Chapitre II

Microsoft Forfront Unified Acces Gateway et Direct Access

I. Microsoft Forefront Unified Access Gateway (UAG)

Avant d'entamer notre projet consistant à mettre en place un serveur UAG qui est un pare-feu et une passerelle d'accès aux applications, il semble pertinent de commencer par préciser qu'est-ce qu'un serveur UAG et de définir quel rôle peut-il jouer dans l'amélioration du HCEFLCD.

I.1. Historique

Historiquement, le premier produit de la gamme Forefront produit chez Microsoft, était Microsoft Internet Security and Acceleration Server 2006, le pare-feu de Microsoft intégrant des fonctionnalités de filtrage avancés aussi bien au niveau réseau qu'applicatif.

C'est en 2006 que Microsoft a racheté la société Whales Communications et son produit « Intelligent Application Gateway and Application Optimizers ». Ce produit se caractérise par le fait d'embarquer ISA Server 2004 pour ses fonctions de pare-feu avancés ainsi que pour se protéger lui-même, rien de plus. Fin 2009, Microsoft a mis à disposition le successeur d'ISA Server : Forefront Threat Management Gateway 2010.

Tout naturellement, Microsoft se devait de proposer une nouvelle version d'IAG. Ce fut chose faîte fin 2009 avec Forefront Unified Access Gateway 2010, réutilisant Forefront TMG 2010 pour se protéger.

I.2. Présentation de Forefront UAG

Forefront Unified Access Gateway assure un accès sécurisé aux ressources de l'entreprise quel que soit leur emplacement ou les terminaux utilisés, y compris les PC et appareils mobiles, gérés ou non, fortement inspiré de Microsoft Intelligent Application

Gateway, Forefront UAG combine diverses options de connectivité du VPN SSL au Windows DirectAccess avec des configurations et des stratégies prédéfinies de protection. Ainsi, Forefront UAG simplifie et centralise l'administration pour en réduire les coûts.

Forefront UAG est un produit un peu différent des autres chez Microsoft car il se positionne sur plusieurs tableaux :

- La publication de ressources de l'entreprise à l'extérieur ;
- La sécurisation des accès aux ressources internes de l'entreprise.

Forefront UAG s'appuie sur une connaissance approfondie des applications publiées, une analyse de l'état des appareils utilisés pour y accéder et l'identification de l'utilisateur, pour assurer un contrôle d'accès fin et précis. De plus, Forefront UAG, il est évolutif. Si une méthode d'authentification n'existe pas, rien ne nous empêche de la développer. UAG bénéficie donc d'une souplesse remarquable.

Une des plus grandes améliorations dont bénéficie Microsoft Forefront UAG en comparaison avec Forefront TMG est la capacité de fournir un portail Web pour les utilisateurs de l'Internet qui ont besoin d'accéder aux applications internes.

Forefront UAG utilise une terminologie appelé « trunk Portal ». Un tronc est une combinaison d'une adresse IP, le port HTTP / HTTP et un certificat quand un tronc HTTPS doit être créé. Le tronc portail est le point d'entrée pour toutes les applications publiées dans ce portail. Il est possible de s'authentifier sur ce portail en utilisant différents services d'annuaires comme Active Directory, Netscape et plus encore. Un tronc portail permet également à l'administrateur de Forefront d'appliquer les politiques d'accès Endpoint UAG. Une politique d'accès Endpoint est en mesure de vérifier l'état de conformité du client. Par exemple, le client doit avoir le Pare-feu Windows activé, toutes les mises à jour Windows doivent être installées sur la machine et la machine doit être joint au domaine Active Directory interne.

I.2.1. Accès en tout lieu

Quel que soit l'emplacement des utilisateurs ou des terminaux utilisés, Forefront UAG sert de passerelle consolidée via un portail unique.

Forefront UAG Simplifie et sécurise l'accès à distance, il prend en charge une vaste gamme d'applications Microsoft (Microsoft SharePoint®, Microsoft Exchange Server, Remote Desktop Services et Microsoft Dynamics® CRM) via des modules d'optimisation prédéfinis. Ces modules analysent le comportement des applications, des interactions navigateur-serveur et des exigences de l'appareil utilisé pour créer des paramètres optimaux et des règles de sécurité spécifiques.

De plus, UAG met DirectAccess à la portée des applications et des ressources exécutées sur l'infrastructure existante, il prend en charge les postes clients de version antérieure ou non-Windows via un VPN SSL ou une autre connexion.

I.2.2. Sécurité intégrée

Afin d'améliorer la sécurité et de renforcer la conformité de l'entreprise, Forefront UAG limite l'exposition avec des contrôles d'accès fins, permet d'une part, une analyse détaillée de l'état des terminaux et des autorisations de l'utilisateur. D'autre part, il permet aux administrateurs d'élaborer des règles précisant les conditions que les postes clients doivent remplir à chaque transaction.

