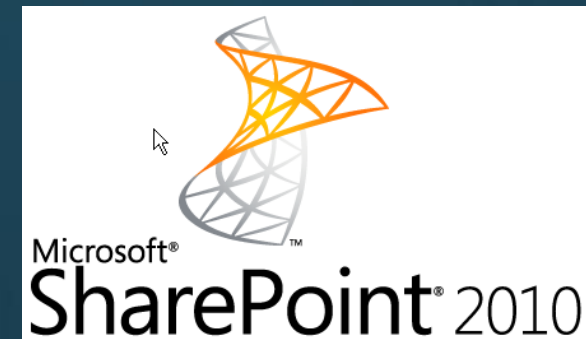
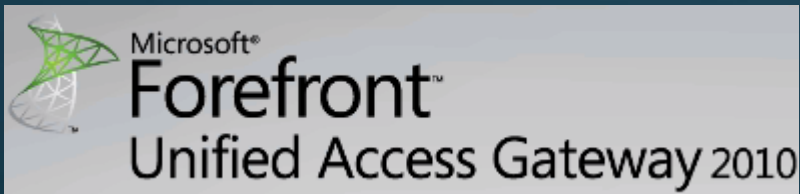


ForeFront pour la protection des portails d'entreprise

Frédéric ESNOUF – Microsoft France
Benoit HAMET – Microsoft France



Agenda

- ⇒ Qu'est-ce que la sécurisation des données
- ⇒ Mise en œuvre de la protection des données dans un environnement SharePoint
- ⇒ Publication d'un portail à l'aide de ForeFront Unified Access Gateway 2010
- ⇒ Sécurité applicative Sharepoint

Qu'est-ce que la sécurisation des données

- ⇒ La sécurité, un problème complexe
 - ⇒ Accès physique
 - ⇒ Accès aux données
 - ⇒ Multiplicité des moyens d'accès
- ⇒ Nécessite des moyens matériels et humains
 - ⇒ Logiciels dédiés (AV, firewall...)
 - ⇒ Mises à jour logicielles
 - ⇒ Formations, sensibilisations
 - ⇒ Procédures...

Sécurité dans le contexte Sharepoint

- ⇒ Sharepoint=collaboration
- ⇒ Collaboration=données (documents,...)
- ⇒ Documents avec différentes \$\$/€€
 - ⇒ Exemple : document fusion/acquisition, recherche, etc
- ⇒ Méthodologie
 - ⇒ Identifier les données et les valeurs : risque
 - ⇒ Analyse de ce risque : contremesures
 - ⇒ Implémenter les solutions/process pour y faire face

Sécurisation et portfolio Microsoft

Microsoft®
Forefront
Endpoint Protection 2010



Mobile



Home / Friend / Kiosk



Internet



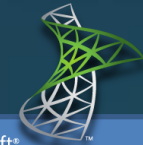
Business Partners / Sub-Contractors



Employees Managed Machines

Layer3 VPN
HTTPS (443)
DirectAccess

Microsoft®
Forefront
Unified Access Gateway 2010



HTTPS / HTTP

Data Center / C

Microsoft®
Forefront
Protection 2010
for SharePoint®

SharePoint



Exchange

RM, IIS based

IBM, SAP, Oracle



Windows
Rights Management Services

top



Non web

AD, ADFS,
RADIUS, LDAP...

NPS, ILM

Mise en œuvre de l'accès aux données dans un environnement SharePoint

- ⇒ Aucun système ne peut être totalement sécurisé mais...on peut limiter les failles
- ⇒ La difficulté de la sécurité est de donner l'accès aux données en limitant les risques
- ⇒ On ne sécurise pas SharePoint mais les données qui y sont stocké

- ⇒ Authentification de l'utilisateur
 - ⇒ IIS
 - ⇒ MOSS
- ⇒ Attribution des droits
 - ⇒ Administrateur
 - ⇒ Collaborateur
 - ⇒ Lecteur
 - ⇒ « Anonyme »

