# Chapitre III

# Mise en place du serveur UAG

## I. Prérequis

Les exigences matérielles, du système et logiciels, requises pour l'installation et le déploiement Forefront Unified Access Gateway (UAG) sont les suivants :

## I.1. Prérequis matériel

- Processeur : 2,66 gigahertz (GHz) ou processeur plus rapide. CPU dual core ;
- Mémoire : 4 Go ;
- Disque dur : 2,5 gigaoctet (Go) (en plus des exigences de Windows).
- Cartes réseau : Deux cartes réseaux qui sont compatibles avec le système d'exploitation de l'ordinateur. Ces cartes réseaux sont utilisées pour la communication avec le réseau interne de l'entreprise, et le réseau externe (Internet).

## I.2. Prérequis logiciel

 Système d'exploitation : Forefront UAG peut être installé sur les ordinateurs exécutant le serveur standard Windows 2008 R2 ou Windows Server 2008 R2 Enterprise, systèmes d'exploitation 64 bits.

## II. Environnement de mise en place

## II.1. Environnement Matériel

Nous avons mis en place notre plateforme sur une lame de processeur **Intel Xeon E5540 @ 2,53 (16 CPUs)**, de disque dur de **300** Go et une RAM de **14** Go, de l'infrastructure de HCEFLCD basée sur HP BladeSystem de modèle Proliant BL460c G6.

MCours.com

## **II.2.** Environnement Logiciel

- Système d'exploitation : Windows Server 2008 R2 X64 ;
- Rôle : HyperV qui est un système de virtualisation.

## III. Architecture

L'architecture de la plateforme Forefront UAG et DirectAccess est la suivante :



## Figure n° 9: Plateforme Forefront UAG et DirectAccess

## **III.1.** Descriptif de l'architecture

- La machine virtuelle DC : joue le rôle du contrôleur du domaine
  - ▶ Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine
  - Mise à jour du système et Activation
  - Paramétrage IPv4 (192.168.10.3)
  - Paramétrage IPv6 : la machine est en ISATAP
  - Ajout du Rôle AD Domain Services
  - > DCPROMO : création du domaine forestierST.ma ;
  - création reverse zone DNS ;

- Installation du Rôle AD CA ;
- Création d'un modèle de certificat DirectAccess IPsec EndPoint ;
- Création d'un modèle de certificat DirectAccess IPsec Tunnel ;
- Création d'un modèle de certificat Web Server exportable ;
- Modification de la GPO Default Domain Policy avec des règles autorisant sur le Pare-feu Windows : Echo Request ICMPv4 et v6 ;
- Config du DNS pour supprimer le nom ISATAP de la default global blocklist ;
- ➢ Config des CRLs ;
- Modification de la GPO default domain policy pour auto enrollment des certificats ordinateurs ;
- Création d'un groupe de sécurité DA\_Clients dans l'Active Directory (Client-PC est membre de ce groupe);
- Création d'un groupe de sécurité DA\_Servers dans l'Active Directory (UAG est membre de ce groupe).

## • La machine virtuelle WEB01 : joue le rôle de NLS

- ▶ Installation du système Windows server 2008 R2 ;
- Changement du nom de machine ;
- Mise à jour du système et activation ;
- Paramétrage IPv4 (192.168.10.5);
- Paramétrage IPv6 : la machine est en ISATAP
- Ajout dans le domaine forestierST.ma ;
- > Demande de certificat de type Web Server exportable ;
- Installation du rôle Web Server ;
- > Binding du certif SSL sur le site web par défaut.

# • La machine virtuelle CRL: joue le rôle de serveur Web servant la liste des certificats révoqués

- Installation du système Windows server 2008 R2 ;
- Changement du nom de machine ;
- Mise à jour du système et activation ;
- Paramétrage IPv4 (192.168.10.6) (131.168.6.41);

- Paramétrage IPv6 : la machine est en ISATAP ;
- Ajout dans le domaine ForestierST.ma ;
- Installation du rôle Web Server.
- La machine virtuelle UAG: joue le rôle de serveur Forefront UAG et de passerelle DirectAccess
  - Installation du système Windows server2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et Activation ;
  - paramétrage IPv4 (192.168.10.2) (131.168.6.38);
  - > paramétrage IPv6 : la machine est en ISATAP ;
  - Ajout dans le domaine ForestierST.ma ;
  - Demande de certificat complémentaire de type Web Server (pour IP-HTTPs);
  - Installation de Forefront UAG (nous allons expliquer les détails de cette installation ultérieurement).
- La machine virtuelle DNS: joue le rôle de serveur DNS publique ainsi que de serveur Web publique
  - Installation du système Windows server 2008 R2 ;
  - Changement du nom de machine ;
  - Mise à jour du système et Activation ;
  - ➢ paramétrage IPv4 (131.168.6.40).

