adresse IP qui a été attribuée à l'hôte client.

I.9.Adressage

Chaque ordinateur du réseau Internet dispose d'une adresse IP unique codée sur32 bits. Plus précisément, chaque interface dispose d'une adresse IP particulière.

En effet, un même routeur interconnectant 2 réseaux différents possède une adresse IP pour chaque interface de réseau. Une adresse IP est toujours représentée dans une notation décimale pointée constituée de 4 nombres (1 par octet) compris chacun entre 0 et 255 et séparés par un point. Plus précisément, une adresse IP est constituée d'une paire *(*id. de réseau, id de machine*)* et appartient à une certaine classe (A, B, C, D ou E) selon la valeur de son premier octet, comme détaillé dans la figure I.8.

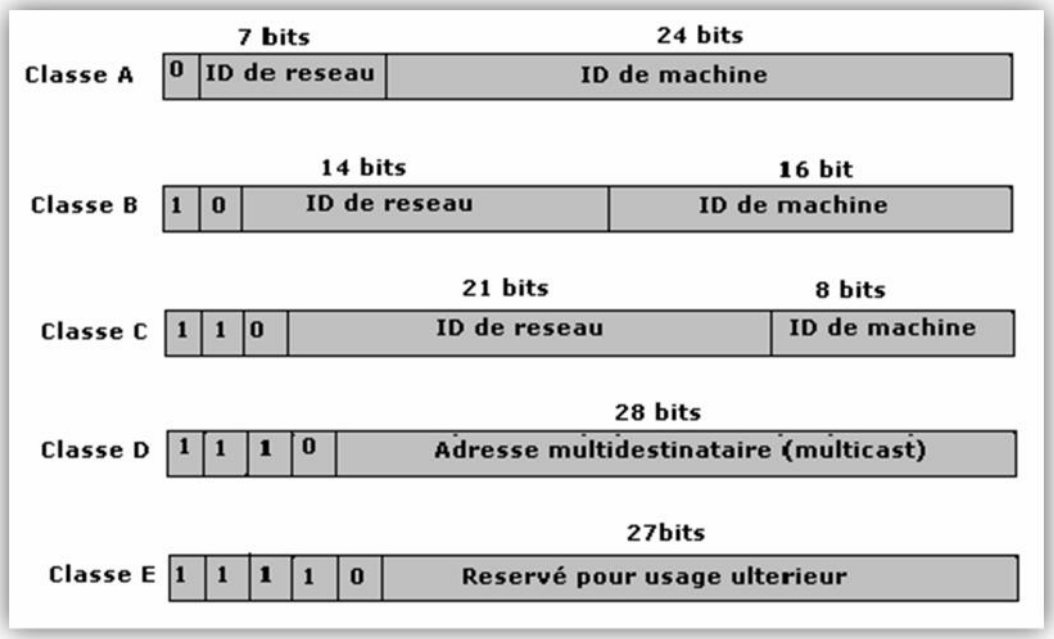


Figure I.8 les cinq classes d'adresses IP.

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Classe	Adresses
A	0. 0. 0. 0 à 127. 255. 255. 255
B	128. 0. 0. 0 à 191. 255. 255. 255
C	192. 0. 0. 0 à 223. 255. 255. 255
D	224. 0. 0. 0 à 239. 255. 255. 255
E	240. 0. 0 .0 à 247. 255. 255. 255

Tableau I.9 : L'espace d'adresse

Adresses particulières sont des adresses à ne pas utiliser comme :

1. La partie machine toute à zéro
2. La partie machine toute a un (1)
3. Adresse locale hôte : 127.0.0.1

Les plages d'adresses suivantes sont réservées à l'usage privé et il ne faut pas qu'elles soient défaussées sur internet :

- 0.0.0.0 ⟶ 10.255.255.255
- 172.16.0.0 ⟶ 172.31.0.0
- 192.168.0.0 ⟶ 192.168.255.255

I.10.Le routage IP

Le routage est l'une des fonctionnalités principales de la couche IP et consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux d'un internet. Ainsi un routeur réémettra des datagrammes venus d'une de ses interfaces vers une autre, alors qu'un ordinateur sera soit l'expéditeur initial, soit le destinataire final d'un datagramme.

D'une manière générale on distingue la remise directe, qui correspond au transfert d'un datagramme entre deux ordinateurs du même réseau, et la remise indirecte qui est mise en œuvre dans tous les autres cas, c'est-à-dire quand au moins un routeur sépare l'expéditeur initial et le destinataire final.

Chapitre 2

Généralité sur la sécurité informatique

II.1. Introduction

La sécurité des systèmes informatiques vise à protéger l'accès et la manipulation des données et des ressources d'un système par des mécanismes d'authentification, d'autorisation, de contrôle d'accès, etc.

Néanmoins, avec l'ouverture et l'interconnexion des systèmes informatiques, des attaques exploitant les failles de ces systèmes et le contournant de leurs mécanismes de sécurité sont toujours possibles. Il n'est donc pas suffisant d'agir préventivement, c'est à dire de définir une politique de sécurité et de la mettre en œuvre. Il faut aussi être capable de détecter toute tentative de violation de la politique de sécurité ou toute intrusion

Nous définissons dans ce chapitre les termes de sécurité des réseaux ainsi que les méthodes des attaques utilisées et comment se protéger contre elles

II.1.1 Qu'est-ce que la sécurité d'un réseau ?

La sécurité d'un réseau est un niveau de garantie que l'ensemble des machines du réseau fonctionnent de façon optimale et que les utilisateurs dites machines possèdent uniquement les droits qui leur ont été octroyé

La mise en œuvre de la sécurité dans un réseau pour le protéger de toute sorte d'intrusion malveillante, implique la réalisation des fonctions essentielles suivantes :

- **Intégrité :** pour garantir que les données sont bien celles que l'on croit être.
- **Confidentialité :** consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction c'est-à-dire consistent à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **Disponibilité:** permettant de maintenir le bon fonctionnement du système d'information quand les informations sont accessibles au moment voulu.
- **Non-répudiation :** permettant de garantir qu'une transaction ne peut être niée

- **Authentification :** garantit l'identité des correspondants ou des partenaires qui communiquent.

II.2. Politique de sécurité

II.2.1 Définition

Une politique de sécurité ou stratégie de sécurité est une déclaration formelle des règles qui doivent être respectées par les personnes qui ont accès aux ressources et données de l'entreprise en vue de protéger son réseau contre les attaques menées soit de l'intérieur, soit de l'extérieur .autrement dit une politique de sécurité est un ensemble de règles qui fixent les actions autorisées et interdites dans le réseau sur les ressources et données de l'entreprise

II.2.2 En quoi consiste une politique de sécurité ?

Une politique mise en œuvre doit contrôler les accès à des zones définies du réseau et comment interdire l'accès à certaines zones des utilisateurs non autorisés. Par exemple, seuls les membres d'un service doivent avoir accès à l'historique des salaries

Les mots de passe empêchent généralement les utilisateurs d'accéder aux zones protégées, mais à la condition que ceux-ci demeurent confidentiels. Des politiques écrites stipulant par exemple, que les utilisateurs ne doivent pas afficher leurs mots de passe sur leur bureau peuvent souvent prévenir certaines failles dans la sécurité.

Les clients ou fournisseurs ayant accès à certaines parties du réseau doivent également être l'objet de règles adéquates de cette politique

II.2.3. Qui doit appliquer et gérer cette politique ?

La personne ou le groupe chargé de gérer et d'entretenir le réseau et sa sécurité doivent avoir accès à toutes ses zones.

La fonction de gestion des politiques de sécurité doit donc être confiée à des personnes particulièrement dignes de confiance et disposant des compétences techniques nécessaires.

La plupart des failles dans la sécurité proviennent de l'intérieur, les personnes ou le groupe ne doivent donc pas constituer une menace potentielle. Une fois désignés, les gestionnaires du réseau bénéficient d'outils logiciels sophistiqués leur permettant de définir, de distribuer, de renforcer et d'évaluer la politique de sécurité

II.3. Les menaces contre la sécurité

II.3.1 Qui sont les ennemis ?

Au fil du temps, les outils et les méthodes permettant d'attaquer les réseaux ont constamment évolués désormais les personnes n'ont plus eu besoin de posséder le même niveau de connaissances qu'auparavant, pour devenir des pirates Des personnes auparavant qui n'auraient pas eu commis de délits informatiques sont à présent à même de le faire.

À mesure que les types de menaces, d'attaques et d'exploits évoluaient, différents termes ont été définis pour désigner les individus impliqués dans ces attaques. Voici quelques exemples des termes les plus courants :

- **Pirate** (cracker) :

  Autre terme désignant les personnes qui utilisent leurs connaissances des systèmes informatiques pour accéder de manière non autorisée à ces systèmes ou réseaux, habituellement dans un but personnel ou lucratif.

- **Bidouilleur** (hacker) :

  Terme général utilisé dans le passé pour désigner un expert en programmation. Actuellement, ce terme est souvent utilisé de manière péjorative pour désigner un individu qui tente d'accéder de manière non autorisée aux ressources des réseaux avec une intention malveillante.

- **Braqueurs**

  Sont plus dangereux que les hackers et mettent en panne des systèmes informatiques entiers, volent ou endommagent des données confidentielles, détériorent des pages Web et vont même jusqu'à interrompre l'activité.

- **Fouineur**

  Individu qui recherche des vulnérabilités dans des systèmes ou réseaux et qui signale ces vulnérabilités à leurs propriétaires de manière à ce qu'ils puissent les éliminer. Ils ont une éthique qui les oppose à tout usage abusif des systèmes informatiques. Les fouineurs tendent généralement à sécuriser les systèmes informatiques, tandis qu'à l'opposé, les pirates veulent y pénétrer par intrusion.

- **Spammeur**

  Individu qui envoie une grande quantité de courriels non sollicités. Les spammeurs utilisent souvent des virus pour prendre possession d'ordinateurs familiaux et utiliser ces derniers pour leurs envois massifs.

- **Hameçonner**

  Individu qui utilise le courriel ou d'autres moyens pour amener par la ruse d'autres utilisateurs à leur fournir des données sensibles, comme des numéros de carte de crédit ou de passeport. L'hameçonner se fait passer pour une institution de confiance qui aurait un besoin légitime de ces données sensibles.

II.3.2 Les types de menaces

Les menaces sont considérées comme une violation potentielle du système de sécurité elles viennent d'individus compétents intéressés par l'exploitation des vulnérabilités (faiblesses) de sécurité. Il existe deux types fondamentaux de menaces :

Les menaces accidentelles

Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet. L'exposition peut émerger des pannes hardware, software ou bien de l'utilisateur et le résultat pourra être une violation de la confidentialité des objets. Par exemple, une exposition se produit quand un utilisateur envoie un e-mail confidentiel à la mauvaise personne. Les menaces accidentelles peuvent se réaliser par elle-même durant les modifications des objets (informations et/ou des ressources). La modification d'une ressource se présente quand une ressource entre dans un état illégal résultant d'un événement accidentel.

Les menaces intentionnelles

L'attaque est une menace intentionnelle. C'est une action exécutée par une entité pour violer la sécurité ; la modification et la violation de l'information, l'utilisation non autorisée des ressources, l'envoi de messages anonymes sont quelques exemples d'attaques.

II.5. Les principales attaques

II.5.1 Que peuvent faire les ennemis ?

La plupart des attaques, de la plus simple à la plus complexe fonctionne selon les différentes étapes suivant :

- **Identification de la cible**

  Cette étape est indispensable à toutes attaques organisées, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS,….

- **Le scanning**

  L'objectif est de compléter les informations réunies sur une cible visées. Il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall….). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

- **L'exploitation**

  Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

- **La progression**

  Il est temps pour l'attaquant de réaliser ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, installation de backdoors, nettoyage des traces,…).

II.5.2. Les différents types d'attaque

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres

II.5.2.1. Attaques contre la communication

- **Ecoute passive**

  Est un type d'attaque contre la confidentialité, qui consiste à accéder sans modification aux informations transmises ou stockées, l'information n'est pas altérée par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement être parées par des mesures préventives.

- **Interposition**

  Il s'agit d'un « déguisement » en émission ou en réception, il consiste à tromper les mécanismes d'authentification pour se faire passer pour un utilisateur (personne ou service disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité.

  Exemple : Le vol d'adresse (IP spoofing)

  Ce type d'attaque n'implique rien de plus que l'usurpation d'une adresse source. Cela consiste à utiliser une machine en se faisant passer pour une autre.

- **Coupure** (message interception) :

  Est un accès avec modification à des informations transmises sur des voies de communication, il s'agit donc d'une attaque contre l'intégrité.

II.5.2.2. Attaques logicielles

- **Les virus**

  Un "virus" est un bout de programme glissé volontairement dans une application dans le but de nuire. Il est possible d'attraper un virus avec n'importe quelle application que l'on a installée et que l'on exécute, ce n'est pas un problème typique d'une connexion permanente. Un virus ne peut être introduit dans sa machine que si l'on exécute une application infectée, application récupérée sur l'Internet ou sur n'importe quel autre support informatique: Disquette, CD ROM etc.

  Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

  • Téléchargement de logiciel puis exécution de celui-ci sans précautions,

  • Ouverture sans précautions de documents contenant des macros,

  • Pièce jointe de courrier électronique (exécutable, script type VBs…),

  • Ouverture d'un courrier au format HTML contenant du JavaScript exploitant une faille de sécurité du logiciel de courrier (normalement JavaScript est sans danger).

- **Le Cheval de Troie**

  Un cheval de Troie ou troyen (Trojan Horse ou Trojan) n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie :

  - Récupération des mots de passe grâce à un key logger.
  - Administration illégale à distance d'un ordinateur.
  - Relais utilisé par les pirates pour effectuer des attaques.
  - Serveur de spam (envoi en masse des e-mails).

- **Les vers**

  Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter. Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, un ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

- **Le sniffing** (l'écoute du réseau)

  Grâce à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par Telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire.

  De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception.

II.5.2.3. Autres attaques

- **Le DoS** (Denial of Service)

  Le DoS est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les faiblesses de l'architecture d'un réseau ou d'un protocole. Il en existe de plusieurs types comme le flooding, le TCP-SYN flooding, le smurf ou le débordement de tampon (buffer-overflow)

- **Intrusion**

  L'intrusion dans un système informatique a généralement pour but la réalisation d'une menace et est donc une attaque. Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage… Le principal moyen pour prévenir les intrusions est le coupe-feu ("firewall"). Il est efficace contre les fréquentes attaques de pirates amateurs, mais d'une efficacité toute relative contre des pirates expérimentés et bien informés. Une politique de gestion efficace des accès, des mots de passe et l'étude des fichiers « log » (traces) est complémentaire

- **Le craquage de mots de passe**

  Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

II.6. Les méthodes de protection

II.6.1. Logiciels antivirus

La plupart des ordinateurs sont dotés d'un logiciel antivirus pré intégré capable de détecter les principales menaces virales s'il est régulièrement mis à jour et correctement entretenu.

Avec des milliers de nouveaux virus générés chaque mois, il est crucial que la base de données des virus soit tenue à jour. La base de données des virus est l'enregistrement du logiciel d'antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

II.6.2. Pare feu

Un pare-feu (appelé aussi *coupe-feu*, *garde-barrière* ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Il est utilisé pour :

Contrôler le trafic sortant d'un réseau, et notamment éviter que les utilisateurs accèdent à certains nœuds du réseau.

Sécuriser le trafic entrant d'un réseau, et empêcher certains nœuds extérieurs de se connecter un réseau local.

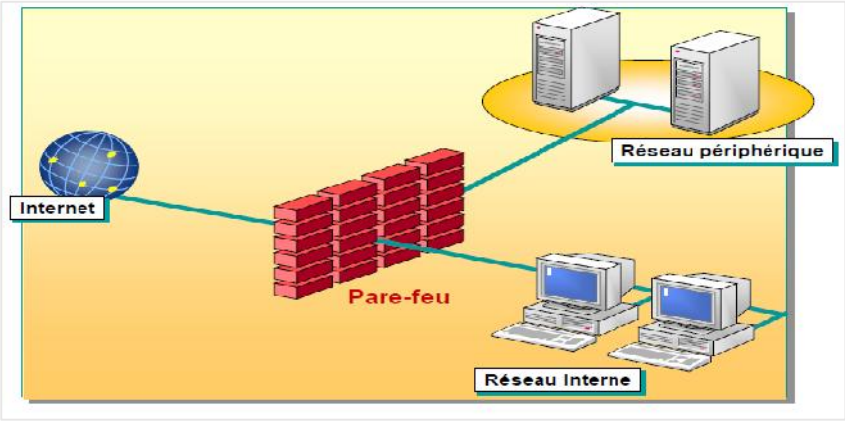


Figure II.1 : Le firewall

Enfin, pour une question de vigilance, et éviter que certaines machines mal configurées du réseau local n'envoient des données vers l'extérieur.

Le firewall ainsi défini permet de filtrer les paquets de données échangés avec le réseau, Il s'agit ainsi d'une passerelle filtrante comportant au minimum deux interfaces réseau : Une interface pour le réseau à protéger (réseau interne).et une interface pour le réseau externe.

II.6.3.Le proxy

Un serveur proxy (traduction en français de proxy server, appelé aussi serveur mandataire) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et Internet.

La plus part de temps le serveur proxy est utilisé pour le Web, il s'agit alors d'un protocole http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, etc).

Le principe de fonctionnement basique d'un serveur proxy est assez simple ; il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

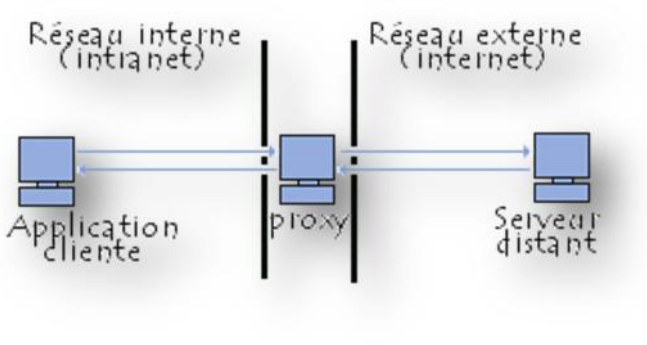


Figure II.2:Le proxy

II.6.5 Le chiffrement

Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message, Ce dernier est décryptable par une clé unique correspondant au cryptage.

Il existe à l'heure actuelle deux grands principes de cryptage : le cryptage symétrique basé sur l'utilisation d'une clé privée et le cryptage asymétrique qui repose sur un codage à deux clés, une privée et l'autre publique.

Le cryptage symétrique

Le cryptage à clé privé ou symétrique est basé sur une clé (ou algorithme) partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages. Les algorithmes de chiffrement les plus connus sont :Kerberos, DES (Data Encryption Standard) et RSA.

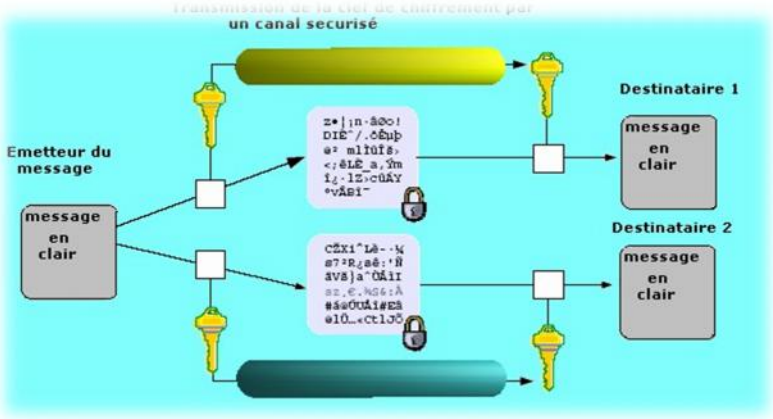


Figure II.3 Cryptage Symétrique.

Le principal problème est le partage de la clé : Comment une clé utilisée pour sécuriser peut être transmise sur un réseau insécurisé ? La difficulté engendrée par la génération, le stockage et la transmission des clés (on appelle l'ensemble de ces trois processus le management des clés : Key management) limite les systèmes des clés privées surtout sur Internet.

Le cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que de l'utilisateur ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

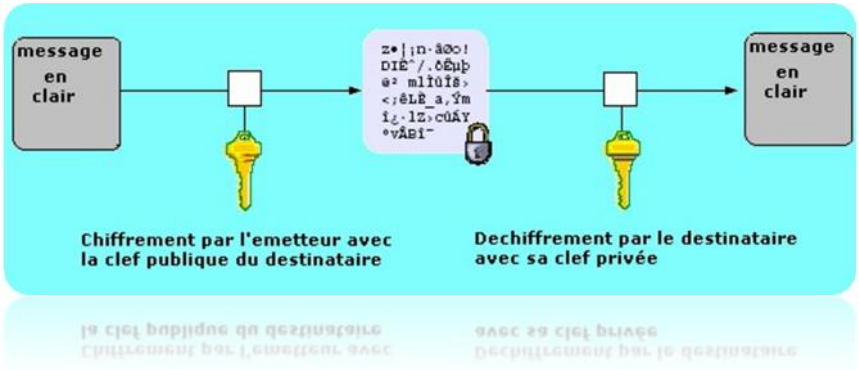


Figure II.4 : cryptage asymétrique.

Ce cryptage présente l'avantage de permettre le placement des signatures numériques dans le message et ainsi permettre l'authentification de l'émetteur. Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :

- Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- Authentification plus flexible.
- Supporte les signatures numériques.

II.6.6 L'authentification

Définition

L'Authentification est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.

La combinaison de plusieurs de ces méthodes (aussi appelées facteurs d'authentification) permet de renforcer le processus d'authentification, on parle alors d'authentification forte.Les techniques d'authentification les plus usitées sont, de loin, les *mots de passe* mais aussi, de plus en plus, les *Certificats de clés publiques*.

Mots de passe

Le moyen le plus simple et le plus classique de s'assurer que seules les personnes autorisées peuvent accéder à une certaine partie du réseau est de protéger certaines zones du réseau par un mot de passe.

De nombreux utilisateurs choisissent des chiffres ou des mots faciles à retenir pour leurs mots de passe, comme des dates d'anniversaires, des numéros de téléphone ou des noms d'animaux de compagnie, d'autres ne changent jamais leurs mots de passe et ne se soucient pas de leur confidentialité.

II.6.7 Certificats numériques

II.6.7.1Présentation

Un certificat numérique (aussi appelé certificat électronique) est un fichier permettant de certifier l'identité du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité. Un certificat est généré dans une infrastructure à clés publiques (aussi appelé PKI pour Public Key Infrastructure) par une autorité de certification (Certification

Authority, CA) qui a donc la capacité de générer des certificats numériques contenant la clé publique en question.

Les certificats numériques sont généralement utilisés à des fins d'identification, lors de l'établissement de tunnels sécurisés sur Internet, comme c'est le cas dans les réseaux virtuels privés (VPN) et sont émis par une autorité de certification.

II.6.7.2 Le rôle d'un certificat

Un certificat numérique intervient dans différents mécanismes permettant de sécuriser l'échange de données sur un réseau. On y retrouve le cryptage asymétrique ou encore la signature électronique combinée à un contrôle d'intégrité des données.

Un certificat numérique permet, lors d'un cryptage asymétrique, de garantir lorsque cela s'avère nécessaire, l'identité des différents intervenants. Par exemple l'envoi d'un message crypté de manière asymétrique entre deux utilisateurs.

II.6.7.3 Les infrastructures à clés publiques

Une PKI (Public Key Infrastructure), aussi appelée IGC (Infrastructure de Gestion de Clés) est une infrastructure réseau qui a pour but final de sécuriser les échanges entre les différents composants d'un réseau. Cette infrastructure se compose de quatre éléments essentiels :

- **L'autorité d'enregistremen**

Registration Autorite C'est cette autorité qui aura pour mission de traiter les demandes de certificat émanant des utilisateurs et de générer les couples de clés nécessaires (clé publique et clé privée). Son rôle peut s'apparenter à la préfecture lors d'une demande de carte d'identité.

- **L'autorité de Certification**

Certification Autorite Elle reçoit de l'Autorité d'Enregistrement les demandes de certificats accompagnées de la clé publique à certifier. Elle va signer à l'aide de sa clé privée les certificats, un peu à la manière de la signature de l'autorité sur une carte d'identité. Il s'agit du composant le plus critique de cette infrastructure en raison du degré de sécurité requis par sa clé privée.

- **L'autorité de Dépôt**

PKI Dépositoires, Il s'agit de l'élément chargé de diffuser les certificats numériques signés par la CA sur le réseau (privé, Internet, etc.).

- **Les utilisateurs de la PKI**

Ce sont les personnes effectuant des demandes de certificat mais aussi ceux qui souhaitent vérifier l'identité d'un certificat qu'ils ont reçu.

II.6.7.4 Les différents Types d'autorités

Il existe deux types principaux d'installation pour l'autorité de certification :

- **Autorité d'entreprise**

A l'utiliser si l'autorité de certification doit délivrer des certificats dans un domaine auquel appartient le serveur (se base sur l'annuaire d'Active Directory). Cette autorité doit-être contrôleur de domaine.

- **Autorité autonome**

Permet de délivrer des certificats dans un réseau comme Internet. Il existe deux niveaux fonctionnels pour chacun de ces deux types d'installation pour l'autorité de certificat :

Autorité racine : Cette autorité de certification est la première du réseau.

- **Autorité secondaire :** dépend d'une autorité racine.

II.7. Les protocoles de sécurité

II.7.1.Le SSL

Le protocole SSL (Secure Socket Layer) permet de sécuriser tout protocole applicatif s'appuyant sur TCP/IP. (HTTP, FTP, etc.….).

Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, mais également les services de confidentialité et d'intégrité.

Le principe d'une authentification du serveur avec SSL est le suivant :

1. Le navigateur du client fait une demande de transaction sécurisée au serveur.
2. Suite à la requête du client, le serveur envoie son certificat au client.
3. Le serveur fournit la liste des algorithmes cryptographiques qui peuvent être utilisés pour la négociation entre le client et le serveur.
4. Le client choisit l'algorithme.
5. Le serveur envoie son certificat avec les clés cryptographiques correspondantes au client.
6. Le navigateur vérifie que le certificat délivré est valide.
7. Si la vérification est correcte alors le navigateur du client envoie au serveur une clé secrète chiffrée à l'aide de la clé publique du serveur qui sera donc le seul capable de déchiffrer puis d'utiliser cette clé secrète. Cette clé est un secret uniquement partagé entre le client et le serveur afin d'échanger des données en toute sécurité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec SSL soit facultative.

II.7.2. Le SSH

Le protocole SSH (*Secure Shell*) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité (personne d'autre que le serveur ou le client ne peut lire les informations transitant sur le réseau). Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (spoofing).

II.7.3. Le IPsec

Les services de sécurité d'IPsec sont fournis au travers de deux extensions du protocole IP appelées AH (Authentication Header) et ESP (Encapsulating Security Payload).

Authentication Header AH est conçu pour assurer l'authenticité des paquets IP sans chiffrement des données. Le principe d'AH est d'adjoindre aux paquets IP un champ supplémentaire permettant à la réception de vérifier l'authenticité des données. Un numéro de séquence permet de détecter les tentatives de rejeu.