Authentification utilisateur



- Authentification utilisateur

- Valider le compte utilisateur
- Gérer la sécurité par des utilisateurs/groupes
- Pas de listes de distribution



- Authentification

- Internet Information Services
 - Anonyme, Basic, Windows intégré, Kerberos, Certificats
- Authentification par formulaire
- Authentification intégrée (Kerberos/NTLM)
- Authentification via ADFS

Right Management Services

- ⇒ Protection numérique des documents
- ⇒ Intégration avec SharePoint
 - ⇒ Protection automatique des documents postés
- ⇒ Conservation des droits

Information Rights Management

IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this server.

Specify the location of Windows Rights Management Services (RMS):

- Do not use IRM on this server
- Use the default RMS server specified in Active Directory
- Use this RMS server:

OK Cancel

ForeFront Protection for SharePoint

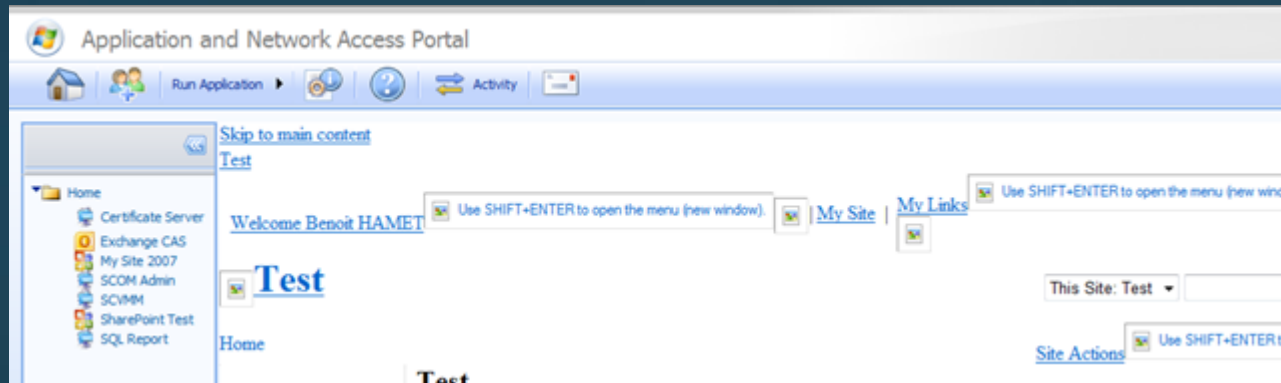
- ⇒ Protection contre les codes malicieux
- ⇒ Plusieurs moteurs antivirus
 - ⇒ Kaspersky Labs
 - ⇒ Microsoft
 - ⇒ Sophos...
- ⇒ Filtrage du type de document

Accès distants, UAG & MOSS

- ⇒ Passerelle officielle pour MOSS (quid TMG?)
- ⇒ Supporte 100% des scénarios
- ⇒ SSO : Web, NTLM/KERB, ADFS, KCD
- ⇒ Intégration office
- ⇒ Politiques de sécurité : application et fonctions
- ⇒ Traçabilité : réseau, et niveau « utilisateur »
- ⇒ Sécurité poste de travail (attachment wiper, ...)
- ⇒ Scénarios externes (mobilité) et internes (SSO)
- ⇒ Supporte nombreux systèmes authentification forte

Configuration AAM

- ⇒ Assistant de publication dans UAG; aussi simple que la publication ISA/TMG
- ⇒ MAIS... configuration des AAM nécessaires



Demo

Publication de SharePoint avec UAG

Authentication



The screenshot shows a web page with a blue header containing the Microsoft TechDays 10 logo and a background image of a blue grid. Below the header is a light blue box with the following elements:

- Log On** heading
- User name:** followed by a text input field.
- Password:** followed by a text input field.
- Language:** followed by a dropdown menu showing "English (en-US)".
- A **Log On** button.
- A horizontal line separating the login area from the footer.
- Text: "This site is intended for authorized users only. If you experience access problems contact the [site administrator](#)."
- Footer: "© 2010 Microsoft Corporation. All rights reserved. [Terms of Use](#)."

