Nouveautés de ISA Server 2004

OSSIR (groupe Windows) – 11 juillet 2005 – EHESS, Paris

Stanislas Quastana, CISSP
Architecte Infrastructure
Microsoft France
squasta@microsoft.com

Agenda

- Introduction
- Présentation générale ISA Server 2004
- Le filtre HTTP
- Le filtre FTP
- Le filtre RPC
- Gestion des réseaux privés virtuels (VPN)
- Synthèse
- Questions / Réponses

Quelques chiffres

- Environ 70% de toutes les attaques Web se passent au niveau de la couche Application (Gartner Group)
- Sur les 10 attaques les plus répandues, 8 sont effectuées au niveau application (Symantec Corp)
- Entre décembre 2003 et 2004, 80% d'augmentation du nombre de vulnérabilités d'application Web découvertes (Symantec Corp)

Top 10 des attaques : 80% d'attaques au niveau de la couche 7

Jul–Dec 2004 Current rank	Jan–Jun 2004 Previous rank	Attack	Jul–Dec 2004 Current percent of attackers	Jan–Jun 2004 Previous percent of attackers
1	1	Microsoft SQL Server Resolution Service Stack Overflow Attack	22%	15%
2	Not ranked (NR)	Generic TCP Syn Flood Denial of Service Attack	12%	NA
3	10	Microsoft Windows DCOM RPC Interface Buffer Overrun Attack	7%	1%
4	6	Generic SMTP Malformed Command/Header Attack	5%	2%
5	2	W32.HLLW.Gaobot Attack Version	4%	4%
6	NR	Generic Invalid HTTP String Attack	4%	NA
7	7	Generic ICMP Flood Attack	3%	2%
8	3	Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request Attack	2%	4%
9	9	Generic HTTP Directory Attack	2%	1%
10	NR	Generic UTF8 Encoding in URL Attack	2%	NA

SQL Server

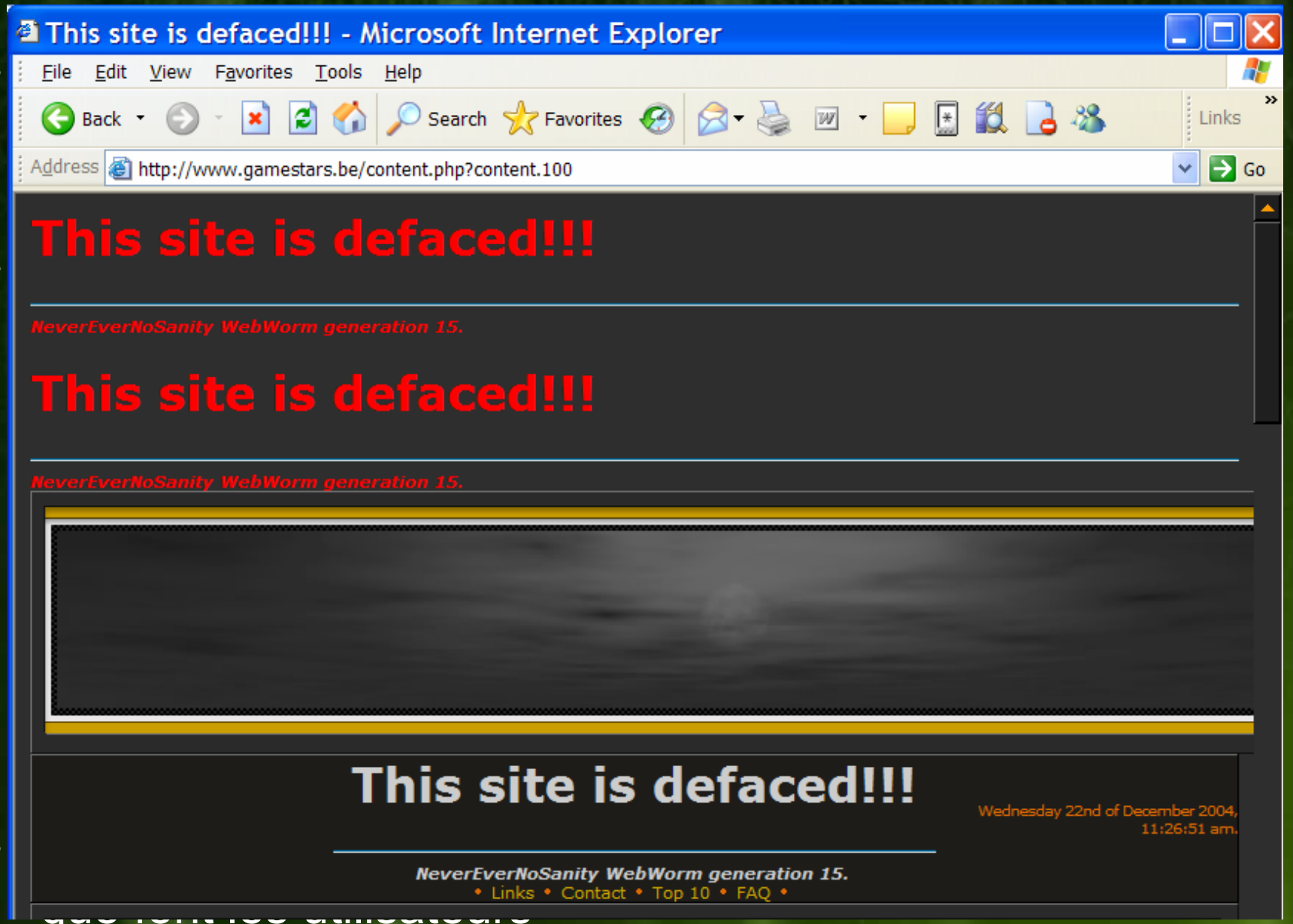
DCOM RPC

SMTP

HTTP

Top attacks (source : Symantec Corporation)

Le problème

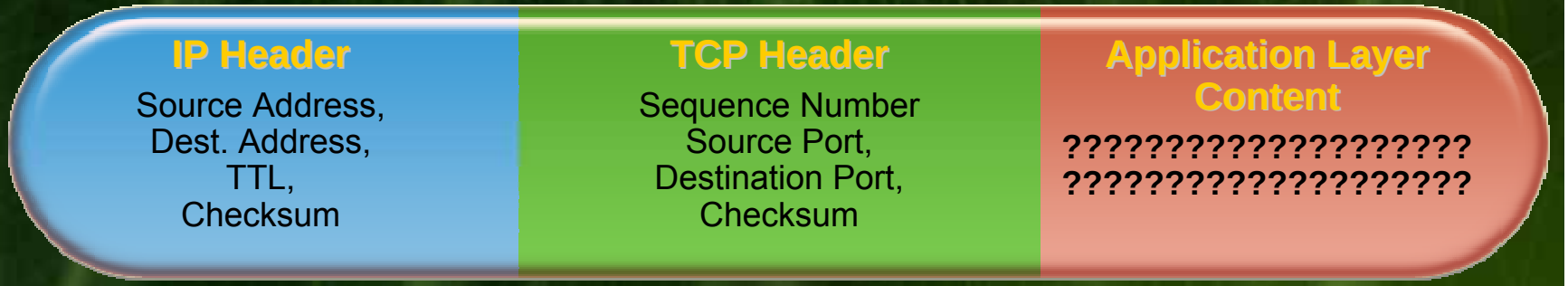


-
-
-
- que font les utilisateurs

Différentes vues d'un paquet

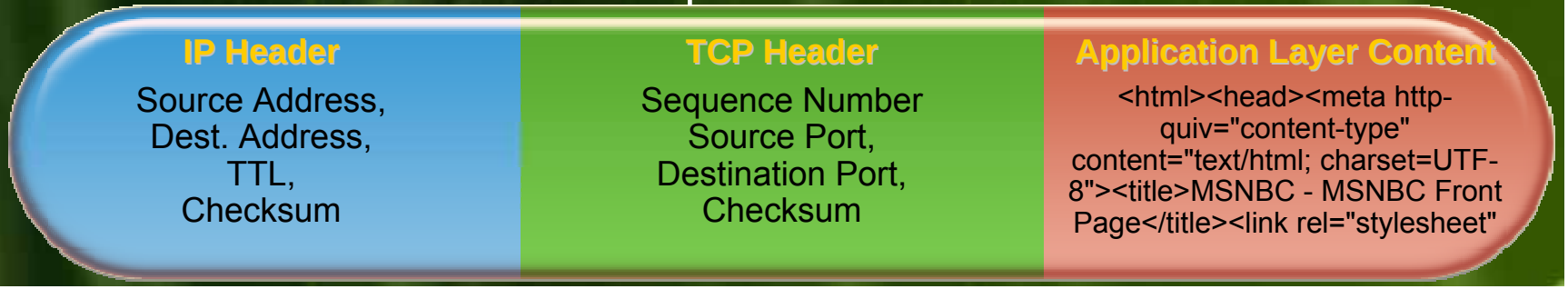
Pare feu "traditionnel"

- Seul l'entête du paquet est analysé. Le contenu au niveau de la couche application est comme une "boite noire"
- La décision de laisser passer est basée sur les numéros de ports