Encapsulating Security Payload ESP a pour rôle premier d'assurer la confidentialité des données mais peut aussi être utilisé pour assurer l'authenticité de celles-ci. Le principe d'ESP consiste à encapsuler dans un nouveau paquet IP le paquet d'origine mais sous une forme chiffrée. L'authenticité des données peut être obtenue par l'ajout d'un bloc d'authentification et la protection contre le rejeu par celui d'un numéro de séquence.

Ces deux services peuvent être utilisés séparément ou conjointement afin d'obtenir les services de sécurité requis. Ces services ne sont pas restreints à un algorithme de chiffrement particulier ; en théorie, n'importe quel algorithme de chiffrement peut être employé, sous réserve que les équipements en communication disposent d'au moins un algorithme en commun, IPsec comporte une liste d'algorithmes proposés pour être

utilisés avec IPsec et dont l'utilisation est négociable en ligne par le biais du protocole IKE (RC5, DES, …).

Pour garantir l'interopérabilité entre les équipements, le standard IPsec rend certains de ces algorithmes obligatoires. Actuellement, DES-CBC et 3DES-CBC sont obligatoires pour le chiffrement ; pour l'authentification, HMAC-MD5 et HMACSHA-1 doivent être présents dans toute implémentation conforme d'IPsec.

D'autre part, pour chacune des extensions IPsec, *deux modes de protection* existent :

- **Le mode transport :**

  Protège uniquement le contenu du paquet IP sans toucher à l'en-tête, ce mode n'est utilisable que sur les équipements terminaux (postes clients, serveurs).

- **Le mode tunnel :**

  Permet la création de tunnels par « encapsulation » de chaque paquet IP dans un nouveau paquet. Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs des en-têtes (adresses source et destination par exemple). Ce mode est celui utilisé par les équipements réseau (routeurs, gardes-barrières...).

II.7.4 Le VPN

L'acronyme VPN correspond à *Virtual Private Network*, c'est-à-dire un réseau privé virtuel. Dans les faits, cela correspond à une liaison permanente, distante et sécurisée entre deux sites d'une organisation. Cette liaison autorise la transmission de données cryptées par le biais d'un réseau non sécurisé, comme Internet. En d'autres termes, un réseau privé virtuel est l'extension d'un réseau privé qui englobe les liaisons sur des réseaux partagés ou publics, tels qu'Internet. Il permet d'échanger des données entre deux entités sur un réseau partagé ou public, selon un mode qui émule une liaison privée point à point.

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des machines distantes au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.

Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail. On peut facilement imaginer un grand nombre d'applications possibles :

Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades.

Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante.

Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet.

Les connexions VPN permettent également aux entreprises de disposer des connexions routées partagées avec d'autres entreprises sur un réseau public, tel qu'Internet, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée.

Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante.

Chapitre 3

La protection d'accès réseau NAP

Partie 1 :
Introduction sur le NAP

III.1. Introduction

Une des tâches les plus fastidieuses auxquelles sont confronté les administrateurs réseau consiste à s'assurer que les ordinateurs qui se connectent au réseau de l'entreprise sont à jour et conformes aux règles d'accès à ce réseau. Cette mission complexe est généralement désignée par les termes « gestion de l'état de l'ordinateur ». L'application des conditions requises est d'autant plus difficile que certains ordinateurs, comme ceux au domicile des employés ou les ordinateurs portables, ne sont pas sous le contrôle. Malheureusement, la connexion d'ordinateurs dont l'état n'est pas garanti fait peser de lourdes menaces sur l'intégrité du réseau. En effet, des personnes mal intentionnées peuvent créer un logiciel ciblant ces ordinateurs. Un utilisateur qui ne met pas à jour son ordinateur personnel avec les signatures antivirus les plus récentes risque de propager des virus sur le réseau de son entreprise lorsqu'il se connecte de chez lui. On n'a pas toujours le temps ni les ressources nécessaires pour s'assurer que tous les logiciels qu'on souhaite imposer sont installés et à jour. On ne peut pas non plus facilement gérer ou modifier les conditions requises aussi souvent qu'on le souhaite.

Network Access Protection offre des composants et un jeu d'API (interfaces de programmation d'applications) qui nous permet d'imposer la conformité aux stratégies d'accès au réseau. Développeurs et administrateurs peuvent créer des solutions pour valider les ordinateurs qui se connectent à leurs réseaux, fournir les mises à jour requises, accéder aux ressources nécessaires (pour la mise à jour) ou limiter l'accès au réseau des ordinateurs non conformes. Les fonctionnalités d'application de Network Access Protection peuvent être intégrées aux logiciels d'autres éditeurs ou à des programmes personnalisés. Les administrateurs ont la possibilité de personnaliser les systèmes qu'ils développent et déploient, que ce soit pour surveiller les ordinateur accédant au réseau en regard du respect des stratégies, la mise à jour logicielle automatique des ordinateurs pour respecter les stratégies, ou pour isoler les ordinateurs qui ne répondent pas aux critères des stratégie en les plaçant dans un réseau plus sécurisé (nommé réseau de quarantaine).

Network Access Protection n'a pas été conçu pour protéger un réseau des utilisateurs malveillants, mais pour maintenir les ordinateurs d'un réseau dans un état sain, ces ordinateurs permettant à leur tour de maintenir l'intégrité globale du réseau.

Ainsi, un ordinateur possédant tous les logiciels requis et la configuration correcte exigée par la stratégie d'accès au réseau, est considéré comme sain et conforme ; il peut alors accéder au réseau de l'entreprise. En revanche, Network Access Protection n'empêche pas un utilisateur autorisé, disposant d'un ordinateur considéré comme sain, à propager un programme malveillant sur le réseau ou à commettre une autre action inappropriée.

III.2 Aspects de NAP

Network Access Protection comporte trois aspects majeurs et distincts :

- **Validation de la stratégie de réseau** Lorsqu'un utilisateur tente de se connecter au réseau, l'état de l'ordinateur est validé par rapport aux stratégies d'accès au réseau telles qu'elles ont été définies. On peut alors choisir l'action à entreprendre si un ordinateur n'est pas conforme. Dans un environnement de surveillance, tous les ordinateurs autorisés bénéficient de l'accès au réseau même si certains d'entre eux ne sont pas conformes aux stratégies d'accès au réseau ; toutefois, l'état de conformité de chaque ordinateur est consigné dans un journal. Dans un environnement d'isolement, les ordinateurs conformes aux stratégies d'accès au réseau sont autorisés à accéder au réseau, tandis que ceux qui ne sont pas conformes ou qui ne sont pas compatibles avec Network Access Protection sont isolés dans un réseau de quarantaine. Néanmoins, dans ces deux environnements, On peut définir des exceptions au processus de validation
- **Conformité aux stratégies de réseau**. On a la possibilité de s'assurer de la conformité aux stratégies d'accès au réseau en mettant à jour automatiquement les ordinateurs non conformes avec les spécifications manquantes via un logiciel d'administration, tel que Microsoft Systems Management Server (SMS). Dans un environnement de surveillance, les ordinateurs ont accès au réseau même avant qu'ils soient mis à jour avec les logiciels requis ou les modifications de configuration. Dans un environnement d'isolement, les ordinateurs non conformes

aux stratégies d'accès au réseau sont isolés jusqu'à ce que les mises à jour logicielles et de configuration soient terminées

- **Isolement vis-à-vis du réseau** On peut protéger les ressources réseau en isolant les ordinateurs qui ne sont pas conformes aux conditions requises. Ces ordinateurs ont un accès réseau, défini peut être limité à un réseau de quarantaine, à une ressource unique ou à aucune ressource interne. Si l'on ne configure pas de ressources de mise à jour, l'ordinateur qui se connecte restera isolé pendant toute la durée de la connexion. Si en revanche, on configure des ressources de mise à jour, l'ordinateur ne restera isolé que le temps de sa mise à jour. Il est souhaitable qu'on utilise à la fois la surveillance et la conformité aux stratégies de réseau dans notre réseau, et qu'on configure également des exceptions.

III.3 Scénarios pour Network Access Protection

Network Access Protection a été conçu dans un objectif de flexibilité. Cette plate-forme peut interagir avec les logiciels de n'importe quel éditeur qui fournit des composants SHA et SHV et qui reconnaît le jeu d'API publiées. Voici quelques exemples de solutions.

- **Vérifier l'état et la conformité des ordinateurs portables itinérants**

La portabilité et la flexibilité constituent les deux principaux avantages des ordinateurs portables, mais ces deux caractéristiques constituent également une menace pour un réseau. En effet, les ordinateurs portables se déconnectent souvent du réseau de l'entreprise. Ils sont alors incapables de recevoir les mises à jour logicielles ou les modifications de configuration les plus récentes. Ils risquent également d'être infectés lorsqu'ils sont exposés sur des réseaux non sécurisés, tels qu'Internet. Grâce à Network Access Protection, on peut vérifier l'état d'un ordinateur portable lorsqu'il se reconnecte au réseau de l'entreprise via une connexion VPN ou directement depuis le bureau.

- **Garantir l'état des ordinateurs de bureau**

Bien que les ordinateurs de bureau ne quittent généralement pas l'entreprise, ils peuvent toujours présenter un risque pour un réseau. Afin de réduire ce risque, on doit maintenir ces ordinateurs avec les mises à jour et les logiciels les plus récents

que l'entreprise exige. Dans le cas contraire, les ordinateurs présentent un risque très élevé d'infection provenant de sites Web, de messageries électroniques, de fichiers partagés et d'autres ressources publiques. Par l'intermédiaire de Network Access Protection, On peut automatiser les vérifications pour contrôler la conformité de chaque ordinateur de bureau aux stratégies d'accès au réseau. Un fichier journal signale les points non respectés. À l'aide d'un logiciel d'administration, on génère des rapports automatiques et crée des mises à jour automatiques sur les ordinateurs non-conformes. Lorsque les stratégies d'accès au réseau sont modifiées, les ordinateurs reçoivent automatiquement les mises à jour les plus récentes.

- **Vérifier la conformité et l'état des ordinateurs situés dans des bureaux distants**

Les ordinateurs situés dans des sites distants ou des filiales ont souvent besoins de se connecter aux mêmes ressources réseau que les ordinateurs de bureau locaux. Il est donc nécessaire de les vérifier et de les contrôler. Network Access Protection nous permet de contrôler automatiquement les ordinateurs distants afin de vérifier la conformité à chaque fois qu'un ordinateur établit une connexion VPN au réseau. Tant que ces vérifications système ne sont pas terminées, les ordinateurs distants peuvent être mis en quarantaine. Lorsque les stratégies d'accès au réseau sont modifiées, les ordinateurs distants peuvent recevoir les mises à jour exactement comme s'ils étaient physiquement connectés au réseau local.

- **Déterminer l'état des ordinateurs portables des visiteurs**

Les entreprises sont fréquemment amenées à autoriser leurs consultants et leurs invités à accéder à leur réseau privé. Or, les ordinateurs portables de ces visiteurs peuvent ne pas respecter les conditions requises et présenter ainsi un risque pour l'intégrité du réseau. Network Access Protection permet de déterminer si les ordinateurs portables des visiteurs sont autorisés à accéder au réseau et, dans le cas contraire, à limiter leur accès réseau à un réseau de quarantaine. En règle générale, on n'exige pas de mise à jour ou de modification de configuration sur les ordinateurs portables des visiteurs. En revanche, on peut configurer un accès Internet spécifique pour les ordinateurs portables visiteurs dans le réseau de quarantaine, accès distinct des autres ordinateurs isolés.

- **Vérifier la conformité et l'état des ordinateurs personnels non gérés**

Les ordinateurs domestiques non gérés constituent un obstacle supplémentaire dans la mesure où ceux-ci n'ont pas d'accès physique à ces ordinateurs. Il n'est donc pas possible d'exiger la conformité aux conditions requises du réseau (telles que l'utilisation d'un programme antivirus). La vérification de l'état de ces ordinateurs est également difficile. Network Access Protection permet de contrôler les programmes, les paramètres de Registre, les fichiers requis ou les combinaisons de ces derniers à chaque fois qu'un ordinateur personnel établit une connexion VPN entre le domicile d'un employé et le réseau de l'entreprise. On peut également placer l'ordinateur en quarantaine jusqu'à ce que toutes ces vérifications soient terminées.

III.4. Composants de Network Access Protection

Network Access Protection comporte des composants d'isolement de réseau pour trois technologies : le protocole DHCP (Dynamic Host Configuration Protocol) et les réseaux privés virtuels (VPN) et le protocole IPsec. On peut utiliser ces technologies séparément ou ensemble pour isoler les ordinateurs dont l'état est incertain. Le serveur IAS (Internet Authentication Service), configuré avec des filtres de quarantaine, peut faire office de serveur de stratégie à la fois pour la Quarantaine DHCP et pour la Quarantaine VPN

Quarantaine DHCP

La Quarantaine DHCP comporte un composant QES (Quarantaine Enfoncement Server), serveur d'application de quarantaine DHCP, et un composant QEC (Quarantaine Enfoncement Client), client d'application de quarantaine DHCP. En utilisant la Quarantaine DHCP, les serveurs DHCP appliquent les conditions d'accès au réseau à chaque fois qu'un ordinateur tente de louer ou de renouveler une adresse IP sur le réseau. Cette fonctionnalité donne à la Quarantaine DHCP une très grande portée d'application car tous les ordinateurs clients doivent louer une adresse IP. En revanche, la Quarantaine DHCP offre un faible niveau d'isolement réseau.

Quarantine VPN

La Quarantaine VPN comporte un composant QES VPN et un composant QEC VPN. Elle permet aux serveurs VPN d'appliquer les conditions d'accès au réseau à chaque fois qu'un ordinateur tente d'établir une connexion VPN au réseau. Elle offre un niveau d'isolement élevé aux ordinateurs accédant au réseau via une connexion VPN.

Quarantaine IPsec

La Quarantaine IPsec comporte un composant QES IPsec et un composant QEC IPsec la Quarantaine 'IPsec est prise avec IPsec, on peut définir des conditions pour des communications protégées avec les ordinateurs sur la base de l'adresse IP ou par-TCP/UDP. La quarantaine IPsec confine la communication aux ordinateurs après qu'ils aient obtenu une ADDRESS IP. La quarantaine d'IPsec est la forme la plus forte de accès ou communication de réseau limité dans le NAP.

IAS/RADIUS

Le composant RADIUS (Remote Authentication Dial-In User Service) fonctionne en tant que serveur de stratégie, conjointement avec les composants QES et QEC, notamment ceux de la Quarantaine DHCP et de la Quarantaine VPN. On doit définir des stratégies de quarantaine et une classe d'utilisateurs de quarantaine sur le serveur IAS. Les serveurs Quarantaine IAS effectuent des vérifications de stratégie et se coordonnent avec le service d'annuaire Active Directory® à chaque fois qu'un ordinateur tente de se connecter à un serveur DHCP ou VPN.

III.5 Composants et ressources supplémentaires de NAP.

Network Access Protection intègre des composants serveurs, des composants clients et des ressources de quarantaine. Les ressources de quarantaine sont composées de serveurs, de services ou d'autres ressources auxquels un ordinateur qui est isolé dans un réseau de quarantaine peut accéder. Ces ressources effectuent la résolution de noms, obtiennent les mises à jour logicielles les plus récentes ou accèdent aux instructions ou composants nécessaires pour rendre l'ordinateur

conforme aux stratégies d'accès au réseau. Par exemple, un serveur DNS secondaire, un serveur de fichiers de signature antivirus ou un serveur de mises à jour logicielles peuvent tous être des ressources de quarantaine.

III.5.1. Composants serveurs de NAP

- **Serveur de quarantaine**

Le serveur de quarantaine est un composant serveur qui coordonne le résultat de tous les valideurs de l'état du système pour déterminer si les composants QES (Quarantine Enforcement Server) doivent ou non isoler un client du réseau en fonction de la conformité à la stratégie. Dans la première version de la plate-forme Network Access Protection, le composant Serveur de quarantaine fonctionne comme un serveur IAS.

- **Validation de l'état du système (SHV)**

La validation de l'état du système est assurée par un logiciel serveur qui valide le résultat d'un agent d'état du système (SHA) correspondant pour vérifier si la déclaration d'état (SoH, Statement of Health) envoyée par un SHA est conforme à la stratégie. Dans la première version de la plate-forme Network Access Protection, les valideurs d'état du système fonctionnent sur le serveur IAS. Un réseau peut comporter plusieurs types de valideurs. Dans ce cas, un serveur de quarantaine doit coordonner le résultat de tous les valideurs pour déterminer si un ordinateur doit être isolé.

- **Serveur de stratégie**

Un serveur de stratégie est un ordinateur qui propose des ressources afin de préserver l'état des clients sur le réseau et de fournir une solution pour les ordinateurs qui n'ont pas un état satisfaisant. Les agents d'état du système, par exemple ceux destinés à l'administration des logiciels antivirus ou des mises à jour logicielles, communiquent avec les serveurs de stratégie pour obtenir les mises à jour les plus récentes. Les valideurs de l'état du système (SHV) communiquent avec les serveurs de stratégie pour valider la déclaration d'état (SoH) provenant d'un agent d'état du système correspondant.

- **Stratégie de quarantaine**

Une stratégie de quarantaine spécifie les conditions requises pour l'accès au réseau. Dans la première version de Network Access Protection, les stratégies de quarantaine sont configurées dans IAS. Un réseau peut posséder plusieurs stratégies de quarantaine. Par exemple, la Quarantaine DHCP et la Quarantaine VPN peuvent utiliser différentes stratégies de quarantaine.

- **Systems Management Server (SMS)**

Systems Management Server gère les applications, les ressources et les mises à jour logicielles sur les serveurs et les clients. SMS possède à la fois des composants de stratégie serveur et client. On peut configurer SMS en tant que valideur de l'état du système (SHV) et en tant qu'agent d'état du système (SHA) dans un réseau pour lequel Network Access Protection a été déployé.

- **Base de données de comptes**

Une base de données de comptes stocke les comptes d'utilisateur et les propriétés de leur accès au réseau.

III.5 2 Composants clients de NAP

- **Agent de quarantaine**

Un agent de quarantaine est un logiciel client qui coordonne des informations entre les différents agents d'état du système (SHA) et clients d'application de quarantaine (QEC).

- **Client de stratégie**

Un client de stratégie est un logiciel client qu'un agent d'état du système (SHA) utilise pour effectuer des fonctions de gestion d'état du système, conjointement à un serveur de stratégie. Par exemple, un SHA SMS utilise le logiciel client SMS installé localement (le client de stratégie) pour effectuer l'installation logicielle et mettre à jour les fonctions avec le serveur SMS (le serveur de stratégie).

- **Agent de l'état du système**

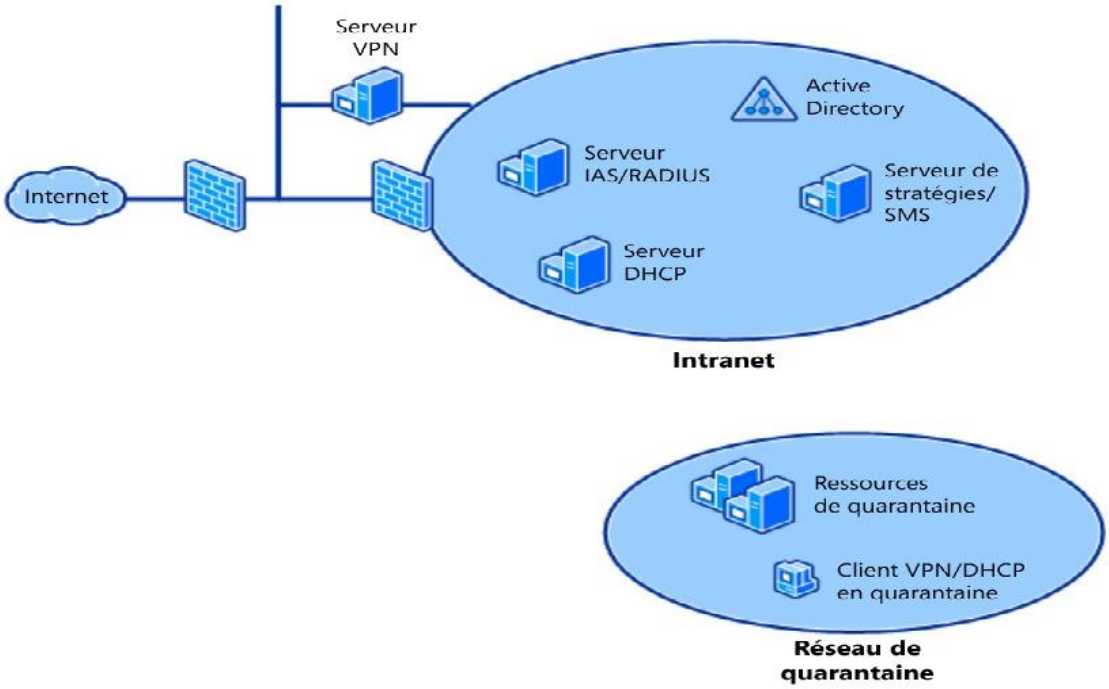
Un agent d'état du système (SHA) est un logiciel client qui s'intègre à l'agent de quarantaine pour effectuer des vérifications de stratégie système et mettre à jour l'état du système. Il communique directement avec un serveur de stratégie ou utilise les fonctions d'un client de stratégie installé, telles que le logiciel client SMS.

III.6 Vue d'ensemble de fonctionnement de NAP

La plate-forme Network Access Protection est conçue de sorte qu'on puisse la configurer afin qu'elle réponde aux besoins de réseaux individuels. Par conséquent, la configuration réelle de Network Access Protection varie en fonction de nos préférences et nos besoins. Cependant, le fonctionnement sous-jacent de Network Access Protection reste inchangé. Le diagramme et la procédure ci-dessous illustrent le fonctionnement de Network Access Protection dans un exemple de réseau.

Network Access Protection n'est pas une solution de sécurité. Cette plate-forme est conçue pour éviter aux ordinateurs dont la configuration présente un risque, de se connecter à un réseau. Elle ne protège pas les réseaux des utilisateurs malveillants qui disposent d'informations d'identification valides et d'ordinateurs répondant aux conditions d'accès au réseau.

La figure 1 illustre un exemple de réseau pour Network Access Protection.



FigureIII 1 Exemple de réseau dans lequel Network Access Protection a été déployé

L'exemple de réseau est configuré pour la Quarantaine DHCP et la Quarantaine VPN. IAS est installé sur un serveur séparé. Le serveur IAS joue à la fois le rôle de serveur de stratégie et de serveur de quarantaine, coordonnant la stratégie à partir du serveur SMS. Le serveur SMS est un serveur de stratégie et un valideur de l'état du système (SHV) ; il fournit des services d'administration logicielle via son composant client qui fait office d'agent d'état du système (SHA). Cet exemple de réseau est configuré pour la validation des stratégies réseau, la conformité des stratégies réseau et l'isolement du réseau.

Lorsqu'il établit une connexion VPN au réseau ou qu'il loue ou renouvelle une adresse IP à partir du serveur DHCP, chaque ordinateur est classé dans une des deux catégories. Les ordinateurs qui satisfont aux stratégies d'accès au réseau sont classés comme sains et bénéficient de l'autorisation d'accès au réseau. Ceux qui ne satisfont pas aux stratégies, sont classés comme à risques et isolés vers le réseau de quarantaine jusqu'à ce qu'ils répondent aux conditions requises. Un ordinateur à risque n'est pas nécessairement infecté par un virus ou par une autre menace active sur le réseau, mais il ne possède pas la configuration et les logiciels requis par la stratégie (définis par l'administrateur et déterminés par SMS, faisant office de serveur de stratégie). Par conséquent, les ordinateurs à risque constituent une menace pour l'état global du réseau. Les administrateurs configurent SMS, l'agent

d'état du système (SHA) et le valideur de l'état du système (SHV) pour qu'ils mettent à jour automatiquement les ordinateurs isolés avec les logiciels requis afin d'obtenir l'accès complet au réseau.

L'exemple de réseau contient un réseau de quarantaine. Ce dernier peut être isolé au niveau logiciel, lorsqu'un réseau local virtuel (VLAN) est utilisé pour les ordinateurs isolés et les ressources de quarantaine. Sinon, il est possible de placer des restrictions (par exemple des filtres IP ou des routes statiques) sur des ordinateurs isolés pour définir les ressources de quarantaine avec lesquelles ils peuvent communiquer.

III.6.1 Quarantaine DHCP

Le processus suivant décrit le fonctionnement de la Quarantaine DHCP sur un réseau configuré comme sur la figure 1, lorsqu'un client DHCP disposant d'un seul agent d'état du système (SHA) doit louer ou renouveler le bail d'une adresse IP :

1. Le client DHCP envoie une demande DHCP dans un message au serveur DHCP.
   A. Si le client DHCP possède une déclaration d'état (SoH), la demande DHCP l'inclut. La SoH fournit des informations sur l'état du client. Le serveur DHCP transmet la SoH au serveur IAS. Ce dernier communique avec le serveur SMS pour déterminer si la SoH est valide. Une SoH est valide si elle correspond à la liste des composants et des configurations que le serveur SMS requiert.
      I. Si la SoH est valide, le serveur DHCP attribue au client DHCP l'adresse IP et le masque de sous-réseau appropriés. Le client DHCP bénéficie alors de l'accès normal au réseau, tel qu'il est défini par la stratégie.
      II. Si la SoH n'est pas valide, le service DHCP isole le client DHCP dans le réseau de quarantaine et lui attribue le masque de sous-réseau de quarantaine et les adresses de routage de quarantaine, tels que l'administrateur réseau les a définis.
   B. Si le client DHCP n'a pas de SoH, il n'est pas conforme. Le serveur DHCP isole alors le client dans le réseau de quarantaine et lui attribue le masque de sous-réseau de quarantaine et les adresses de routage de quarantaine, tels que

l'administrateur réseau les a définis.

2. L'agent de quarantaine situé sur le client DHCP isolé signale son état au serveur SMS et demande des mises à jour.
3. Le serveur SMS fournit au client DHCP les mises à jour requises afin de le mettre en conformité avec la stratégie réseau. La SoH du client DHCP est également mise à jour.
4. Le client DHCP isolé envoie au serveur DHCP une demande DHCP dans un message, en incluant la SoH mise à jour. Lorsque le serveur IAS valide la SoH mise à jour, le serveur DHCP attribue au client DHCP l'accès normal au réseau, tel qu'il est défini par la stratégie.

III.6.2 Quarantaine VPN

Qui ne possède qu'un seul agent d'état du système (SHA) sur un réseau configuré similairement au réseau de la figure 1 :

1. Le client VPN établit une connexion au serveur VPN.
2. Le client VPN transmet ses informations d'authentification au serveur VPN à l'aide du protocole PEAP (Protected Extensible Authentication Protocol).
3. Si les informations d'authentification sont valides, le serveur VPN demande une SoH au client VPN.
4. Si le client VPN possède une SoH, il la transmet au serveur VPN, qui la transmet à son tour au serveur IAS. Ce dernier, faisant office de serveur de quarantaine, communique avec le serveur SMS pour déterminer si la SoH est valide. Une SoH est valide si elle correspond à la liste des composants et des configurations que le serveur SMS requiert.
   A. Si la SoH est valide, le serveur VPN termine la connexion et attribue au client VPN l'accès normal au réseau, tel qu'il est défini par la stratégie.
   B. Si la SoH n'est pas valide, le serveur VPN termine la connexion, mais isole le client VPN dans le réseau de quarantaine. Le client VPN peut alors envoyer du trafic uniquement vers le réseau de quarantaine, le serveur VPN et le serveur SMS.
5. Si le client VPN ne possède pas de SoH, il n'est pas conforme. Le serveur VPN

termine alors la connexion, mais isole le client VPN dans le réseau de quarantaine.

