Guide d'installation et de configuration d'Isa Server 2006 :

1	INTR	ODUCTION :	4
	1 1		Д
	1.1	OUTELECHARGER LA DERNIERE VERSION DE CE DOCUMENT '	4
2	LES N	NOTIONS INDISPENSABLES POUR DEPLOYER ISA SERVER 2006 :	5
	2.1	Adresse IP privee / publique et le NAT :	5
	2.2	LE ROUTAGE IP :	5
	2.3	LES PORTS TCP / UDP ET LES SERVICES RESEAUX ASSOCIES :	5
	2.4	LES PARE FEU AVEC ETATS (STATEFULL) ET SANS ETATS (STATELESS) :	5
	2.5	COMMENT TESTER ET VALIDER QU'UNE APPLICATION RESEAU EST ACCESSIBLE :	6
	2.6	LES PROTOCOLES RESEAUX :	6
	2.6.1	Le protocole DNS :	6
	2.6.2	Les protocoles web HTTP, FTP :	6
	2.6.3	Protocole SMTP	7
	2.6.4	Le protocole RDP (Terminal Server mode administration à distance) :	7
	2.6.5	E service d'annuaire Active Directory :	7
	2.6.6	Ees certificats :	8
2	DRES	ENTATION D'ISA SERVER 2006 ·	٩
3	FNLS		
	3.1	PRESENTATION GENERALE :	9
	3.2	SCENARIO DE DEPLOIEMENT :	10
	3.3	UN PRODUIT EXTENSIBLE :	11
	3.4	Le successeur d'Isa Server 2006 :	11
4	DEFI	NIR SON ARCHITECTURE RESEAU CIBLE :	12
	4.1	DEFINIR L'ARCHITECTURE CIBLE ISA SERVER 2006 :	12
	4.2	Architecture de resolution de noms DNS :	12
	4.3	LE TYPE DE CLIENT ISA SERVER :	12
	4.4	QUELQUES SITES WEB SUR ISA SERVER 2006 :	13
5	INST	ALLATION D'ISA SERVER 2006 :	14
•			
	5.1	INSTALLATION D'ISA SERVER 2006 :	14
	5.2	INSTALLER LE SERVICE PACK 1 D'ISA SERVER 2006 :	16
	5.3	RENFORCER LA SECURITE D'ISA SERVER 2006 (A FAIRE UNE FOIS TOUTES LES REGLES CONFIGUREES) :	17
	5.4	DESACTIVER LE TOE (TCP OFFLOAD ENGINE)	19
	5.5	EXECUTER ISA SERVER BEST PRACTICE ANALYSER :	19
	5.6	OPTIMISER LES PERFORMANCES D'ISA SERVER 2006 :	20
6	CON	FIGURATION DU SERVEUR ISA SERVER 2006 :	21
	6.1	CONFIGURATION DES RESEAUX ISA SERVER 2006 :	21
	6.1.1	Faire un schéma de son réseau :	21
	6.1.2	Les réseaux Isa Server 2006 :	21
	6.1.3	Quelques réseaux ISA Server à connaître :	24
	6.1.4	Configurer les règles de réseaux :	25
	6.2	REGLE D'ACCES OU REGLE DE PUBLICATION :	26
	6.3	LES ACCES PAR DEFAUT AU NIVEAU DU SERVEUR ISA SERVER 2006 :	27
	6.4	LES STRATEGIES SYSTEMES :	28
	6.5	CREATION DE REGLE D'ACCES :	30
	6.6	LES REGLES DE PUBLICATION :	32
	6.6.1	Création d'une règle de publication de serveur non web :	32
	6.6.2	Les règles de publication de serveur web :	34
	6.6.3	Configuration des règles de publication web HTTPS et des règles pour publier Outlook Web	Access,
	Activ	eSync et Outlook Anywhere :	39

	6.7	CONFIGURATION DE LA MISE EN CACHE AVEC ISA SERVER 2006 :	40
	6.7.1	Activer le cache sur le serveur Isa Server 2006 :	40
	6.7.2	Configurer les règles de cache :	40
	6.7.3	Création de tâches de téléchargement de contenu :	41
	6.7.4	Gestion du contenu du cache :	41
	6.8	CONFIGURATION DE LA DECOUVERTE AUTOMATIQUE :	42
	6.9	CONFIGURATION DE LA DETECTION D'INTRUSION :	42
	6.10	Mise en œuvre du filtrage applicatif avec Isa Server 2006 :	43
	6.10.	1 Présentation du filtre applicatif SMTP	44
	6.10.	2 Présentation du filtre applicatif HTTP :	45
7	LES 1	ACHES D'ADMINISTRATION COURANTE D'ISA SERVER :	46
	7.1	SAUVEGARDER SON SERVEUR ISA SERVER :	46
	7.2	Miss of guilde of the option of the university of the Source 2000 -	10
	· · -	IVISE EN ŒUVRE DE LA DELEGATION D'ADMINISTRATION AVECTSA SERVER 2006 :	40
	7.3	Configuration de Rapports avec Isa Server 2006 :	46 46
	7.3 7.4	Wise en œuvre de la delegation d'administration avec isa Server 2006 : Configuration de rapports avec Isa Server 2006 : Troubleshouting avec l'onglet Surveillance\Journalisation :	46 46 48
8	7.3 7.4 MISE	Configuration de Rapports avec Isa Server 2006 : Troubleshouting avec l'onglet Surveillance\Journalisation :	46 46 48 48
8	7.3 7.4 MISE 8.1.1	WISE EN CEUVRE DE LA DELEGATION D'ADMINISTRATION AVEC ISA SERVER 2006 : CONFIGURATION DE RAPPORTS AVEC ISA SERVER 2006 : TROUBLESHOUTING AVEC L'ONGLET SURVEILLANCE\JOURNALISATION : EN CEUVRE DES VPN : Configuration d'Isa Server comme serveur VPN L2TP :	46 46 48 48 .49 49

1 Introduction :

1.1 Objectifs de ce document :

Ce document a pour objectif de présenter lsa Server 2006. Il n'est pas exhaustif. Certaines fonctionnalités d'Isa Server comme la configuration d'Isa Server 2006 ne sont pas abordées (peut être dans une prochaine version...).

1.2 Où télécharger la dernière version de ce document :

Ce document peut être téléchargé sur http://msreport.free.fr.

2 Les notions indispensables pour déployer lsa Server 2006 :

2.1 Adresse IP privée / publique et le NAT :

Il existe deux types d'adresses IP :

- Les adresses IP publiques : elles sont routables sur Internet.
- Les adresses IP privées : elles ne sont pas routables sur Internet.
- Pour plus d'informations sur les adresses privées / publiques, voir :
- http://www.commentcamarche.net/contents/internet/ip.php3

Un serveur NAT permet à des équipements réseaux avec une adresse IP privée de communiquer avec des équipements réseaux avec une adresse IP publique.

Le NAT permet d'altérer les paquets en remplaçant une adresse IP privée par l'adresse IP publique et inversement.

Attention, certaines protocoles / applications ne supportent pas le NAT comme IPSEC. En effet le NAT modifie le paquet IP alors qu'IPSEC garantit que ce dernier n'a pas été altéré.

- Pour plus d'informations sur le NAT, voir :
- <u>http://fr.wikipedia.org/wiki/Network_address_translation</u>
- http://www.commentcamarche.net/contents/internet/nat.php3

Pour utiliser le NAT avec IPSEC, il faut utiliser le protocole NAT-T :

- http://support.microsoft.com/kb/885348/en-us
- http://support.microsoft.com/kb/818043/en-us
- <u>http://www.isaserver.org/tutorials/Allowing-Inbound-L2TPIPSec-NAT-Traversal-Connections-through-Back-Back-ISA-Server-Firewall-DMZPart1.html</u>

2.2 Le routage IP :

Pour plus d'informations sur la notion de routage :

http://www.frameip.com/routage/

Windows 2003 intègre un service de routage appelé RRAS (Routage et Accès distant). Pour plus d'informations sur le service RRAS, voir <u>http://technet.microsoft.com/fr-fr/library/bb967586.aspx</u>.