## • La machine virtuelle, Client-Pc est un client Windows 7 Entreprise, configurée comme client DirectAccess

- Installation de WIN7DA
- Ajout dans le domaine ForestierST.ma ;
- Deux interfaces réseau (LAN, WAN)

Adresse sur la carte WAN : 131.168.6.33

Adresse sur le LAN : 192.168.10.4

## IV. Installation et configuration du serveur Forefront UAG

Une fois toutes les machines installées, nous allons passer à la préparation de la machine UAG qui va exécuter Forefront Unified Access Gateway.

Lors de l'installation de Forefront UAG, vous devez disposer des autorisations d'administrateur sur le serveur local. Vous devez également, être un utilisateur du domaine auquel appartient le serveur Forefront UAG,

Quand toutes ces conditions sont remplies nous pouvons commencer le processus d'installation.



## Figure n° 10: Installation de Forefront UAG

Durant l'installation, nous veillons à lire l'accord de licence d'utilisation et à le valider, puis, nous définissons l'emplacement d'installation de Forefront UAG. Alors que l'installateur s'occupe d'installer les rôles et les composantes nécessaires, ainsi qu'il installe Forefront TMG packagé spécialement pour UAG et qui joue le rôle de pare-feu réseau et protège la machine.



### Figure n° 11: Installation avancée de Forefront UAG

Une fois, l'installation terminée il est nécessaire d'effectuer un redémarrage, Après le redémarrage, nous pouvons ouvrir la console d'administration de Forefront UAG.

L'assistant de configuration nous permet d'accéder à certains paramètres de configuration réseau de base comme les paramètres de la carte réseau et ceux de la topologie du serveur UAG.

Hierosoft Forefront Unified Access date	way Hanagement	X
Berefront Unified Access Gateway UAS01 HTTP Connections HTTPS Connections		
Contract Access	Getting Started Warrel  Welcome to Hicrosoft Forefront Unified Access Gateway 2010  This ward helps you configure your network settings and system policies.	X
	Configure Network Settings Specify how Forefront UAG is connected to your network.	
	Define: Server: Topology Optionally join this Forefront UAG server to an array.	
	Join Microsoft Update Optionally join Microsoft Update to receive updates for Forefront UAG.	
	Qose	
Messare Time Messare Turu	Messare	
resage the		
Ready		0

Figure n° 12 : Assistant de configuration

Définir les réglages des cartes réseaux est important pour informer l'UAG à la fois du type de la carte réseaux qui se connecte au réseau interne (confiance) et de celle qui se connecte au réseau externe (non fiable).

Adapter name	Internal	External	Unassigned
LAN	- <b>-</b>		
WAN		~	
Adapter name: LAN IP DHCP enabled: No IP address: 192.168.10.2			

Figure n° 13: Définir les adaptateurs réseau

Ensuite nous allons choisir la topologie utilisée : ferme de serveurs UAG ou bien machine indépendante.

Select Configuration
Specify whether this is a single Forefront UAG server, or configure it as an array member.
Single server
C Array member
Forefront UAG array members must belong to a domain.
< Précédent Suivant > Annuler

Figure n° 14 : Définir la topologie du serveur UAG

La dernière étape de configuration consiste à activer la mise à jour via Microsoft Update (si ce n'est pas déjà fait)



Figure n° 15 : Activation des mises à jour

Et voilà, l'installation est presque prête, il reste à activer la configuration (opération classique pour les administrateurs IAG/UAG).

1	Specify how Forefront LIAG is connected to your network
	You have completed the Getting Started Wizard. You can run this wizard again to make changes to the configuration. Do you want to activate the configuration now?
	Oui Non

Figure n° 16: Demande d'activation

Et là c'est réellement terminé, le serveur Forefront UAG est prêt à être configuré pour les accès distants (Portail, Passerelle Terminal Server, VPN, DirectAccess).