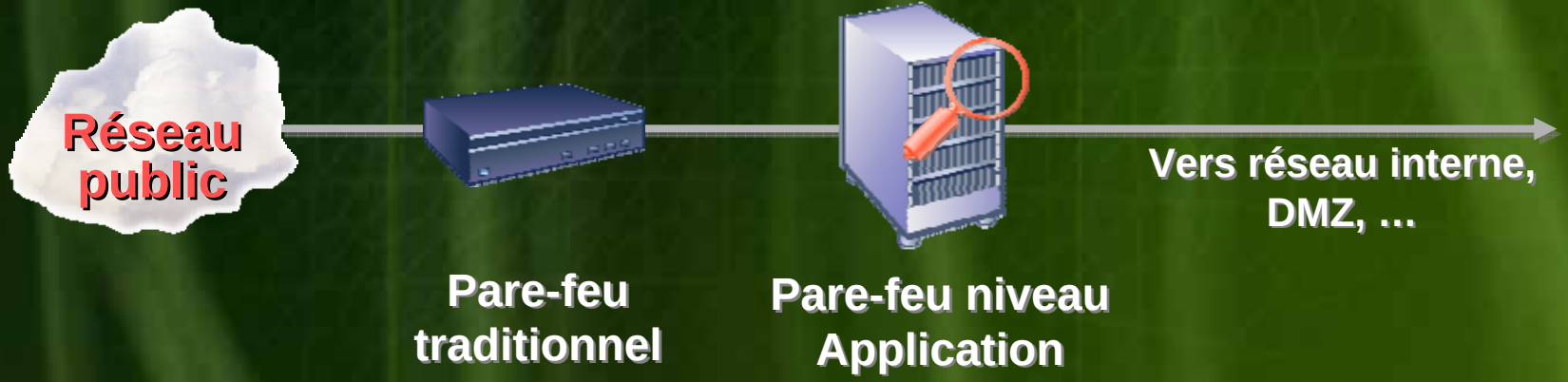
ISA Server 2004

- Les entêtes du paquet et le contenu sont inspectés
  - Sous réserve de la présence d'un filtre applicatif (comme le filtre HTTP)
- Les décisions de laisser passer sont basées sur le contenu



Quel pare-feu utiliser ?

- Les pare-feu applicatif sont aujourd'hui nécessaires pour se protéger des attaques évoluées car ils permettent une analyse approfondie du contenu des paquets réseaux.
- Comprendre ce qu'il y a dans la partie données est désormais un pré requis
- Néanmoins, le remplacement n'est pas forcément la meilleure solution

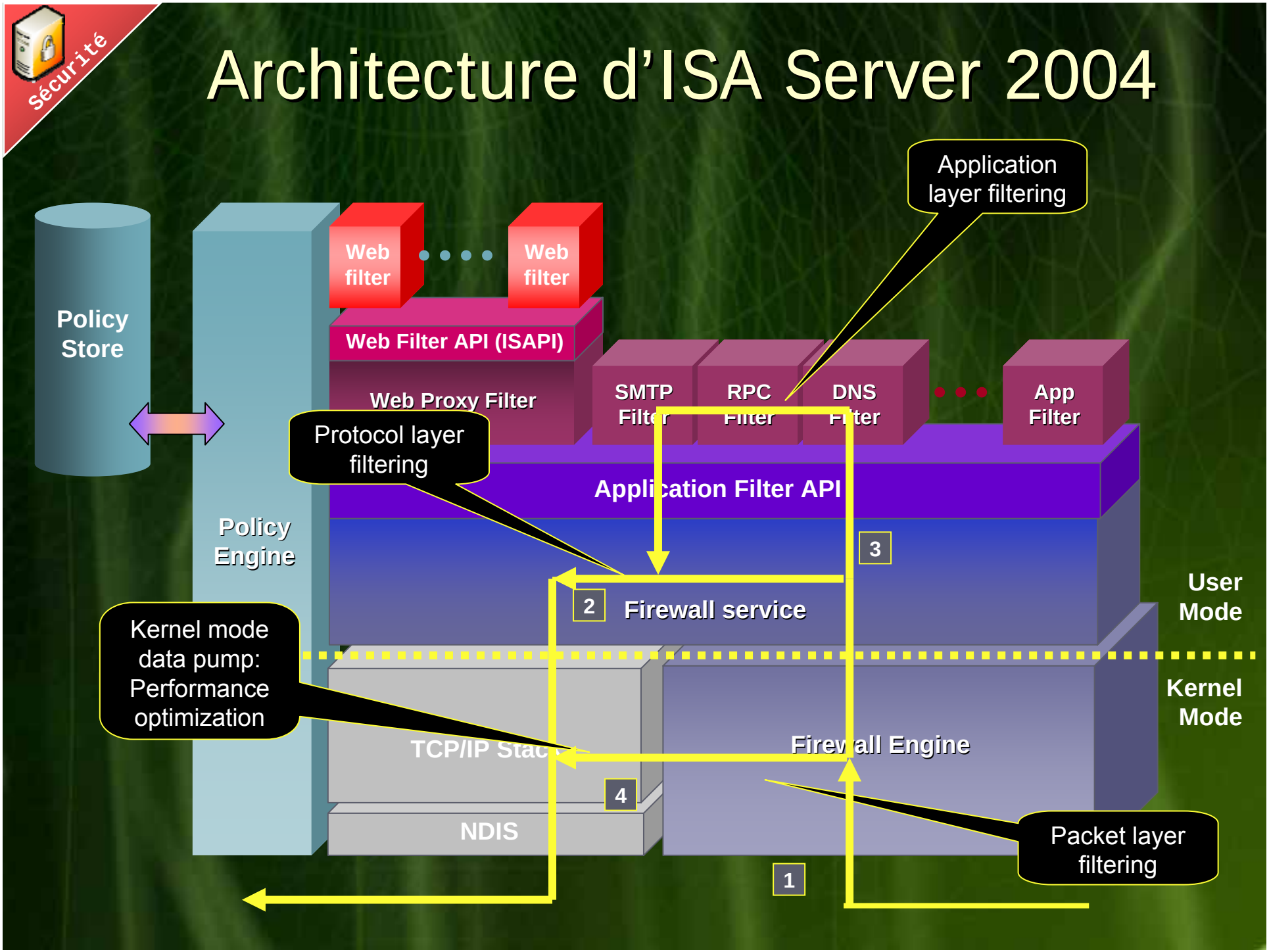


ISA Server 2004 en quelques mots

- 2ème génération de pare-feu de Microsoft
- Pare-feu multicouches (3,4 et 7)
- Capacité de filtrage extensible
- Proxy applicatif (sortant et/ou reverse)
- Nouvelle architecture
- Intégration des fonctionnalités de VPN

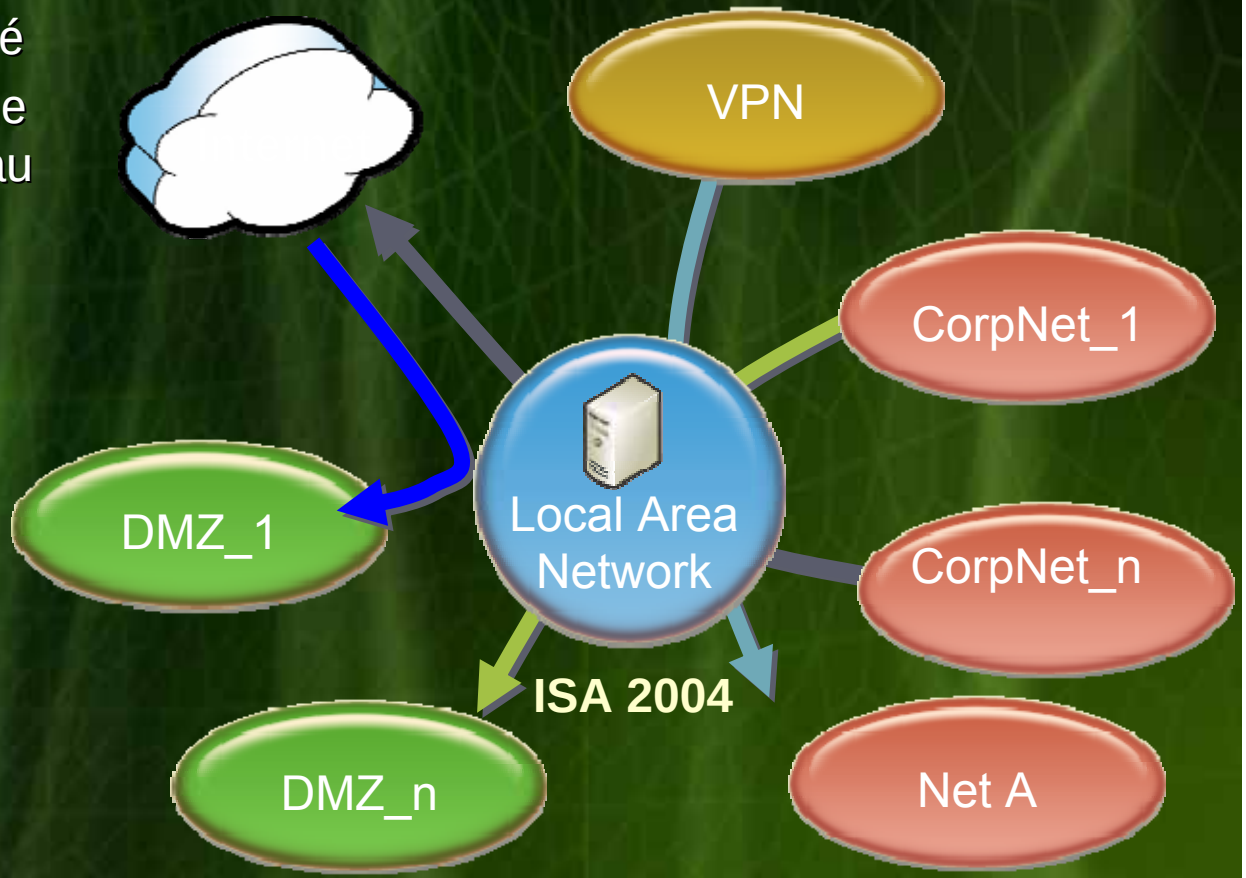
Microsoft
Internet Security & Acceleration Server 2004