6. L'agent de quarantaine situé sur le client VPN isolé signale son état au serveur SMS et demande des mises à jour.
7. Le serveur SMS fournit au client VPN les mises à jour requises afin de le mettre en conformité avec la stratégie réseau. La SoH du client VPN est mise à jour.
8. Le client VPN envoie sa SoH mise à jour au serveur VPN dans un échange PEAP. Lorsque le serveur IAS valide la SoH mise à jour, le serveur VPN attribue alors au client VPN l'accès normal au réseau, tel qu'il a été défini par la stratégie.

III.7. Conclusion

Selon les besoins du réseau, on peut dispenser certains ordinateurs, périphériques ou utilisateurs des conditions d'accès au réseau. Par exemple, certaines versions de Windows ne prennent pas en charge Network Access Protection, si bien que les ordinateurs qui utilisent ces versions de Windows sont toujours isolés par défaut. Dans ce cas, on peut configurer une exception pour ces ordinateurs, de sorte que leur conformité n'est pas vérifiée et qu'ils obtiennent toujours un accès normal au réseau.

Partie 2 :
Architecture de NAP

III.1. Introduction

Network Access Protection (NAP) est un nouvel ensemble de composants du système d'exploitation qui fournit une plate-forme pour l'accès protégé aux réseaux privés. La plate-forme NAP offre un moyen intégré de détecter l'état d'un client réseau qui essaie de se connecter à un réseau et de restreindre l'accès du client réseau jusqu'à ce que les exigences de la stratégie pour la connexion au réseau soient satisfaites.

Pour protéger l'accès à un réseau, une infrastructure réseau doit couvrir les domaines de fonctionnalité suivants :

- **Validation de la stratégie.** Détermine si les ordinateurs sont conformes à la stratégie de sécurité. Les ordinateurs conformes sont considérés comme « sains ».
- **Restriction du réseau**. Restreint l'accès en fonction de l'état du système.
- **Correctifs.** Fournit les mises à jour nécessaires pour permettre à l'ordinateur d'être considéré comme sain.
- **Conformité.** Autorise l'accès au réseau tant que l'ordinateur satisfait aux exigences de la stratégie.

La plate-forme NAP renforce la configuration des adresses DHCP (Dynamic Host Configuration Protocol), les connexions réseau de type réseau privé virtuel VPN et les communications basées sur IPsec (Internet Protocol security), et fournit une architecture où la validation des stratégies, les restrictions réseau, les correctifs et l'analyse de la conformité peuvent être assurés par des composants supplémentaires provenant de fournisseurs de logiciels.

III.2. Conception de réseau

La figure III 1 présente les composants réseau de la plate-forme NAP.

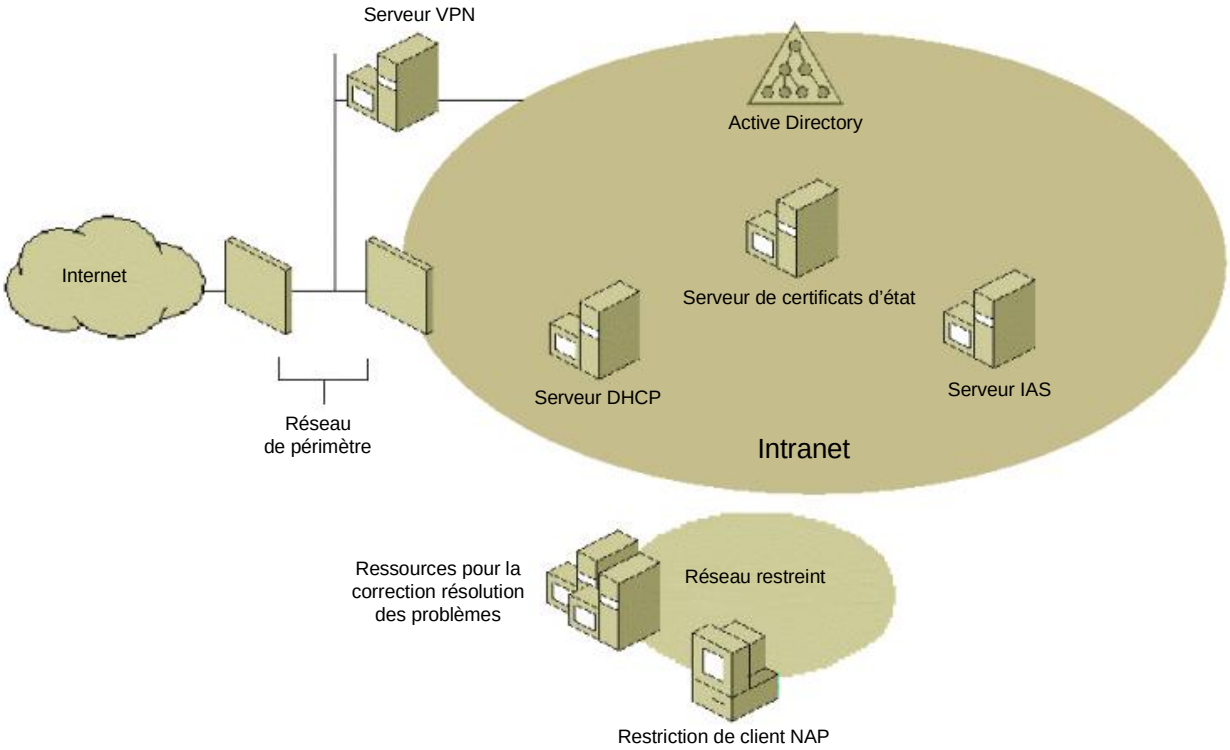


Figure III 1 - Composants réseau de la plate-forme NAP proposée.

La conception de réseau NAP inclut les éléments suivants :

- **Serveur VPN.** Le service de routage et d'accès à distance (RRAS, Routing and Remote Access) autorise les connexions d'accès à distance VPN à un intranet privé.
- **Serveur DHCP.** Le service serveur DHCP fournit la configuration automatique des adresses IPv4 aux clients d'un intranet privé.
- **Serveur IAS.** Le service IAS (Internet Authentication Service) fournit le contrôle de la stratégie d'accès réseau pour les clients DHCP ou VPN. IAS peut tourner sur un serveur VPN ou DHCP, ou, comme indiqué à la figure 1, sur un serveur distinct pour la configuration centralisée des stratégies d'accès réseau.
- **Serveur de certificats d'éta**t. Autorité de certification (CA) basée sur Windows Server exécutant les services Internet (IIS) qui émet des certificats pour les clients NAP sains.

- **Service d'annuaires Active Directory** Service d'annuaires Windows qui stocke les informations d'identification des utilisateurs pour les connexions VPN.
- **Réseau restreint**. Réseau logique ou physique distinct qui contient :
  - **des ressources de correction**, c'est-à-dire des ordinateurs serveurs qui contiennent des ressources permettant à un client NAP de mettre à jour son état de façon à se conformer aux exigences de la stratégie réseau. Les exemples incluent les serveurs DNS (Domain Name System), les serveurs de mise à jour des signatures antivirus et les serveurs de mise à jour de logiciels ;
  - **des clients NAP** dans un état restreint, qui sont placés sur le réseau restreint lorsqu'ils ne se conforment pas aux stratégies d'accès réseau et que des correctifs s'avèrent nécessaires.

III.2.1. Architecture de la plate-forme Network Access Protection

Les principaux ordinateurs qui interagissent pour l'accès réseau protégé sont les suivants :

- **Clients NAP.** Qui prennent en charge la plate-forme NAP pour la configuration DHCP, les connexions VPN d'accès à distance et la communication sécurisée avec IPsec.
- **Serveurs NAP.** Qui prennent en charge l'application de l'accès réseau restreint pour les clients DHCP, les clients VPN ou les clients NAP basés sur IPsec qui ne satisfont pas aux exigences actuelles relatives à l'état du système.
- **Serveurs IAS.** Qui prennent en charge la configuration de la stratégie système et la coordination de l'inspection de l'état pour les clients NAP.
- **Serveurs de stratégie.** Qui contiennent des ressources pour maintenir les clients réseau conformes à la stratégie et pour fournir des correctifs destinés aux clients NAP qui ne sont pas conformes à la stratégie. Exemples : les serveurs de distribution des signatures antivirus et les serveurs de mise à jour de logiciels.
- **Serveur de certificats d'état.** Qui émettent des certificats d'état pour les clients NAP basés sur IPsec.

III.2.2 Les interactions de base entre les éléments

Les interactions de bases pour ces éléments sont les suivants :

- Entre le client NAP et le serveur DHCP :

Le client NAP faisant office de client DHCP utilise des messages DHCP pour obtenir une configuration d'adresse IPv4 valide et pour indiquer l'état d'état actuel de son système. Le serveur NAP utilise des messages DHCP afin d'allouer soit une configuration d'adresse IP pour le réseau restreint et les instructions de correction (si le client DHCP n'est pas conforme à la stratégie), soit une configuration d'adresse IP pour l'accès normal à l'intranet.

- Entre le client NAP et le serveur VPN :

Le client NAP faisant office de client VPN utilise des messages PPP (Point-to-Point Protocol) pour établir une connexion VPN et des messages PEAP (Protected Extensible Authentication Protocol) sur la connexion PPP pour indiquer l'état d'état actuel de son système au serveur IAS. Le serveur IAS utilise des messages PEAP soit pour indiquer les instructions de correction (car le client VPN n'est pas conforme à la stratégie) soit pour signaler que le client VPN peut accéder normalement à l'intranet. Les messages PEAP entre le client VPN et le serveur IAS sont acheminés à travers le serveur VPN.

- Entre le client NAP et le serveur de certificats d'état :

Le client NAP basé sur IPsec utilise le protocole HTTPS (HyperText Transfer Protocol over Secure Socket Layer (SSL)) pour créer une session sécurisée avec le serveur de certificats d'état afin d'indiquer l'état d'état actuel de son système. Le serveur de certificats d'état utilise la session HTTPS sécurisée pour envoyer des instructions de correction (si le client basé sur IPsec n'est pas conforme à la stratégie) ou un certificat d'état pour authentifier les communications déclenchées avec d'autres clients basés sur IPsec sur l'intranet.

- Entre le client NAP et le serveur de stratégie :

Tant que le client NAP peut accéder normalement à l'intranet, il accède au serveur de stratégie pour s'assurer qu'il reste sain. Par exemple, le client NAP accède périodiquement à un serveur d'antivirus pour s'assurer qu'il dispose du dernier fichier de signature antivirus ou à un serveur de mise à jour de logiciels, tel

Windows Update Services, pour s'assurer qu'il dispose des dernières mises à jour du système d'exploitation.

Si le client NAP est connecté au réseau restreint, il accède au serveur de stratégie pour devenir conforme à la stratégie réseau, en fonction des instructions du serveur IAS. Par exemple, si, pendant le processus de validation de la stratégie d'accès réseau, le serveur IAS a déterminé que le client NAP ne possède pas le fichier de signature antivirus le plus récent, le serveur IAS ordonne au client NAP de mettre à jour son fichier de signature local avec le dernier fichier stocké sur un serveur d'antivirus spécifié.

- Entre le serveur DHCP et le serveur IAS :

Le serveur DHCP envoie des messages RADIUS (Remote Authentication Dial-In User Service) au serveur IAS qui contient les paramètres de l'état du système du client DHCP.

Le client IAS envoie des messages RADIUS au serveur DHCP pour :

- indiquer que le client DHCP bénéficie d'un accès normal, car est conforme à la stratégie d'accès réseau ;
- indiquer que le client DHCP doit être placé sur le réseau restreint jusqu'à l'exécution d'un ensemble de fonctions correctives.
- Entre le serveur VPN et le serveur IAS :

Le serveur VPN envoie des messages RADIUS pour transférer les messages PEAP envoyés par un client NAP basé sur VPN.

Le serveur IAS envoie des messages RADIUS pour :

- indiquer que le client VPN bénéficie d'un accès normal, car est conforme à la stratégie d'accès réseau ;
- indiquer que le client VPN doit être placé sur le réseau restreint jusqu'à l'exécution d'un ensemble de fonctions correctives ;
- envoyer des messages PEAP à un client NAP basé sur VPN.

- Entre le serveur de certificats d'état et le serveur IAS :

Le serveur de certificats d'état envoie des messages RADIUS contenant les paramètres de l'état du système du client NAP basé sur IPsec au serveur IAS.

Le serveur IAS envoie des messages RADIUS pour :

- indiquer que le client NAP basé sur IPsec bénéficie d'un accès normal, car est conforme à la stratégie d'accès réseau. En fonction de cette réponse, le serveur de certificats d'état émet un certificat pour le client NAP basé sur IPsec ;
- indiquer que le client NAP basé sur IPsec doit être placé sur le réseau restreint jusqu'à l'exécution d'un ensemble de fonctions correctives. En fonction de cette réponse, le serveur de certificats d'état n'émet pas de certificat pour le client NAP basé sur IPsec.

- Entre le serveur IAS et le serveur de stratégie :

Lorsqu'il exécute une validation de l'accès réseau pour un client NAP, le serveur IAS peut être amené à contacter un serveur de stratégie afin d'obtenir des informations sur les exigences actuelles relatives à l'état du système. Par exemple, le serveur IAS peut être obligé de contacter un serveur antivirus pour rechercher la version du dernier fichier de signature ou de contacter un serveur de mise à jour de logiciels pour obtenir la date du dernier jeu de mises à jour du système d'exploitation.

La figure III 2 résume ces interactions.

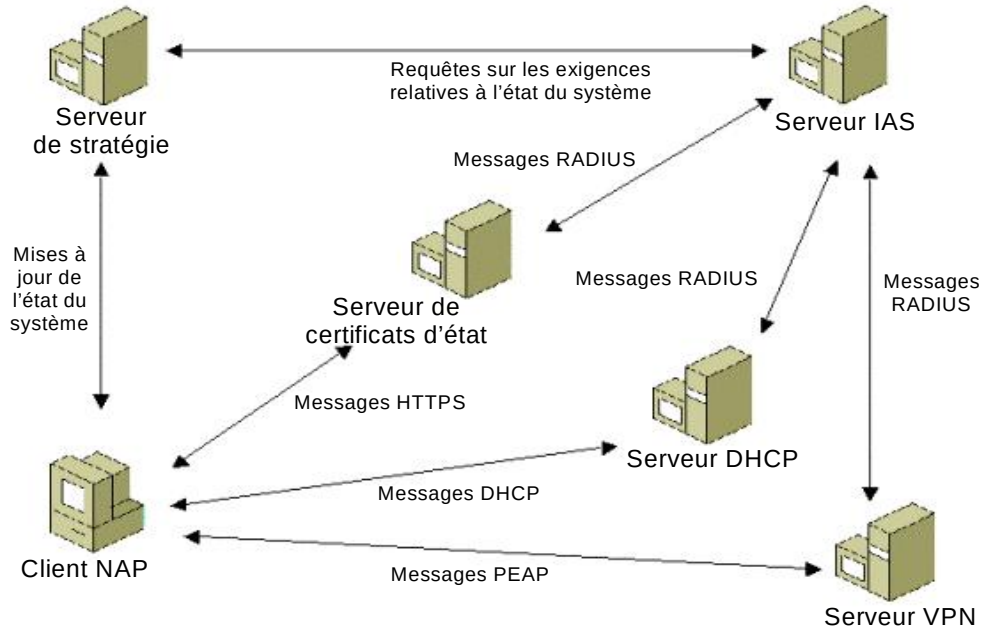


Figure III 2 - Interactions entre les composants de la plate-forme NAP.

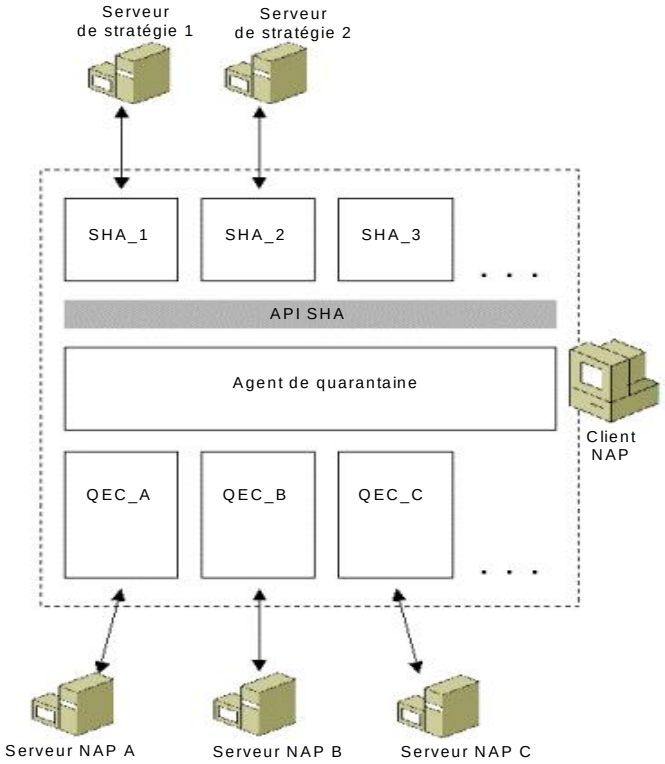
Remarque

Il existe cependant une exception à ce jeu d'interactions : lorsque le serveur IAS est installé en tant que composant réseau sur le serveur NAP (le serveur DHCP, le serveur VPN ou le serveur de certificats d'état). Dans ce cas, le serveur NAP et le serveur IAS correspondent au même ordinateur et le serveur NAP exécute les requêtes sur les exigences relatives à l'état du système. Cette configuration convient pour la configuration d'un petit réseau en combinaison avec une infrastructure réseau à un seul serveur

Un réseau d'entreprise, cependant, inclut toujours plusieurs serveurs DHCP et normalement plusieurs serveurs VPN. Dans ce cas, l'utilisation d'un serveur IAS distinct nous permet de centraliser la configuration des stratégies d'accès réseau au lieu de configurer ces stratégies sur chaque serveur NAP.

III.2.3. Architecture du client NAP

Un client NAP est un ordinateur exécutant un système d'exploitation, qui supporte la plate-forme NAP. La figure 3 illustre l'architecture de la plate-forme NAP sur un



client NAP.

Figure 3 - Architecture de la plate-forme NAP sur le client NAP.

L'architecture du client NAP inclut les éléments suivants :

- **Une couche de composants Client d'application de quarantaine (QEC, Quarantine Enforcement Client).** Chaque QEC est défini pour un type d'accès réseau différent. Par exemple, il existe un QEC pour la configuration DHCP et un QEC pour les connexions VPN. Le QEC est normalement mis en correspondance avec un type de serveur NAP spécifique. Par exemple, le QEC DHCP est conçu pour fonctionner avec un serveur NAP basé sur DHCP. Les QEC sont fournis avec la plate-forme NAP.
- **Une couche de composants Agent de l'état du système (SHA, System Health Agent).** Chaque SHA est défini pour chaque type d'exigence relative à l'état du système. Par exemple, il peut exister un SHA pour les signatures antivirus et un SHA pour les mises à jour du système d'exploitation. Un SHA spécifique peut être mis en correspondance avec un serveur de stratégie. Par exemple, un SHA pour le contrôle des signatures antivirus sera mis en correspondance avec le serveur qui contient le dernier fichier de signature antivirus. Les SHA n'ont pas forcément un serveur de stratégie correspondant. Par exemple, un SHA peut simplement contrôler les paramètres système locaux pour s'assurer qu'un pare-feu basé sur l'hôte est activé.
- **Agent de quarantaine.** Conserve une liste à jour qui décrit l'état d'état actuel du client NAP et facilite la communication entre les couches QEC et SHA. L'agent de quarantaine est fourni avec la plate-forme NAP.
- **Interface de programmation d'applications (API)** SHA. Fournit un ensemble d'appels de fonction qui permettent aux SHA de s'inscrire auprès de l'agent de quarantaine, d'indiquer l'état d'état du système, de répondre aux requêtes de l'agent de quarantaine concernant l'état d'état du système et, pour l'agent de quarantaine, de transmettre les informations de correction de l'état du système à un SHA. L'API SHA est fournie avec la plate-forme NAP.

Pour indiquer l'état d'un élément spécifique de l'état du système, par exemple, l'état du logiciel antivirus exécuté sur l'ordinateur ou la dernière mise à jour du système d'exploitation qui a été appliquée, les SHA créent une déclaration d'état (SoH, Statement of Health) et la transmettent à l'agent de quarantaine. Lorsqu'un SHA met à jour son état, il crée une nouvelle SoH et la transmet à l'agent de quarantaine.

III.2.3.1 Client d'application de quarantaine (QEC, Quarantine Enforcement Client)

Un QEC demande un certain niveau d'accès à un réseau, transmet l'état d'état de l'ordinateur à un serveur NAP qui fournit l'accès réseau et indique l'état restreint du client NAP aux autres composants de l'architecture du client NAP.

Les QEC de la plate-forme NAP sont un QEC DHCP pour la configuration des adresses IPv4 basées sur DHCP, un QEC VPN pour les connexions VPN et un QEC IPsec pour les communications basées sur IPsec.

QEC DHCP

Le QEC DHCP est une nouvelle fonctionnalité du service client DHCP qui utilise des messages DHCP standard de l'industrie pour échanger des messages sur l'état du système et des informations sur l'accès réseau restreint. Le QEC DHCP obtient la liste de SoH de l'agent de quarantaine. Le service client DHCP fragmente la liste de SoH, si besoin est, et place chaque fragment dans une option DHCP spécifique au fournisseur Microsoft qui est envoyée dans des messages DHCPDiscover, DHCPRequest ou DHCPInform. Les messages DHCPDecline et DHCPRelease ne contiennent pas la liste de SoH.

QEC VPN

Le QEC VPN est la nouvelle fonctionnalité du service Gestionnaire de connexion d'accès distant qui obtient la liste de SoH de l'agent de quarantaine et l'envoie sous la forme d'un message PEAP-TLV (Type-Length-Value).

QEC IPsec

Le QEC IPsec est un nouveau composant qui obtient le certificat d'état courant du serveur de certificats d'état et dialogue avec les éléments suivants :

- le magasin de certificats pour stocker le certificat d'état courant ;
- les composants IPsec de la pile de protocoles TCP/IP pour s'assurer que la communication basée sur IPsec utilise le certificat d'état courant pour l'authentification IPsec ;
- le pare-feu basé sur l'hôte afin que le trafic sécurisé par IPsec soit autorisé par celui-ci.

Agent de l'état du système (SHA, System Health Agent)

Un SHA exécute les mises à jour de l'état du système et publie son état sous la forme d'une SoH dans l'agent de quarantaine. La SoH contient des informations dont le serveur IAS peut se servir pour vérifier que l'ordinateur client est dans l'état d'état requis.

Un SHA est mis en correspondance avec un vérificateur de l'état du système (SHV, System Health Validator) côté serveur de l'architecture de la plate-forme NAP. Le SHV correspondant peut renvoyer une SoHResponse au client, laquelle est transmise par le QEC et l'agent de quarantaine au SHA, l'informant de ce qu'il doit faire s'il n'est pas dans l'état d'état requis. Par exemple, la SoHResponse envoyée par un SHV d'antivirus peut ordonner au SHA d'antivirus correspondant d'interroger un serveur de signatures antivirus afin d'obtenir la dernière version du fichier de signature antivirus. La SoHResponse peut également inclure le nom ou l'adresse IPv4 du serveur de signatures antivirus à interroger.

Un SHA peut utiliser un client de stratégie installé localement (non visible à la figure 3) pour aider les fonctions de gestion de l'état du système en combinaison avec un serveur de stratégie. Par exemple, un SHA de mise à jour de logiciels peut utiliser le logiciel client du logiciel installé localement (le client de stratégie) pour effectuer la vérification et l'installation de version, et mettre à jour les fonctions avec le serveur de mise à jour de logiciels (le serveur de stratégie).

Agent de quarantaine

L'agent de quarantaine fournit les services suivants :

- Collecte les SoH de chaque SHA et les met en cache. Le cache SoH est mis à jour à chaque fois qu'un SHA fournit une nouvelle SoH ou une SoH mise à jour.
- Fournit la liste de SoH aux QEC sur demande.
- Transmet des notifications aux SHA lorsque l'état restreint change.
- Maintient l'état restreint du système et collecte les informations d'état de chaque SHA.
- Transmet les SoH Response au SHA approprié.

III.2.4. Architecture du serveur NAP

La figure 4 présente l'architecture du support côté serveur pour la plate-forme NAP, constituée de composants sur un serveur NAP et un serveur IAS.

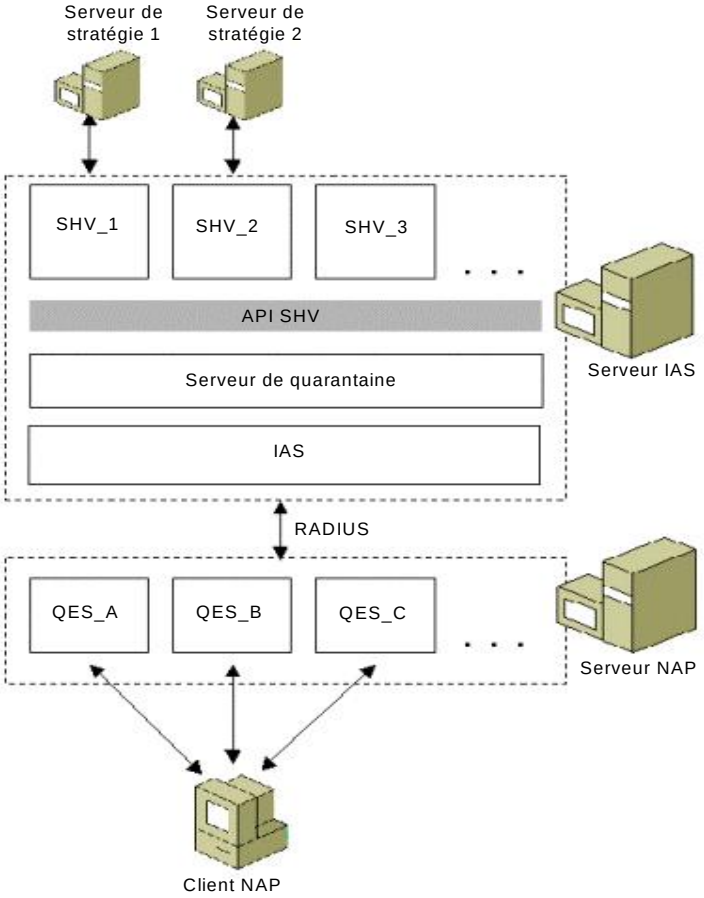


Figure 4 - Architecture de la plate-forme NAP côté serveur.