## IV.1. Configuration de DirectAccess

Avant de commencer la configuration du DirectAccess, il faut s'assurer que toutes les conditions préalables ont été remplies. Sinon les étapes de l'assistant ne seront pas achevées convenablement.



## Figure n° 17 : Console DirectAccess dans Forefront UAG

Nous voulons permettre aux clients DirectAccess de se connecter aux ressources internes et nous souhaitons aussi lui permettre la gestion à distance des ordinateurs DirectAccess comme le montre la capture d'écran ci-dessous.



Figure n° 18 : Activer DirectAccess pour accéder aux ressources internes

Après avoir activé DirectAccess pour les ordinateurs clients de notre infrastructure Active Directory, maintenant nous devons sélectionner le domaine auquel nous désirons activer DirectAccess.





Forefront UAG crée automatiquement trois objets de stratégie de groupe qui seront liés plus tard au plus haut niveau du domaine Active Directory et filtrés par filtrage de sécurité de stratégie de groupe. Les administrateurs sont en mesure de modifier les paramètres par défaut.

Clients and GPOs Configur	POs Configuration			Ac		
Deployment Model Client Domains Policy Management Client Groups	Forefront UAG uses GPOs and application servers. U existing GPOs you have de	Forefront UAG uses GPOs to deliver UAG DirectAccess policy settings to client computers, the UAG DirectAccess server, and application servers. UAG DirectAccess can create the GPOs automatically, or you can save policy settings to existing GPOs you have designated for DirectAccess.				
chelic Groups	GPO	Name	Location			
	Clients	UAG DirectAccess: Clients (WIN-6A8R0JTN91.FORESTIER	forestierST.ma			
	Gateway Application Servers	UAG DirectAccess: Gateways (WIN-6A8R0JTN9LFOREST UAG DirectAccess: AppServers (WIN-6A8R0JTN9LFORES	forestierST.ma forestierST.ma			
			Modify	s		
	C Save the UAG DirectAc	cess settings to these existing GPOs:				
	GPO	Name	N			
	Clients Gateway Application Servers					
			Assign			

Figure n° 20 : Création automatiquement des objets de stratégie de groupe

Il est possible d'activer DirectAccess pour un groupe de sécurité Active Directory ou pour les unités d'organisation (UO).

Forefr	ont UAG			
→ Dire	Clients and G	POs Configuration		Acces
	Deployment Model Client Domains	From the client computer domains, select organ will be allowed to connect using UAG DirectAcc	nizational units (OU) or security groups containing clients the ess. Client GPO policy settings are applied to these	at
	Policy Management	Sélectionnez un groupe	<u>? ×</u>	
	Client Groups	Sélectionnez le type de cet objet :		
		un groupe	Types d'objets	
		A partir de cet emplacement :		
		forestierST.ma	Emplacements	
		Entrez le nom de l'abjet à sélectionner (exemples) :	Add	
		DA client	Vérifier les noms Remove	s
		Aurorat 1	OK Annufar	
		Avance		
	Lange more		< Back Navt > Finish	Concel

Figure n° 21: Activer DirectAccess pour groupe

Maintenant nous allons activer l'assistant de Connectivité de Client, qui constitue une aide visuelle pour l'utilisateur connecté en DirectAccess.

	tion ivity Assistant Configuration	Acces
Client Connectivity Connection Verification Troubleshooting Portal Diagnostic Logging	Specify connectivity and troubleshooting settings for the DirectAccess Connectivity Assistant. Settings are stored in the client GPO, and applied on DirectAccess client computers running the DirectAccess Connectivity Assistant application: To you want to configure settings for the DirectAccess Connectivity Assistant application?	5
Learn more	< Back Next > Finish Cance	

Figure n° 22 : Assistant de configuration du client connectivité

Il est possible de définir des vérificateurs de connectivité qui permettent de savoir si le client DirectAccess dispose d'un accès aux ressources hébergées dans le système d'information.