Architecture d'ISA Server 2004



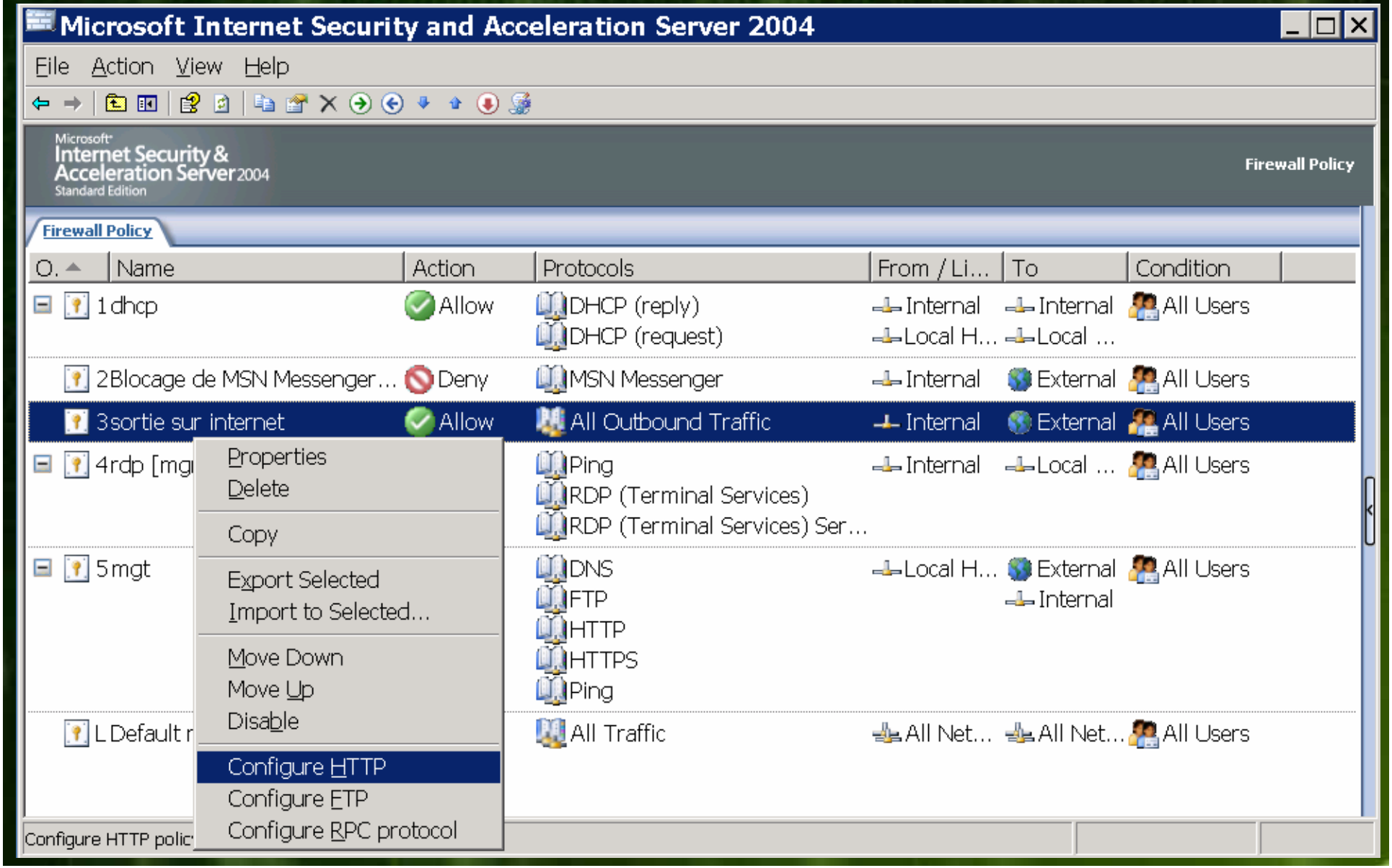
Modèle réseau ISA Server 2004

- Nombre de réseaux illimité
- Type d'accès NAT/Routage spécifique à chaque réseau
- Les réseaux VPN sont considérés comme des réseaux à part entière
- La machine ISA est considéré comme un réseau (LocalHost)
- Stratégie de filtrage par réseau
- Filtrage de paquet sur toutes les interfaces



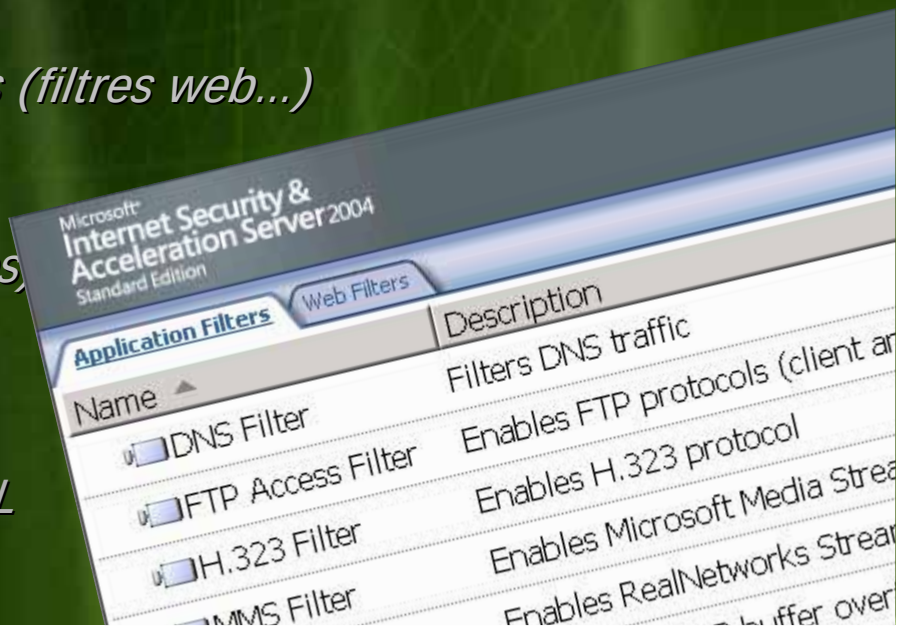
Toutes topologies / stratégies

Structure des règles de pare-feu ISA



Les filtres d'ISA Server 2004

- Filtres applicatifs
  - FTP : *permet de bloquer les envois*
  - SMTP : *gestion des commandes et filtrage des messages (contenu, extension, taille...)*
  - POP3 : *détection d'intrusion*
  - RTSP, MMS, PNM, H.323*: Streaming*
  - DNS: *détection d'intrusions, transfert de zones*
  - RPC: *publication de serveurs, filtrage sur les interfaces*
  - PPTP : *permet la traversée de connexions VPN (Tunneling)*
  - SOCKS V4
  - Web Proxy *: gestion de HTTP, HTTPs (filtres web...)*
- Filtres Web
  - Filtre HTTP *: analyse du contenu des requêtes web (entêtes et données)*
  - Authentification RSA SecureID
  - Authentification Radius
  - Authentification OWA Web Forms
  - Translateur de liens *: réécriture d'URL*



Les versions d'ISA Server 2004

Édition Standard

- Inclus toutes les fonctionnalités de :
  - Pare-feu (niveaux 3,4,7)
  - Passerelle VPN
  - Proxy cache

  sur un même serveur

- Disponible depuis Mai 2004
- 1 licence par processeur physique
- Également disponible sous la forme d'appliance

Édition Entreprise

- Ajoute la haute disponibilité et la tolérance de panne
- Ajoute la capacité à monter en charge en utilisant plusieurs serveurs (groupes)
- Ajoute l'administration centralisée au niveau entreprise

- Disponible depuis Mars 2005
- 1 licence par processeur physique

SBS 2003

Le Service Pack 1 de Windows 2003 Small Business Server 2003 met à jour les version Premium avec ISA Server 2004 Standard SP1

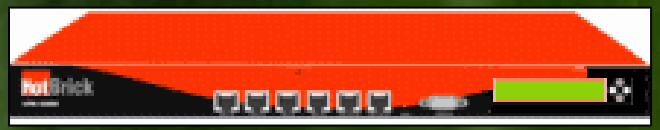
- Disponible depuis Mai 2005

Nouveautés de la version Entreprise

- Groupes de serveurs
  - Un ensemble de serveurs (entité d'administration) configurés de la même façon
  - Jusqu'à **31** serveurs !!!
- Stratégies d'Entreprise
- Équilibrage de charge réseau
  - Assistant de configuration dans la console d'ISA 2004
  - Surveillance des services NLB (**N**etwork **L**oad **B**alancing)
- Cache Web distribué
  - Support de CARP (**C**ache **A**rray **R**outing **P**rotocol*)*
- Deux nouveaux rôles d'administration
  - Au niveau entreprise
  - 5 au total (dont 3 au niveau groupe)
- Supervision centralisée et globale
- Serveur de configuration
  - Configuration Storage Server (CSS) → basé sur AD/AM