2.3 Les ports TCP / UDP et les services réseaux associés :

Chaque application réseau est associée à un ou plusieurs ports TCP / UDP / ICMP. Un serveur web tourne par exemple sur le port TCP 80. Seule une application peut s'exécuter sur un port TCP / UDP donnée. Dans le cas contraire il y a conflit.

La liste de tous les ports connus est disponible sur un serveur Windows 2003 dans le fichier C:\windows\system32\drivers\etc\services

Pour plus d'informations sur les applications associées à chaque port TCP / UDP :

<u>http://www.frameip.com/liste-des-ports-tcp-udp/affichage-liste-des-ports-tcp-udp.php?plage=1</u>

2.4 Les pare feu avec états (statefull) et sans états (stateless) :

Il existe deux grandes familles de pare feu :

- Les pare feu sans états : ce type de pare feu nécessite de créer une règle pour le trafic généré par un équipement réseau (requête http par exemple) qui initie la communication et une règle pour l'équipement réseau qui répond.
- Les pare feu avec états : ce type de pare feu nécessite uniquement de créer une règle pour le trafic généré par l'équipement réseau (requête http par exemple) qui initie la communication. La règle correspondant au trafic généré par l'équipement réseau qui répond à la requête est créée dynamiquement par le pare feu avec états.

Isa Server 2006 est un pare feu avec états.

Pour plus d'informations voir http://fr.wikipedia.org/wiki/Pare-feu.

2.5 Comment tester et valider qu'une application réseau est accessible :

Il existe des outils qui permettent de tester les connexions réseaux.

- Telnet (pour les ports TCP uniquement) : exemple : telnet www.google.fr 80)
- ZenMaps (http://nmap.org/zenmap) permet sous Windows de générer des connexions TCP / UDP.

2.6 Les protocoles réseaux :

2.6.1 Le protocole DNS :

Le protocole DNS permet de résoudre des noms complets DNS (FQDN) en adresses IP et inversement. Pour plus d'informations sur le protocole DNS :

http://www.microsoft.com/DOWNLOADS/details.aspx?familyid=15D276A5-4BF6-4ADD-9F67-56B38CCB576B&displaylang=en

2.6.2 Les protocoles web HTTP, FTP :

Isa Server 2006 est la solution idéale pour sécuriser les serveurs web IIS 5, 6 et 7 de Microsoft. Il n'est en effet pas prudent de publier directement sur Internet un serveur web IIS (c'est tout aussi vrai pour un serveur web Apache).

lsa Server 2006 permet par exemple de bloquer certaines méthodes HTTP ou de détecter la signature d'un programme pour le bloquer.

Un pré-requis à la mise en œuvre d'Isa Server 2006 est donc de connaître le fonctionnement du protocole HTTP et FTP :

- http://www.commentcamarche.net/contents/internet/http.php3
- <u>http://www.commentcamarche.net/contents/internet/ftp.php3</u>
- http://fr.wikipedia.org/wiki/File Transfer Protocol
- http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html
- http://www.webdav.org/specs/rfc2518.html

Pour plus d'informations sur IIS :

- http://www.mmt-fr.org/article283.html
- http://www.lhebergeur.fr/iishelp/iis/htm/core/iiiisin.htm
- http://www.laboratoire-microsoft.org/videos/5359
- http://technet.microsoft.com/fr-fr/library/cc785089(WS.10).aspx

Attention, par défaut Isa Server 2006 bloque l'accès en écriture au site web FTP.

Pour désactiver, cela il faut configurer le filtre applicatif FTP au niveau de la règle d'accès qui autorise le FTP en sortie par exemple.



2.6.3 Protocole SMTP

Le protocole SMTP est le protocole standard pour la messagerie. Isa Server est capable de bloquer certaines méthodes SMTP à l'aide du filtre d'application SMTP intégré nativement dans lsa Server. Pour plus d'informations sur le protocole SMTP :

<u>http://www.commentcamarche.net/contents/internet/smtp.php3</u>

2.6.4 Le protocole RDP (Terminal Server mode administration à distance) :

Il est utilisé pour permettre la prise en main à distance d'une station de travail (à partir de Windows XP) ou d'un serveur (depuis Windows 2000 Server).

Pour se connecter en bureau à distance, utiliser le client Bureau à distance : MSTSC.EXE. Pour activer le bureau à distance sur une station de travail ou un serveur, aller dans le panneau de configuration | Système et cliquer sur « *Utilisation à distance* ».

Il peut être intéressant de configurer le protocole RDP pour n'écouter que sur une carte réseau spécifique (sur Windows Server 2000 Server et ultérieur).



Pour plus d'informations :

- http://technet.microsoft.com/en-us/library/cc754746(WS.10).aspx
- http://www.microsoft.com/windowsserver2003/techinfo/overview/quickstart.mspx
- http://support.microsoft.com/kb/324820/en-us

2.6.5 Le service d'annuaire Active Directory :

Isa Server 2006 peut être configuré pour filtrer l'application des règles selon des ensembles d'utilisateurs. Ces derniers peuvent être entre autres des utilisateurs ou des groupes du domaine Active Directory. Pour plus d'informations sur Active Directory :

- http://www.windowsreference.com/dns/step-by-step-guide-for-windows-server-2003-domaincontroller-and-dns-server-setup/
- http://msreport.free.fr/?p=85
- http://msreport.free.fr/?p=155

2.6.6 Les certificats :

Pour créer une règle de publication web de type pontage SSL (deux sessions HTTPS), il est nécessaire d'installer un certificat sur le serveur Isa Server 2006.

Isa Server 2006 doit aussi être capable d'établir une connexion HTTPS au serveur web interne sans émettre d'alerte. Pour cela le certificat du serveur web interne doit :

- Ne pas avoir expiré.
- Avoir été généré par une autorité de certification de confiance.
- Contenir le nom avec lequel Isa Server a établi la connexion.

Pour plus d'informations sur les certificats et les autorités de certification :

- http://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman
- http://fr.wikipedia.org/wiki/Certificat %C3%A9lectronique
- http://www.laboratoire-microsoft.org/videos/10692/
- http://technet.microsoft.com/fr-fr/library/aa998956(EXCHG.65).aspx

3 Présentation d'Isa Server 2006 :

3.1 Présentation générale :

Isa Server 2006 est :

- Un pare feu qui peut filtrer sur les couches 3, 4 et 7 du modèle OSI.
- Un routeur.
- Un serveur NAT.
- Un serveur VPN.
- Un serveur proxy / reverse proxy.
- Un IDS / IPS (très basique).

Isa Server 2006 existe en deux versions :

- Standard.
- Entreprise.

Le tableau ci-dessous liste les différences entre les deux versions :

Feature	Standard Edition	Enterprise Edition
Scalability		
Networks	Unlimited	Unlimited Adds enterprise networks
Scale up	Up to 4 CPUs, 2-gigabyte (GB) RAM	Unlimited (per operating system)
Scale out	Single server	Up to 32 nodes through Network Load Balancing
Caching	Single-server store	Unlimited (through Cache Array Routing Protocol [CARP])
Availability		
Windows Network Load Balancing (NLB) Support	Not supported	Yes (integrated)
Manageability		
Policies	Local	Array and enterprise policies use Active Directory Application Mode (ADAM)
Branch office	Through the manual import and export of policy	Enterprise-level and array-level policies
Monitoring/alerting	Single-server monitoring console Microsoft Operations Manager (MOM) Management Pack	Multiserver monitoring console MOM Management Pack
Multiple networks	Templates	Templates

Pour plus d'informations :

http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/editions.aspx

3.2 Scénario de déploiement :

Isa Server peut être déployé selon plusieurs scénarios :

- Pare feu de périmètre : Dans ce scénario, Isa Server dispose de deux cartes réseaux. Il peut servir pour faire du filtrage (sur les niveaux 3, 4 et 7 de la couche OSI), de serveur proxy (proxy / reverse proxy), d'IDS / IPS et de serveur VPN.
- Pare feu avant / pare feu arrière : ce mode consiste à déployer deux pare feu (de préférence deux modèles différents) entre le réseau interne et le réseau externe. Ce mode de déploiement permet de créer un réseau de périmètre (ou DMZ) entre les deux pare feu. La Best Practice consiste alors à déployer tous les serveurs à publier sur Internet au niveau de la DMZ.
- Single Network Card : Isa Server dispose alors d'une seule carte réseau. Dans ce mode, Isa Server 2006 fonctionne uniquement comme un serveur proxy et reverse proxy.