Forefront UAG	ents and GPOs Configuration	ity Assistant Configuration		Acces
Clier Cont Trou	nt Connectivity nection Verification bleshooting Portal	Select how connectivity between DirectAccess cli verified. When connectivity verification fails, a no of the DirectAccess client computer. Connectivity verifiers:	ients and the internal network is automatically tification is displayed in the taskbar notification are	a
Diag	nostic Logging	Address	Method	
		http://WEB01.forestierST.ma	нттр	
				Add
				Edit.
				Remove

Figure n° 23: Vérification du client connectivité

Forefront UAG DirectAccess nécessite deux Internet conducteur face adresses IPv4. Et en ce qui concerne l'adresse IP interne du serveur Forefront UAG nous devons créer un enregistrement d'hôte avec le nom ISATAP dans le DNS interne zone de recherche directe de notre infrastructure Active Directory.

Nous avons pris en considération toutes ces mesures et conditions comme nous avons également supprimé ISATAP de la liste des blocs de requête : DNS mondial. Pour pouvoir accéder aux éléments de paramétrage du serveur DirectAcces.

Forefre	UAG DirectAccess Server Config	guration		× Acce
Dire		s Server Configuration		nece.
	UAG Directacces	s server configuration		
	Connectivity			ers
	IP-HTTP5 Certificate	To set up the UAG DirectAccess server, assign IP address	es to the Internet-facing and internal networks.	
	IPsec Certificate Authentication	Internet-facing First Internet-facing IPv4 address:	DirectAccess Internal rebustk Internal Internal IP-A address used when ISATAP is declarated on the IIAG DirectAcress sense:	
		131.168.6.38	192.168.10.2	s
		Second Internet-facing IPv4 address: 131.168.6.39	Internal IPv6 address:	
		ISATAP IPv6 transition technologies will be en DNS name TSATAP' with "192.168.10.2" on the these domains. In addition ensure that ISATAP DNS servers.	abled on the UAG DirectAccess server. Register the DNS in all domains to enable IPv6 connectivity on is not blocked in the <u>Global Query Block List</u> on all	

Figure n° 24: Configuration des adresses IP

L'étape suivante consiste à sélectionner le certificat de serveur utilisé pour authentifier les clients DirectAccess. Le certificat en question est utilisé pour IP-HTTPS. Il s'agit de la dernière technologie de transition utilisée par un client DirectAccess lorsque la connectivité IPv6 native ou une connexion Teredo n'est pas possible.



Figure n° 25: Certificat pour IP -HTTPs

Les clients DirectAccess nécessitent un certificat d'ordinateur pour établir un tunnel d'infrastructure IPsec, maintenant nous sommes appelées à sélectionner le CA qui va délivrer des certificats pour l'authentification IPsec.



Figure n° 26: Certificat racine

Durant la prochaine étape, nous devons spécifier l'URL utilisé par les clients DirectAccess pour déterminer leur connectivité au réseau d'entreprise ou à Internet.



Figure n° 27: URL pour NLS

L'étape suivante est importante vu que durant elle que s'effectue la résolution des noms DNS internes pour les clients DirectAccess connectés à l'Internet. Les suffixes DNS que nous allons spécifier ici seront résolus par Forefront UAG DNS64.

ont UAG To Infrastructure Server Configu Infrastructure Se	uration erver Configuration	م ا×
Network Location Server	Enter the name suffixes and IP addr	esses of internal DNS servers used to resolve DNS suffix queries.
UNS Surfixes	Name Suffix	IP address of DNS Server
Authentication Domains	.forestierST.ma	[DNS64]
Management Servers	nls.forestierst.ma	[Excluded]
	* Double-click here to add.	
	Select a local name resolution opti C Only use local name resolution Eall back to local name resolution	s If the name does not exist in DNS (most restrictive) ion if the name does not exist in DNS or the DNS servers are mputer is on a private network (recommended)

## Figure n° 28: Résolution du nom via Forefront UAG

L'assistant suivant permet aux administrateurs d'ajouter des serveurs de gestion interne. Ces serveurs de gestion sont en mesure d'accéder au client DirectAccess après l'établissement du premier tunnel IPsec (le tunnel d'infrastructure).

bcef-lab - C	Connexion Bureau à distance				
🖳 UAG2-lab su	ur localhost - Connexion à un ordin	ateur virtuel			_ 🗆 🗙
Fichier Action	Support Presse-papiers Affichage	Aide			
3 0 0 (	0 0 11 12 35 5				
Microsoft Fe	orefront Unified Access Gateway M	lanagement			- 12 -
File View Adn	nin Messages Help				
E S Forefro	ont UAG			xil.	
Direc	Infrastructure Se	rver Configuration	s to DirectAccess clients. Add internal mana	igement servers to	ccess
	DNS Suffixes	discoverable built-in groups, and user-defined gro	oups.	100000	
	Authentication Domains	Add Group 🥂 🔍 Refresh All	Add Server - Do	Select All	
	Management Servers	Access Enabling Groups:	Servers forestierST ma		
		Consume Controllers HRA Servers Acti-Virus Servers Acti-Virus Servers Windows Update Servers User-Defined Server Groups	CoursestierST.ma	s	
	Learn more	Q. Discoverable groups were last refreshed on	mercredi 15 mai 2013 13:10. < <u>B</u> ack <u>N</u> ext >	Einish Cancel 25.	