Disponible en appliance

- **RimApp ROADBLOCK Firewall**
  http://www.rimapp.com/roadblock.htm
- **HP ProLiant DL320 Firewall/VPN/Cache Server**
  http://h18004.www1.hp.com/products/servers/software/microsoft/ISAserver/index.html
- **Network Engines NS Appliances**
  http://www.networkengines.com/sol/nsapplianceseries.aspx
- **Celestix Application-Layer Firewall, VPN and Caching Appliance**
  http://www.celestix.com/products/isa/index.htm
- **Pyramid Computer ValueServer Security 2004**
  http://www.pyramid.de/e/produkte/server/isa_2004.php
- **Avantis ISAwall**
  http://www.avantisworld.com/02_securityappliances.asp
- **Corrent**
  http://www.corrent.com/Products/products_sr225.html
- **SecureGUARD**
  http://www.secureguard.at/isaserver/index.html
- **Hot Brick ISA 6000**
  http://www.hotbrick.com/isa.asp



ISA Server 2004 : un produit évolutif

- Filtrage applicatif
- Haute disponibilité
- Antivirus
- Détection d'intrusion
- Reporting
- Accélérateurs SSL
- Contrôle d'URLs
- Authentification

+ d'une trentaine de partenaires !!!

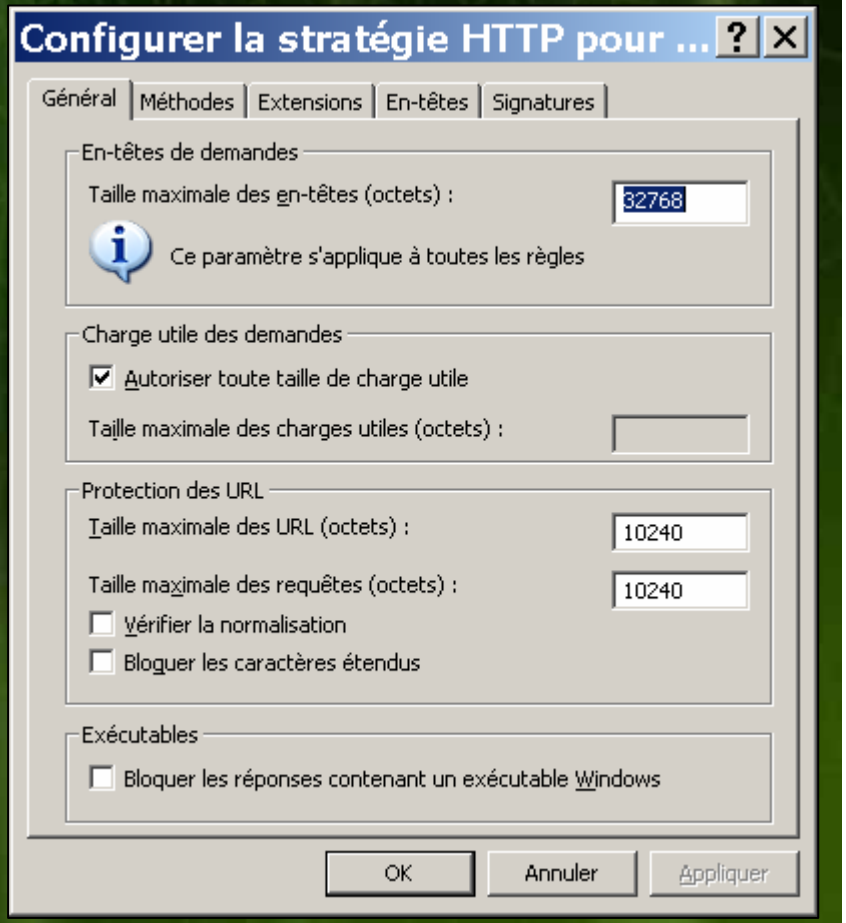
Plus de partenaires :
http://www.microsoft.com/isaserver/partners/default.asp

Le filtre HTTP

Le filtre HTTP peut être défini sur toutes les règles de pare-feu qui utilisent HTTP (flux sortant ou entrants)

Les options suivantes sont disponibles:

- Limiter la taille maximale des entêtes (header) dans les requêtes HTTP
- Limiter la taille de la charge utile (payload) dans les requêtes
- Limiter les URLs qui peuvent être spécifiées dans une requête
- Bloquer les réponses qui contiennent des exécutables Windows
- Bloquer des méthodes HTTP spécifiques
- Bloquer des extensions HTTP spécifiques
- Bloquer des entêtes HHTP spécifiques
- Spécifier comment les entêtes HTTP sont retournés
- Spécifier comment les entêtes HTTP Via sont transmis ou retournés
- Bloquer des signatures HTTP spécifiques



En complément de ce filtre, il est possible de créer des filtres Web complémentaires via le SDK : http://msdn.microsoft.com/library/en-us/isasdk/isa/internet_security_and_acceleration_server_start_page.asp

Protection des serveurs Web
avec le filtre HTTP

- Filtre les requêtes entrantes en fonction d'un ensemble de règles
- Permet de se protéger des attaques qui
  - Demandent des actions inhabituelles
  - Comportent un nombre important de caractères
  - Sont encodés avec un jeu de caractères spécifique
- Peut être utilisé en conjonction avec l'inspection de SSL pour détecter les attaques sur SSL

Protection des serveurs Web

Filtrage avancé de HTTP

ISA pré authentifie les utilisateurs, éliminant les boites de dialogues redondantes et n'autorise que le trafic valide à passer

ISA ce qui permet aux attaques applicatives, virus, vers de se propager

ISA peut déchiffrer, inspecter le trafic SSL avant de l'envoyer vers le serveur Web interne

L'analyse des URL par ISA 2004 peut stopper les attaques Web au niveau réseau, y compris en cas d'utilisation de SSL

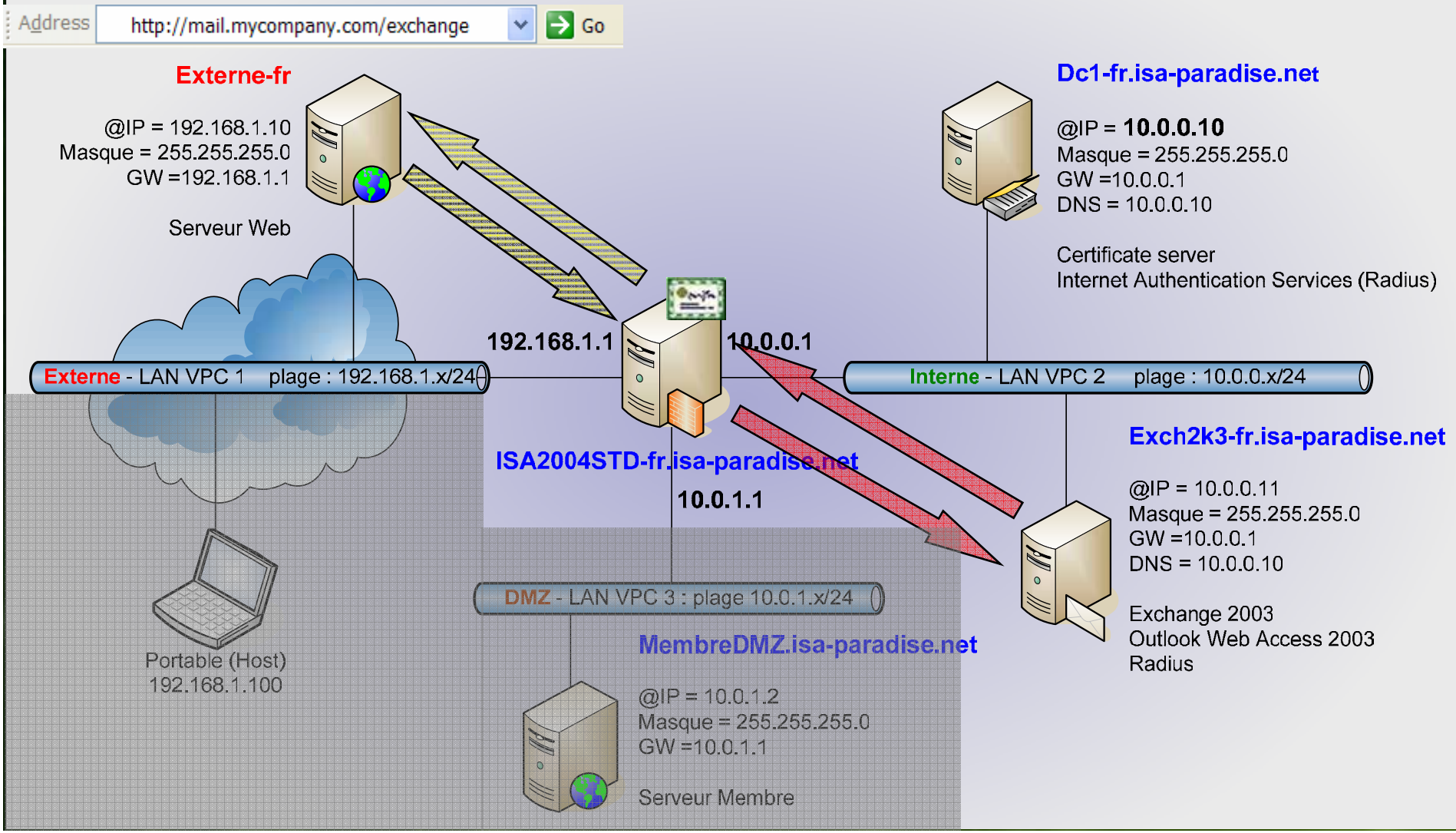
Analyse HTTP

SSL passe au travers des pare-feu traditionnels sans contrôle du fait du chiffrement…