Pour plus d'informations sur le scénario de déploiement d'Isa Server 2006 avec une seule carte réseau :

- <u>http://technet.microsoft.com/en-us/library/bb794774.aspx</u>
- http://microsoftsolution.blogspot.com/2008/03/configuration-of-isa-server-2006-in.html
- http://www.isaserver.org/tutorials/ISA-Server-2006-Network-Templates.html
- http://technet.microsoft.com/en-us/library/cc302586.aspx

Pour plus d'informations sur les scénarios de déploiement d'Isa Server 2006 :

http://www.labo-microsoft.com/whitepapers/21518

3.3 Un produit extensible :

Il existe de nombreux plugins qui permettent d'étendre les fonctionnalités d'Isa Server. Le module additionnel <u>Kaspersky Anti-Virus for Microsoft ISA Server</u> permet par exemple de détecter les virus et les spyware au niveau des flux HTTP et FTP qui transitent à travers Isa Server 2006. Une liste des modules additionnels pour Isa Server est fournit par le site web <u>http://www.isaserver.org</u> (au niveau de la page d'accueil).

3.4 Le successeur d'Isa Server 2006 :

Le successeur d'Isa Server 2006 s'appelle Forefront Threat Management Gateway (TMG) 2010. Le programme a été complètement redéveloppé.

Pour plus d'infirmations :

- http://www.microsoft.com/Forefront/edgesecurity/iag/en/us/default.aspx
- http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=e05aecbc-d0eb-4e0fa5db-8f236995bccd
- http://www.mslive.fr/actualites-640-forefront-threat-management-gateway-(tmg)-2010-est-rtmtestez.aspx

4 Définir son architecture réseau cible :

Avant tout déploiement d'Isa Server 2006, il faut définir son architecture cible.

4.1 Définir l'architecture cible Isa Server 2006 :

Avant de se lancer dans l'installation d'Isa Server 2006, il faut déterminer l'architecture réseau cible. Pour cela, il faut répondre aux questions suivantes :

- Quels sont les sous réseaux IP au niveau du réseau local ?
- Quels est le type de relation entre chaque réseau (interne, externe, périmètre) ? Il existe deux types de relation réseau possible, NAT ou ROUTAGE.
- Dois-je créer un réseau de périmètre ?
- Quels sont mes besoins en termes de bande passante ?
- Quel sera le scénario de déploiement d'Isa Server 2006 ?
- Quel est mon budget ?

La majorité des incidents Isa Server sont le fait d'une mauvaise configuration des réseaux Isa Server. Certains clients oublient par exemple de déclarer dans la TAL (dans le réseau Interne d'Isa Server) certains sous réseaux IP du LAN. Isa Server considère alors que ces réseaux sont externes à l'entreprise et refuse alors toutes demandes depuis les machines de ces sous réseaux IP. Ces dernières arrivent en effet via la patte interne de l'ISA alors qu'elles devraient arriver par la patte externe. Pour plus d'informations sur la configuration des réseaux Isa Server 2006, voir :

<u>http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx</u>

4.2 Architecture de résolution de noms DNS :

Un autre point très important concerne la résolution de noms DNS. Il y a deux grandes écoles :

- Tous les équipements réseaux sur le LAN autres que le serveur ISA ne peuvent pas résoudre les noms DNS externes.
- Les équipements réseaux sur le LAN peuvent résoudre les noms DNS externes. Dans ce cas, il faut créer une règle d'accès qui autorise le protocole DNS (TCP 53 / UDP 53) du réseau interne vers le réseau externe.

Pour plus d'informations :

- <u>http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part1.html</u>
- <u>http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part2.html</u>
- <u>http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part3.html</u>
- http://www.isaserver.org/tutorials/Definitive-Guide-ISA-Firewall-Outbound-DNS-Scenarios-Part4.html

4.3 Le type de client Isa Server :

Isa Server 2006 dispose de trois types de client :

- Le client proxy web : il permet d'utiliser le moteur proxy d'Isa Server. Ce client permet de filtrer uniquement l'accès aux sites web HTTP, HTTPS et FTP. Le client proxy web permet de filtrer sur des ensembles d'utilisateurs.
- Le client Secure NAT : il permet d'utiliser le moteur de routage / NAT d'Isa Server 2006 et donc de filtrer les accès à tous les protocoles. Il ne permet pas de filtrer sur des ensembles d'utilisateurs. Pour être client Secure NAT, le flux réseau doit transiter par le serveur Isa Server. Le cas le plus simple est celui d'une station de travail qui a Isa Server comme passerelle par défaut.
- Le client pare feu : il s'agit d'un logiciel à déployer sur toutes les stations de travail Windows. Ce dernier est disponible sur le CD d'installation dans le dossier client ou sur Internet. <u>http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=05C2C932-B15A-4990-B525-66380743DA89</u>

Ce type de client permet de filtrer les accès à tous les protocoles et d'utiliser le filtrage sur les ensembles d'utilisateurs.

4.4 Quelques sites web sur Isa Server 2006 :

Site web français :

- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb758895.aspx
- http://www.microsoft.com/france/Vision/Recherche.aspx?Qry=&S=x&Did=&Pid=611c646f-3a25-4594-8c6a-6daff00e1a0b&Nid=&Cid=&Tid=&x=52&y=6
- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb758895.aspx
- http://www.labo-microsoft.com/articles/server/ISA2004/
- http://www.labo-microsoft.com/whitepapers/isa server 2000 et 2004

Site web Technet anglais :

- http://technet.microsoft.com/en-us/library/bb898433.aspx
- http://www.isaserver.org/
- http://technet.microsoft.com/fr-fr/forefront/edgesecurity/bb734830.aspx

5 Installation d'Isa Server 2006 :

Les étapes suivantes doivent être effectuées lors d'une installation d'Isa Server 2006 :

- Installer Windows 2003 SP2 + derniers correctifs.
- Installer Isa Server 2006.
- Installer le service pack 1 d'Isa Server 2006.
- Sécuriser le serveur lsa Server 2006 (documenter et former l'équipe d'administration du client). A faire après avoir configurer toutes les règles de filtrage et activer toutes les fonctionnalités (VPN...).
- Désactiver le TOE.
- Exécuter Isa Server Best Practice Analyser.
- Optimiser les performances d'Isa Server 2006.

Remarque :

• Ne pas définir de passerelle par défaut sur la carte réseau interne d'Isa Server 2006.

5.1 Installation d'Isa Server 2006 :

Les sources d'installation d'Isa Server 2006 peuvent être téléchargées à l'adresse suivante :

http://www.microsoft.com/downloads/details.aspx?familyid=6331154B-A923-45DD-8520-48B63B6BE97B&displaylang=fr

Avant de lancer l'installation d'Isa Server 2006, vérifier que votre serveur respecte les pré-requis pour l'installation d'Isa Server 2006.

http://technet.microsoft.com/en-us/library/cc304520.aspx



Dans notre cas, nous allons installé le premier serveur lsa Server 2006 Entreprise Edition. Il nous faut donc installer un serveur de stockage de configuration et les services lsa Server 2006.



Nous allons créer un nouveau Isa Server 2006 Entreprise.