Le serveur NAP, comme l'indique la figure 4, possède une couche de composants Serveur d'application de quarantaine (QES, Quarantine Enforcement Server). Chaque QES est défini pour un type d'accès réseau différent. Par exemple, il existe un QES pour la configuration DHCP et un QES pour les connexions VPN. Le QES est normalement mis en correspondance avec un type de client compatible avec NAP. Par exemple, le QES DHCP est conçu pour fonctionner avec un serveur NAP basé sur DHCP. Les QES sont fournis avec la plate-forme NAP.

Un QES obtient la liste de SoH du QEC correspondant et les envoie à un serveur IAS sous la forme d'un message RADIUS Access-Request.

Le serveur IAS, comme l'indique la figure 4, inclut les composants suivants :

- **IAS.** Reçoit le message RADIUS Access-Request, extrait la liste de SoH et transmet ces dernières au composant Serveur de quarantaine
- **Serveur de quarantaine**. Facilite la communication entre IAS et les SHV. Le composant Serveur de quarantaine est fourni avec la plate-forme NAP.
- **Une couche de composants Vérificateur de l'état du système (SHV, System Health Validator).** Chaque SHV est défini pour chaque type d'exigence relative à l'état du système. Par exemple, il peut exister un SHV pour les signatures antivirus et un SHV pour les mises à jour du système d'exploitation. Un SHV spécifique peut être mis en correspondance avec un serveur de stratégie. Par exemple, un SHV pour le contrôle des signatures antivirus sera mis en correspondance avec le serveur qui contient le dernier fichier de signature. Les SHV n'ont pas forcément un serveur de stratégie correspondant. Par exemple, un SHV peut simplement demander aux clients compatibles avec NAP de contrôler les paramètres système locaux pour s'assurer qu'un pare-feu basé sur l'hôte est activé
- **API** SHV. Fournit un ensemble d'appels de fonction qui permettent aux SHV de s'inscrire auprès du composant Serveur de quarantaine, de recevoir des SoH du composant Serveur de quarantaine et de transmettre les informations de correction de l'état du système à un SHA correspondant sur un client NAP. L'API SHV est fournie avec la plate-forme NAP.

Comme cela a été décrit plus haut, la configuration la plus courante pour l'infrastructure de serveur NAP sera constituée de serveurs NAP fournissant un accès réseau d'un type spécifique et de serveurs IAS fournissant la validation et la correction de l'état du système. Il est possible d'installer IAS sur chaque serveur NAP, mais chaque serveur NAP doit alors être configuré séparément avec les stratégies d'accès réseau. Si IAS est installé sur un serveur NAP, tous les composants NAP côté serveur sont présents sur le serveur NAP, comme illustré par la figure 5.

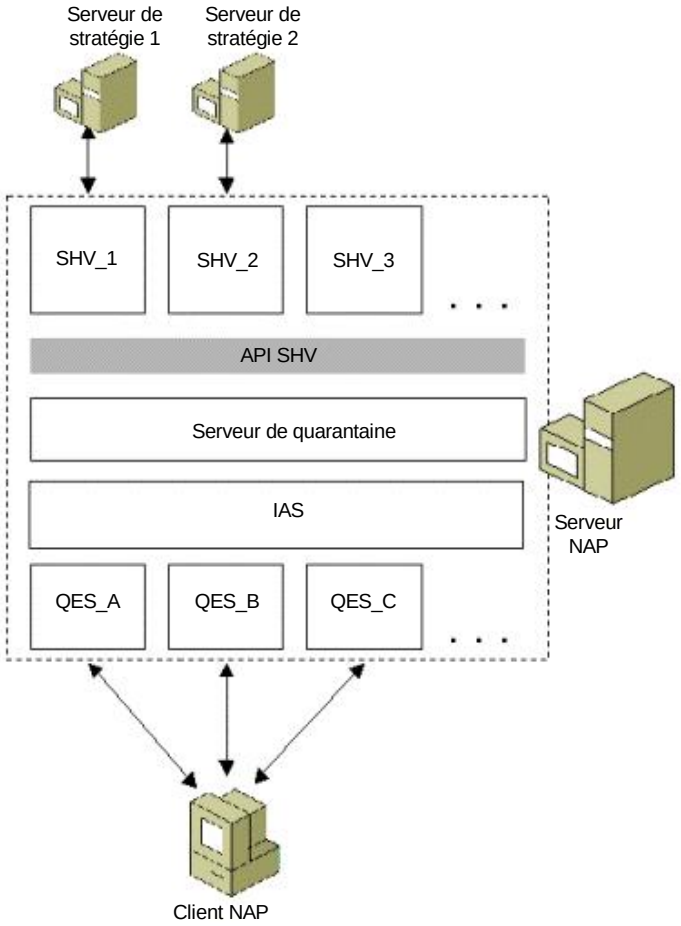


Figure 5 - Architecture NAP côté serveur lorsque IAS est installé sur le serveur NAP.

L'architecture NAP globale inclut huit composants :

- les trois composants client NAP (une couche SHA, l'agent de quarantaine et une couche QEC) ;
- les quatre composants NAP côté serveur (une couche SHV, le serveur de quarantaine, IAS et une couche QES) ;
- les serveurs de stratégie.

La figure 6 présente les relations entre les composants de la plate-forme NAP.

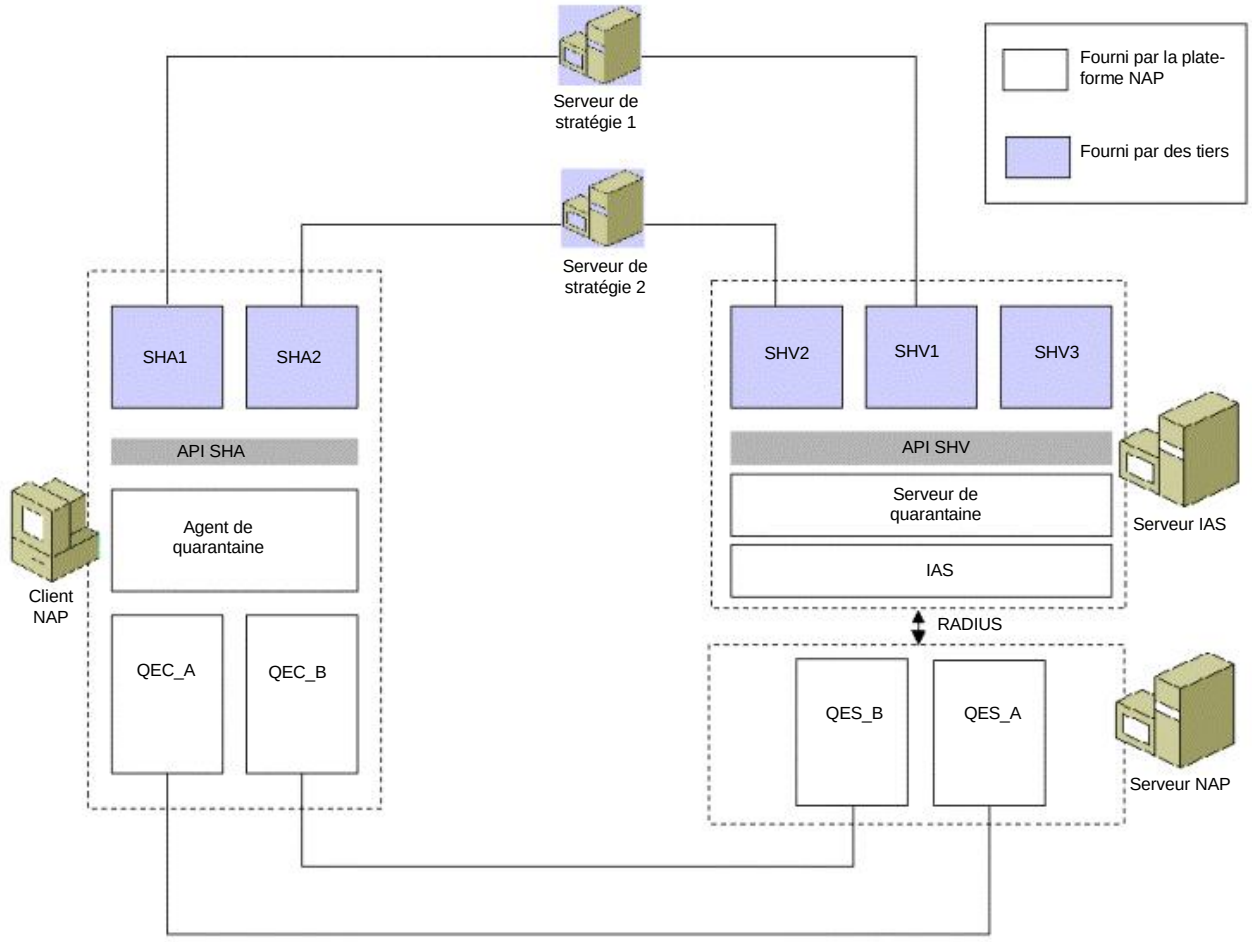


Figure 6 - Relations entre les composants de la plate-forme NAP.

On note la correspondance entre les ensembles de composants suivants :

- Les QEC et les QES sont normalement mis en correspondance.

Par exemple, le QEC DHCP sur le client NAP est mis en correspondance avec le QES DHCP sur le serveur NAP.

- Les SHA, les SHV et les serveurs de stratégie peuvent être mis en correspondance.
- Par exemple, un SHA d'antivirus sur le client est mis en correspondance avec un SHV d'antivirus sur le serveur de quarantaine et avec un serveur de stratégie de signature antivirus.
- Le serveur NAP peut inclure des SHV auxquels ne correspond aucun SHA ou serveur de stratégie, par exemple, un SHV qui contrôle les paramètres de Registre du client ou un SHV qui effectue un contrôle avec un serveur de système de

détection des intrusions (IDS, Intrusion Detection System) avant de prendre la décision de mise en quarantaine.

Remarque

Pour étendre la plate-forme NAP et créer une nouvelle méthode permettant d'évaluer l'état d'un client qui se connecte, des fournisseurs de logiciels tiers doivent créer un SHA pour le client NAP, un SHV pour le serveur IAS ou les serveurs NAP qui fournissent ou autorisent l'accès réseau et, si nécessaire, un serveur de stratégie. Si le serveur de stratégie existe déjà, dans le cas, par exemple, d'un serveur de distribution des signatures antivirus, alors seuls les composants SHA et SHV correspondants doivent être créés.

III.2.4.1 Composants de la plate-forme NAP côté serveur

Les sections suivantes décrivent les composants de la plate-forme NAP côté serveur plus en détail.

Serveur d'application de quarantaine (QES, Quarantine Enforcement Server)

Un QES autorise un certain niveau d'accès réseau, peut transmettre l'état d'état d'un client NAP à IAS pour évaluation et, en fonction de la réponse de IAS pour l'accès réseau, peut fournir l'implémentation de l'accès réseau restreint.

Les QES pris en considération dans la version initiale de la plate-forme NAP sont un QES DHCP pour la configuration des adresses IP basées sur DHCP et un QES VPN pour les connexions VPN.

- Le QES DHCP est une nouvelle fonctionnalité du service serveur DHCP qui utilise des messages DHCP standard de l'industrie pour communiquer avec les QEC DHCP sur les clients NAP. L'implémentation DHCP pour l'accès réseau restreint est réalisée par le biais d'options DHCP.
- Le QES VPN est une nouvelle fonctionnalité du service de routage et d'accès à distance (RRAS, Routing and Remote Access) qui utilise l'encapsulation EAP (Extensible Authentication Protocol) RADIUS (l'encapsulation des messages EAP à l'intérieur des messages RADIUS) pour transmettre des messages sur l'état du système avec PEAP-TLV entre les clients NAP et le serveur IAS. L'implémentation VPN est réalisée par le biais du filtrage des paquets IP.

Pour la communication basée sur IPsec, le serveur de certificats d'état transmet les informations sur l'état d'état du client NAP au serveur IAS.

- **Serveur de quarantaine**

  Le composant Serveur de quarantaine fournit les services suivants :

  - Collecte la liste de SoH à partir du QES (via IAS).
  - Distribue les SoH de la liste de SoH au SHV approprié.
  - Collecte les SoHResponse des SHV et les transmet à IAS pour évaluation.

- **IAS**

  RADIUS est un protocole très répandu qui permet de centraliser l'authentification, les autorisations et la comptabilité pour l'accès réseau. Développé à l'origine pour l'accès à distance, RADIUS est aujourd'hui pris en charge par les points d'accès sans fil, les commutateurs d'authentification Ethernet, les serveurs VPN, les serveurs d'accès DSL (Digital Subscriber Line) et d'autres serveurs d'accès réseau. IAS est l'implémentation d'un serveur et d'un proxy RADIUS. Pour la plate-forme NAP, IAS a été mis à jour de façon à inclure le composant Serveur de quarantaine, un support pour l'API SHV et les SHV installables, ainsi que des options de configuration pour configurer l'accès réseau et des stratégies de communication sécurisées.

- **Valideur de l'état du système (SHV, System Health Validator)**

  Un SHV reçoit une SoH du serveur de quarantaine et vérifie que les informations de contrôle de l'état du système dans la SoH sont conformes à l'état d'état du système requis. Par exemple, si la SoH provient d'un SHA d'antivirus et contient le numéro de version du dernier fichier de signature de virus, le SHV d'antivirus correspondant peut contrôler le numéro de la dernière version avec le serveur de distribution des signatures pour valider la SoH du client NAP.

  Le SHV renvoie une SoHResponse, qui est transmise au SHA sur le client NAP, indiquant comment le SHA peut devenir conforme à la stratégie réseau. Par exemple, la SoHResponse envoyée par le SHV d'antivirus peut ordonner au SHA d'antivirus d'interroger un serveur pour obtenir la dernière version du fichier de signature antivirus. La SoHResponse peut également inclure le nom ou l'adresse IPv4 du serveur à interroger.

III.2.4.2 Communication entre les composants client et serveur NAP

Le composant Agent de quarantaine peut communiquer avec le composant Serveur de quarantaine en transmettant la liste de SoH actuelle au QEC. Le QEC transmet

la liste de SoH au QES, qui la transmet alors au serveur de quarantaine. Le serveur de quarantaine peut communiquer avec l'agent de quarantaine en transmettant une liste de SoHResponse au QES, qui la transmet au QEC, lequel la transmet à l'agent de quarantaine.

Un SHA peut communiquer avec le SHV correspondant en transmettant une SoH à l'agent de quarantaine, qui la transmet au QEC, qui la transmet au QES, qui la transmet au serveur de quarantaine, lequel la transmet au SHV. Un SHV peut communiquer avec le SHA correspondant en transmettant une SoHResponse au serveur de quarantaine, qui la transmet au QES, qui la transmet au QEC, qui la transmet à l'agent de quarantaine, lequel la transmet au SHA.

La figure 7 illustre le processus de communication entre les composants client NAP et les composants serveur NAP correspondants.

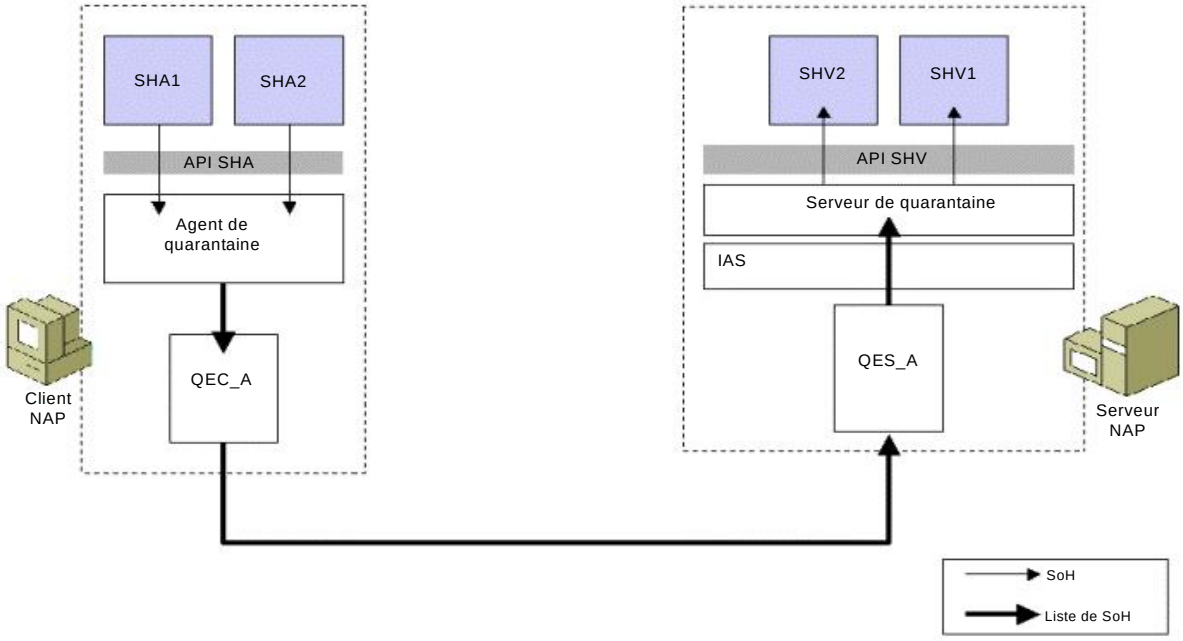


Figure 7 - Processus de communication entre les composants client NAP et les composants serveur NAP correspondants.

La figure 8 illustre le processus de communication entre les composants serveur NAP et les composants client NAP correspondants.

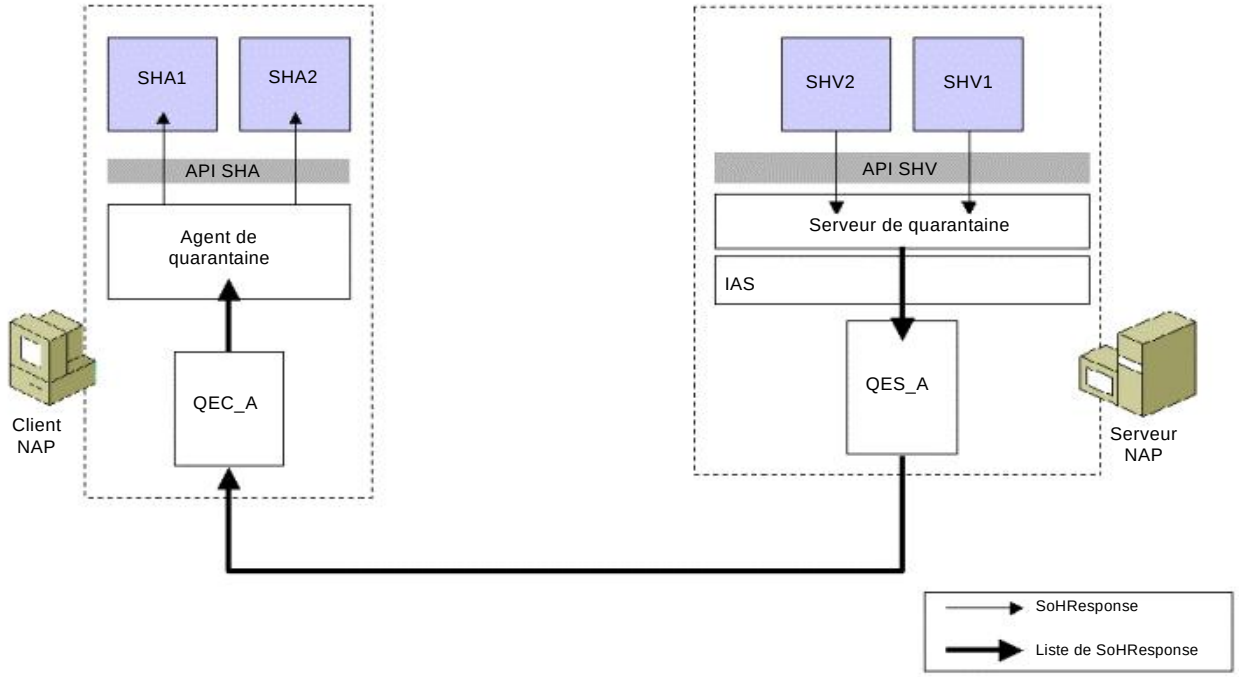


Figure 8 - Processus de communication entre les composants serveur NAP et les composants client NAP correspondants.

III.3. Fonctionnement de NAP

Cette section explique comment les composants de la plate-forme NAP assurent la génération de rapports d'état sur l'état du système, la vérification de la conformité à la stratégie réseau, la restriction de l'accès réseau, ainsi que la correction pour la communication authentifiée avec IPsec et l'accès réseau basé sur DHCP et VPN.

Remarque Dans cette section on présuppose que IAS est installé sur un serveur à part, plutôt que sur le serveur avec lequel le client NAP communique pour obtenir soit l'accès réseau soit un certificat d'état.

III.3.1 Accès basé sur DHCP

L'accès basé sur DHCP restreint l'accès réseau pour le client DHCP par le biais de sa table de routage IP.

Par exemple, la quarantaine DHCP fixe la valeur de l'option de routeur DHCP à 0.0.0.0 : aucune passerelle par défaut n'est configurée sur l'ordinateur restreint. Elle fixe également la valeur du masque de sous-réseau pour l'adresse IP allouée à 255.255.255.255 : il n'existe aucun itinéraire vers le sous-réseau connecté.

Pour autoriser l'ordinateur restreint à accéder aux ressources de correction sur le réseau restreint, le serveur DHCP affecte l'option DHCP Itinéraires statiques sans classe, qui contient un ensemble d'itinéraires hôtes vers des ordinateurs spécifiques tels que les serveurs DHCP, DNS et les serveurs de mise à jour de logiciels.

Le résultat final de la mise en quarantaine DHCP est une table de configuration et de routage qui autorise la connectivité uniquement vers des adresses de destination spécifiques. Par conséquent, lorsqu'une application essaie d'effectuer un envoi vers une adresse IP multidiffusion autre que celles fournies via l'option Itinéraires statiques sans classe, le protocole TCP/IP renvoie une erreur de routage.

Remarque Dans la mesure où la quarantaine DHCP est basée sur des entrées dans la table de routage IP, elle ne peut pas empêcher un utilisateur malveillant qui est un administrateur local de modifier manuellement la table de routage IP et d'obtenir un accès réseau complet.

Le processus suivant a lieu lorsqu'un client DHCP compatible avec NAP essaie d'obtenir d'un serveur DHCP compatible avec NAP une configuration d'adresse IPv4 :

1. Le QEC DHCP sur le client NAP (un composant du service client DHCP) demande au composant Agent de quarantaine la dernière liste de SoH.
2. L'agent de quarantaine, qui a mis en cache les dernières SoH de l'ensemble des SHA installés, répond au QEC DHCP avec la liste de SoH actuelle.
3. Le service client DHCP construit et envoie un message DHCPDiscover. Le message DHCPDiscover contient la liste de SoH dans une ou plusieurs options DHCP spécifiques au fournisseur Microsoft.

4. Le service serveur DHCP sur le serveur DHCP compatible avec NAP reçoit le message DHCPDiscover. Le QES DHCP sur le serveur DHCP (un composant du service serveur DHCP) extrait la liste de SoH du message DHCPDiscover et l'envoie au serveur IAS sous forme d'attributs spécifiques au fournisseur RADIUS dans un message RADIUS Access-Request.
5. Le serveur IAS reçoit le message RADIUS Access-Request, extrait la liste de SoH des attributs spécifiques au fournisseur RADIUS et la transmet au composant Serveur de quarantaine.
6. Le serveur de quarantaine reçoit la liste de SoH et transfère ces dernières au SHV approprié.
7. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au serveur de quarantaine.
8. Le serveur de quarantaine transmet la liste de SoHResponse à IAS.
9. IAS compare la liste de SoHResponse avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.
10. IAS construit et envoie un message RADIUS Access-Accept contenant la décision de quarantaine et la liste de SoHResponse sous forme d'attributs spécifiques au fournisseur RADIUS.
11. Le serveur DHCP reçoit le message RADIUS Access-Accept, extrait la liste de SoHResponse et reformate ces dernières comme des options spécifiques au fournisseur DHCP.
12. Le serveur DHCP envoie un message DHCPOffer contenant une configuration d'adresse IPv4.
13. Le client DHCP envoie un message DHCPRequest demandant la configuration d'adresse IPv4 proposée.
14. Le serveur DHCP envoie un message DHCPAck contenant la configuration d'adresse IPv4 proposée, la décision de quarantaine et la liste de SoHResponse dans une ou de plusieurs options DHCP spécifiques au fournisseur Microsoft.

Si le client NAP n'est pas restreint, le message DHCPAck contient l'option de routeur DHCP définie avec la valeur de la passerelle par défaut appropriée et un masque de sous-réseau pour le sous-réseau auquel le client NAP est connecté, mais il ne contient pas l'option Itinéraires statiques sans classe. À ce stade, le client NAP dispose d'un accès réseau complet.

- **Le client NAP basé sur DHCP est restreint**

Si le client NAP est restreint, le message DHCPAck contient l'option de routeur DHCP paramétrée à 0.0.0.0, l'option Masque de sous-réseau paramétrée à 255.255.255.255, et l'option Itinéraires statiques sans classe contient l'ensemble des itinéraires hôtes statiques vers les ressources sur le réseau restreint.

Le processus suivant effectue les corrections requises pour un accès réseau complet :

1. Le QEC DHCP transmet les SoHResponse à l'agent de quarantaine.
2. L'agent de quarantaine transmet les SoHResponse au SHA approprié.
3. Chaque SHA analyse sa SoHResponse et, en fonction du contenu, effectue les corrections requises pour corriger l'état d'état du système du client NAP.
4. Une fois que le SHA a exécuté la fonction corrective, il transmet une SoH mise à jour à l'agent de quarantaine.
5. L'agent de quarantaine collecte les SoH mises à jour à partir de tous les SHA qui nécessitaient une correction, crée une nouvelle liste de SoH et la transmet au QEC DHCP.
6. Le QEC DHCP envoie au serveur DHCP un message DHCPRequest contenant la nouvelle liste de SoH pour renouveler sa configuration d'adresse IPv4 actuelle.
7. Le service serveur DHCP sur le serveur DHCP compatible avec NAP reçoit le message DHCPRequest. Le composant QES DHCP du service serveur DHCP extrait la liste de SoH du message DHCPRequest et l'envoie au serveur IAS sous forme d'attributs spécifiques au fournisseur RADIUS d'un message RADIUS Access-Request.

8. Le serveur IAS reçoit le message RADIUS Access-Request, extrait la liste de SoH des attributs spécifiques au fournisseur RADIUS et la transmet au composant Serveur de quarantaine.
9. Le serveur de quarantaine reçoit la liste de SoH et, à supposer qu'il n'ait pas encore mis en cache les SoHResponse, transmet les SoH de la liste au SHV approprié.
10. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au serveur de quarantaine.
11. Le serveur de quarantaine transmet la liste de SoHResponse à IAS.
12. IAS compare la liste de SoHResponses avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.
13. IAS construit et envoie un message RADIUS Access-Accept contenant la décision de quarantaine et la liste de SoHResponse sous forme d'attributs spécifiques au fournisseur RADIUS.
14. Le serveur DHCP reçoit le message RADIUS Access-Accept, extrait la liste de SoHResponses et reformate ces dernières sous forme d'options spécifiques au fournisseur DHCP.
15. Le serveur DHCP envoie un message DHCPAck qui contient l'option de routeur DHCP définie avec la valeur de la passerelle par défaut appropriée et un masque de sous-réseau pour le sous-réseau auquel le client NAP est connecté, mais qui ne contient pas l'option Itinéraires statiques sans classe. Le client DHCP possède à présent une configuration d'adresse IPv4 renouvelée pour un accès réseau complet.