Après avoir fini les étapes de configuration avec succès, nous devons cliquer sur « Appliquer la stratégie ». Il est important de souligner à ce stade que Forefront UAG nous permet de revoir les étapes de configuration avant de créer les objets de stratégie du groupe.



Figure n° 30: Paramètres de stratégie du groupe créé par DA

Pour effectuer un test, nous devons se connecter sur le poste client DirectAccess (connecté sur le LAN). Faire un Gpupdate / force pour appliquer la configuration DirectAccess. Déconnecter le client du LAN et le connecter sur le WAN (Internet). Ainsi, nous pouvons vérifier la connexion à une ressource interne fonctionne.





Sur le serveur Forefront UAG, il est possible d'utiliser le Web Monitor pour vérifier le bon fonctionnement de DirectAccess :

Application Monitor									
Current Status	Array Hamber	w State	ADMISEA		Mahuark Sacurity	Witted Doutlet	SATAD Bouter	Tarada Canuar	ATO
Active Sessions	UAG	Hapithy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healt
Statistics -	9mg	ringend	meanin	meanin	(append	meaning	meaning	riedanij	- Propage
Alexandra Alexandra									
User Monitor									
Current Status									
Active Sessions									
G Statistics									
DirectAccess Monitor									
Q Correct Status									
E John Sanatana									
and Active Sessions									
Farm Monitor									
Current Status									
Array Monitor									
Current Status									
Event Viewer									
Da Al									
Will Swatern									
A Security									
a session									
C Appacation									
Event Query									
NAP Troubleshooting	ł.								
	121								1×
	17.1								

**Figure n° 32: Web monitor** 

## IV.2. Création d'un portail et publication

Dans cette phase nous allons créer un portail tronc HTTPS. Ce tronc portail sera utilisé pour publier des applications différentes.





Avant de créer un nouveau portail, nous allons d'abord créer l'authentification et le référentiel d'autorisation. Dans notre cas, nous allons utiliser Active Directory en tant que fournisseur d'authentification.

Scrosoft Forefront Unifier	Access Gabeway Managemen	Add Authentication	Server	×
	inde.	Server type:	S. Active Directory	]
		Server name:	DC.forestierST.ma	
HTTP: Connections HTTP: Connections DirectAccess	Forefront Unified Access Gatew	Connection settings	-	
	Welcome to Forefront UA(	C Define domain o	Directory forest authentication	
	Forefront UAG provides remo started deploying Forefront I	Search settings Specify the search root and scope.		hge of client devices. Use the links in this page to ge
	Deploy UAG DirectAccess	Base DN:	CN=Users,DC=forestierST,DC=ma	works.
	Allow remote access to th	Server access Specify credentials used to access Active Directory for retriainen user information and charmion passwords		
	Create UAG trunks for client	User (domain\user)	foresteirST\Administrateur	Exchange, over an HTTPS connection.
	Allow remote access to th	Password:		
	Create UAG trunks for client	Provide a default d	e omain when users log on. This setting is	
	😧 Other helpful links 🦷	authenticating user sign-on (S50).	s to published applications with single	
	Read the UAG <u>deploymer</u> Read about <u>deploying Fc</u>	Domain:		
	Read about Forefront UA			

## Figure n° 34: Configuration des serveurs d'autorisation

Après la configuration d'authentification avec succès, nous sommes en mesure de créer un nouveau portail.

iew Admin Messages Help	•	reate Trunk Wizard X	
Prorefront UAG HTTPS Connections HTTPS Connections DirectAccess	A Forefront UAG t connection to acc Cick here to cree Cick here to	Step 1 - Select Trunk Type     Select the trunk type through which to publish your applications.        • Publish Exchange applications that can be accessed with the portal.         • Publish Exchange applications via the portal         • Publish Exchange applications Services (AD FS) 1.x trunk lise this option to publish an AD FS 1.x server for session authentication server.         • Note: To authenticate using an AD FS 2.0 server, greate a portal trunk and define the AD FS 2.0 server as an authentication server.         • HTIP to HTIPS redirection         • thise         • Precedent        • Precedent         • Annuler	HT



Nous allons attribuer un nom au Portail et donner aussi un nom d'hôte public que les clients peuvent utiliser pour accéder au portail. Le nom d'hôte public doit correspondre au nom du certificat que nous utilisons pour la connexion HTTPS.