Nous verrons par la suite que nous pourrons créer des règles d'entreprise et des règles pour des groupes lsa Server.

🚏 Microsoft ISA Server 2006 - Assistant Installation	🔀 🖟 Microsoft ISA Server 2006 - Assistant Installation	
Sélection de composants	Options d'installation pour ISA Server Enterprise	
Les fonctionnalités sélectionnées seront installées.	Créez-vous sur ce Serveur de stockage de configurations un nouvel ISA Server Enterprise ou un replica d'une configuration ISA Server Enterprise existante ?	
Cliquez sur une icône de la liste pour voir ou modifier le mode d'installation d'une fonctionnalité.	 Créer un nouvel ISA Server Enterprise Le choix de cette option aura pour effet la création d'un nouvel ISA Server Enterprise. Cet ordinateur va devenir un Serveur de stockage de configurations mis au service des groupes. Créer un replica d'une configuration ISA Server Enterprise Le choix de cette option aura pour effet la reproduction sur cet ordinateur des paranèters de configuration ISA Server Enterprise 	
requièrent 80 Mo sur le disque dur.	stockage de configurations. Cette option diminue la vulnérabilité aux erreurs par la mise à disposition d'un replica de la configuration ISA Server Enterprise. Les groupes de serveurs ISA Server nouvront écalement utiliser ce Serveur de stockage	
Installer dans :	de configurations.	
C:\Program Files\Microsoft ISA Server\ Modifier		
Ajde Espace < Brécédent Quivant > Annuler	<pre></pre>	

L'étape ci-dessous permet de configurer le réseau interne de l'Isa Server 2006.

La TAL (Table d'adresses locales) correspond en fait aux plages d'adresses IP du réseau interne. Attention, vous devez ajouter tous les sous réseaux IP de votre LAN et pas seulement le sous réseau IP correspondant à la patte interne de votre Isa Server 2006.

🖟 Microsoft ISA Server 2006 - Assistant Installation	Adresses	×
Réseau interne	Liste des plages d'adresses IP définies da	ins ce réseau :
Spécifiez la plage d'adresses à ajouter au réseau interne ISA Server.	Adresse de début Adresse de fin	Ajouter une carte
Cliquez sur Ajouter pour spécifier les plages d'adresses réseau.		Modi <u>f</u> ier
Plages d'adresses du réseau interne (début-fin) :		Supprimer
		Ajout un réseau pri <u>v</u> é
		Ajouter une plage
Pour plus d'informations, consultez le Guide d'installation.	_	
< Précédent Suivant > Annuler	Ī	OK Annuler

Sélectionner les cartes réseau	🛱 Microsoft ISA Server 2006 - Assistant Installation
Sélectionnez les cartes réseau associées au réseau que vous configurez.	Connexion des clients de pare-feu
Cartes réseau :	Indiquez si ISA Server 2006 accepte les connexions des clients de pare-feu pour lesquels le chiffrement n'est pas pris en charge.
Nom ImpLAN - interne ImpLAN - interne ImpLAN - interne ImpLanterNET - externe ImpLanterNET - exterNET - exterNET -	ISA Server 2006 chiffre les échanges avec les clients de pare-feu effectués via leur canal de contrôle pour les ordinateurs exécutant le logiciel Client de pare-feu 4.0 ou une version ultérieure.
	ISA Server 2006 ne chiffre pas les échanges avec les clients de pare-feu exécutant une version antérieure du logiciel Client de pare-feu, ou installés sur un ordinateur équipé de Windows 98 SE, Windows ME ou Windows NT 4.0.
Informations sur la carte réseau :	
Nom : Carte AMD PCNET Family Ethernet PCI #2 Adresses IP : 192.168.67.4 Informations de routage : 192.168.67.0 - 192.168.67.255	Autoriser la conne <u>xion des clients de pare-feu non cryptés</u>
×	client de pare-feu.
OK Annuler	< Précédent Suivant > Annuler
🖗 Microsoft ISA Server 2006 - Assistant Installation	📕 🚰 Microsoft ISA Server 2006 - Assistant Installation
Avertissement relatif aux services	Installation du logiciel Microsoft ISA Server 2006
Lors de l'installation, certains services s'exécutant localement sur cet ordinateur peuvent être redémarrés ou désactivés.	Les composants que vous avez sélectionnés vont être installés.
Les services suivants vont être redémarrés au cours de l'installation :	Veuillez patienter pendant l'installation du logiciel Mcrosoft ISA Server 2006 . Cette opération peut durer plusieurs minutes.
Service SNMP Service de publication FTP	
Protocole NNTP Service d'administration IIS	Etat :
Service de publication World Wide Web	instalation sur de veur de stockage de configurations
Les services suivants vont être désactivés au cours de l'installation :	
Pare-feu de connexion Internet (ICF) / Partage de connexion Internet (ICS) Traducteur d'adresses réseau IP	
< Précédent Suivant > Ar	nuler Spérédent Quivant > Annuler

Pour plus d'informations :

- http://technet.microsoft.com/en-us/library/bb794846.aspx
- http://technet.microsoft.com/en-us/library/bb794856.aspx

5.2 Installer le service pack 1 d'Isa Server 2006 :

Installer le service pack 1 est très fortement recommandé. Il apporte de nombreuses fonctionnalités et corrections de bugs dont :

- Le suivi des modifications de la configuration : cela permet d'enregistrer toutes les modifications de configuration appliquées à ISA Server. Penser à créer des comptes d'administration lsa Server nominatif pour bénéficier pleinement de cette fonctionnalité.
- Le bouton *Tester* : teste la cohérence d'une règle de publication Web entre le serveur publié et ISA Server.
- Le simulateur de trafic : simule le trafic réseau conformément à des paramètres de demande spécifiques, tels qu'un utilisateur interne et le serveur Web, et fournit des informations sur les règles de stratégie du pare-feu évaluées pour la demande.
- La visionneuse Journalisation des diagnostics : désormais intégrée comme onglet dans la Console d'administration d'ISA Server, cette fonction affiche des événements détaillés sur l'évolution d'un paquet et fournit des informations sur le traitement et la mise en correspondance d'une règle.
- La prise en charge du mode d'équilibrage de charge réseau intégré en trois modes, dont monodiffusion, multidiffusion et multidiffusion avec protocole IGMP (Internet Group Management Protocol). Auparavant, ISA Server n'intégrait que le mode monodiffusion pris en charge par l'équilibrage de charge réseau.
- La prise en charge de l'utilisation de certificats de serveur contenant plusieurs entrées SAN (Subject Alternative Name). Auparavant, ISA Server était en mesure d'utiliser soit uniquement le nom de l'objet (nom commun) d'un certificat de serveur, ou la première entrée de la liste SAN

(Subject Alternative Name). Cette fonction est très importante surtout si vous souhaitez publier Outlook Anywhere (Exchange 2007).

 La prise en charge de l'authentification entre les domaines à l'aide de la délégation Kerberos contrainte (KCD). Les informations d'identification des utilisateurs situés dans un autre domaine qu'ISA Server mais dans la même forêt peuvent désormais être déléguées à un site Web publié interne à l'aide de la délégation Kerberos contrainte.