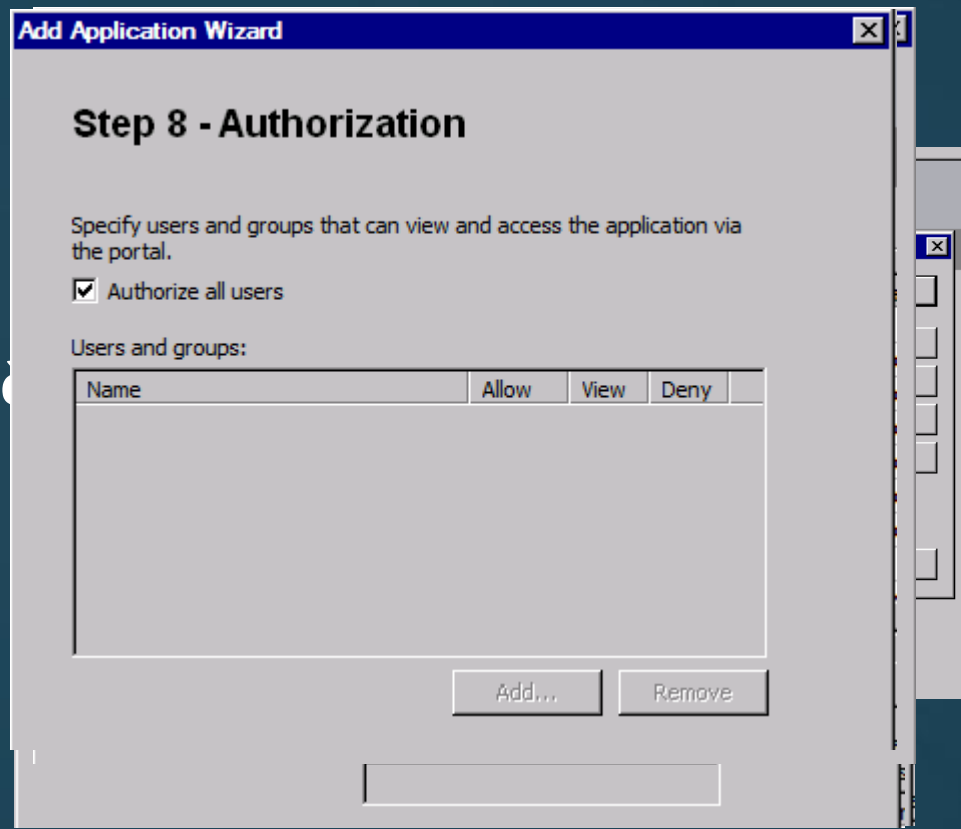
Portail

The screenshot displays the "Tech Days" Application and Network Access Portal. The interface includes a top navigation bar with a "Run Application" button, an "Activity" link, and a "Log Off" button. A left-hand navigation pane, highlighted with a red border, lists the following items: Home, Demo RemoteApp, File Access, FIM, WB CorpWeb (R&D), WB Intranet, WB Mail, and Web Monitor. The main content area, titled "Home", features a search bar and a "Sort by: Name" dropdown. It displays several application tiles, each with an icon, a title, and a brief description:

- Demo RemoteApp**: Represented by a folder icon.
- File Access**: "Explore Your Files (Your computer does not meet the security policy requirements of this application) [Details]"
- FIM**: "Microsoft Forefront Identity Manager 2010 stockholm"
- WB Intranet**: "Microsoft Office SharePoint Server 2007 SharePoint 2007 Sydney"
- Web Monitor**: "Monitoring and reporting web application"
- WB CorpWeb (R&D)**: "Microsoft SharePoint Server 2010 Seattle, confidential"
- WB Mail**: "Microsoft Outlook Web App madrid"

Assistant de publication pour MOSS Publication à travers UAG

Définition des autorisations
Définition de la sélection des services de la fonctionnalité de publication dans le portail (UAG ne/publique)
Définition des utilisateurs et groupes d'accès au portail (UAG ne/publique)



Assistant de publication pour MOSS

Paramétrage des AAM

Alternate Access Mapping Collection

Alternate Access Mapping Collection: **SharePoint - MySite**

Select an Alternate Access Mapping Collection.