I.2.3. Administration simplifiée

Forefront UAG Offre plus de souplesse en proposant plusieurs types d'équipements dont des appliances matérielles, des appliance virtuelles ou des logiciels serveurs. Il facilite le regroupement de plusieurs serveurs Forefront UAG en une grille dont tous les membres partagent la même configuration et qui sont gérés comme une seule entité. Il utilise aussi des assistants pour simplifier le déploiement initial et les tâches courantes. Et il s'intègre à Microsoft SQL Server et à System Center Operations Manager pour simplifier respectivement la journalisation et l'administration.

II. Forefront UAG et DirectAccess

Forefront Unified Access Gateway (UAG) DirectAccess supporte les dernières innovations de Microsoft dans le domaine de mobilité, en particulier il intègre le DirectAccess. Forefront UAG DirectAccess permet aux utilisateurs distants avec l'expérience d'une connexion transparente au réseau interne en tout moment d'avoir accès à

Internet. Lorsque Forefront UAG DirectAccess est activé, les demandes de ressources réseau interne (telles que les serveurs de courrier électronique, les dossiers partagés, les serveurs de gestion, ou les sites Web intranet) sont bien dirigées vers le réseau interne, sans avoir besoin de se connecter à un VPN.

II.1. C'est quoi DirectAccess ?

DirectAccess permet de se connecter à distance au réseau de son entreprise. Cependant, cela diffère d'une connexion VPN puisqu'il n'y a pas besoin d'établir une connexion dans le gestionnaire de connexion. Une fois connecté, l'utilisateur accède au réseau comme s'il était à son entreprise.

Grâce à DirectAccess, il est possible de manager facilement le parc d'ordinateurs d'une entreprise puisque les mises à jour des GPO ou les mises à jour software par exemple, se feront indépendamment de la connexion ou non d'un utilisateur. L'ordinateur client est donc constamment à jour avec les normes de sécurité de l'entreprise. L'interconnexion entre les postes se fait donc de façon bilatéral.

IPsec et IPv6 qui sont utilisés pour DirectAccess permettent notamment une encryption des données en utilisant différents algorithmes comme AES ou 3DES. Ainsi les communications restent protégées. Mais il est aussi possible de décider à quelles applications ou quels serveurs auront accès les utilisateurs.

II.2. Le puzzle DirectAccess

DirectAccess est un sujet à la fois simple et complexe. C'est simple car ce n'est que l'assemblage de technologies existantes, c'est complexe car il faut en maîtriser l'assemblage. Nous sommes donc en face d'un puzzle qui, une fois assemblé, donne entière satisfaction. Passons en revue les pièces qui le composent :

- **IPv6 :** DirectAccess est basé nativement sur le couple IPv6 / IPsec. Bien évidemment, la technologie IPv4 étant encore massivement répandue et IPv6 n'étant pas près de la remplacer avant plusieurs années, des technologies ont été mises au point afin d'encapsuler des paquets IPv6 dans des paquets IPv4 ;
  En fonction du type de réseau il est préférable d'utiliser certaines technologies :

Scénario	*Protocole*	*Technologie*
Adressage IPv6 sur le réseau Interne de l'entreprise reposant sur IPv4	**ISATAP**	Encapsule le trafic IPV6 dans des trames IPv4
Poste de travail avec connectivité internet publique	**6to4**	Encapsule le trafic IPV6 dans des trames IPV4
Poste de travail avec connectivité Internet assurée par un mécanisme de translation (NAT)	**Teredo**	Encapsule le trafic IPV6 dans le protocole UDP
Poste de travail disposant d'une connectivité Internet limitée à HTTPS	**IP-HTTPS**	Encapsule le trafic IPV6 dans le protocole HTTPS
Résolution de noms DNS interne	**DNS64/NAT64**	Assure la résolution des noms DNS internes et met en place une translation pour les systèmes non compatibles avec IPV6

Tableau n° 2: technologies de transition vers IPv6

- **IPSec :** la sécurisation des flux de données échangées entre un client en situation de mobilité et le réseau interne de l'entreprise repose sur des tunnels IPSEC. On distinguera plusieurs types de tunnels IPSEC :

  - Tunnel d'infrastructure : Ce premier tunnel est initialisé par le système d'exploitation entre le client DirectAccess et le serveur Microsoft Forefront Unified Access Gateway. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi que sur une authentification. Ce tunnel est limité au système d'exploitation pour lui permettre d'accéder à des ressources d'infrastructure (DNS, Antivirus, …) et d'administrer le poste de travail ;