Le service pack 1 d'Isa Server 2006 peut être téléchargé à cette adresse :

http://www.microsoft.com/downloads/details.aspx?FamilyID=d2feca6d-81d7-430a-9b2db070a5f6ae50&displaylang=fr

Pour plus d'informations sur les nouveautés du service pack 1 :

- http://www.isaserver.org/tutorials/New-ISA-Firewall-2006-Service-Pack1-Part1.html
- http://www.isaserver.org/tutorials/New-ISA-Firewall-2006-Service-Pack1-Part2.html
- http://technet.microsoft.com/en-us/library/cc707227.aspx

Pour déterminer le niveau de service pack de chaque composant d'Isa Server 2006 :

<u>http://www.isaserver.org/tutorials/Determine-Correct-ISA-Server-Version-Service-Pack-Information.html</u>

5.3 Renforcer la sécurité d'Isa Server 2006 (à faire une fois toutes les règles configurées) :

Microsoft préconise de dédier un serveur à Isa Server 2006. Les services Windows non nécessaires au fonctionnement d'Isa Server peuvent donc être désactivés afin de réduire la surface d'attaque. Attention ce type de paramétrage étant très complexe, il est préconisé :

- De valider sur maquette le bon fonctionnement d'Isa Server avec ce paramétrage.
- De documenter ce paramétrage.
- De former les équipes d'administration du client.
- En cas d'ouverture d'incident au support Microsoft, pensez toujours à signaler que l'assistant de configuration renforcé de la sécurité à été exécutée sur le serveur lsa Server 2006.

L'article suivant explique comment renforcer la sécurité du serveur lsa Server 2006 :

http://technet.microsoft.com/fr-fr/magazine/2008.09.isahardening.aspx



Penser à télécharger la mise à jour de l'assistant de configuration de la sécurité pour lsa Server 2006.

http://www.microsoft.com/downloads/details.aspx?familyid=2748a927-bd3c-4d87-80fa-8687d5e2ab35&displaylang=en

Ouvrir ensuite le document IsaScwHlp.doc et appliquer la procédure indiquée.

Attention, si le serveur lsa Server 2006 est membre du domaine, penser à autoriser les services nécessaires au bon fonctionnement du domaine !

Si le serveur Isa est serveur VPN aussi, pensez à autoriser le service VPN. Le VPN d'Isa Server 2006 s'appuie en effet sur le service RRAS de Windows 2003 Server.

Penser à sélectionner le service client DHCP. C'est lui qui gère la mise à jour dynamique DNS. Ce service doit être démarré !





5.4 Désactiver le TOE (TCP Offload Engine)

Le service pack 2 de Windows 2003 Server active par défauts les nouvelles fonctionnalités de TOE (TCP Offload Engine). Hors ces fonctionnalités sont incompatibles avec lsa Server 2006.

Type de l'événement :AvertissementSource de l'événement :Microsoft ISA Server ControlCatégorie de l'événement :AucunID de l'événement :30520Date :07/02/2010Heure :12:11:47Utilisateur :N/AOrdinateur :ISAGM40Description :Windows Server 2003 Scalable Network Pack, qui est inclus

Windows Server 2003 Scalable Network Pack, qui est inclus dans Windows Server 2003 Service Pack 2, est activé. Certaines fonctionnalités d'ISA Server ne fonctionnent pas correctement si une carte réseau installée sur un ordinateur ISA Server prend en charge et utilise les fonctionnalités du Scalable Network Pack. Pour plus d'informations, voir l'article 948496 de la Base de connaissances Microsoft. Si vous ne possédez pas de carte réseau prenant en charge les fonctionnalités du Scalable Network Pack, vous pouvez désactiver l'alerte active Windows Server 2003 Scalable Network Pack.

Une Best Practice est donc de désactiver ces fonctionnalités. Pour plus d'informations, voir :

- <u>http://isafirewalls.org/blogs/isa/archive/2007/03/29/attention-il-y-a-qque-soucis-isa-server-avec-le-sp2-de-windows-2003.aspx</u>
- http://msreport.free.fr/?p=163

Pour plus d'informations sur le TOE, voir :

http://en.wikipedia.org/wiki/TCP Offload Engine

5.5 Exécuter Isa Server Best Practice Analyser :

Le Best Practice Analyser peut être téléchargé à l'adresse suivante :

http://www.microsoft.com/downloads/details.aspx?FamilyId=D22EC2B9-4CD3-4BB6-91EC-0829E5F84063&displaylang=en

Lancer un scan et afficher le rapport ensuite.

Mirrosoft 15A Server Best	Practices Analyzer Tool		Microsoft SA Server Best Tructices Andrees Teal				
Microsoft ISA Server Best Practices Analyzer Tool			Microsoft ISA Server Best Practices Analyzer Tool				
We reame State a scan State a scan State a scan State a Beel Plact cer attento vieco	Start a Scan	Scende is so typreisen	Wenne Scanning Completed Set a rev Section 4 Section 4				
They a separat	Scantype	Health Check	G Start BPA2Mae	Scarring nummer			
Schadule a scien	Discussion		Ses also	Tote: 4 completed			
See alm			The ISA Server Bott Decision Analogy Ketto				
The ISA Server Bed Disclore: Assignment Late			🗇 Stout the ISO Server Bert	Hadwae	() Competence		
About the ISA Server Best			Send at your feedback.	15A Seriganter	Completed		
Placitice: Analyze:				ISA isstalation	Carrietor vel		
Updates and Oustomer				Objecting System	Complexed		

Dans l'exemple ci-dessous, le Best Practice Analyser remonte entre le fait que l'on n'a pas désactivé le pack SNP de Windows 2003 SP2.

Microsoft ISA Server Best P	ractices Analyzer Tool
Microsoft ISA S	erver Best Practices Analyzer Tool
Welcome Suit a scan Select a Ben Practices scan to view Weiw a model Start BPA2visis Schedule a scan Sec also The ISA Server Beet Practise Analyzer Heb Photo the ISA Server Beet Practise Analyzer Send us your feedbock Update and Outbomor Facdback	View Best Practices Report Sen dels configuiént Sett Report Type:

Attention dans certains cas, lsa Server peut remonter des faux positifs ou encore remonter un problème qui a été corrigé.

Purger le contenu du journal application (où est référencée l'erreur) permet de faire disparaître certaines entrées du Best Practice Analyser.

Pour plus d'informations sur le Best Practice Analyser Tool :

http://www.isaserver.org/tutorials/ISA-Best-Practices-Analyzer-Visio.html

5.6 Optimiser les performances d'Isa Server 2006 :

Appliquer les préconisations de l'article Microsoft suivant :

http://www.isaserver.org/tutorials/Optimizing-ISA-performance-Part2.html

6 Configuration du serveur Isa Server 2006 :

Pour découvrir lsa Server, je vous préconise la lecture des articles SUPINFO suivants :

- http://www.labo-microsoft.com/articles/server/ISA2004/
- http://www.labo-microsoft.com/whitepapers/isa server 2000 et 2004

6.1 Configuration des réseaux Isa Server 2006 :

Dans cette partie nous allons voir comment :

- Lister les principaux réseaux lsa Server 2006.
- Créer et configurer les réseaux lsa Server 2006.
- Comment configurer les règles de réseau Isa Server 2006 (NAT ou routage).

6.1.1 Faire un schéma de son réseau :

Tout d'abord, il nous faut un schéma de notre réseau.



Dans notre cas, le réseau local est divisé en trois sous réseaux IP :

- 192.168.67.0 /24
- 192.168.68.0 / 24
- 192.168.69.0 / 24

6.1.2 Les réseaux lsa Server 2006 :

Attention, Isa Server 2006 ne peut filtrer le trafic qu'entre deux réseaux Isa Server 2006.

Il est donc important de bien définir les réseaux Isa Server (toute la complexité d'Isa Server 2006 est là). A l'installation, on doit saisir la TAL (Table d'adresses locales). Cette TAL correspond en fait au réseau INTERNE d'Isa Server.