III.3.2 Accès basé sur VPN

La Quarantaine VPN utilise un ensemble de filtres de paquets IP d'accès à distance pour restreindre le trafic du client VPN de telle sorte qu'il puisse atteindre uniquement les ressources de correction. Le serveur VPN applique les filtres de paquets IP au trafic IP reçu du client VPN et élimine en silence tous les paquets qui ne correspondent pas à un filtre de paquets configuré.

Le processus suivant a lieu lorsqu'un client VPN compatible avec NAP se connecte à un serveur VPN compatible avec NAP :

1. Le client VPN établit une connexion au serveur VPN en utilisant soit le protocole PPTP (Point-to-Point Tunneling Protocol), soit le L2TP/IPsec (Layer Two Tunneling Protocol avec Internet Protocol Security).
2. Le QES VPN sur le serveur VPN (un composant du service de routage et d'accès à distance (RRAS, Routing and Remote Access) envoie un message EAP-Request/Identity au QEC VPN sur le client VPN.
3. Le QEC VPN sur le client VPN (un composant du service Gestionnaire de connexion d'accès distant) répond avec un message EAP-Response/Identity contenant le nom d'utilisateur du client VPN.
4. Le QES VPN sur le serveur VPN envoie le message EAP-Response/Identity au serveur IAS sous la forme d'un message RADIUS Access-Request. Pour tous les autres messages basés sur PEAP, la communication logique a lieu entre le serveur IAS et le QEC VPN sur le client VPN, le serveur VPN faisant office de périphérique de relais. Les messages entre le serveur VPN et le serveur IAS sont une suite de messages RADIUS Access-Request, Access-Challenge et Access-Accept.
5. Le serveur IAS envoie un message EAP-Request/Start PEAP au client VPN.
6. Le client VPN et le serveur IAS échangent une série de messages TLS afin de négocier la suite de cryptage pour le canal TLS et le serveur IAS envoie une chaîne de certificat au client VPN pour authentification.
7. Le serveur IAS envoie une demande au client VPN pour obtenir la liste de SoH en utilisant un message PEAP-TLV.
8. Le QEC VPN demande la liste de SoH actuelle à l'agent de quarantaine.

9. Le QEC VPN transmet la liste de SoH actuelle au serveur IAS en utilisant un message PEAP-TLV.
10. Le serveur IAS demande que le client VPN s'authentifie lui-même en utilisant ses informations d'authentification client, avec une méthode d'authentification PEAP telle que le protocole MS-CHAP v2 (PEAP-Microsoft Challenge Handshake Authentication Protocol version 2).
11. Le client VPN s'authentifie sur le serveur IAS en utilisant la méthode d'authentification PEAP négociée.
12. Le composant IAS sur le serveur IAS extrait la liste de SoH du message PEAP-TLV envoyé à l'étape 9 et la transmet au composant Serveur de quarantaine.
13. Le composant Serveur de quarantaine transmet les SoH de la liste de SoH aux SHV appropriés.
14. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au serveur de quarantaine.
15. Le serveur de quarantaine transmet la liste de SoHResponse à IAS.
16. IAS compare la liste de SoHResponses avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.
17. IAS construit et envoie au client VPN un message PEAP-TLV contenant la décision de quarantaine et la liste de SoHResponse.
18. IAS envoie au serveur VPN un message RADIUS Access-Accept contenant sa décision de quarantaine.
    - Si la connexion VPN doit être restreinte, le message RADIUS Access-Accept contient également un ensemble de filtres de paquets IP qui limitent le trafic du client VPN au réseau restreint.
    - Si la connexion VPN ne doit pas être restreinte, le message RADIUS Access-Accept ne contient pas de filtres de paquets IP pour limiter l'accès réseau. Lorsque l'établissement de la connexion VPN est terminé, le client NAP dispose d'un accès réseau complet.

19. Le client VPN et le serveur VPN terminent l'établissement de la connexion VPN.

▪ **Le client NAP basé sur VPN est restreint**

Si le client VPN est restreint, les filtres de paquets restreints sont appliqués à la connexion VPN et le client VPN ne peut atteindre que les ressources de correction. Le processus suivant effectue les corrections requises pour un accès réseau complet :

1. Le QEC VPN extrait la liste de SoHResponse dans le message PEAP-TLV reçu du serveur IAS et la transmet à l'agent de quarantaine.
2. L'agent de quarantaine transmet les SoHResponse au SHA approprié.
3. Chaque SHA analyse sa SoHResponse et, en fonction du contenu, effectue les corrections requises pour corriger l'état d'état du système du client NAP.
4. Une fois que le SHA a exécuté la fonction corrective, il transmet une SoH mise à jour à l'agent de quarantaine.
5. L'agent de quarantaine collecte les SoH mises à jour à partir de tous les SHA qui nécessitaient une correction, crée une nouvelle liste de SoH et la transmet au QEC VPN.
6. Le QEC VPN transmet la liste de SoH actuelle au serveur IAS en utilisant un message PEAP-TLV.
7. Le composant IAS sur le serveur IAS extrait la liste de SoH du message PEAP-TLV et la transmet au composant Serveur de quarantaine.
8. Le composant Serveur de quarantaine transmet les SoH incluses dans la liste de SoH aux SHV appropriés.
9. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au serveur de quarantaine.
10. Le serveur de quarantaine transmet la liste de SoHResponse à IAS.
11. IAS compare la liste de SoHResponses avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.

12. IAS construit et envoie au client VPN, via le serveur VPN, un message PEAP-TLV contenant la décision Pas de quarantaine et la liste de SoHResponses.
13. IAS construit et envoie au serveur VPN un message RADIUS Access-Accept contenant la décision Pas de quarantaine ; il n'inclut aucun filtre de paquets IP pour restreindre l'accès réseau.
14. À la réception du message RADIUS Access-Accept, le serveur VPN supprime les filtres de paquets IP de la connexion VPN et le client VPN dispose d'un accès réseau complet.

III.3.3 Communication basée sur IPsec

La Quarantaine IPsec restreint la communication pour les clients NAP basés sur IPsec en ignorant les tentatives de communication entrante envoyées depuis des ordinateurs qui ne possèdent pas de certificats d'état valides. À la différence de la Quarantaine DHCP et VPN, la Quarantaine IPsec est appliquée individuellement par chaque ordinateur, et non au point d'entrée du réseau. Étant donné qu'on peut bénéficier des paramètres de stratégie IPsec, l'implémentation de certificats d'état valides peut être réalisée pour tous les ordinateurs d'un domaine, certains ordinateurs d'un sous-réseau, un ordinateur spécifique, un ensemble spécifique de ports TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol), ou pour un ensemble spécifique de ports TCP ou UDP sur un ordinateur particulier.

La Quarantaine IPsec divise un réseau physique en trois zones logiques. Un ordinateur est membre d'une seule zone à la fois. Les zones sont définies en fonction des ordinateurs qui possèdent des certificats d'état courants et de ceux qui exigent une authentification IPsec avec des certificats d'état valides pour les tentatives de communication entrante. Les zones autorisent la quarantaine et les correctifs, et fournissent aux ordinateurs sécurisés un niveau de protection contre les ordinateurs défectueux.

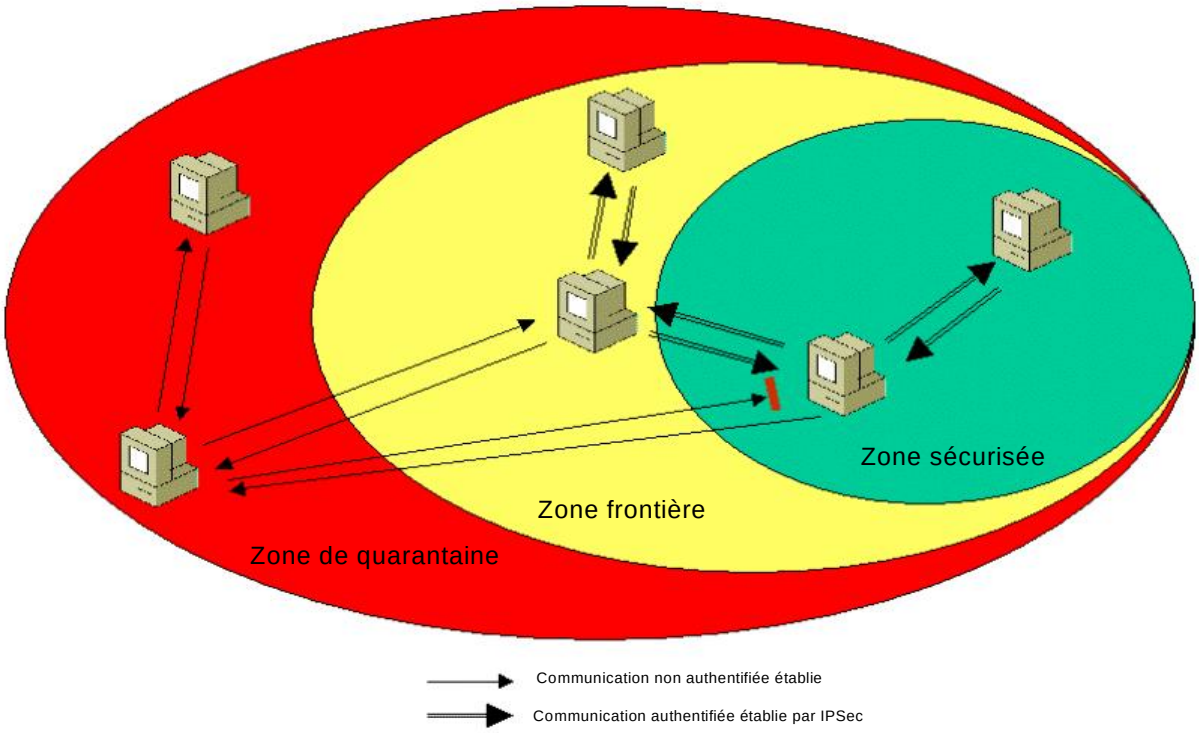


Figure 9 - Zones avec Quarantaine IPsec.

La Quarantaine IPsec définit les zones suivantes :

- **Zone sécurisée** Ensemble d'ordinateurs qui possèdent des certificats d'état et exigent que les tentatives de communication entrante utilisent IPsec et des certificats d'état pour l'authentification IPsec. Sur un réseau géré, la plupart des ordinateurs serveurs et clients membres du domaine Active Directory seraient dans la zone sécurisée.
- **Zone frontière** Ensemble d'ordinateurs qui possèdent des certificats d'état, mais qui n'exigent que les tentatives de communication entrante utilisent IPsec et des certificats d'état pour l'authentification IPsec. Les ordinateurs de la zone frontière doivent être accessibles aux ordinateurs sur l'ensemble du réseau.
- **Zone de quarantaine** Ensemble d'ordinateurs qui ne possèdent pas de certificats d'état. Il s'agit d'ordinateurs qui n'ont pas effectué de contrôles d'état, qui sont invités sur le réseau ou qui ne sont pas compatibles avec NAP (ordinateurs exécutant des versions de Windows qui ne prennent pas en charge NAP, ordinateurs Apple Macintosh ou Unix, etc.).

  En fonction de la définition des trois zones, les types de communications établies suivants sont possibles :

- Les ordinateurs de la zone sécurisée peuvent établir des communications avec les ordinateurs situés dans les trois zones. Les communications établies avec des ordinateurs de la zone sécurisée ou de la zone frontière sont authentifiées avec IPsec et des certificats d'état. Les communications établies avec des ordinateurs de la zone de quarantaine ne sont pas authentifiées avec IPsec.

  Les ordinateurs de la zone sécurisée accepteront les communications établies à partir d'ordinateurs des zones sécurisées et frontière qui sont authentifiés avec IPsec, mais n'accepteront pas les communications établies à partir d'ordinateurs de la zone de quarantaine.

  Par exemple, un ordinateur client de la zone sécurisée peut demander une page Web située sur un serveur Web dans la zone de quarantaine. Toutefois, un ordinateur client dans la zone de quarantaine n'a pas cette possibilité. Les exigences pour la communication établie peuvent être configurées sur la base d'un port TCP ou UDP pour restreindre des types de trafic spécifiques. Il est possible, par exemple, d'exiger une authentification IPsec avec des certificats d'état pour le trafic des appels de procédure distante (RPC, Remote Procedure Call), mais pas pour le trafic Web. Dans ce cas, un ordinateur client dans la zone de quarantaine pourrait demander une page Web située sur un serveur Web dans la zone sécurisée, mais être dans l'incapacité d'utiliser RPC pour se connecter à ce même serveur.

- Les ordinateurs de la zone frontière peuvent établir des communications avec les ordinateurs de la zone sécurisée ou frontière qui sont authentifiés avec IPsec et des certificats d'état ou avec les ordinateurs de la zone de quarantaine qui ne sont pas authentifiés avec IPsec.
- Les ordinateurs de la zone frontière accepteront les communications établies à partir d'ordinateurs de la zone sécurisée ou frontière qui sont authentifiés avec IPsec et des certificats d'état, et à partir d'ordinateurs de la zone de quarantaine qui ne sont pas authentifiés avec IPsec.

  Les membres de la zone frontière incluront uniquement le serveur de certificats d'état et les serveurs de stratégie NAP. Les serveurs de la zone frontière doivent être accessibles à partir des clients NAP défectueux de la zone de quarantaine

(pour exécuter les fonctions correctives initiales et obtenir des certificats d'état) et à partir des ordinateurs sains de la zone sécurisée (pour exécuter les fonctions correctives permanentes, renouveler les certificats d'état et gérer les ordinateurs de la zone frontière).

Un ordinateur est membre de la zone sécurisée ou frontière pendant le délai spécifié dans la période de validité du certificat d'état. Avant l'expiration du certificat d'état, le client NAP basé sur IPsec contacte le serveur de certificats d'état pour obtenir un nouveau certificat. La période de validité peut être configurée sur le serveur de certificats d'état.

- Les ordinateurs de la zone de quarantaine peuvent établir des communications avec les ordinateurs des zones de quarantaine et frontière. Les ordinateurs de la zone de quarantaine ne peuvent pas établir de communications avec les ordinateurs de la zone sécurisée (sauf s'ils y sont spécifiquement autorisés par le biais des paramètres de stratégie IPsec des ordinateurs de la zone sécurisée).

Les ordinateurs de la zone de quarantaine accepteront les communications établies à partir d'ordinateurs situés dans les trois zones.
Pour obtenir un certificat d'état courant et devenir membre de la zone sécurisée, un client NAP utilisant la Quarantaine IPsec démarre sur le réseau et procède comme indiqué ci-après :

1. Lorsque l'ordinateur démarre, le pare-feu basé sur l'hôte est activé mais n'accepte aucune exception, de sorte qu'aucun autre ordinateur ne peut établir de communication avec lui. À ce stade, l'ordinateur est dans la zone de quarantaine parce qu'il n'a pas de certificat d'état courant. L'ordinateur peut communiquer avec les autres ordinateurs des zones de quarantaine et frontière, et il peut accéder à Internet. Il ne peut cependant pas établir de communication avec les ordinateurs dans la zone sécurisée.
2. Le client NAP obtient l'accès réseau et une configuration d'adresse IP.
3. Le QEC IPsec sur le client NAP crée un canal de communication HTTPS sécurisé avec le serveur de certificats d'état.
4. Le QEC IPsec envoie ses données d'identification et sa liste de SoH actuelle au serveur de certificats d'état sur le canal HTTPS.

5. Le serveur de certificats d'état transmet la liste de SoH au serveur IAS dans un message RADIUS Access-Request.
6. Le serveur IAS reçoit le message RADIUS Access-Request, extrait la liste de SoH des attributs spécifiques au fournisseur RADIUS et la transmet au composant Serveur de quarantaine.
7. Le serveur de quarantaine reçoit la liste de SoH et transfère ces dernières au SHV approprié.
8. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au composant Serveur de quarantaine.
9. Le serveur de quarantaine transmet la liste de SoHResponse à IAS.
10. IAS compare la liste de SoHResponses avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.
11. IAS construit et envoie un message RADIUS Access-Accept contenant la décision de quarantaine et la liste de SoHResponse sous forme d'attributs spécifiques au fournisseur RADIUS.
12. Le serveur de certificats d'état renvoie la liste de SoHResponse au QEC IPsec. Si le client NAP est sain, le serveur de certificats d'état émet également un certificat d'état.

Si un certificat d'état est émis pour le client NAP, ce dernier l'ajoute au magasin de certificats de l'ordinateur de l'ordinateur. Le QEC IPsec configure les paramètres IPsec de façon à effectuer l'authentification avec le certificat d'état pour les communications basées sur IPsec et configure le pare-feu basé sur l'hôte de façon à autoriser les communications entrantes depuis n'importe quel homologue utilisant un certificat d'état valide pour l'authentification IPsec. Le client NAP est à présent membre de la zone sécurisée.

Le QEC IPsec exécute les étapes 3-12 lorsque de nouvelles informations SoH parviennent à l'agent de quarantaine ou lorsque le certificat d'état actuel est sur le point d'expirer.

Le client NAP basé sur IPsec est restreint

Si le client NAP basé sur IPsec est restreint (dans la zone de quarantaine), le client NAP n'a pas de certificat d'état valide et ne peut établir aucune communication avec les ordinateurs situés dans la zone sécurisée.

Le client NAP exécute le processus correctif suivant pour devenir membre de la zone sécurité :

1. Le QEC IPsec transmet la liste de SoHResponse à l'agent de quarantaine.
2. L'agent de quarantaine transmet les SoHResponse au SHA approprié.
3. Chaque SHA analyse sa SoHResponse et, en fonction du contenu, effectue les correctifs requis pour corriger l'état d'état du système du client NAP.
4. Une fois que le SHA a exécuté la fonction corrective, il transmet une SoH mise à jour à l'agent de quarantaine.
5. L'agent de quarantaine collecte les SoH mises à jour à partir de tous les SHA qui nécessitaient des correctifs, crée une nouvelle liste de SoH et la transmet au QEC IPsec.
6. Le QEC IPsec établit une nouvelle session HTTPS sécurisée avec le serveur de certificats d'état et envoie la nouvelle liste de SoH.
7. Le serveur de certificats d'état reçoit la liste de SoH et envoie ces dernières au serveur IAS sous forme d'attributs spécifiques au fournisseur RADIUS dans un message RADIUS Access-Request.
8. Le serveur IAS reçoit le message RADIUS Access-Request, extrait la liste de SoH des attributs spécifiques au fournisseur RADIUS et la transmet au composant Serveur de quarantaine.
9. Le serveur de quarantaine reçoit la liste de SoH et, à supposer qu'il n'ait pas encore mis en cache les SoHResponse, transmet les SoH de la liste au SHV approprié.
10. Les SHV analysent le contenu des SoH transmises par le serveur de quarantaine, puis construisent et envoient des SoHResponse au serveur de quarantaine.
11. Le serveur de quarantaine transmet la liste des SoHResponse à IAS.
12. IAS compare la liste de SoHResponses avec un ensemble de stratégies d'accès réseau configuré, puis prend une décision Quarantaine/Pas de quarantaine.
13. IAS construit et envoie un message RADIUS Access-Accept contenant la décision de quarantaine et la liste de SoHResponse sous forme d'attributs spécifiques au fournisseur RADIUS.

14. Le serveur de certificats d'état reçoit le message RADIUS Access-Accept, extrait la liste de SoHResponse et envoie ces dernières au client NAP sur la session HTTPS. Ensuite, dans la mesure où le client NAP est à présent sain, le serveur de certificats d'état émet un certificat d'état courant pour le client NAP.

III.4. Conclusion

L'architecture de la plate-forme NAP est constituée de composants client (une couche SHA, un agent de quarantaine et une couche QEC), de composants côté serveur (une couche SHV, un serveur de quarantaine, IAS et une couche QES) et de serveurs de stratégie. Les QEC et les QES sont normalement mis en correspondance. Ils fournissent l'accès réseau et appliquent les restrictions d'accès réseau et de communication pour les clients réseau défectueux. Les SHA, les SHV et les serveurs de stratégie sont mis en correspondance pour signaler l'état, effectuer la validation et corriger une condition d'état du système spécifique. Le composant Agent de quarantaine coordonne le flux d'informations entre les SHA et les QEC. Le composant Serveur de quarantaine coordonne le flux d'informations entre les SHV et les QES. IAS offre un moyen de configurer et centraliser les exigences de la stratégie d'accès réseau.

L'accès réseau DHCP utilise des messages DHCP pour transporter les SoH et les SoHResponse entre les clients DHCP compatibles avec NAP et les serveurs. La quarantaine DHCP est effectuée par le biais d'options DHCP qui configurent la table de routage IP du client DHCP et limitent l'accès aux ressources réseau.

L'accès réseau VPN utilise des messages PEAP-TLV pour transporter les SoH et les SoHResponse entre les clients VPN compatibles avec NAP et le serveur sur lequel IAS est installé. La quarantaine VPN est effectuée par le biais de filtres de paquets IP qui sont appliqués à la connexion VPN et limitent l'accès aux ressources réseau

La communication basée sur IPsec utilise un canal HTTPS sécurisé pour transporter les SoH et les SoHResponse entre un client NAP basé sur IPsec et le serveur de certificats d'état. La Quarantaine IPsec consiste à ne pas émettre de certificats d'état pour les clients NAP défectueux afin qu'ils ne puissent établir aucune communication avec les clients NAP basés sur IPsec dans la zone sécurisée.

Chapitre 4

La mise en oeuvre de NAP avec serveur DHCP

IV.1 Introduction

Actuellement, il devient de plus en plus difficile de garantir que tous les ordinateurs de l'entreprise sont intègres, ce qui les rend à terme plus vulnérables puisqu'ils n'effectuent pas forcément le contrôle d'intégrité qu'on veut exiger.

La solution proposée est la mise en quarantaine réseau nommée NAP (Network Access Protection).

En déployant Protection d'accès réseau NAP sur notre réseau, nous garantirons que les ordinateurs accédant à des ressources importantes répondent à certaines mesures de référence en matière d'intégrité client. Ces références incluent (sans être limite) l'application des mises à jour, l'actualisation logiciels antivirus et anti espion, ainsi que la mise en œuvre de technologies de sécurité majeures comme pare-feu Windows

Cette partie va être consacrée à la mise en place de NAP avec la méthode d'enfoncement DHCP. Cela permettra d'illustrer la manière de fonctionnement de cette méthode.

IV.2. Infrastructure

IV.2.1 Objectifs

Dans cette partie nous allons voir comment installer et configurer les différentes entités qui constituent le NAP pour contrôler l'intégrité des ordinateurs clients qui demandent une adresse IP à un serveur DHCP et cela à l'aide de deux ordinateurs serveurs et d'un ordinateur client et un moyen d'Ethernet (switch).

IV.2.2 Scénario pour la mise en œuvre de NAP via DHCP

On a décidé de limiter l'accès au réseau de l'entreprise uniquement aux ordinateurs dont l'intégrité est conforme à la stratégie définie et de limiter l'accès aux autres ordinateurs en utilisant la protection de l'accès réseau NAP associée au serveur DHCP.

La stratégie consiste à vérifier que le pare-feu est bien activé. Plusieurs scénarios vont être joués afin de simuler différents clients possibles Enfin, nous devons tester la solution dans les cas suivants :

1. Tester le client non compatible NAP.
2. Tester le client .non conforme.
3. Tester le client conforme.

IV.2.3 Les exigences de matériel et des logiciels

Ce qui suit sont les composants exigés Pour l'application

1. Un CD pour le produit Windows serveur 2008
2. Un CD pour le produit Windows 7
3. Un CD pour le produit Windows Server 2003 avec Service Pack 2 (SP2).
4. Un ordinateur qui satisfait les exigences minimum de matériel pour Windows serveur 2003 SP2.
5. Un ordinateur qui satisfait les exigences minimum de matériel pour Windows serveur 2008.
6. Un ordinateur qui satisfait les exigences minimum de matériel pour Windows 7
7. Un moyen pour Ethernet un hub ou un switch.

IV.3. Les Étapes pour la configuration de NAP avec serveur DHCP

Il y a trois étapes globales exigées pour configurer cette méthode, une étape pour chaque ordinateur.

1. Configurer DC1

DC1 est l'ordinateur serveur qui exécutera le système d'exploitation Windows serveur 2003. DC1 sera configuré comme un contrôleur de domaine avec l'annuaire Active Directory et comme serveur primaire de DNS.

2. **Configurer NPS1.**

NPS1 est l'ordinateur serveur qui exécutera le système d'exploitation Windows serveur 2008. NPS1 sera configuré avec le service du serveur de stratégie (NPS), qui fonctionne comme serveur de stratégie de sante NAP et comme serveur RADIUS. NPS1 sera également configuré avec le service DHCP et fonction comme serveur d'enfoncement NAP.

Remarque

Le serveur NPS joue le même rôle que le serveur IAS

3. **Configurer CLIENT1.**

CLIENT1 est un ordinateur client qui exécutera le système d'exploitation de Windows 7. CLIENT1 sera configuré en tant qu'un client DHCP et client NAP.

La figure suivante illustre l'environnement de la configuration

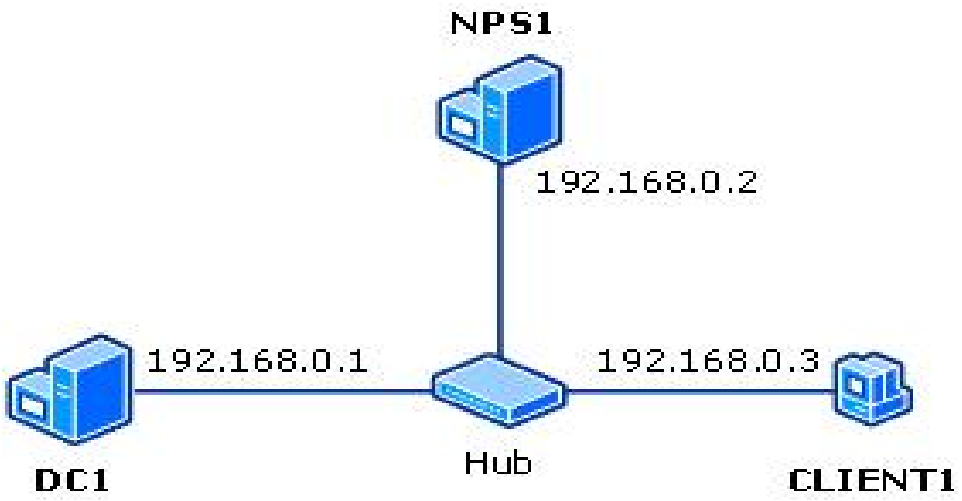


Figure IV.1 infrastructure de la configuration de mise en Conformité DHCP

IV.3.1 La Configuration de DC1

DC1 est un ordinateur qui exécutera Windows serveur 2003 et fournit les services suivants :

1. Un contrôleur de domaine pour **ummto.dz** de domaine active directory
2. Un serveur DNS pour le domaine **ummto.dz.**

La configuration de DC1 comprend les étapes suivantes :

1. Installer le système d'exploitation.
2. Configurer TCP/IP.
3. Installer Active Directory et le serveur DNS

Les sections suivantes expliquent ces étapes en détail.