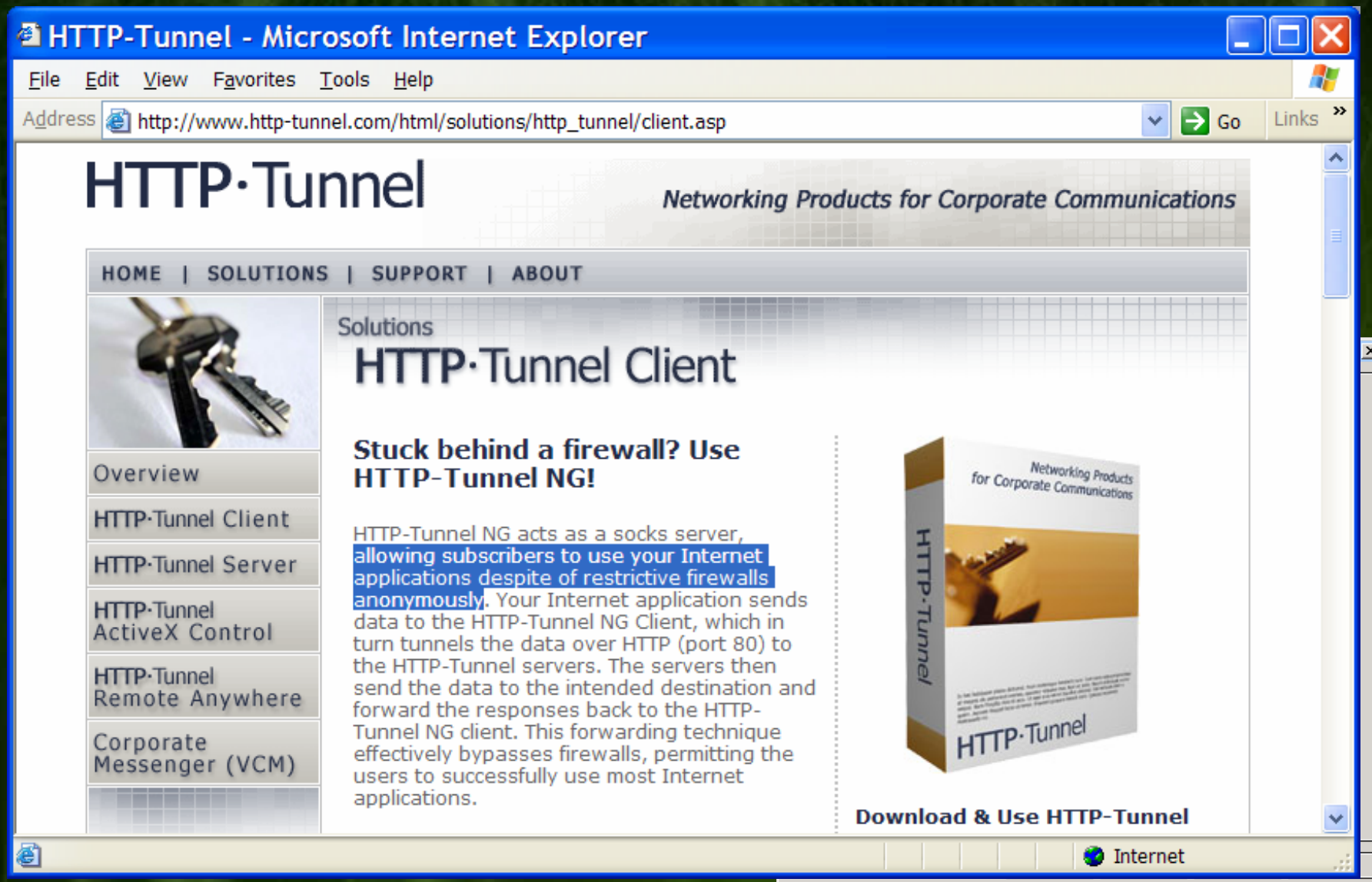
…et d'infecter les serveurs internes !

Une fois inspecté le trafic peut être envoyé vers le serveur interne de nouveau chiffré ou en clair.

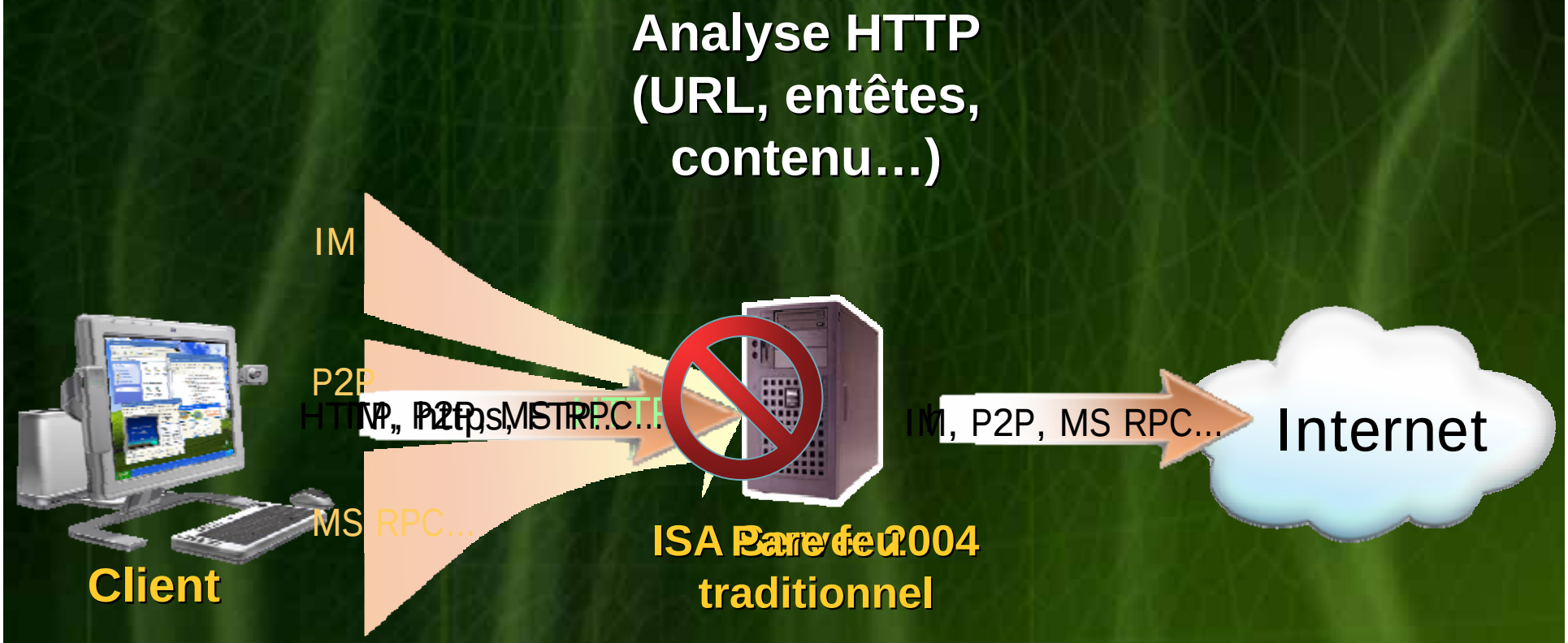
Démonstration : publication OWA



Http : le protocole universel...