  - Tunnel utilisateur : Ce second tunnel est initialisé par l'utilisateur quand il tente d'accéder à une ressource de l'entreprise. Il est initialisé entre le client DirectAccess et le serveur Microsoft ForeFront Unified Access Gateway. L'authentification de ce tunnel repose sur le certificat « ordinateur » ainsi que sur l'authentification. Ce tunnel est dédié à

l'utilisateur pour accéder aux ressources internes de l'entreprise. Il est possible de mettre en œuvre une authentification forte à ce niveau ;

- Tunnel application : Ce dernier type de tunnel est optionnel. Il permet de configurer un groupe de serveurs de l'entreprise pour établir un tunnel IPSEC qui se terminera sur ces serveurs. L'intérêt de cette démarche est de pouvoir exiger d'appliquer de nouveaux critères pour l'authentification (utilisateur ou ordinateur appartenant à un groupe donné, authentification carte à puce obligatoire, exigence de conformité du poste de travail, …).

- **Pare-Feu personnel :** Depuis Windows Vista, le pare-feu personnel du système d'exploitation intègre la prise en charge d'IPSEC. Pour cette raison, il est nécessaire de conserver un pare-feu sur le poste de travail. Côté client, celui du système d'exploitation peut être conservé, Côté serveur, c'est la même chose. nous conservons le pare-feu personnel de Windows Server 2008 R2 ;

- **Systèmes d'exploitation :** côté client seules les éditions Entreprise et Ultimate de Windows 7 sont éligibles à DirectAccess, ces systèmes sont nécessairement membre d'un domaine. Côté serveur, les seuls systèmes d'exploitation supportés sont Windows Server 2008 R2 standard et ultérieurs;

- **Name Resolution Policy Table :** comment s'effectue la résolution de noms DNS? La résolution des noms DNS interne repose : côté client, sur la «Name Resolution Policy Table ». La configuration mise en place dans la NRPT indique que la résolution des noms DNS est assurée par un hôte IPv6 qui est en fait le serveur UAG. DNS64/NAT64 récupère alors les demandes de résolution de noms DNS et assure le traitement de la manière suivante :

  - Demande de résolution du nom DNS en IPv6 et IPv4 ;
  - Si la réponse retournée est directement en IPv6 alors l'information retourne au client ;
  - Si la réponse est uniquement IPv4 dans ce cas l'information est transmise à NAT64 ;

- NAT64 va par la suite générer une adresse IPv6 temporaire et assurer la correspondance avec l'adresse IPv4;
- Finalement, l'information IPv6 est retournée au client.

- **Network Location Server :** est un serveur Web qui va héberger une URL de localisation accessible via HTTPS seulement depuis l'intranet de l'entreprise. Il montrera que nous avons accès au réseau interne ;

- **Forefront Unified Access Gateway :** Certes, il est possible de faire du DirectAccess sans UAG, mais l'utilisation de ce dernier sera plus avantageuse D'abord, vu sa capacité d'assurer la haute disponibilité. Ensuite, parce qu'il permet la répartition de charge matérielle ou logicielle au sein de la ferme UAG. Et enfin, parce qu'il propose également un portail d'applications publiées avec prise en charge du SSO, etc.

- **DirectAccess Connectivity Wizard :** est un composant optionnel mais tellement nécessaire pour l'utilisateur final. DirectAccess est tellement transparent pour l'utilisateur au point qu'il ne sait pas si cela fonctionne ou non. Pour régler cet problème, Microsoft a mis à disposition avec le Microsoft ForeFront Unified Access Gateway une version du « DirectAccess Connectivity Wizard » ;

- **Network Access Protection :** Composant optionnel, servant à encourager la mise en conformité des ordinateurs aux spécifications de sécurité et d'intégrité, et sert aussi à réduire le risque de dissémination des programmes malveillants. Les ordinateurs non conformes peuvent être interdits d'accès aux ressources intranet ou de communication avec les ordinateurs conformes ;

- **Authentification double facteur :** Plus personne ne propose de solution de nomadisme sans prise en charge d'un ou de plusieurs moyens d'authentification à double facteur (ce que je détiens et ce que je sais voire qui je suis). DirectAccess n'échappe pas à cette règle. Avec Microsoft ForeFront Unified Access Gateway 2010, les possibilités ont été accrues. L'authentification du tunnel IPSEC « utilisateur » peut désormais exploiter :

- Une authentification par carte à puce ;
- Un mécanisme d'authentification de type « One Time Password » (OTP).