Microsoft Internet Security and Acceleration Ser	ver 2006				_ 8
Eicher Action Affichage					
⇔ → È 🗷 😤 🖬 🖹 😤 🔶 😔					
Microsoft Internet Security and Acceleration Server 20 B Entreprise Groupes Security Security	Microsoft* Internet Security & Acceleration Server 20 Enterprise Edition	_{XX6} Serveur de stockage de cor	nfigurations : isagm40).production40.l	an Réscoux
Surveillance Stratégie de pare-feu (isagm40)	() <u>Cliquez ici pour en savoir</u>	plus sur le Programme d'amélio	ration du produit.		
Réseaux privés virtuels (VPN)	Réseaux				
Général Pépannage	Réseaux Ensembles de ré-	Pare-feu de périmètre Réseau interne Réseau V Chaine	Réseau ex (Intern cal	eau Clients VFN terne et	
	Nom -	Plages d'adresses	Réseaux d'entreprise	Lieu de la défi	Description
	Réseaux				
	Clients VPN	🖽 Aucune adresse IP n'est actu		Local	Objet réseau dynamique intégré
	🚜 Clients VPN en quarant	💷 Aucune adresse 1P n'est actu		Local	Réseau dynamique intégré repré
	Externe	📼 Adresses IP externes aux rés		Local	Objet réseau dynamique intégré
	👍 Hôte local	🖽 Aucune adresse IP n'est asso		Local	Objet réseau dynamique intégré
		192 192 168.67.0 - 192,168.67.255	2	Local	Réseau représentant le réseau i

Dans notre cas, le réseau interne doit donc être configuré de la manière suivante :

ropriétés de Interne 🥂 🗙						
Client de pare-feu Proxy Web CARP Équilibrage de charge réseau						
Général Adresses	Domaine Navigateu	r Web	Détection automatiqu	je į		
Plages d'adresses IP incl	uses dans ce réseau :					
Adresse de début	Adresse de fin	Ajou	uter une carte			
192.168.67.0	192.168.67.255					
192.168.68.0	192.168.68.255		Modifier			
192.168.69.0 192.168.69.255						
		Supprimer				
		Ajout	er un réseau pri <u>v</u> é 👘			
Ajouter une plage						
Réseaux d'entrepris	se :	Aiou	iter un réseau			

Attention, il faut que la configuration des réseaux lsa Server (dont le réseau INTERNE) soit cohérente avec la table de routage du serveur ISA SERVER 2006.

Pour cela, aller dans l'invite de commande Windows et taper la commande *ROUTE PRINT*.

C:\WINDOWS\system32\CMD.exe

C:\Documents and Settings\Administrateur.PRODUCTION40>route print

IPv4 Table de routa	age			
Liste d'Interfaces 0×1 0×1000308 00 2 0×1000408 00 2	MS T 7 52 54 77 7 87 aa 30	CP Loopback inter Carte AMD PCNET F Carte AMD PCNET F	face amily Ethernet P(amily Ethernet P(====================================	:I :I #2 ======
=======================================		====================		=====
ltineraires actifs	: <u> </u>	~ 1 1		M44
Destination reseau	Masque reseau	Hdr. passerelle	Hdr. interface	metrique
0.0.0.0		173.252.17.254	173.252.17.1	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.67.0	255.255.255.0	192.168.67.254	192.168.67.254	20
192.168.67.254	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.67.255	255.255.255.255	192.168.67.254	192.168.67.254	20
193.252.19.0	255.255.255.0	193.252.19.1	193.252.19.1	20
193.252.19.1	255.255.255.255	127.0.0.1	127.0.0.1	20
193.252.19.255	255.255.255.255	193.252.19.1	193.252.19.1	20
224.0.0.0	240.0.0.0	192.168.67.254	192.168.67.254	20
224.0.0.0	240.0.0.0	193.252.19.1	193.252.19.1	20
255.255.255.255	255.255.255.255	192.168.67.254	192.168.67.254	1
255.255.255.255	255.255.255.255	193.252.19.1	193.252.19.1	1
Passerelle par défa	aut : 193.252.1	9.254		
				=====
Itinéraires persist Aucun	tants :			
C:\Documents and Se	ettings\Administra	teur.PRODUCTION40	>_	

Dans notre cas Isa Server 2006 dispose de deux cartes réseau :

- La carte réseau interne est en 192.168.67.254/24 (adresse IP privée).
- La carte réseau externe est en 193.252.19.1/24 (adresse IP publique)
- La passerelle par défaut sur la carte externe est 193.252.19.254 (adresse IP publique).
- Il n'y a pas de route statique.

Dans notre cas le serveur ISA a donc une carte réseau sur Internet (adresse IP publique). La relation réseau entre le réseau interne et externe doit donc être NAT car le sous réseau IP interne est en adressage IP privé.

Il y a cependant une erreur de configuration dans la table de routage. Les réseaux 192.168.68.0/24 et 192.168.69.0/24 ne sont pas déclarées et sont donc considérées comme des sous réseaux externes.

D'après le schéma, ces réseaux sont accessibles depuis lsa Server **via le routeur en 192.168.67.253.** Pour rappel, il est interdit de définir une passerelle par défaut au niveau de la carte réseau interne d'Isa Server 2006. Nous allons donc ajouter des routes statiques vers les réseaux 192.168.68.0 et 192.168.69.0.

Pour cela, il faut taper les commandes suivantes :

- Route add 192.168.68.0 mask 255.255.255.0 192.168.67.253 -p
- Route add 192.168.69.0 mask 255.255.255.0 192.168.67.253 -p

On affiche ensuite la table de routage avec la commande route print.

_ 8

Documents and Settings\Administrateur.PRODUCTION40>Route add 192.168.68.0 mas 255.255.255.0 192.168.67.253 -p C:\Documents and Settings\Administrateur.PRODUCTION40>Route add 192.168.69.0 mas k 255.255.255.0 192.168.67.253 -p C:\Documents and Settings\Administrateur.PRODUCTION40>route print IPv4 Table de routage Liste d'Interfaces MS TCP Loopback Øх1 interface 0x10003 ...08 00 27 52 54 77 0x10004 ...08 00 27 87 aa 30 Carte AMD PCNET Family Ethernet PCI Carte AMD PCNET Family Ethernet PCI #2 Itinéraires actifs : Destination réseau 0.0.0.0 127.0.0.0 192.168.67.0 192.168.67.254 25 192.168.67.255 192.168.68.0 192.168.68.0 Masque réseau 0.0.0.0 255.0.0.0 255.255.255.0 Adr. passerelle 193.252.19.254 127.0.0.1 192.168.67.254 Adr. interface Métrique 193.252.19.1 20 127.0.0.1 1 20 20 20 192.168.67 127 168.67.25 168.67. 192 192 192.168 192.168. 1 192.168 168.69.0 252.19.0 252.19.1 2.19.255 255 192 1 168 20 20 20 255 19 3 255. 255. 255. 127.0 255 255 255 3 192. 20 20 20 240.0.0.0 240.0.0.0 255.255.255 255.255.255 192.168.67 224.0. 224.0. Ø. Й 168 193.252.19.1 192.168.67.254 193.252.19.1 Ø. Ø И 255. 168.67 255 255.255.255 192 255.255.255 255.255 193.252. 255 1 193.252.19.254 Passerelle par défaut : _____ ______ Itinéraires persistants : Adresse réseau Masqu 192.168.68.0 255. 192.168.69.0 255. lasque réseau 255.255.255.0 255.255.255.0 Adresse passerelle Métrique 192.168.67.253 1 192.168.67.253 1 Masque C:\Documents and Settings\Administrateur.PRODUCTION40>_

Pour plus d'informations sur la configuration des réseaux Isa Server 2006, voir :

- http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx
- http://technet.microsoft.com/en-us/library/bb794774.aspx
- <u>http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-</u> Part1.html
- http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part2.html
- <u>http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part3.html</u>

6.1.3 Quelques réseaux ISA Server à connaître :

- Hôte local : c'est le serveur ISA Server
- Client VPN : ce sont tous les clients externes qui ont établis une connexion en VPN sur le serveur Isa Server 2006.
- Client VPN en quarantaine : ce sont tous les clients externes qui ont établis une connexion en VPN sur le serveur Isa Server 2006 et qui sont en quarantaine (la fonction de quarantaine VPN est désactivée par défaut dans Isa Server 2006).

Cela veut donc dire qu'il est possible de filtrer le trafic par exemple entre autres entre :

- Le réseau interne et le serveur lsa Server 2006 (réseau hôte local).
- Le réseau VPN et le réseau interne. Il sera donc nécessaire de créer des règles d'accès pour permettre au client VPN d'accéder aux applications / serveurs sur le réseau interne ou d'accéder à Internet.