Protection des accès sortants



Exemples de signature d'applications :
http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/commonapplicationsignatures.mspx

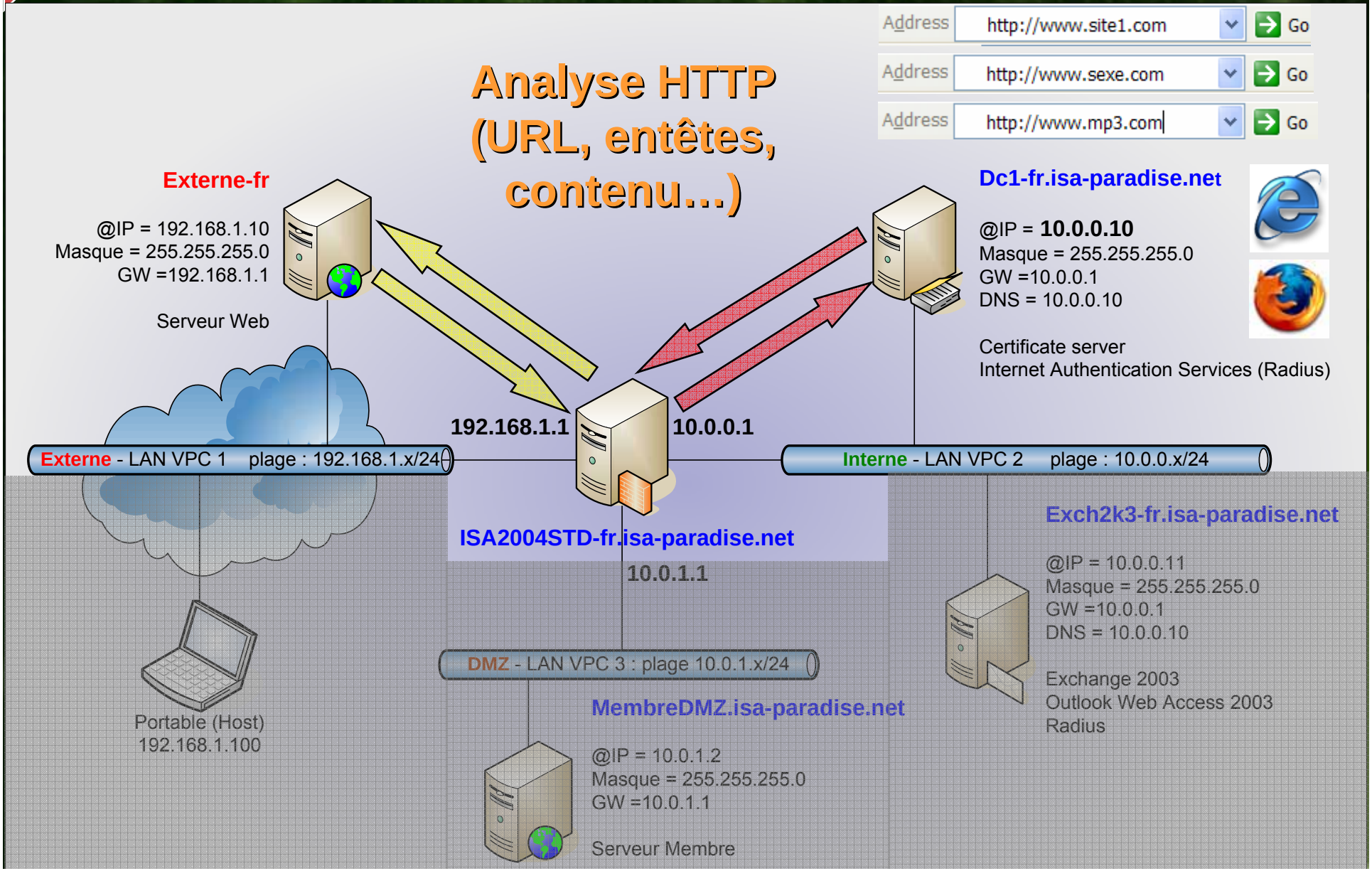
Filtre applicatif HTTP

Exemple de filtrage en fonction du contenu de l'en-tête

```
POST http://64.4.1.18/gtw/gtw.dll?SessID=1
HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0
    1.1.4322; MSN Messenger 6.2.0133)
Host: 64.4.1.18
Proxy-Connection: Keep-Alive
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-msn-messenger
Content-Length: 7
```

Common Application Signatures
http://www.microsoft.com/technet/prodtechnol/isa/2004/plan/commonapplicationsignatures.mspx

Démonstration : filtre HTTP



Le filtre FTP

- C'est un **filtre applicatif** qui permet de limiter certaines actions dans l'utilisation du protocole FTP. Par défaut, ce filtre est activé avec l'Option Lecture seule.

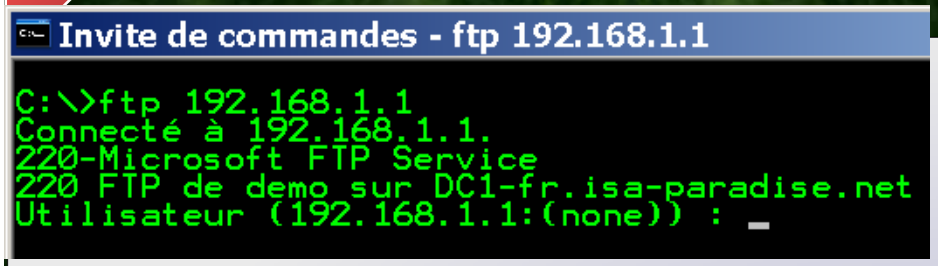
  Quand le mode lecture seule est activé, le filtre FTP bloque toutes les commandes à l'exception des suivantes : ABOR, ACCT, CDUP, CWD /0, FEAT, HELP, LANG, LIST, MODE, NLST, NOOP, PASS, PASV, PORT, PWD /0, QUIT, REIN, REST, RETR, SITE, STRU, SYST, TYPE, USER, XDUP, XCWD, XPWD, SMNT.

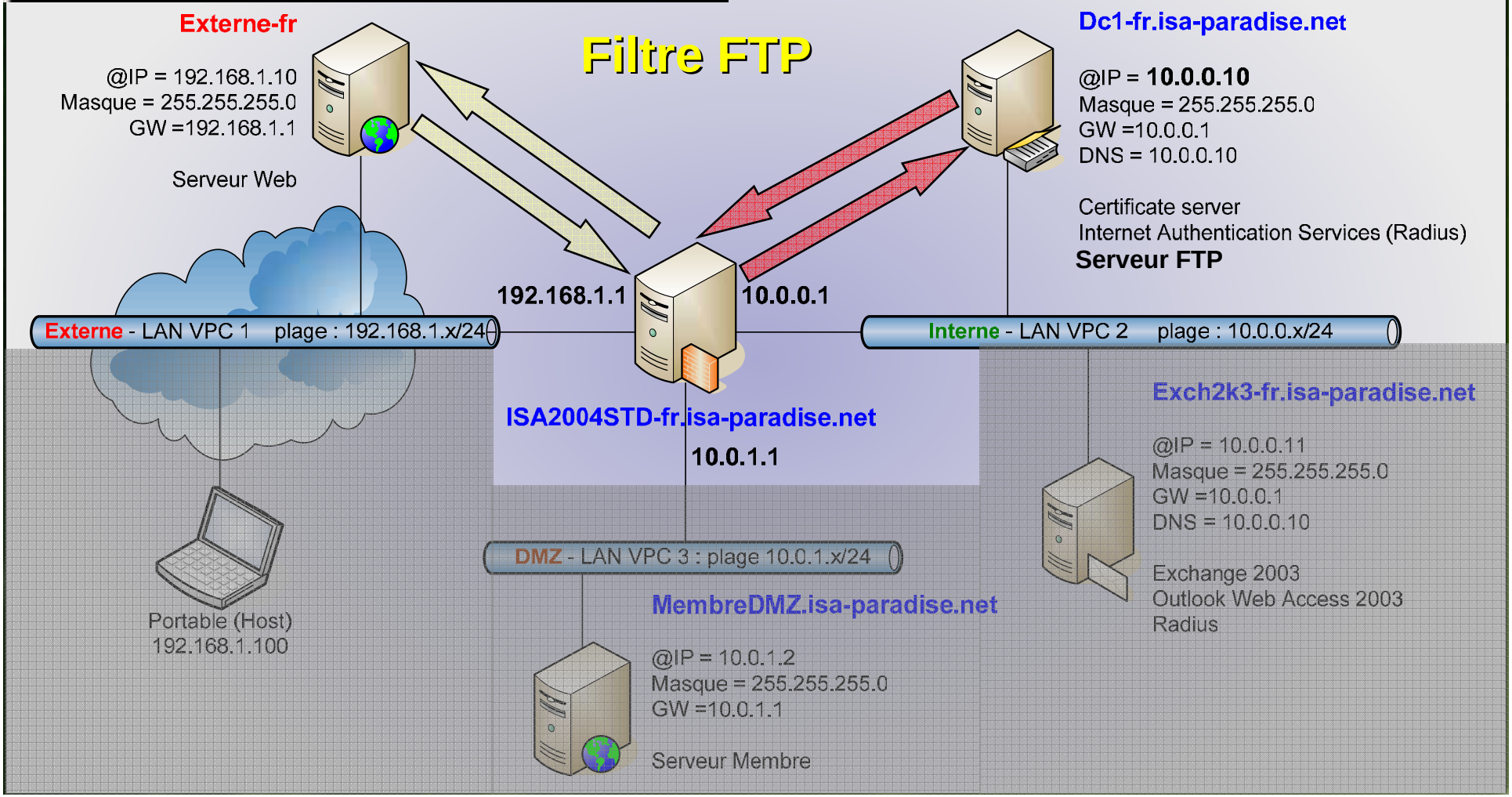
- Ainsi, il ne devrait pas être possible d'exécuter des commandes modifiant des informations sur le serveur FTP (via une commande PUT ou MKDIR par exemple).