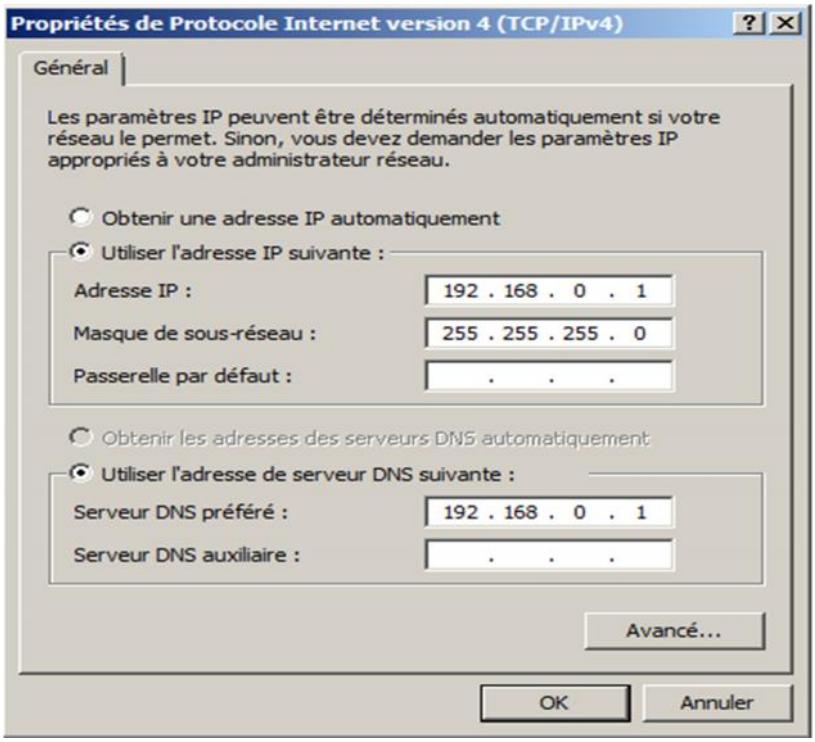
1. Installation de système d'exploitation sur DC1

On installe Windows serveur 2003 comme serveur autonome.

1. Mettre en marche l'ordinateur en utilisant le CD Windows serveur 2003
2. Une fois terminé. On tape le nom d'ordinateur DC1.

2. Configuration TCP/IP sur DC1

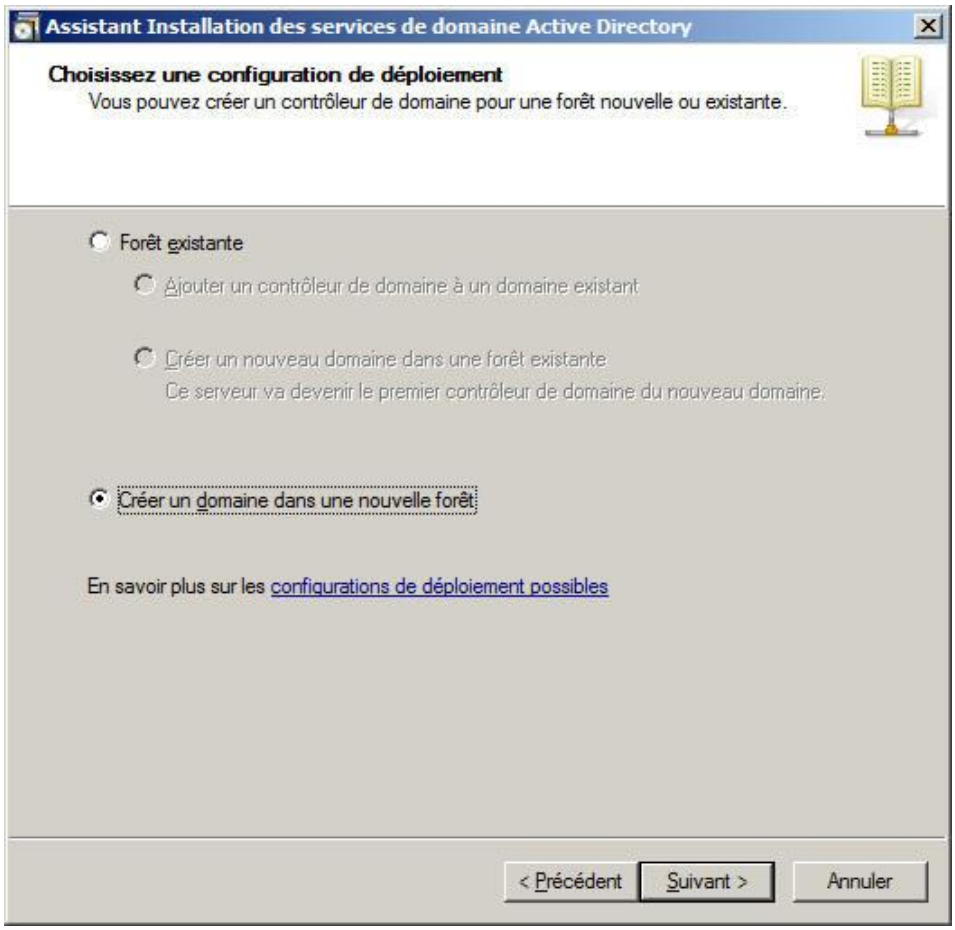
On configurer le protocole TCP/IP avec une adresse IP statique `192.168.0.1` et mask sous-réseau `255.255.255.0`.



3. Installation de serveur Dns et l'active directory

DC1 servira seul comme contrôleur de domaine et serveur DNS pour le domaine **ummto.dz.**

1. Pour démarrer l'assistance d'installation d'active directory on tape dcpromo dans la fenêtre exécute.
2. Maintenant dans l'assistant d'installation d'active directory nous vérifions que le contrôleur de domaine est choisi, comme un nouveau contrôleur de domaine. On coche la case créer un domaine dans une nouvelle forêt



3. Sur la page qui indique **l'installation et configuration DNS**, on choisit juste d'installer le DNS sur cet ordinateur. Puis on tape **Ummto.dz** sous la fenêtre nom de DNS pour le nouveau domaine qui apparaît.
4. Attendre tandis que l'assistance accomplit la configuration de l'active directory et de service DNS, et puis on clique sur termine

IV.3.2 La Configuration de NPS1

NPS1 exécutera Windows serveur 2008, et accueillera le service de NPS, qui fournit l'authentification radius, l'autorisation et la comptabilisation

La configuration NPS1 comprend les étapes suivantes :

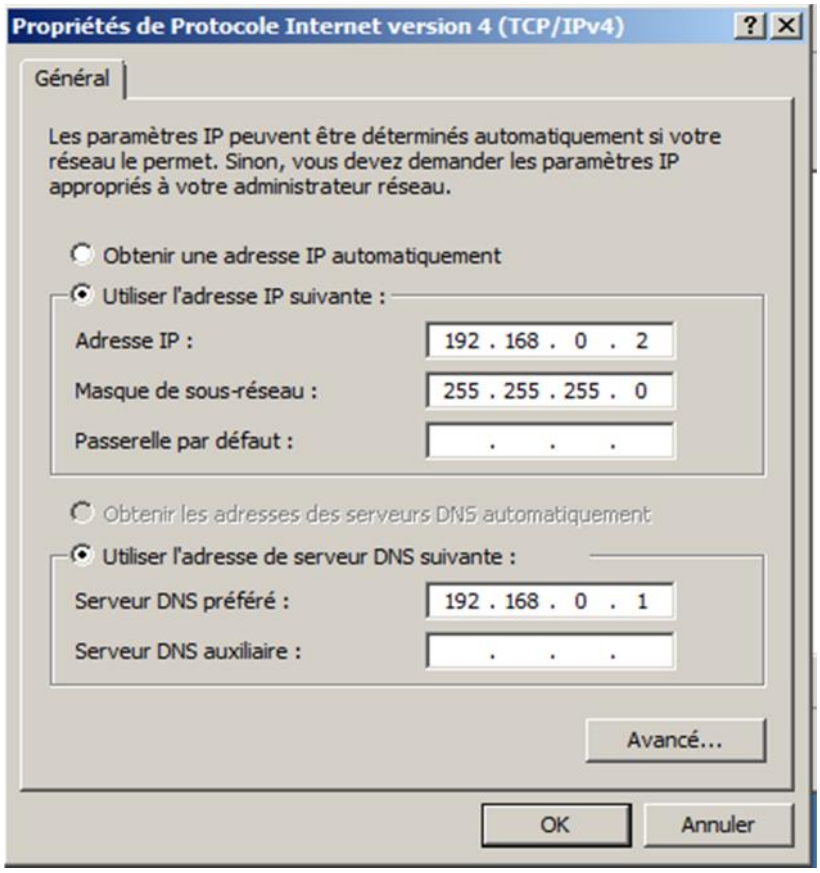
1. Installer le système d'exploitation.
2. Configurer TCP/IP.
3. Installer NPS et serveur DHCP.
4. Configurer NPS.
5. Configurer DHCP.

1. Installation de système d'exploitation sur NPS 1

1. Mettre en marche l'ordinateur en utilisant le CD Windows serveur 2008
2. On Suit les instructions qui apparent sur l'écran jusqu'à la fin de l'installation.
3. Une fois terminé. On tape le nom d'ordinateur NPS1.
4. On ajoute le serveur NPS1 au domaine ummto.dz.

2. Configuration des propriétés de TCP/IP sur NPS1

1. On configurer le protocole TCP/IP avec **une adresse IP** statique **192.168.0.2** et le **mask sous-réseau 255.255.255.0**.
2. Et pour **le serveur préféré de DNS** on utilise l'adresse suivante **192.168.0.1.**



3. Installation de serveur NPS.

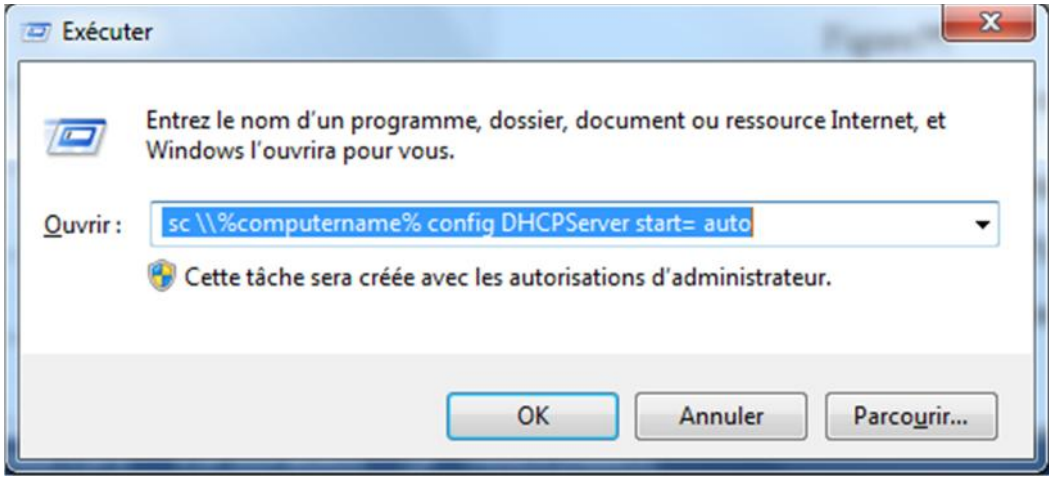
On installe le serveur NPS avec la commande `servermanagercmd -install NPAS-Policy-Server` dans la fenêtre Exécute

Le rôle serveur NPS (Network Policy Server), c'est à dire un serveur de stratégies réseau est installé sur le serveur NPS1.

4. Installation de serveur DHCP.

1. Dans la fenêtre exécute on tape la commande `servermanagercmd -install DHCP` le rôle serveur DHCP est installé sur la machine NPS1
2. On devra mettre le service en démarrage automatique avec la commande :

`Sc \\%computername% config DHCPServer start= auto` dans la fenêtre exécute.



Le rôle de serveur DHCP est installé et mis en démarrage automatique sur le serveur NPS1.

5. Configuration de NPS

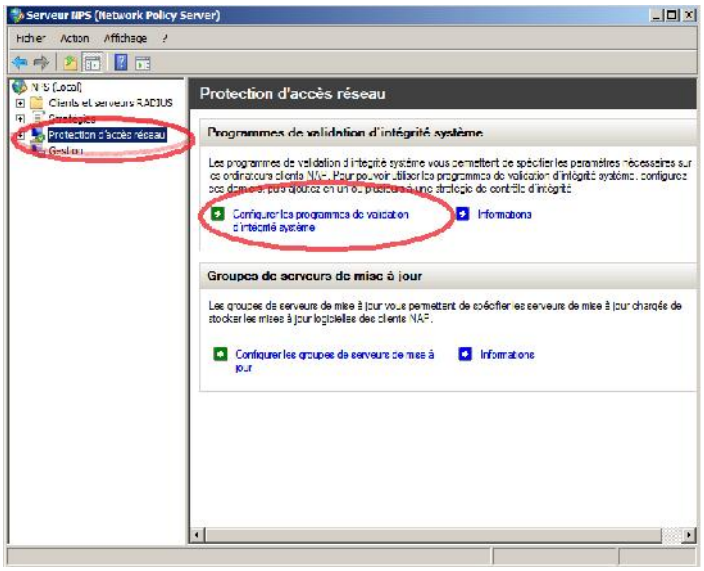
Configurer NPS1 comme serveur de stratégies de santé de NAP

La configuration de NPS comme serveur de stratégie de santé NAP comprend les étapes suivantes :

1. Configurer SHV.
2. Configurer les groupes de serveur de remédiation.
3. Configurer les stratégies de santé.
4. Configurer les stratégies de réseau.
5. Configuration de serveur DHCP pour activer la stratégie NAP.

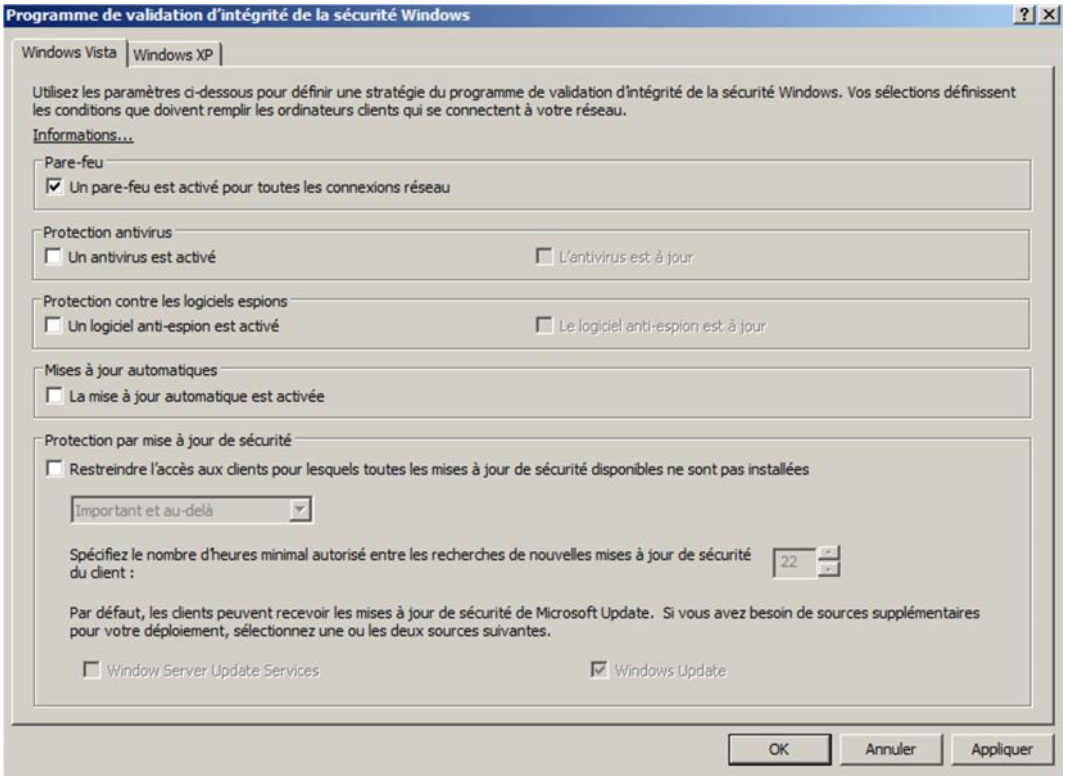
6. Configurer SHV

1. Ouvrir la console de gestion de NPS, nous écrivons la commande nps.msc dans exécute.
2. Dans l'administration du serveur NPS**,** Protection d'accès réseau On sélectionne le conteneur Programmes de validation d'intégrité système.



3. On Configure ensuite le système de validation fourni par défaut appelé **Validateur d'intégrité de la sécurité Windows**.
4. On Clique sur le **bouton Configurer** pour accéder aux propriétés à tester.
5. À noter qu'il y a un onglet différent pour XP et pour Vista.

Dans notre cas une configuration simplifiée basée sur **la présence du pare-feu**

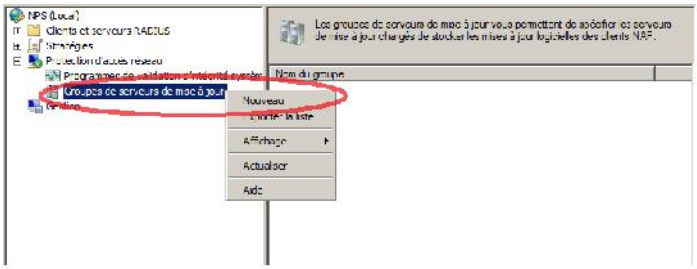


6. Clique **ok** pour fermer la zone de dialogue de validation d'intégrité système.

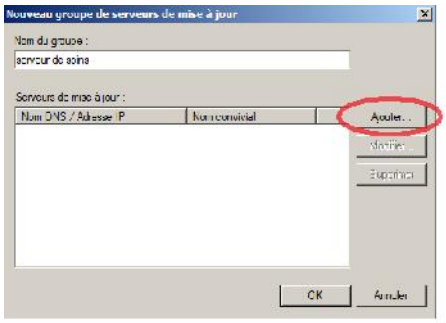
7. Configurer les groupes de serveur de remédiation

Les groupes de serveur de remédiation sont des listes d'ordinateurs aux lesquels les clients non conforme de NAP peuvent accéder pour les aider à mettre à jour leur configuration. Dans notre cas, DC1 sera ajouté au groupe de serveur de remédiation de telle sorte que CLIENT1 ait accès au DNS quand il est non conforme

1. Dans **console de gestion de NPS**, sous **la protection d'accès de réseau**,
2. On clique droit sur **les groupes de serveur de remédiation** et on clique **nouveau**



3. Sous le nom de groupe, on écrit serveurs de soins
4. À côté des serveurs de remédiation, on clique **ajoute**.



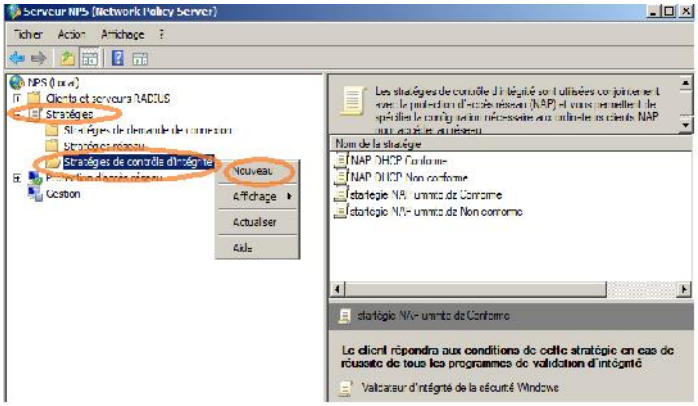
5. Dans la nouvelle zone de dialogue de serveur, sous le nom DNS/ adresse IP, on donne l'adresse IP **192.168.0.1**
6. On clique alors deux fois sur **OK** pour terminer.

8. Configurer les stratégies de santé

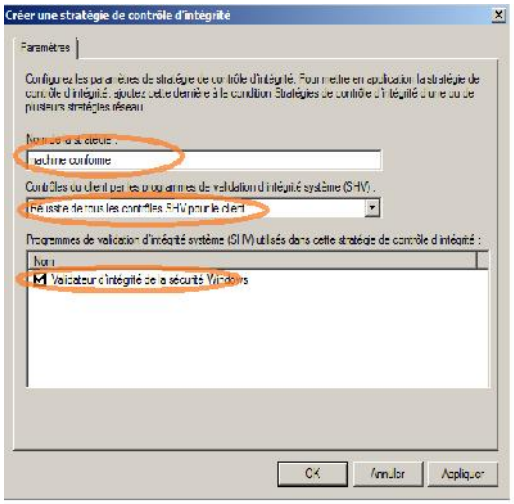
Les stratégies de santé définissent quel SHV sont évalués, et comment elles sont employées en validant la configuration des ordinateurs qui essayent de se connecte aux réseaux. Basé sur les résultats des contrôles de SHV, les stratégies de santé classifient l'état de santé de client. Ici On définit deux stratégies de santé: une qui correspond à un état de santé conforme et une autre qui correspondent à un état de santé non conforme

a)Une pour les machines conformes

1. On Double-clique sur la stratégie.
2. on clique Droit sur les stratégies de contrôle d'intégrité, et on clique alors nouveau.

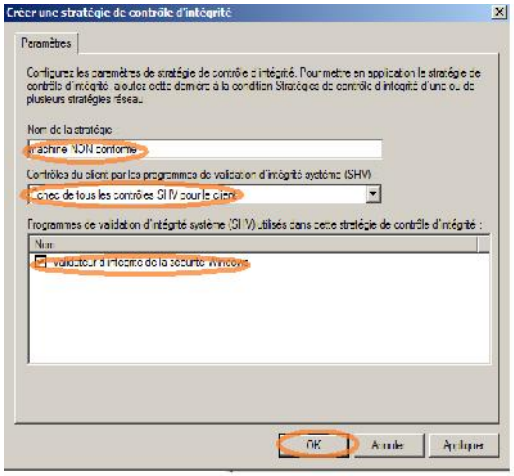


3. Dans la nouvelle zone de dialogue stratégies de santé crée, sous le nom de stratégie, on type le nom machine conforme.
4. Sous contrôles du client par les programmes de validation d'intégrité de système SHV, On choisit **réussite de tous les contrôles de SHV pour le client**
5. et on coche la case de la boîte de Validateur d'intégrité de la sécurité Windows, et on clique sur ok pour terminer comme montré dans l'exemple suivant.



b) Une pour les machines non conformes

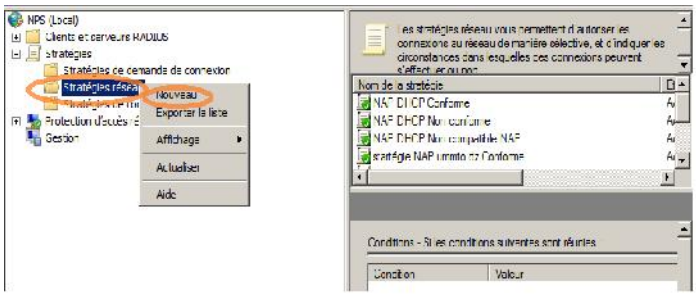
On sélectionne même validateur que pour une machine conforme, mais on définisse la règle sur **Echec d'un ou de plusieurs contrôles SHV pour le client**.et le nom de la stratégie la machine non conforme



9. Configuration des stratégies réseau

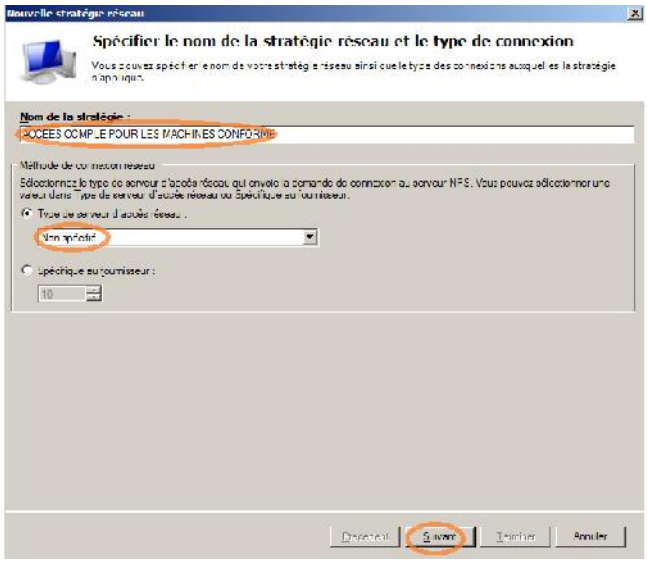
a) Création de la stratégie réseau pour les machines conformes

1. On clique avec le bouton droit sur Stratégies Réseau.
2. Puis on choisit Nouveau dans le menu.

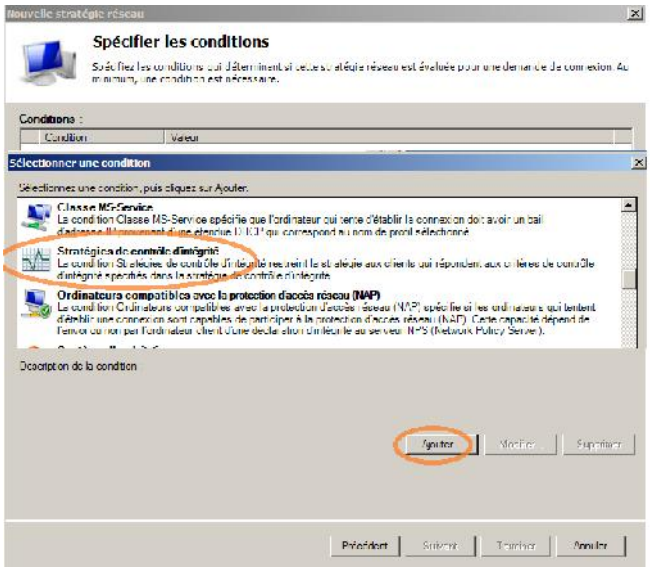


3. On Nomme la stratégie **Accès complet pour les machines conformes**, on laisse le type de réseau sur Non spécifié.

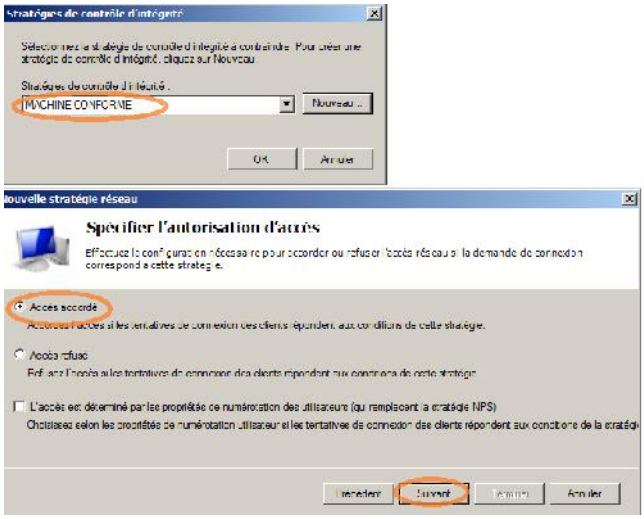
Non spécifié signifie que la stratégie sera appliquée quel que soit le type d'accès réseau utilisé.