6.1.4 Configurer les règles de réseaux :

Il faut ensuite vérifier nos règles de réseaux.

Le réseau interne ISA Server dispose d'un réseau interne avec 3 sous réseaux IP en adressage IP privé.

Le réseau externe d'Isa Server 2006 en est en adressage IP publique (Internet).

Il nous faut donc une règle de réseau de type NAT entre le réseau interne et le réseau externe.

A savoir :

 Pour qu'une règle d'accès / règle de publication soit analysée, une règle de réseaux doit toujours existée entre le réseau source et le réseau de destination de la règle d'accès / règle de publication. Si cette règle de réseau n'existe pas, le trafic réseau est refusé par défaut par ISA Server 2006.



Propriétés de Accès Internet			opriétés de Accès Inter	net		<u>?</u> ×
Général Réseaux source Réseaux de destination Relation rés	eau	1	Général 🛛 Réseaux source	Réseaux de destination	Relation réseau	
Cette règle s'applique au trafic émanant de ces sources :			Cette règle s'applique au	i trafic envoyé à ces desti	nations :	
Clients VPN Clients VPN en quarantaine Interne Sup	iter Ifjer		Sxterne		Ajouter Modifjer Supprime	r



Pour plus d'informations sur la configuration des règles de réseaux :

- http://technet.microsoft.com/fr-fr/library/cc302676(en-us).aspx
- <u>http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part1.html</u>
- <u>http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part2.html</u>
- <u>http://www.isaserver.org/tutorials/Overview-ISA-TMG-Networking-ISA-Networking-Case-Study-Part3.html</u>

6.2 Règle d'accès ou règle de publication :

Une fois que l'on a créé les règles de réseaux, il faut créer les règles d'accès et les règles de publication.

Tout d'abord, avant de se lancer dans la configuration d'Isa Server, écrivez vos règles de filtrage sur papier.

Une fois les règles de filtrage écrites sur papier, il faut déterminer si l'on doit créer des règles d'accès ou des règles de publication. Pour cela, voir le tableau ci-dessous.

Relation entre le réseau source et le réseau destination	Sens	Règles ISA
Routage	Entrant ou sortant	Règle d'accès
NAT	Sortant	Règle d'accès
NAT	Entrant	Règle de publication

Remarque sur le sens :

Cas 1 :

- Source : réseau avec adresse IP privé
- Destination : réseau avec adresse publique
- Sens : sortant

Cas 2 :

- Source : réseau avec adresse publique
- Destination : réseau avec adresse IP privé
- Sens : entrant

6.3 Les accès par défaut au niveau du serveur lsa Server 2006 :

Par défaut, lsa Server bloque tout le trafic réseau. Il existe en effet une règle par défaut qui interdit tout le trafic réseau.



6.4 Les stratégies systèmes :

Par défaut, lsa Server 2006 crée des règles de stratégie système pour filtrer les accès vers et depuis le réseau Hôte Local (lsa Server).

Pour afficher ces règles, cliquer sur le menu « Affichage » puis « Afficher les règles de stratégie système ».

Eichier Action Affrichage 2							
💠 🔶 💽 🗊 🗸 Afficher les règles de	stratégie s <u>y</u> stèm	e					
Microsoft Inter Entreprise Groupes	stratégie d'entre	prise ≁ 2& ver:	2006 Serveur de stockage o	le configura	tions : ISARW4		Stratégi
E- JISARW Bersonnaiser			ir plus sur le Programme d'a	mélioration	du produit		
Stratégie de pare-feu (ISA	U Ciddez ici	DOUL EN SAVO	r blos sur le Programme o a	menoration	da produk.		
- 🧔 Réseaux privés virtuels (Vi	Stratégie de	pare-feu					
E-🎲 Configuration	Ordre +	Stratégie	Nom	Action	Protocoles	De l'Port découte	à
Berveurs		Fuctórna	A tericer les demandes HTT	Autovican		L HStolacol	🔁 Filos o devisó
	20	Systeme	Actoriseries demandes Pirra.	- Altoriser	MITPS		g sites autorise
Add-Ins	27	Système	Autoriser NTP depuis ISA Se	🕜 Autoriser	🖳 NTP (UDP)	👍 Hôte local	👍 Interne
	28	Système	Autoriser SMTP depuis ISA 5	🕝 Autoriser	🔍 SMTP	👍 Hôte local	📥 Interne
	29	Système	Autoriser HTTP depuis ISA 5	🕜 Autoriser	👰 НТТР	📥 Hōte local	🛓 Tous les rése
	🖃 📝 30	Système	Autoriser la communication e	🥑 Autoriser	🔣 Tout le trafic	👍 Hôte local	🍓 Ordinateurs d 🍓 Ordinateurs d
	🖃 💽 31	Système	Autoriser l'accès à distance	🕝 Autoriser	🖳 Stockage Par	👍 Hôte local	📥 Tous les rése 📋 Serveurs de s
	■ 👔 32	5ystème	Autoriser l'accès depuis des	⊘ Autoriser	Microsoft CIF Microsoft CIF Stockage Par	Hôte local Grdinateurs d Crdinateurs d Crdinateurs 1 Répliquer les Serveurs de g	👍 Hôte local
	🖃 💽 33	Système	Autoriser la réplication d'un	🥝 Autoriser	🖳 Réplication du 🖳 RPC (toutes i	👍 Hôte local 🍓 Répliquer les	👞 Hôte local 🍓 Répliquer les
	a 🛐 34	Système	Autoriser la communication i…	S Autoriser	Contrôle Pare Microsoft CIF Microsoft CIF Microsoft CIF Microsoft CIF	🌉 Serveurs de g	🚑 5erveurs de g

Ces règles peuvent être modifiées.

Isa Server 2006 a besoin d'un serveur DHCP pour attribuer des IP aux clients VPN. Le premier paramètre de la stratégie système va permettre de déterminer quels sont les serveurs DHCP qu'Isa Server peut utiliser.

diteur de stratégie système		?
Groupes de configuration	Général De	
 Services réseau DHCP DHCP DNS NTP Services d'authentificatic Active Directory RADIUS RSA SecurID Téléchargement de li Administration à distance Console MMC (Micro- 	Cette règle s'applique au trafic émanant d	de ces sources : Ajouter Modiĝer Supprimer
Administration Web ICMP (Ping) Services de diagnostic ICMP Gestion du réseau W Rapport d'erreurs Mi Vérificateurs de conr Journalisation	Exceptions :	Ajouter Modrier Supprimer
		OK Annuler

Le paramètre ci-dessous permet d'autoriser lsa Server à se connecter au domaine. Décocher la case « *Appliquer une conformité RPC stricte* ».



Le paramètre ci-dessous permet de configurer lsa Server pour télécharger les dernières listes de révocation de certificats (CRL).



Pour plus d'informations sur les stratégies systèmes :

http://technet.microsoft.com/en-us/library/bb794729.aspx

6.5 Création de règle d'accès :

Les règles d'accès permettent de filtrer :

- Sur l'adresse IP source / destination, sur une URL (champs De et A).
- Sur un type de protocole (filtrage sur le port source / destination).
- Sur une plage horaire.
- Sur un ensemble d'utilisateurs.
- Sur les éléments de la couche 7 du modèle OSI (filtrage applicatif).
- Les types de contenus.

Une règle d'accès peut autoriser ou interdire le trafic.



Attention les définitions de protocoles ont un sens.

Pour autoriser en sortie le protocole HTTPS, il faut sélectionner la définition de protocole HTTPS (sens en sortie) et non la définition de protocole Serveur HTTPS (sens : en entrée).