- La liste par défaut des commandes autorisées peut être remplacée par une liste personnalisée qui contiendrait par exemple des commandes/Paramètre spécifiques (FPCVendorParametersSets) à une implémentation spécifique du service FTP.
  - Note : pour que les modifications soient prises en comptes, il faut redémarrer le service Pare-feu

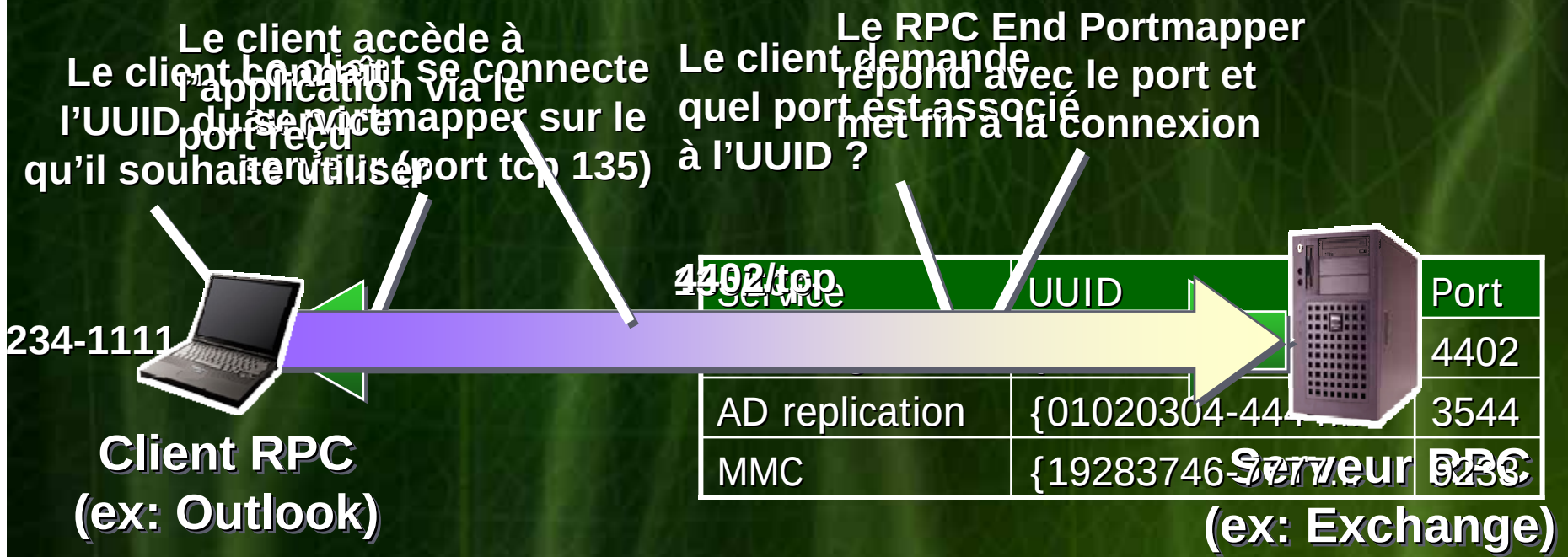
- Informations complémentaires et exemple de script pour personnaliser le filtre FTP : http://msdn.microsoft.com/library/default.asp?url=/library/en-us/isasdk/isa/configuring_add_ins.asp

Démonstration : publication FTP





Fonctionnement des RPC DCE



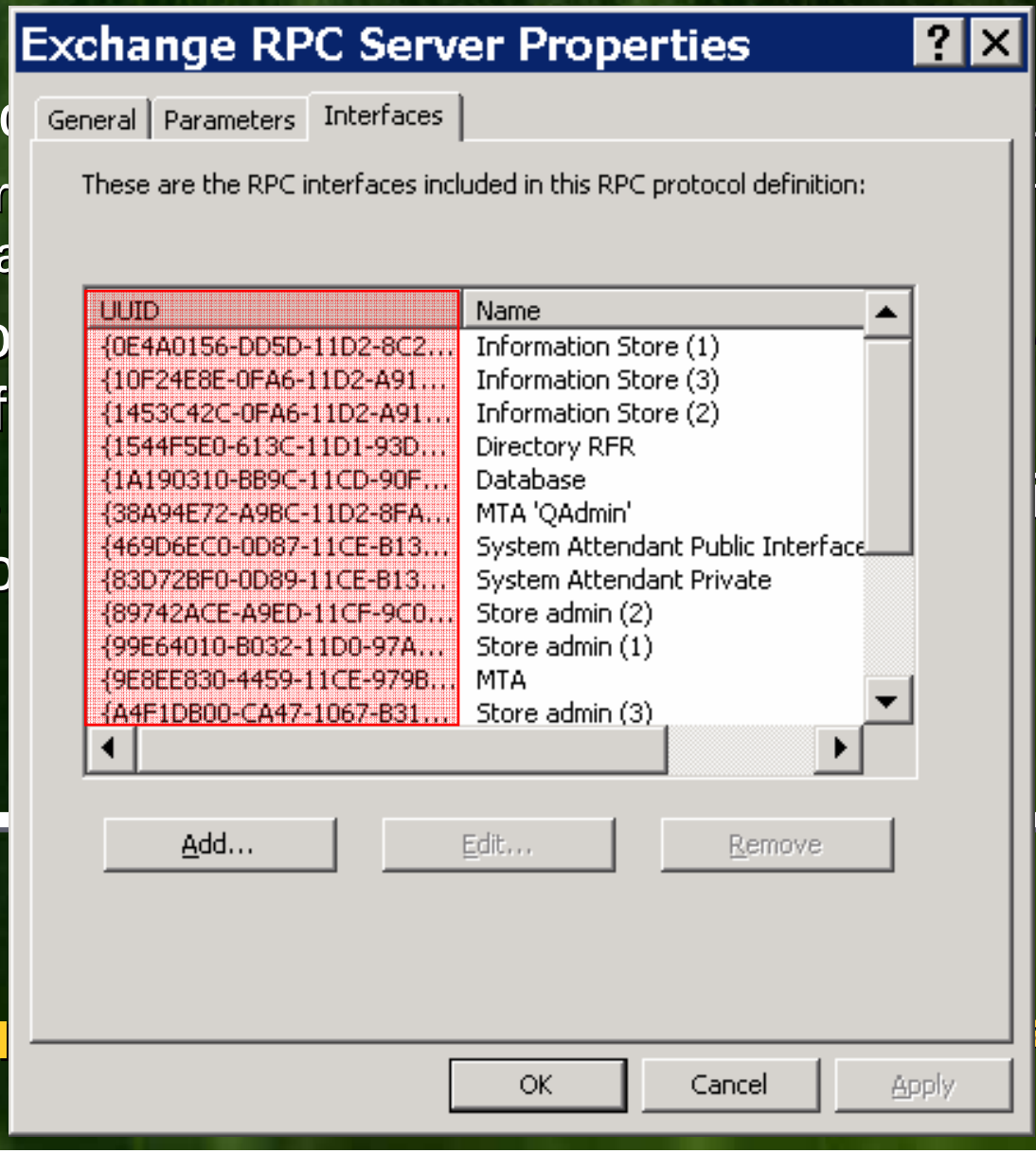
- Du fait de la nature aléatoire des ports utilisés par les RPC, l'implémentation et le filtrage des RPC est difficile sur la majorité des pare-feu
  - L'ensemble des 64,512 ports supérieurs à 1024 ainsi que le port 135 doivent être ouverts sur des pare feu traditionnels

Filtrage applicatif RPC - principe

- Seul le po… ouvert
  - Les por… nt pour les clients (applica…
- Inspectio… r au niveau applicatif
- Seuls les … isés à l'exceptio…

Application cl…

Serveur application RPC



ISA 2004 et les VPNs

Sécurité

VPN nomade

- Protocoles supportés
  - L2TP/IPSec
  - PPTP
- Authentification par mot de passe, certificat (SmartCard, token), SecureID…
- Par défaut 2 objets réseau “VPN Client” et « VPN Quarantine Client »
- Règle d’accès unifiée avec les règles pare-feu
- Les stratégies d’accès se font par utilisateur ou groupe d’utilisateurs
- Support de NAT-T

- Fonction de mise en quarantaine des postes VPN nomades

VPN site à site

- Protocoles supportés :
  - L2TP/IPSec
  - PPTP
  - IPSec en mode tunnel
- Authentification par certificat ou clé prépartagée
- Configuration et administration dans la console de gestion d’ISA
- Les sites distants sont vus comme des objets réseaux

- ISA Server 2004 a été certifié par le VPN Consortium (www.vpnc.org) pour l’interopérabilité basique.