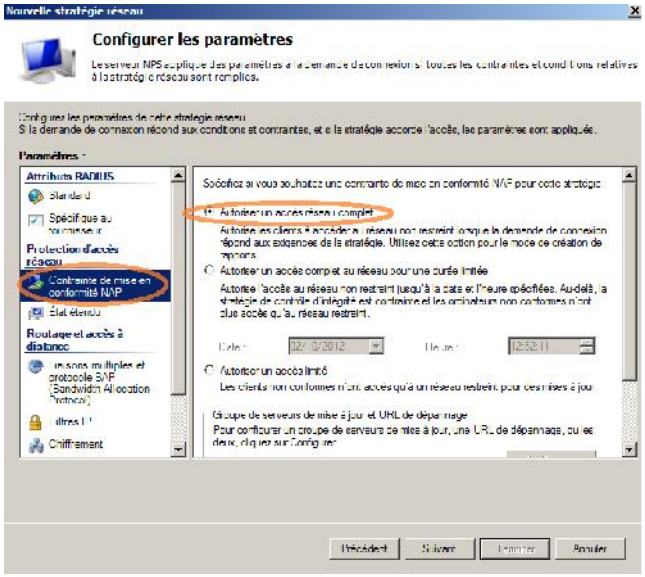
4. Sur l'écran Spécifier les conditions, on préciser à qui s'applique cette stratégie, on clique sur Ajouter. Et on sélectionne **Stratégies de contrôle d'intégrité.**



5. Dans la liste proposée on Choisit la stratégie Machine Conforme, puis on passe à l'écran suivant. On spécifie Accès accordé



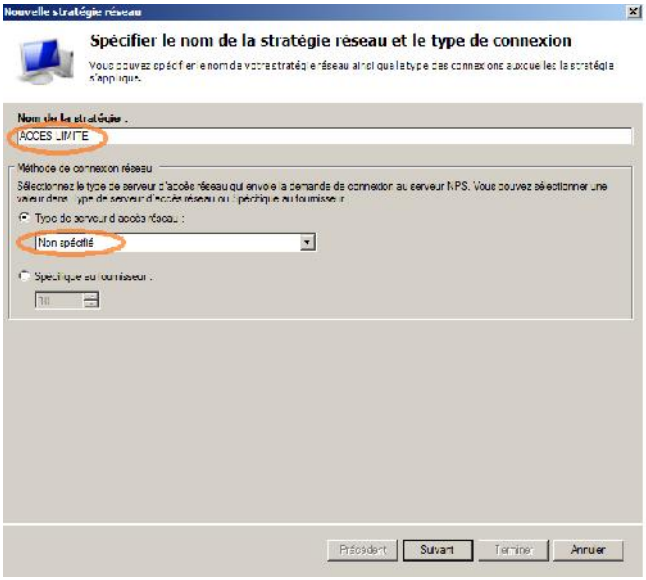
6. Aucune authentification donc On Vérifier uniquement l'intégrité de l'ordinateur Sur l'écran Configurer des contraintes, aucune valeur n'est à modifier.
7. Sur l'écran Configurer les paramètres, dans la section Protection d'accès réseau, on va Autoriser **un accès réseau complet**.



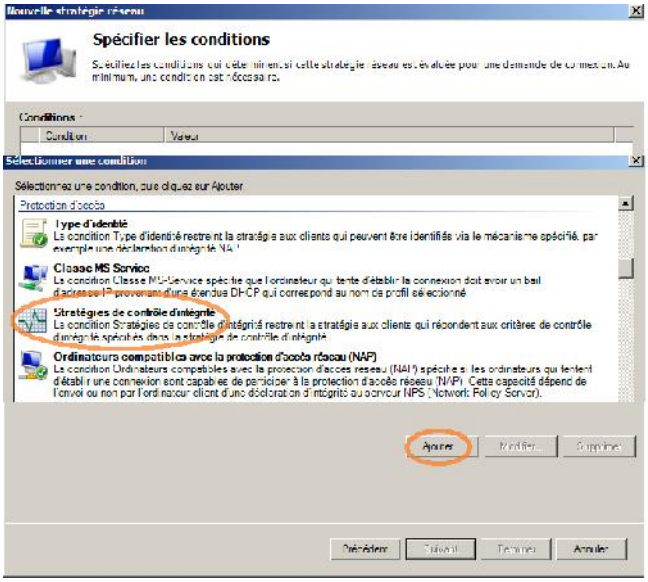
8. On clique sur Terminer sur l'écran final

b) Création de la stratégie réseau pour les machines non conformes

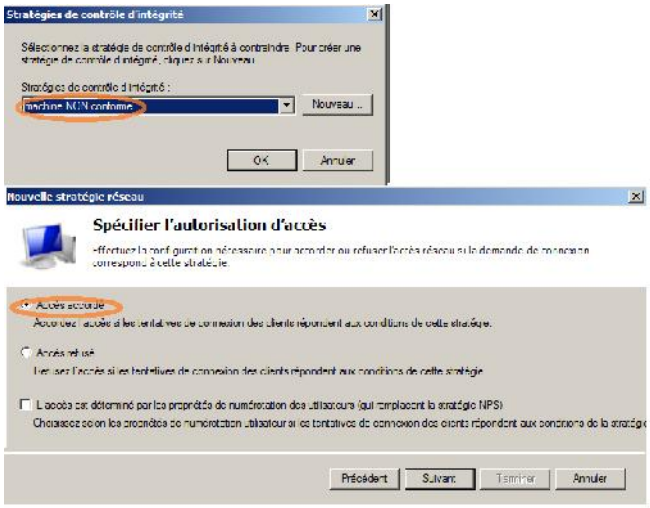
1. On clique avec le bouton droit sur Stratégies Réseau puis on choisit Nouveau dans le menu.
2. On nomme la stratégie **Accès limite pour les machines non conformes**, on laisse le type de réseau sur Non spécifié



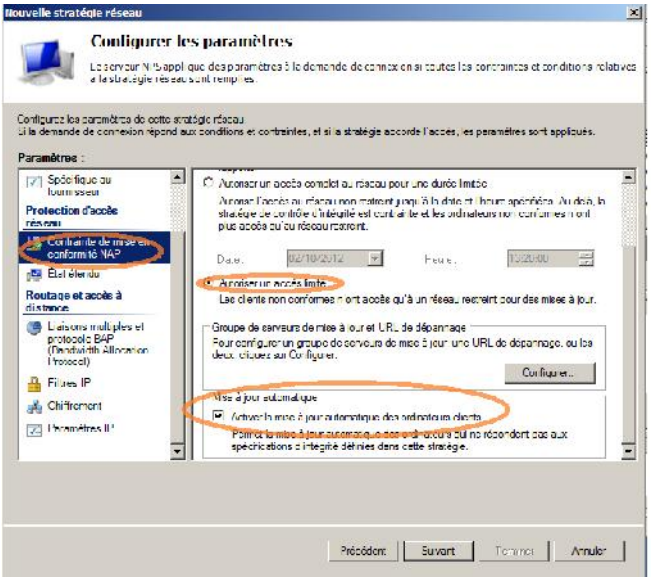
3. Sur l'écran Spécifier les conditions, On précise à qui s'applique cette stratégie, on clique sur Ajouter et on sélectionne Stratégies de contrôle d'intégrité.



4. On choisit dans la liste proposée la stratégie Machine non Conforme, puis on passe à l'écran suivant et on spécifie **Accès accordé**



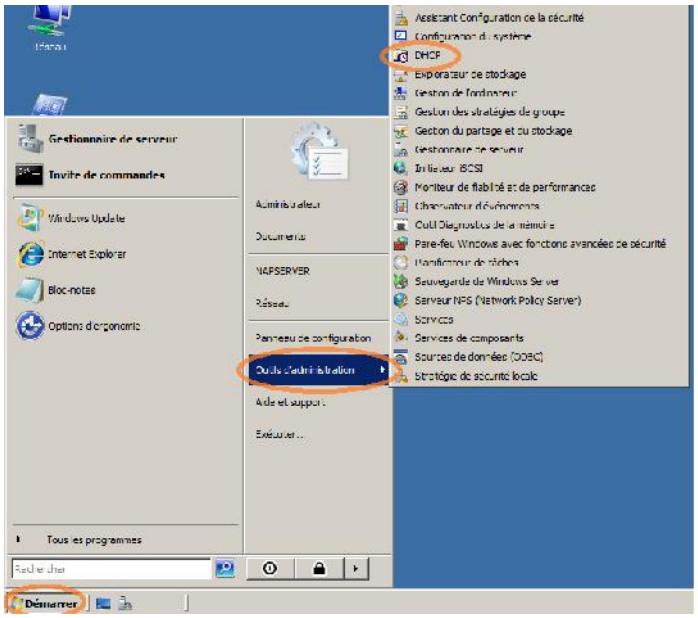
5. Aucune authentification n'est requise pour ce type de quarantaine, On sélectionne donc Vérifier uniquement l'intégrité de l'ordinateur.
6. Sur l'écran Configurer des contraintes, aucune valeur n'est à modifier.
7. Sur l'écran Configurer les paramètres dans la section Protection d'accès réseau, on va **Autoriser un accès limité**.



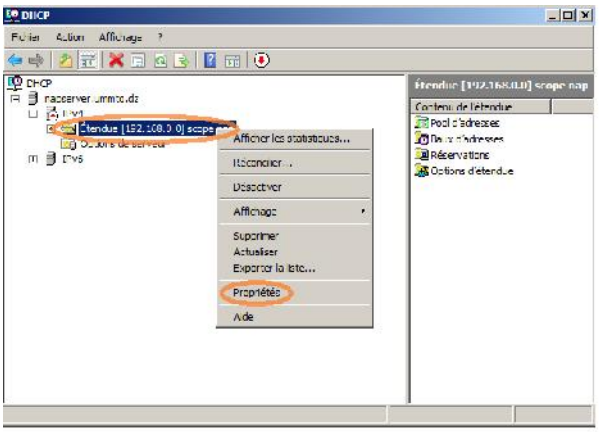
8. On clique sur Terminer sur l'écran final qui résume l'ensemble de la stratégie.

10. Configuration de serveur DHCP pour activer la stratégie NAP

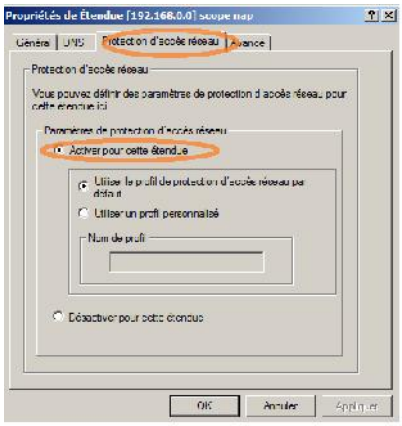
1. On démarre la console DHCP



2. Dans l'arborescence, on développe l'étendue existante puis cliquez avec le bouton droit de la souris pour faire apparaître les propriétés de l'étendue.



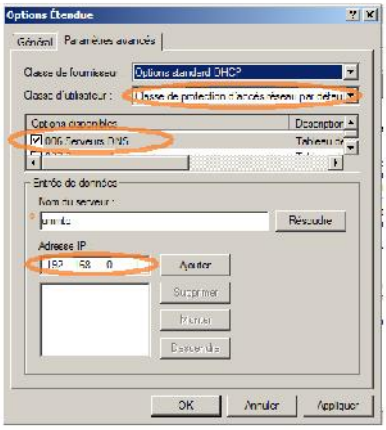
3. On clique sur l'onglet Protection d'accès réseau.
4. On Sélectionne l'option Activer pour cette étendue puis on clique sur OK. La partie serveur de la stratégie NAP est opérationnelle



5. .On ajoute l**es options d'étendues** suivantes pour les ordinateurs non conformes :

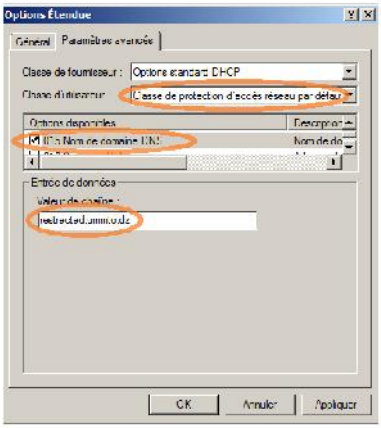
006 Serveur DNS 192.168.0.1

Classe de protection d'accès réseau par défaut.



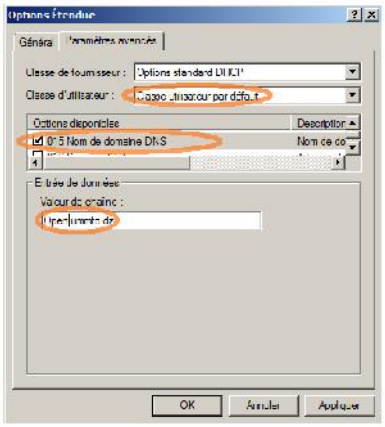
015 Nom de domaine DNS restricted.ummto.dz

Classe de protection d'accès réseau par défaut.



015 Nom de domaine DNS open.ummto.dz

Classe utilisateur par défaut.



IV.3.3 Configuration de CLIENT1.

CLIENT1 est l'ordinateur qui exécutera Windows 7 qu'on emploiera pour démontrer comment le NAP peut être employé avec DHCP pour aider à protéger un réseau à partir des ordinateurs de client.

La configuration de CLIENT1 comprend les étapes suivantes.

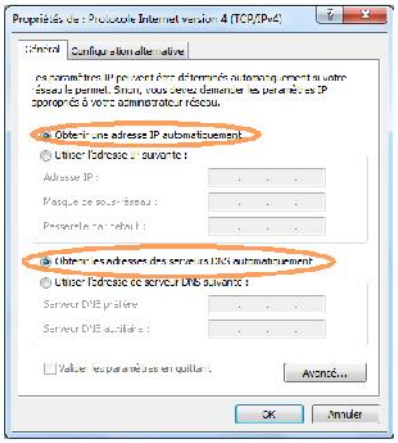
1. Pour installer le système d'exploitation Windows 7 sur CLIENT1

1. Mettre en marche notre ordinateur en utilisant le CD Windows 7.
2. Une fois démarre pour un nom d'ordinateur, on écrit **CLIENT1**.
3. Suivre le reste des instructions qui apparent sur notre écran pour finir l'installation.

2. Configurer TCP/IP.

1 On clique sur **Internet Protocol version 4 (TCP/IPv4)**, et puis sur **propriétés.**

2 On vérifier qu'obtenir une adresse IP **Automatiquement** et **obtenir les adresses des serveurs de DNS automatiquement** sont choisi**.**



3 On Clique **OK**, pour finir

IV.4 Vérification de la fonctionnalité de NAP

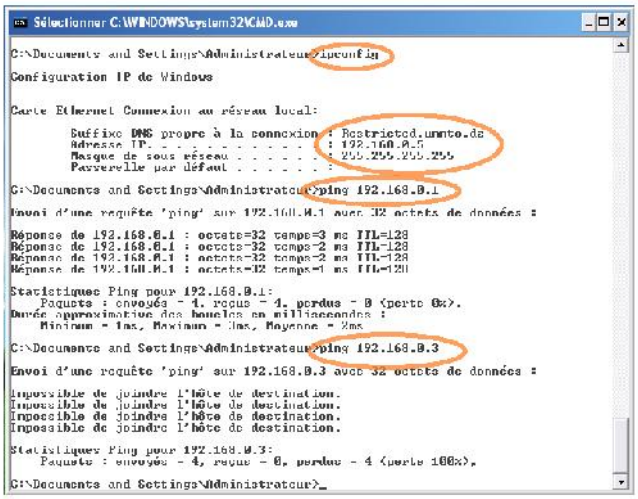
IV.4.1 Pour les machines non compatibles NAP

1. On démarre la machine client.

2. Dans une invite de commande, on saisisse **ipconfig**, le client acquis **une adresse IP de 192.168.0.5** et **un masque de sous-réseau 255.255.255.255**. Comme le masque de sous réseau est invalide (se devrait être 255.255.255.0), cela indique que l'ordinateur client a échoué au contrôle d'intégrité et se trouve dans la zone restreinte.

3. Sur l'invité de commande nous exécutons la commande **Ping 192.168.0.1** (cette adresse correspond au serveur de mise à jour que nous avons configuré).DC1 répond au Ping confirment la disponibilité de serveur de mise à jour

4. sur l'invité de commande nous exécutent la commande **Ping 192.168.0.3.** La commande échoue avec une erreur impossible de joindre l'hôte de destination puisqu'il n'existe pas de route pour la destination



L'ordinateur est considéré comme un client Non compatible NAP puisque par défaut le service Agent de protection d'accès réseau n'est pas démarré.

Le client non compatible NAP se trouve dans la zone restreinte.

IV.4.2 Pour les machines non conforme à la stratégie NAP

Pour qu'un ordinateur client puisse envoyer son état d'intégrité au serveur NAP, il faut que les conditions suivantes soient réunies :

1 - Le service Agent de protection d'accès réseau doit être être actif sur les postes clients, c'est-à-dire que le service doit être en démarrage automatique.

2 - Activer le client de contrainte DHCP.

3 - Garantir que le service Centre de sécurité est démarré.

4 - On ajoute le client au domaine ummto.dz.

Dès que toutes ces conditions sont réunies, alors l'ordinateur client devrait pouvoir envoyer son état de santé au serveur NAP c'est à dire le SOH pour que le SHV puisse vérifie si les stratégies demandées sont validées.

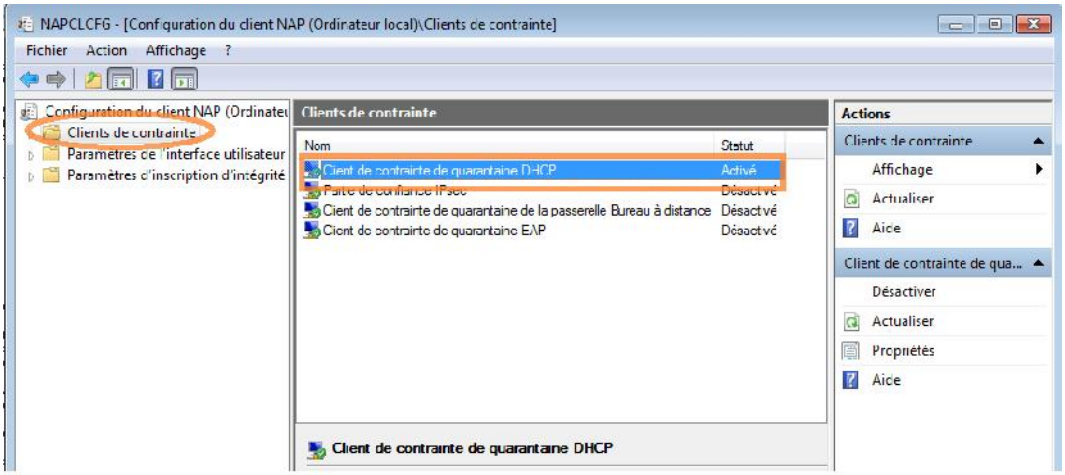
1. On libéré l'adresse IP avec la commande **ipconfig /release**.

2. En utilisant la commande **net start wscsvc** nous démarrons le service Centre de sécurité

3. On faite de même avec le service Agent de protection d'accès réseau avec la commande **net start napagent**

4. Démarrez la console **napclcfg.msc** sur CLIENT1.

5. Dans l'arborescence on clique sur Clients de contrainte puis dans la section de détail, nous activons **Client de contrainte de quarantaine DHCP.**



6. puis nous demandons une adresse IP avec la commande **ipconfig /renew.**

7. Ensuite, nous pouvons vérifier la configuration de client en exécutant la commande suivante sur l'invité de commande **: netsh nap client show state**

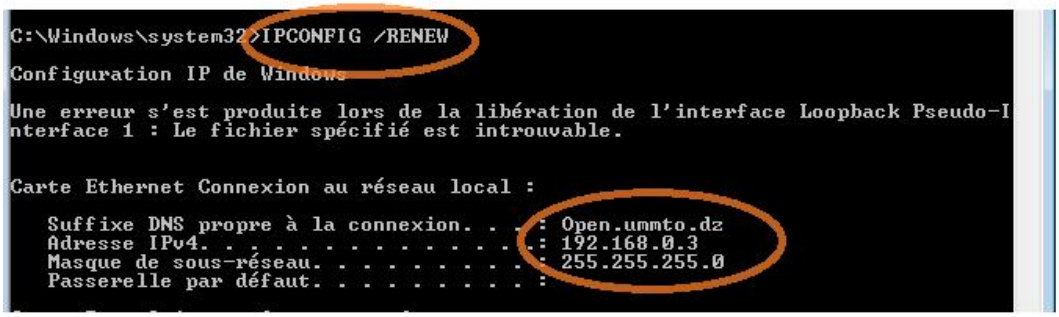
Nous trouvons qu'il est indiqué que l'ordinateur est placé en quarantaine et la raison est **le pare-feu est désactive** .c'est à dire client Non conforme NAP.

IV.4.3 Test d'un client conforme

1. Sur le client sur démarre\panneau de configuration\pare-feu Windows nous activons le pare-feu.
2. Dans l'invité de commande nous exécutant les commandes suivantes pour recevoir de nouveaux paramètres d'adresse IP du serveur DHCP :

Ipconfig /release.

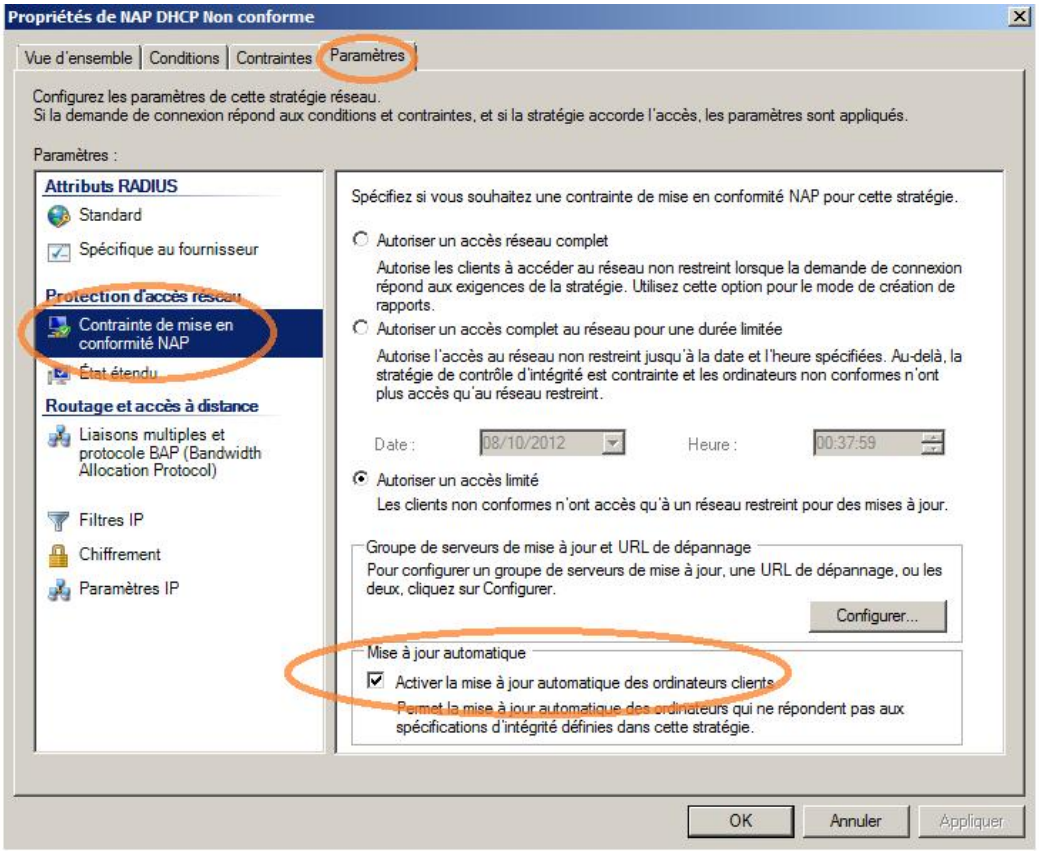
Ipconfig /renew.



3. L'ordinateur client affiche une nouvelle configuration d'adresse IP, avec une **adresse IP de 192.168.0.3** et un masque **de sous-réseau de 255.255.255.0.** Puisque le masque sous-réseau est désormais valide, l'ordinateur pourra se connecter à d'autres ordinateur de sous réseau.

IV.4.4 Vérification d'auto-remédiation de NAP

1. Dans La stratégie réseau des machines non conforme NAP On autoriser la remise à niveau automatique (et donc autoriser les serveurs de remédiation), On clique Sur démarre\outil d'administration\serveur nps\stratégie réseau\Accès limite pour les machines non conformes\paramétré\contrainte de mise en conformité NAP, on coche la **case Active la mise à jour automatique des ordinateurs client .**



2. On vérifier que CLIENT1 est remédie automatiquement à un état conforme quand le pare-feu Windows est arrêté. Nous cliquons sur démarrer\panneau de configuration \pare-feu Windows\activer ou désactiver le pare-feu. Nous désactivons le pare-feu

Au centre de sécurité de Windows, nous voyons que le statut du pare- feu Windows est visualise désactiver et ensuite il est visualise activer.

Le client de NAP allumera automatiquement le pare-feu Windows pour devenir conforme avec les conditions de la stratégie réseau.

IV.5 Conclusion

La mise en conformité DHCP fournit des donnés d'adressage IPv4pour accès illimité aux machines conforme et des données d'adressage IPv4 pour accès limite aux machines non conforme

L'application de NAP se produit au moment où les ordinateurs clients essayent d'accéder au réseau par des serveurs d'accès au réseau, tels qu'une obtention d'une adresse IP à partir de serveur DHCP, ou quand les clients essayent de communiquer avec d'autres ressources de réseau

Conclusion générale

Conclusion :

En déployant la Protection d’accès réseau NAP (Network Access Protection) dans un réseau, nous a apporté une plate-forme permettant de valider l’intégrité des systèmes informatiques avant de les autoriser à accéder à des réseaux protégés. A chaque nouvelle connexion, il est ainsi possible d’assurer qu’un ordinateur a au moins été « inspecté » avant d’accéder au réseau privé.

Lors de la mise en œuvre de la méthode de mise en conformité DHCP, nous a fourni des données d’adressage IPv4 pour accès illimité aux machines conformes et des données d’adressage IPv4 pour accès limite aux machines non conformes. Pour déployer la mise en conformité DHCP nous avons utilisé un serveur DHCP Windows server 2008 car il inclut le service de mise en conformité DHCP. Le client de mise en conformité DHCP est inclut dans le service client DHCP de Windows 7 ou vista ou Windows XP SP 3.