Add Internal URL	Zone	Public URL for Zone
Enter the p http://my2010.benoithamet.local	Default	http://my2010.benoithamet.local
https://my2010.hametbenoit.info	Extranet	https://my2010.hametbenoit.info
http://my2010.hametbenoit.info	Extranet	https://my2010.hametbenoit.info

Intranet
Internet
Custom
Extranet

Save Cancel

Ajouter une URL interne

Associer l'URL à la zone correspondant à l'URL public

Microsoft Unified Access Gateway

Fournit aux *employés, partenaires* et *clients*, un *accès par politiques de sécurité*, aux *données et applications* depuis poste *managé* ou *non managé*

	Field Consultant			Kiosk		Limited Webmail: no attachments				
	Logistics Partner			Partner Desktop		Limited Intranet		Restricted SharePoint		
	Project Manager Employee			Corporate Laptop		Full Intranet		Supply Chain		File Access
	Project Manager Employee			Unmanaged Home PC		Production Report		Payroll & HR		

UAG & défense en profondeur

Who can see this data?

What are attempting?

What can you Access?

Who are You?

Where are you coming from?

Remote User



Endpoint Check

Does policy known Assets
 Check and A without VPN
 Out of box c Anti-Malwa

Authenticati

Support of m
 •Active Direc
 •LDAP
 •TACACS
 •RADIUS
 •RSA
 •Smart Card
 •Certificates
 •Customized - using IA

Authori

Group a applicat
 Transpa ShareP
 Single Si replicat
 Role bas

Level of access granted based on e eg SharePoint upload?
 Customizable Endpoint Check

Application Security

Information Security

Prevents information leakage by clearing cache
 Attachment wiper automatically:
 •clears browser
 •removes cookies, history, auto-complete
 •Triggers session timeout - varies based on location
 Out of the box network attack prevention
 Proxy requests protect Servers from direct remote connections.

Application Optimizers for multiple Microsoft and non-Microsoft applications



Demo

Vérification de la conformité

Authentication and SingleSignOn

➡ Strong Authentication



Application and Network Access Portal

Log On

5	5	1	5	6
8	6	2	4	4
3	4	9	0	1
7	0	0	3	2
7	9	6	9	8

User name:

Password:

Language:

Microsoft GrIDsure SKYNETRIX

This site is intended for authorized users only.
If you experience access problems contact the [site administrator](#).

© 2010 Microsoft Corporation. All rights reserved. [Terms of Use](#).

➡ Single Sign On

Ressources additionnelles

⇒ ForeFront Security For SharePoint Virtual Lab:

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032329673&EventCategory=3&culture=en-US&CountryCode=US>

⇒ Publication de SharePoint avec UAG:

<http://blog.hametbenoit.info/Lists/Posts/Post.aspx?ID=497>

⇒ Démonstration / labs en ligne:

<http://mssalesdemos.com/>

⇒ Démonstration ForeFront Protection for SharePoint:

<http://www.microsoft.com/forefront/serversecurity/sharepoint/en/us/demo.aspx>

⇒ Right Management Service avec SharePoint:

<http://msdn.microsoft.com/en-us/library/ms458245.aspx>

<http://blogs.technet.com/stanislas/archive/2008/07/21/utiliser-ad-right-management-services-avec-sharepoint-2007.aspx>

⇒ Démonstration authentification forte avec UAG:

<http://vsa.tagattitude.fr/iag/login.aspx> <http://gridsure.uagdev.skynetrix.com>

Merci de votre attention

Votre potentiel, notre passion™

Microsoft®

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.