VPNC CERTIFIED Basic Interop

Sécuriser les connexions VPN nomades (1/2)

- Exiger une authentification forte à 2 voire 3 facteurs
  - Ce que je sais : mot de passe, code PIN
  - Ce que je possède : SmartCard, jeton, calculette...
  - Ce que je suis : reconnaissance biométrique

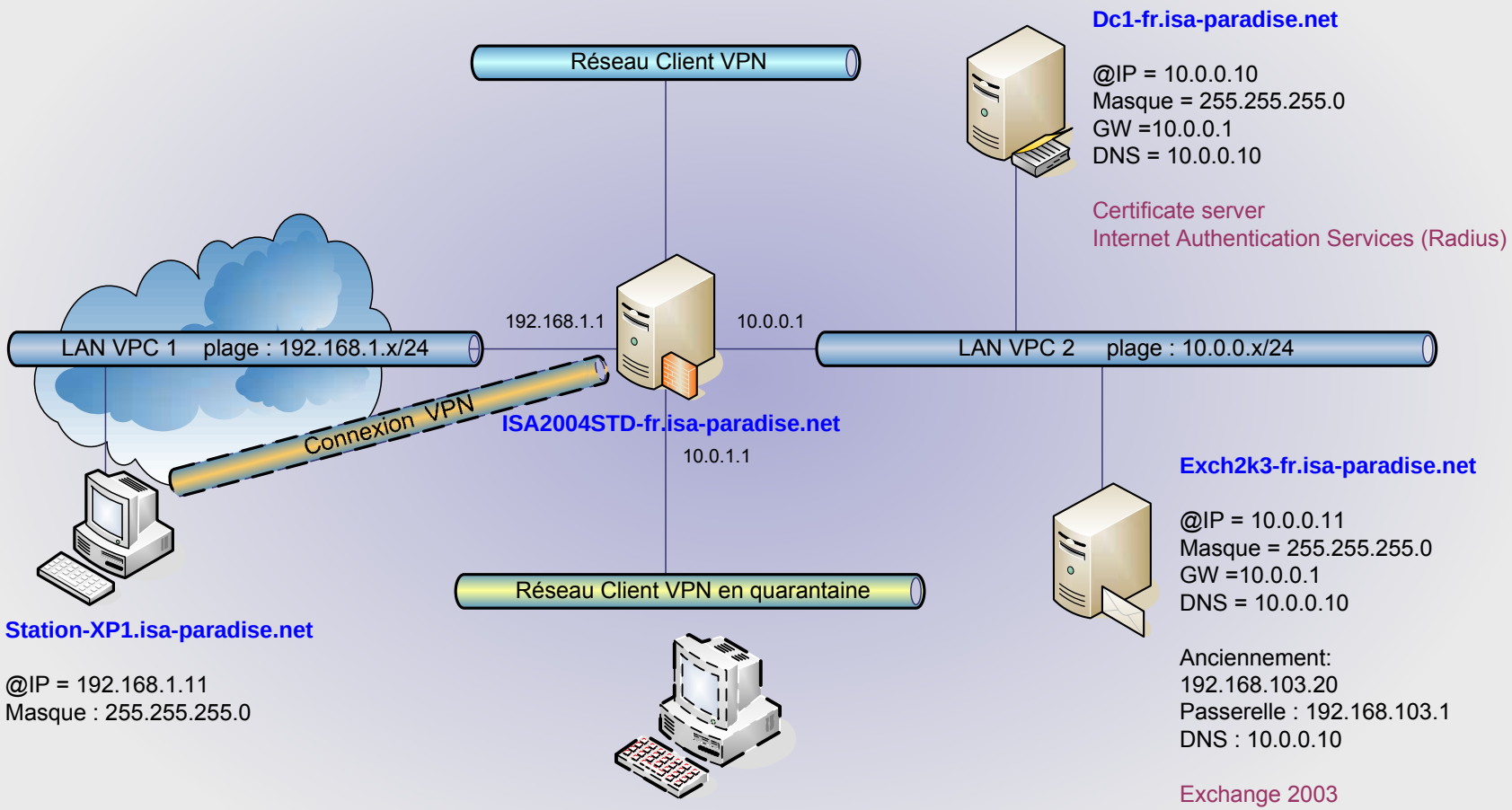
- Augmenter le niveau de chiffrement des communications
  - 3DES
  - AES

- Journaliser, surveiller et analyser l'activité des utilisateurs connectés en VPN

Sécuriser les connexions VPN nomades (2/2)

- Vérifier lors de la connexion la conformité du poste client VPN:
  - Mécanisme d'analyse
  - Mise en quarantaine
- Limiter les accès autorisés pour les sessions VPN
  - Seules les ressources nécessaires sont accessibles
  - L'ensemble du réseau interne ne devrait pas être accessible
- Utiliser du filtrage applicatif pour analyser les communications à destination des ressources internes.
  - Possibilité de faire de l'analyse antivirale
  - Filtrage des flux RPC, http, FTP, SMTP, DNS...

ISA 2004 : VPN et quarantaine



ISA 2004 Feature Pack 1

- Annoncé au TechEd 2005 US (juin 2005)
- 3 fonctionnalités majeures
  - Mise en cache du protocole BITS (utilisé par Microsoft Update)
  - Compression HTTP
  - Qualité de service sur HTTP
- Disponible à la fin de l'année
- Mise à jour gratuite
- Pour les versions Standard et Entreprise

- Informations complémentaires : http://www.microsoft.com/isaserver/solutions/isabranch_updates.mspx

En résumé

ISA 2004 pour protéger vos ressources

- Un pare-feu qui permettant de concevoir un grand nombre de scénarios
  - Protection des flux sortants vers Internet
  - Protection des serveurs exposés sur Interne
  - Protection des ressources internes par segmentation et filtrage applicatif
  - Interopérabilité avec la majorité des passerelles VPN du marché
  - VPN avec mise en quarantaine
  - …
- Défense en profondeur
  - Analyse au niveau des couches 3,4 et 7
  - Nombreux filtres applicatifs inclus en standard (HTTP, RPC, SMTP, DNS…)
  - Nombreux filtres complémentaires disponible auprès d'éditeurs tiers
  - Produit extensible adaptable à vos besoins grâce au SDK
  - Nouveau pack de fonctionnalité spécial réseaux Branch Office

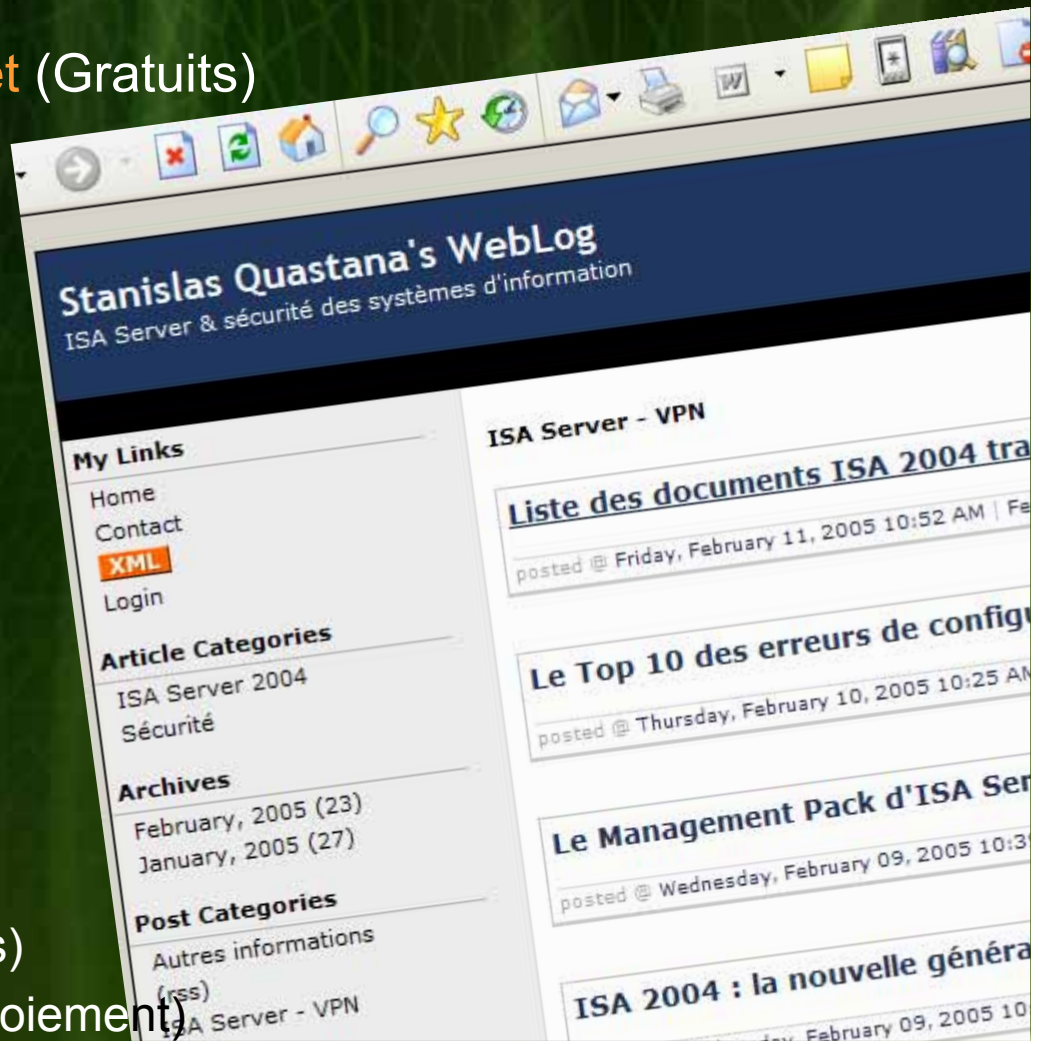
Diapositive 34

SQ1

Joana
Stanislas Quastana; 04/04/2005

Ressources utiles

- Site Web Microsoft
  - www.microsoft.com/isaserver
  - www.microsoft.com/france/isa
- Webcast et séminaires TechNet (Gratuits)
- Sites externes
  - www.isaserver.org
  - www.isaserverfr.org
  - isatools.org
  - www.esnouf.net (QSS)
- Newsgroup français
  - Microsoft.public.fr.isaserver
- Kits de déploiement
- Blogs
  - Blogs.msdn.com/squasta
- Kits d'évaluation ISA Server
  - Version d'évaluation (120 jours)
  - CD (livres blancs et guide déploiement)



sécurité

Questions / Réponses


Sécurité
Microsoft®