Ce travail m’a permis de mieux comprendre et d'appréhender l'organisation des réseaux informatique, comme il m’a également permis d'apprendre considérablement sur la sécurité des réseaux informatiques, j’ai compris l'importance des mécanismes de sécurité comme la protection d’accès réseau NAP et ces méthodes de mise en œuvre, et comment répondre à ces problématiques.

En conclusion, je suis très satisfait de ce travail qui a ajouté une dimension professionnelle ainsi qu'un apport personnel crucial pour ma poursuite d'étude et mon avenir professionnel.

Annexe

Introduction

Windows Server 2008 tire pleinement parti des grandes innovations qui sont intervenues depuis la mise à disposition de ses prédécesseurs : l'évolution des processeurs vers le 64bit et les architectures multi-cœurs, généralisation de la virtualisation, pilotage fin des bilans énergétiques, nouvelles méthodes de développement et de test sécurisées (TWC).

Windows Server 2008 est une solution conçue pour répondre aux problématiques de montée en charge, de haute disponibilité et d'agilité requises dans les centres de traitement et habituellement résolues avec des mainframes ou des Unix historiques.

En même temps, il conserve l'ergonomie de ses prédécesseurs et met à la disposition des organisations de toute taille les technologies de virtualisation, de sécurité et de haute disponibilité qui leur étaient inaccessibles.

Pour cela, Windows Server 2008 innove sur 4 axes majeurs :

➢ *Aider à gérer la complexité*

De nouveaux outils de gestion des serveurs permettent d'automatiser les tâches récurrentes (Windows Power Shell) en vous offrant la possibilité d'installer, de configurer et d'administrer vos serveurs locaux et distants depuis une interface unique et centralisée (la console Server Manager). La fonction de clusters dans Windows Server 2008 a été améliorée pour offrir une solution de haute disponibilité qui protège les applications critiques, les services et les informations des utilisateurs. Les services de déploiement Windows (WDS) réduisent le coût et la complexité des déploiements des systèmes d'exploitation sur les postes clients et les serveurs. Enfin l'installation de Windows Server 2008 en mode minimaliste (Server Core) permet de ne pas s'encombrer des composants inutiles. Cela réduit les interventions de mises à jour et les interruptions de services qui peuvent en découler.

➢ *Ouvrir le réseau et protéger les données*

NAP (Network Access Protection) est une fonctionnalité clé de Windows Server 2008 qui permet de contrôler l'accès au réseau des ordinateurs en vérifiant la bonne santé de leur système et leur conformité aux politiques de sécurité de l'entreprise. Citons également le renforcement des services

Windows pour un système d'exploitation plus résistant contre les attaques, la nouvelle option d'installation Server Core qui diminue la surface exposée aux risques informatiques, ainsi que

le contrôleur de domaine en lecture seule (RODC) qui permet de renforcer la sécurité dans les sites distants. Enfin, Windows Server 2008 contient le serveur Active Directory Right Management Server qui permet de contrôler et de restreindre la diffusion et l'accès aux informations de l'entreprise.

➢ *Rationaliser les infrastructures avec la virtualisation*

Windows Serveur 2008 permet de consolider les serveurs X86 (virtualisation de serveurs) et de centraliser les applications (virtualisation de présentation). Hyper-V, l'hyperviseur de Windows Server 2008, est une architecture moderne de para-virtualisation conçue pour héberger des machines virtuelles multi-processeurs et 64 bits et permettre ainsi de rationaliser les investissements matériels. Cette technologie est intégrée directement dans le système d'exploitation et ne requiert donc aucun investissement complémentaire. La génération 2008 de cette technologie est parfaitement compatible avec les précédentes et utilise les mêmes outils de supervision (System Center Virtual Machine Manager). Pour les entreprises qui ont une stratégie de centralisation des applications, les nouveaux services Terminal Services intégrés à Windows Server 2008 proposent trois innovations très significatives, notamment pour les populations nomades : une fonction de passerelle d'accès aux applications qui permet d'y accéder à partir de n'importe quelle connexion internet, l'amélioration de l'ergonomie d'accès aux applications et la fonction « EasyPrint » qui permet d'exploiter plus simplement les imprimantes.

➢ *Faciliter l'évolution du Web*

Internet Information Server 7.0 (IIS 7), le nouveau serveur Web de Windows Server 2008, permet une montée en puissance des infrastructures Web pour internet ou pour les intranets. Il permet aussi de reprendre l'existant – ASP, ASP.NET et PHP – avec un minimum de modifications. Fortement intégré à Windows Server 2008, il tire pleinement parti des fonctions de celui-ci pour la sécurité, l'administration, la haute disponibilité et la montée en charge. Windows® Sharepoint Services 3.0 (WSS 3.0) est un service téléchargeable pour Windows Server 2008 qui permet de créer des sites web spécialisés pour le partage d'informations et de documents dans l'entreprise. WSS 3.0 permet de déployer rapidement des démarches collaboratives et sa mise en œuvre est couverte par les licences de Windows Server 2008.

Présentation de Windows Server 2008

Microsoft Windows Server 2008 est une nouvelle génération du système d'exploitation Windows

Server conçue pour aider les administrateurs système à rationaliser leurs infrastructures.

Windows Server 2008 innove sur 4 axes majeurs :

➢ *Virtualisation*

Terminal Services : est une fonction de Windows Server 2008 qui permet de faire fonctionner une ou plusieurs applications sur un serveur centralisé en déportant uniquement les interfaces utilisateurs vers le poste de travail de l'utilisateur.

Terminal Services Gateway : est une extension à Terminal Services qui permet d'accéder à Terminal Services sans être connecté directement au réseau de l'entreprise. C'est une fonction très intéressante pour les populations nomades.

Terminal Services Easy Print : permet d'utiliser des imprimantes locales au poste de travail sans avoir à monter des pilotes d'impression sur le serveur.

Terminal Services Remote App : est une extension de Terminal Services qui permet d'améliorer l'expérience de l'utilisateur Grâce à cette nouvelle fonction, l'utilisateur ne fait plus du tout la différence entre une application locale et une application qui est exécutée à distance. Cela améliore leur productivité et diminue les coûts de support et de formation aux utilisateurs.

Hyper-V : l'hyperviseur de Windows Server 2008, est une très fine couche de logiciel qui s'intercale entre le matériel et les systèmes d'exploitation (les serveurs virtualisés) pour que ceux-ci se partagent les ressources mémoire et processeurs de la machine. Les serveurs virtualisés n'opèrent pas nécessairement sous les mêmes environnements. Cela permet de faire passer le taux d'utilisation des serveurs x86 d'une tranche de 8-15% à une tranche de 30-40% et donc de rationaliser les investissements en terme de matériel.

➢ *Sécurité*

Windows Right Management Server est un service inclus dans Windows Server 2008 et qui permet de gérer ce que chacun a le droit de faire d'un document donné. Ainsi l'auteur d'un document va pouvoir en restreindre la lecture, la modification, l'impression ou le transfert par mail à un nombre limité de personnes.

Network Access Protection (NAP) est une technologie Microsoft permettant de contrôler l'accès au réseau d'un ordinateur en se basant sur la santé de son système. NAP est utilisée pour faire respecter la stratégie de sécurité de l'entreprise : lorsqu'un ordinateur, qu'il appartienne à un utilisateur interne, à un utilisateur mobile ou à un visiteur, tente de se connecter au réseau de l'entreprise, NAP vérifie sa conformité à la stratégie de sécurité de l'entreprise. Si cet ordinateur s'avère infecté ou non conforme, NAP lui refuse l'accès au réseau et tente de mettre à jour le système avant qu'il puisse se connecter au réseau.

Windows BitLocker Drive Encryption, ou chiffrement complet de l'espace de stockage, est une fonctionnalité clé de Windows Server 2008 améliorant la protection des serveurs, des postes de travail, ordinateurs portables et autres équipements mobiles. Il encode le contenu du disque dur afin que les données soient protégées, même si elles tombent dans de mauvaises mains.

Read-Only Domain Controller (RODC), ou contrôleur de domaine en lecture seule, permet de sauvegarder des comptes utilisateurs là où la sécurité physique ne peut être garantie. RODC fournit une authentification locale pour les utilisateurs des succursales et des agences sans copier entièrement la base de données Active Directory, ce qui réduit les risques.

Active Directory Federation Services (ADFS) est un composant de Windows Server 2008 qui offre à l'utilisateur une expérience d'authentification unique. Avec ADFS, l'utilisateur peut donc accéder à des applications distinctes dans des entreprises indépendantes sans avoir à présenter des informations d'identification à chaque application.

- ***Web***

Internet Information Server 7.0 (IIS 7) est le serveur Web livré avec Windows Server 2008. C'est le composant fondateur d'une infrastructure de site Web pour Internet, de site intranet, ou bien encore pour déployer ou intégrer des services Web. Fortement intégré à Windows Server 2008 il tire pleinement parti des fonctions de celui-ci pour la sécurité, l'administration, la haute disponibilité et la montée en puissance.

Windows SharePoint Services (WSS) 3.0 est un service téléchargeable pour Windows Server

2008 qui permet de créer des sites Web spécialisés pour le partage d'informations et de documents.

Il permet de déployer rapidement des démarches collaboratives. La mise en œuvre de WSS 3.0 est couverte par les licences de Windows Server.

➢ *Fondations du système*

Windows PowerShell est un langage de script en mode ligne de commande qui permet aux administrateurs d'automatiser et de personnaliser les tâches d'administration en toute sécurité. Server Manager est un nouvel outil permettant d'installer, de configurer et d'administrer les serveurs depuis une seule et unique console.

La fonction de clusters (failover clustering) dans Windows Server 2008 a été améliorée en vue de simplifier sa mise en œuvre et d'améliorer la stabilité des clusters. Cette fonctionnalité permet d'offrir aux organisations une solution de « haute disponibilité » afin que les applications critiques, les services et les informations restent à la disposition de tous les utilisateurs, y compris en cas de catastrophe.

Server Core est une nouvelle option d'installation pour certains scénarios d'usage qui permet de n'installer un serveur qu'avec les éléments strictement nécessaires à son fonctionnement. Avec cette option, vous diminuez la charge de mises à jour du serveur et les interruptions éventuelles liées à la maintenance. En n'installant que les composants nécessaires pour un rôle, vous réduisez également la surface d'exposition aux risques informatiques.

Windows Deployment Services, ou services de déploiement Windows (WDS), est une version repensée des services d'installation à distance, qui accélère le déploiement rapide et massif des systèmes d'exploitation Windows à partir d'une image. Avec WDS, vous pouvez effectuer une installation réseau de Windows Server 2008 (ainsi que de Windows Vista) sur des ordinateurs nus (qui ne disposent pas de système d'exploitation). Ainsi, les services de déploiement Windows offrent une solution complète pour le déploiement des systèmes d'exploitation Windows sur les postes clients et les serveurs, et réduit le coût total de possession et la complexité des déploiements

Windows Server 2008 et Windows Vista.

Task scheduler est un ordonnanceur de tâche.

Windows Remote Shell permet d'exécuter des commandes primitives du système d'exploitation à distance.

Ensemble des rôles d'Active Directory

➢ *Services de certificats Active Directory*

Les services de certificats Active Directory (AD CS) fournissent des services personnalisables pour l'émission et la gestion de certificats qui sont utilisés dans les systèmes de sécurité logiciels employant des technologies de clé publique.

Dans les sections suivantes, découvrez les services AD CS, les fonctionnalités requises et facultatives dans les services AD CS, ainsi que les logiciels et le matériel utilisés pour l'exécution des services AD CS. À la fin de cette rubrique, apprenez à ouvrir l'interface des services AD CS et à découvrir plus d'informations sur les services AD CS.

Fonctionnalités des services AD CS

À l'aide du Gestionnaire de serveur, vous pouvez configurer les composants suivants des services

AD CS :

- Autorités de certification. Des autorités de certification racine et secondaires sont utilisés pour émettre des certificats aux utilisateurs, aux ordinateurs et aux services, et pour gérer la validité des certificats.
- Inscription via le Web. L'inscription via le Web permet aux utilisateurs de se connecter à une autorité de certification au moyen d'un navigateur Web afin de demander des certificats et de récupérer des listes de révocation de certificats.
- Répondeur en ligne. Le service Répondeur en ligne décode les demandes d'état de révocation pour des certificats spécifiques, évalue l'état de ces certificats et renvoie une réponse signée contenant les informations demandées sur l'état des certificats.
- Service d'inscription de périphériques réseau. Le Service d'inscription de périphériques réseau permet aux routeurs et à d'autres périphériques réseaux ne possédant pas de comptes de domaine d'obtenir des certificats.

➢ *Services de domaine Active Directory*

En utilisant le rôle de serveur Services de domaine Active Directory (AD DS) sous le système d'exploitation Windows Server 2008, vous pouvez créer une infrastructure évolutive, sécurisée et gérable pour la gestion des utilisateurs et des ressources et vous pouvez assurer la prise en charge des applications utilisant un annuaire, telles que Microsoft® Exchange Server.

Dans les sections suivantes, vous obtiendrez plus d'informations sur AD DS, les fonctionnalités proposées dans AD DS, ainsi que sur les considérations d'ordre logiciel et matériel. Pour plus d'informations sur la planification, le déploiement et l'utilisation du rôle de serveur AD DS, et pour obtenir une référence technique qui explique comment AD DS fonctionne et les différents outils et paramètres que ces services utilisent.

Qu'est-ce que le rôle de serveur AD DS ?

AD DS fournit une base de données distribuée qui stocke et gère des informations sur les ressources réseau et les données spécifiques à des applications provenant d'applications utilisant un annuaire. Les administrateurs peuvent utiliser AD DS pour organiser les éléments d'un réseau, tels que les utilisateurs, les ordinateurs et les autres périphériques, en une structure hiérarchique de type contenant- contenu.

La structure hiérarchique de type contenant-contenu inclut la forêt Active Directory, les domaines inclus dans la forêt et les unités d'organisation (OU) de chaque domaine. Un serveur qui exécute AD DS est nommé contrôleur de domaine.

L'organisation des éléments d'un réseau en une structure hiérarchique de type contenant-contenu offre les avantages suivants :

- La forêt agit comme une limite de sécurité pour une organisation et définit l'étendue de l'autorité des administrateurs. Par défaut, une forêt contient un domaine unique, appelé également domaine racine de la forêt.
- Des domaines supplémentaires peuvent être créés dans la forêt pour assurer le partitionnement des données AD DS, ce qui permet aux organisations de répliquer des données uniquement là où cela est nécessaire. Cela permet le dimensionnement global des services AD DS sur un réseau disposant d'une bande passante limitée. Un domaine Active Directory prend en charge également plusieurs autres fonctions principales liées à l'administration, dont notamment l'identité des utilisateurs, l'authentification et les relations d'approbation à l'échelle du réseau.
- Les unités d'organisations simplifient la délégation de l'autorité pour faciliter la gestion d'un grand nombre d'objets. Par le biais de la délégation, des propriétaires peuvent transférer une autorité complète ou limitée sur des objets à d'autres utilisateurs ou groupes. La délégation est importante car elle aide à distribuer la gestion d'un grand nombre d'objets à plusieurs personnes chargées d'effectuer des tâches de gestion.

Fonctionnalités proposées dans AD DS

La sécurité est intégrée dans AD DS par le biais de l'authentification d'ouverture de session et le contrôle d'accès aux ressources de l'annuaire. À l'aide d'une ouverture de session réseau unique, les administrateurs peuvent gérer les données et l'organisation de l'annuaire par le biais de leur réseau.

Les utilisateurs réseau autorisés peuvent également utiliser une ouverture de session réseau unique pour accéder à des ressources à tout emplacement sur le réseau. L'administration basée sur des stratégies facilite même la gestion des réseaux les plus complexes.

Autres fonctionnalités des services AD DS :

- Un ensemble de règles, le schéma, qui définit les classes d'objets et les attributs contenus dans l'annuaire, les contraintes et les limites qui s'appliquent aux instances de ces objets, ainsi que le format de leurs noms.
- Un catalogue global qui contient des informations sur chaque objet de l'annuaire. Les utilisateurs et les administrateurs peuvent utiliser le catalogue global pour rechercher des informations dans l'annuaire, quel que soit le domaine de l'annuaire qui contient les données.
- Un mécanisme de requête et d'index, de sorte que les objets et leurs propriétés puissent être publiés et recherchés par les utilisateurs du réseau ou des applications.
- Un service de réplication qui distribue les données d'annuaire sur l'ensemble du réseau. Tous les contrôleurs de domaine accessibles en écriture dans un domaine participent à la réplication et contiennent une copie complète de toutes les informations d'annuaire liées à leur domaine. Toute modification des données d'annuaire est répliquée sur tous les contrôleurs de domaine inclus dans le domaine.
- Les rôles de maître d'opérations (également appelés opérations à maître unique flottant ou FSMO). Les contrôleurs de domaine qui détiennent des rôles de maître d'opérations sont désignés pour effectuer des tâches spécifiques pour assurer la cohérence et éliminer les entrées en conflit dans l'annuaire.

➢ *Services ADFS (Active Directory Federation Services)*

Vous pouvez utiliser le rôle de serveur AD FS (Active Directory Federation Services) du système d'exploitation Microsoft Windows Server 2008 pour créer une solution d'accès aux identités sécurisée, hautement évolutive et pouvant être étendue à Internet, qui peut fonctionner sur plusieurs plateformes à la fois, qu'il s'agisse d'environnements Windows ou non-Windows.

Qu'est-ce qu'AD FS ?

AD FS est une solution d'accès aux identités qui offre aux clients de navigateur (appartenant ou non à votre réseau) un accès transparent en une seule étape à une ou plusieurs applications protégées qui sont tournées vers Internet, même lorsque les comptes d'utilisateurs et les applications ne se trouvent pas du tout sur le même réseau ou dans la même organisation.

Lorsqu'une application se trouve sur un réseau et les comptes d'utilisateurs sur un autre, il est habituellement demandé aux utilisateurs de fournir des informations d'identification secondaires lorsqu'ils tentent d'accéder à l'application. Ces informations d'identification secondaires représentent l'identité des utilisateurs dans le domaine où réside l'application. Le serveur Web qui héberge l'application a généralement besoin de ces informations d'identification pour pouvoir prendre la décision d'autorisation la plus appropriée.

AD FS rend les comptes secondaires et leurs informations d'identification inutiles en fournissant des relations d'approbation que vous pouvez utiliser pour transmettre l'identité numérique et les droits d'accès d'un utilisateur aux partenaires approuvés. Dans un environnement fédéré, chaque organisation continue à gérer ses propres identités, mais peut aussi, en toute sécurité, transmettre et accepter des identités provenant d'autres organisations.

En outre, vous pouvez déployer des serveurs de fédération dans plusieurs organisations pour faciliter les transactions inter-entreprises (B2B) entre des organisations partenaires approuvées. Dans un partenariat inter-entreprises fédéré, chaque partenaire commercial est identifié selon les types d'organisation suivants :

- Organisation de ressource : les organisations qui possèdent et gèrent des ressources accessibles à partir d'Internet peuvent déployer des serveurs de fédération AD FS et des serveurs Web prenant en charge AD FS pour gérer l'accès aux ressources protégées pour les partenaires approuvés. Ces partenaires approuvés peuvent inclure des tiers externes ou d'autres services ou filiales de la même organisation.

- Organisation de compte : les organisations qui possèdent et gèrent des comptes d'utilisateurs peuvent déployer des serveurs de fédération AD FS qui authentifient les utilisateurs locaux et créent des jetons de sécurité que les serveurs de fédération de l'organisation de ressource utilisent ensuite pour prendre des décisions d'autorisation.

On appelle authentification unique (SSO) le processus consistant à s'authentifier sur un réseau tout en accédant à des ressources se trouvant sur un autre réseau, sans avoir à s'identifier plusieurs fois.

AD FS fournit une solution SSO basée sur le Web qui authentifie les utilisateurs dans plusieurs applications Web au cours d'une même session de navigateur.

Services du rôle AD FS

Le rôle de serveur AD FS inclut des services de fédération, des services de proxy et des services d'agent Web que vous configurez pour activer l'authentification Web SSO, pour fédérer les ressources

Web, pour personnaliser le processus d'accès et pour gérer la manière dont les utilisateurs sont autorisés à accéder aux applications.

En fonction des impératifs de votre organisation, vous pouvez déployer des serveurs exécutant n'importe lequel des services du rôle AD FS ci-dessous :

- Service de fédération : le service de fédération comprend un ou plusieurs serveurs de fédération qui partagent une stratégie d'approbation commune. Vous utilisez les serveurs de fédération pour acheminer les demandes d'authentification émises par les comptes d'utilisateurs d'autres organisations ou par des clients se trouvant n'importe où sur Internet.
- Proxy du service de fédération : le proxy du service de fédération fait office de proxy pour le service de fédération dans le réseau de périmètre (également appelé zone démilitarisée et sous-réseau filtré). Le proxy du service de fédération utilise les protocoles WS-F PRP (WS Federation Passive Requestor Profile) pour collecter les informations d'identification des utilisateurs auprès des clients de navigateur, puis envoie de leur part les informations d'identification au service de fédération.
- Agent prenant en charge les revendications : l'agent prenant en charge les revendications peut être utilisé sur un serveur Web hébergeant une application prenant en charge les revendications pour permettre l'interrogation des revendications des jetons de sécurité AD FS. Une application prenant en charge les revendications est une application Microsoft ASP.NET qui utilise les revendications présentes dans un

jeton de sécurité AD FS pour prendre des décisions d'autorisation et personnaliser des applications.

- Agent basé sur les jetons Windows : l'agent basé sur les jetons Windows peut être utilisé sur un serveur Web hébergeant une application basée sur une autorisation de jeton Windows NT pour prendre en charge la conversion d'un jeton de sécurité AD FS en jeton d'accès Windows NT d'emprunt d'identité. Une application basée sur une autorisation de jeton Windows NT est une application qui utilise des mécanismes d'autorisation basés sur Windows.

➢ *Services AD LDS (Active Directory Lightweight Directory Services)*

À l'aide du rôle Windows Server 2008 AD LDS (Active Directory® Lightweight Directory Services), anciennement appelé Active Directory Application Mode (ADAM), vous pouvez fournir des services d'annuaire aux applications utilisant un annuaire sans être soumis à la surcharge représentée par les domaines et les forêts, ou à l'obligation de disposer d'un schéma unique dans l'ensemble d'une forêt.

Consultez les sections suivantes pour en savoir plus sur le rôle de serveur AD LDS, ses fonctionnalités et les considérations logicielles et matérielles relatives à son installation.

Fonctionnalités du rôle de serveur AD LDS

Vous pouvez utiliser le rôle de serveur AD LDS pour créer plusieurs instances AD LDS sur un même ordinateur. Chaque instance s'exécute en tant que service distinct dans son propre contexte d'exécution. Le rôle de serveur AD LDS offre les fonctionnalités suivantes pour faciliter la création, la configuration et la gestion des instances AD LDS :

- Un Assistant qui vous guide tout au long du processus de création d'une instance AD LDS ;
- des outils en ligne de commande pour effectuer une installation ou une suppression sans assistance d'instances AD LDS ;
- des composants logiciels enfichables MMC (Microsoft Management Console) pour configurer et gérer les instances AD LDS, y compris le schéma de chaque instance ;
- des outils en ligne de commande spécifiques à AD LDS pour gérer, peupler et synchroniser les instances AD LDS.

➢ *Services AD RMS (Active Directory Rights Management Services)*

Active Directory Rights Management Services (AD RMS) et le client AD RMS permettent de renforcer la stratégie de sécurité d'une organisation en protégeant les informations en appliquant en permanence des stratégies d'utilisation aux informations, même si ces dernières sont déplacées. Vous pouvez utiliser AD RMS pour renforcer la protection des informations sensibles, telles que les rapports financiers, les spécifications de produits, les données des clients et les messages électroniques confidentiels, afin d'empêcher des personnes non autorisées d'avoir accès à ces informations accidentellement ou non.

Fonctions des services AD RMS

Vous pouvez configurer les composants suivants d'AD RMS à l'aide du Gestionnaire de serveur :

- Services AD RMS (Active Directory Rights Management Services). Le service de rôle Active Directory Rights Management Services (AD RMS) est un service de rôle obligatoire qui installe les composants AD RMS permettant de publier du contenu protégé par des droits et d'y accéder.
- Prise en charge de la fédération des identités. Le service de rôle de prise en charge de la fédération des identités est un service de rôle facultatif permettant aux identités fédérées d'accéder à du contenu protégé par des droits à l'aide des services de fédération Active Directory (ADFS, Active Directory Federation Services).

GLOSSAIRE

VPN: virtual private network

DES : Data Encryption Standard

AH: Authenticati Header

ESP: Encapsulating Security Payload.

WAN: Wide Area Network.

LAN: Local Area Network

MAN: Metropolitan Area Network

OSI: Open System Interconnections

ISO : International Standard Organisatior

IP : Internet Protocole

ARP : Adresse Résolution Protocole

FTP : File Transfert Protocole

SMTP: Simple Mail Transfert Protocole

IGP: Interior Gateway Protocol

VLAN: virtual local area network

PEAP: Protected Extensible Authentication Protocc

RRAS: Routing and Remote Access

HTTP: HyperText Transfer Protocol

TLV: Type Length-Value

IDS: Intrusion Detection System

EAP: Extensible Authentication Protocol

DSL: Digital Subscriber Line

PPTP: Point-to-Point Tunneling Protocol

L2TP: Layer Two Tunneling Protocol.

RPC: Remote Procedure Call

MS-CHAP v2: PEAP-Microsoft Challenge Handshake Authentication Protocol version 2

IPsec: Internet Protocol Security

PPP: Point-to-Point Protocol

SSL: Secure Socket Layer

SSH: Secure Shell

TCP: Transmission Control Protocol

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

UDP: User Datagram Protocol

SHA: System Health Agent

SHV: System Health Validator

SoH: Statement of Health

RADIUS: Remote Authentication Di -In User Service

API: Interface programming application

NPS: Network Policy Server

SMS: Systems Management Server

IAS : Internet Authentication Service

QES : Quarantaine Enfoncement Server

QEC : Quarantine Enforcement Client

IAS: Internet Authentication Service

IIS: internet information service

PKI : Public Key Infrastructure

CA : Certification Autori

Bibliographie

Thèses :

Mr :Haddad. A. Mlle .ALICHE Sonia: « Implémentation d'une politique de sécurité au niveau de département informatique de l'entreprise ENIEM de Tizi-Ouzo»,ELN ,Ummto ,these master,…,2010\2011

Mokrane A : « Implémentation du protocole d'authentification 802.1x avec le serveur RADIUS dans les réseau informatique ».ELN ,ummto,these master,2010/2001

Livres

-P. FREDDI : « Windows Server 2008 MCTS 70-642 - Configuration d'une infrastructure réseau », Edition eni, année 2008.
-T. DEMAN Freddy, E. Mathieu, CH. S.NEILD : « Windows Server 2008 Administration avancée » édition eni année 2010.

Sites internet

http:/go.microsoft.com/fwlink/ ?linkld=85897

http:/www.microsoft.com/toutwindows/ ?linkld=85897