🕑 🗩 🞯 🔘 📗 II	0 10 2				
<b>Ticrosoft Forefront Unified</b>	Access Gateway Ha	Create Trunk Wizard		×	
View Admin Messages	Help	Step 2 - Setting th	ne Trunk		
Prorefront UAG	A Forefront Unified Acces	Enter the details for Trunk name: Public host name: External Web Site IP address: HTTP port: HTTPS port:	your trunk. Portal da.stage.ma 131 . 168 . 6 . 38 ¥ 80 ¥ 443 ¥	co	HTTPS Connections
			< Précédent Suivant >	Annuler	

## Figure n° 36: paramètre du portail

L'étape suivante consiste à sélectionner le certificat qui doit être utilisé pour établir la connexion SSL entre les clients externes et les Forefront UAG Server. Maintenant, il faut choisir la politique d'accès Endpoint UAG, nous pouvons utiliser NAP (protection d'accès au réseau) pour vérifier les clients avant qu'ils ne peuvent utiliser le portail.

Lorsque l'assistant est terminé, nous pouvons voir le portail crée comme il est indiqué sur la capture d'écran ci-dessous.

osoft Forefront Unifie	d Access Gateway Management			
r Admin Messages	Help			
1 III				
S 100				
orefront UAG				
HTTPS Connections				
Portal DirectAccess	Portal			
	External Site Name	Applications		T :
	Specify the name that clients type in the browser to access the site.	Application Name	Application Type	1
	Public host name: da.stage.ma Port: 443	Forta	Portai	
	External Site Address			380
	HTTPS Port: 🗢 443 💌			
				*
	IP address: 131 . 168 . 6 . 38 💌			
		1.	1 1	
		Add	Edit Remove	
		Limit applications to the following	ng subnets:	
		Subnet Address	Subnet Mask	I
	Initial Internal Application			
	Portal home page: Portal	Add	Edit Remove	1
	Display home page within portal frame			-
	Trunk Configuration			
	Configure to ski settinger			

Figure n° 37: portail UAG

#### **IV.2.1.** Publication d'Exchange :

Pour publier un Microsoft Exchange Server 2010 Outlook Web App, Il faut se diriger vers le portail HTTPS créé à l'avance et cliquer sur « Ajouter » dans la fenêtre des applications.

C Built-in services:		
Portal		-
Microsoft Exchange Serve	er (all versions)	-
C Client/server and legac	y:	
Generic Client Application		-
C Browser-embedded:		
Generic Browser-Embedde	ed Application (multiple s	erver 💌
C Terminal Services (TS)/	Remote Desktop Service	s (RDS):
RemoteApp		*
1. C		

Figure n° 38: publication OWA via UAG

Il est nécessaire par la suite de donner un nom à la nouvelle application. Nous avons choisi de nommer l'application OWA, nous insérons également le nom de domaine complet interne de Microsoft Exchange Server 2010 et le port que nous souhaitons utiliser lorsque Forefront UAG doit accéder au serveur Exchange interne.

Dés que la configuration des paramètres s'achève, nous pouvons tester la connexion d'un client externe en ouvrant le site portail.

adminU	
•••••	
English (en-US)	
Log On	
	English (en-US)

Figure n° 39: log On dans le portail UAG

Après l'authentification, nous pouvons accéder au portail UAG Forefront et utiliser donc l'application Web App Outlook publiée.

😰 Viel Glueck be	ei Sharepoint		
👚 🥂 Run Aas	akaton 🕨 🚱 😨 🛱 Activity 🖃		01:58:57 🚺 Log Off
G	Home	Search application	Sort by: Name •
The Home Over	OWA		

Figure n° 40: Access a OWA par portail

## MCours.com