Ci-après le montage du puzzle pour un meilleur fonctionnement :

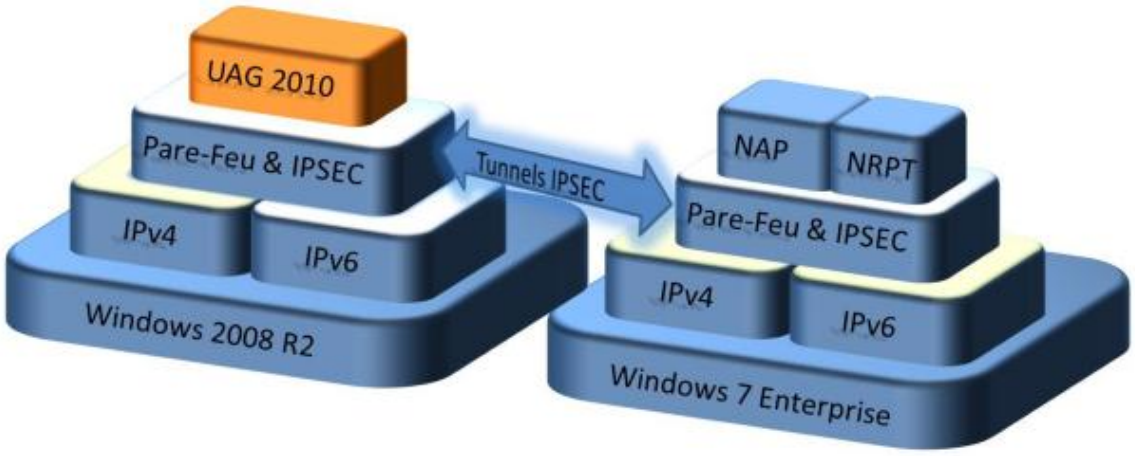

Figure n° 7: Le puzzle DirectAcceess

II.3. Les avantages du déploiement DirectAccess et Forefront UAG Ensemble

Lorsque Windows DirectAccess et Forefront UAG sont déployées ensemble, elles offrent une solution de sécurité d'accès améliorée et unifiée à travers ainsi que au-delà de l'environnement de l'entreprise. La valeur combinée de ces deux technologies permet aux services informatiques de fournir une meilleure productivité de l'utilisateur en établissant un équilibre entre l'exposition des ressources d'entreprise vers le monde extérieur et permet aussi de maintenir la sécurité et la conformité réglementaire. Forefront UAG s'allie à DirectAccess pour :

- Etendre ces bénéfices aux systèmes de version antérieure ou non-Windows via un VPN SSL et d'autres types de connexion ;
- Limiter les risques liés à la connexion de systèmes non gérés, de version

antérieure ou non-Windows, à l'aide de contrôles d'accès très fins ;

- Protéger la passerelle DirectAccess avec une solution Edge renforcée et un pare-feu intégré ;
- Simplifier le déploiement avec des assistants et des outils intégrés ;
- Assurer la montée en charge et l'administration à l'aide de groupes de serveurs et d'un équilibrage de la charge.

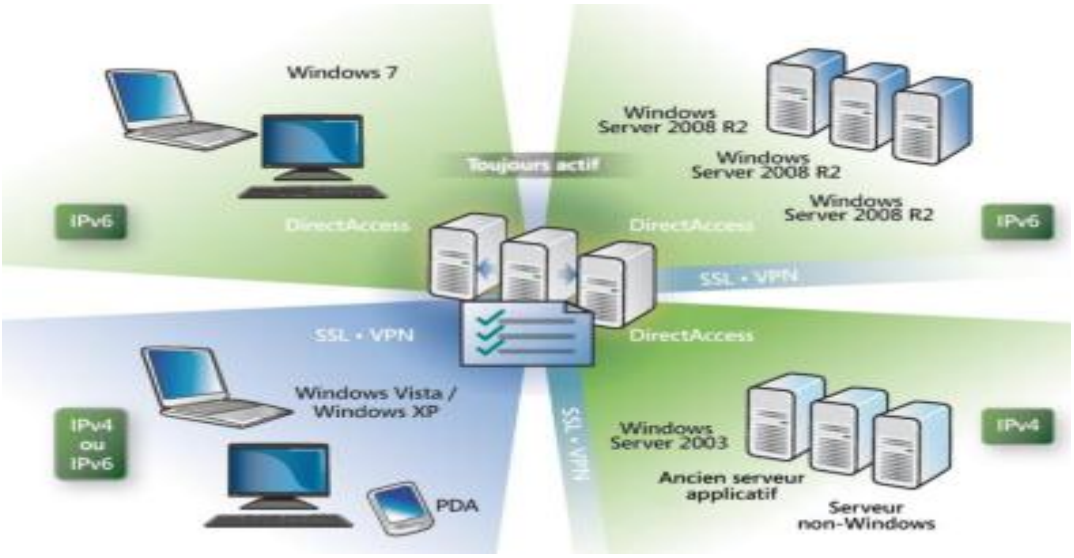

Figure n° 8: Forefront UAG et DirectAccess