Exemple avec le protocole FTP :

Propriétés de FTP				? ×
Général Paramètres]			
<u>Connexions</u> principal	es			-
Plage de ports	Type de prot	Sens	Ajou <u>t</u> er	
21	TCP	en sortie	Modifie <u>r</u>	
			Supprimer	
Connexions seconda	ires			
Plage de ports	ros Ivpe de prot	Sens	Aiouter	1
	· / F = F · - · · · · ·		Modifier	
			Supprimer	-
				┙╽
Eiltres d'application				-
Filtre d'accès FTP				
☑ <u>N</u> 'afficher que le	es filtres d'applica	ations sélectionnés		
		OK Ann	uler Applic	quer

Il faut ensuite spécifier la source (réseau interne) et la destination (réseau externe).

Dans notre cas, nous ne filtrons pas sur les ensembles d'utilisateurs. Il faut donc sélectionner « Tous les utilisateurs » (à la place de « *Tous les utilisateurs authentifiés* »).



Une fois la règle créée, il faut cliquer sur « Appliquer » pour qu'elle soit prise en compte.

6.6 Les règles de publication :

Il existe deux grands types de règle de publication :

- Les règles de publication de site web. C'est le moteur proxy d'Isa Server 2006 qui gère ce type de règles.
- Les règles de publication de protocoles de serveur non web. C'est le moteur NAT d'Isa Server qui gère ce type de règles.

Remarque :

- La règle de publication de l'accès de client web Exchange est une règle de publication du site web préconfigurée pour l'accès Outlook Web Access, ActiveSync et RPC over HTTPS. Cette règle permet de prédéfinir les répertoires virtuelles Exchange à publier entre autres.
- Pour plus d'informations sur les règles de publication : <u>http://technet.microsoft.com/en-us/library/bb794758.aspx</u>

6.6.1 Création d'une règle de publication de serveur non web :

Dans l'exemple ci-dessous, on va publier un serveur DNS situé sur le réseau interne 192.168.67.105. Comme il s'agit d'une règle de publication des protocoles de serveurs non web, c'est le moteur NAT d'Isa Server qui est utilisé. Il faut donc configurer le serveur DNS pour être client Secure NAT ; **Pour cela, configurer le serveur DNS avec comme passerelle le serveur ISA (192.168.67.254).**

- Add-ins d'entreprise	(1) Cliquez ici pour en sav	oir plus sur le Programme d'a	mélioration du produit.		Assistant Nouvelle règle de p	ublication de serveur
Sarr5 Surveilance Surveilance Surveilance Actu	Tableau de bord V Alertes	Y Sessions Y Services Y Config	ration Y Rapports Y Verficate	urs de c	Microsoft Internet Security & Acceleration Server 2006	Assistant Nouvelle règle de publication de serveur
Canliguer Experi A Server Iligae A See Mod Cach Mod Gene Gene V Dépanna Alde	rter ster fer la stratégie système (2000 0) 11:51:10 (2) jeud 4 février 2010 11:50:10 (2)	Appliquer le filtre Règle de publication de l'accès Règle de publication des serveu Règle de publication des stres 5 Règle de publication des protoc Bègle d'accès	Afficher tout de cleret Web Exchange de gourier haregoint b eles de serveurs gon-Web	prent Fide		De Ansistant vous side à créar une nouvelle règle de publication de service. Les ingées de publication de server magners les demandes des clients au serveur interne appripre. Non de la règle de publication de serveur : publication serveur DNS 152-158-57-105 Cliques au Suivent pour continues.
	 jeudi 4 février 2010 11:47:18 	ISAOR/S\oliver	Règle de stratégie [test] a	sjoutée		
	使 jeudi 4 février 2010 11:34:06	ISAORS\Administrateur	Groupe [isaor5] modifiée			< Frésédent Survant > Annuler
	11:47:18 (*) jeudi 4 février 2010 11:34:06	ISAOR5\Administrateur	Groupe [isaor5] modifie			Characterit Suvant> Annular

On rentre l'adresse IP de notre serveur DNS.

Il est possible de filtrer la connexion selon le port source ou de changer le port destination en cliquant sur l'onglet Ports.

En effet, Isa Server permet de configurer une règle qui permet de se connecter sur la patte externe du serveur Isa sur le port TCP 53 et de rediriger le trafic sur un serveur interne sur le port TCP 54 (Isa fait du *Port Translation Address* ou PAT). Dans notre cas il faudrait cependant reconfigurer le serveur DNS interne pour écouter les demandes sur le port TCP 54 au lieu du port TCP 53.

Assistant Nouvelle règle de publication de serveur	Assistant Nouvelle règle de publication de serveur	×
Sélectionner un serveur Spécifiez l'adresse IP réseau du serveur que vous publiez.	Sélectionnez un protocole Sélectionnez le protocole utilisé par le serveur publié.	
Agresse IP du serveur :	Protocole sélectionné :	P <u>r</u> opriétés
192 . 168 . 67 . 105 Parcounir		Ports
< <u>P</u> récédent <u>S</u> uivant > Annuler	Serveur NNTP Serveur NNTPS Serveur PNM	nt > Annuler

Il faut autoriser les demandes depuis le réseau externe. Le but est que notre serveur DNS soit accessible depuis Internet.

Assistant Nouvelle règle de publication de	e serveur 🔀	Assistant Nouvelle règle de p	ublication de serveur
Adresses IP des ports d'écoute résea Sélectionnez les adresses IP sur l'ordina demandes à destinction du serveur publ	u leur ISA Server qui écouteront les é.	Microsoft Internet Security & Acceleration Server 2006	Fin de l'Assistant Nouveau Règle de publication de serveur
É <u>c</u> ouler les demandes émanant de ces rése	eux :		L'Assistant Nouveau Bègle de publication de serveur est
Nom	Adlesses IP sélectionnées		présentera la configuration suivante :
🗖 🈂 Clients VPN	<toutes adiesses="" ip="" les=""></toutes>		
🔲 📥 Clients VPN en quarantaine	<toutes adiesses="" ip="" les=""></toutes>	_	
🗹 🌑 Externe	<toutes adiesses="" ip="" les=""></toutes>		Nom:
🔲 📥 Hôte local	<t adresses="" ip="" les="" putes=""></t>	The second second	Serveur publié :
🔲 🛁 Interne	<toutes adiesses="" ip="" les=""></toutes>		192.168.67.105
Contraction of the second seco	ZT as the subsection IDs		Service publié :
			Écouter sur :
	Adresse		Externe
Aide sur les ports d'écoute réseau			<u>•</u>
And an los pars a counte reseau			Cliquez sur Teiminer pour fermer l'Assistant.
	(Précédent Suivant > Annuler		CPrécédent Terminer Annuler

Depuis Internet, il est maintenant possible de se connecter au serveur DNS en se connectant sur le port TCP 53 sur l'IP de la carte réseau externe du serveur ISA.

Dans notre cas il faut faire un TELNET 193.252.19.1 53

6.6.2 Les règles de publication de serveur web :

On va maintenant voir comment publier un serveur web HTTP.

Tout d'abord, il faut comprendre que ce type de règle passe par le moteur proxy d'Isa Server 2006. Isa Server 2006 va donc jouer le rôle de mandataire.

Quand un utilisateur externe (sur Internet) se connecte sur un serveur web interne publié avec Isa Server 2006, deux sessions sont établies :

La première session est entre le client Internet et le serveur Isa.

• La seconde session est entre le serveur lsa et le serveur web interne.

Dans le langage Isa Server, on parle de pontage HTTP / HTTP.



La première partie de règle permet de configurer la session entre lsa Server et le serveur web interne. Attention dans le cas d'une règle de publication HTTPS – HTTPS (pntage SSL), il faut que le nom du serveur interne soit le même que celui contenu dans le certificat du serveur web interne.

Il est possible de publier qu'une partie d'un site web (un répertoire virtuel). Pour publier uniquement le répertoire virtuel OWA, mettre /**owa**/* **Ne pas oublier le** /*. **Dans le cas contraire la règle de publication ne fonctionnera pas.**

Assistant Nouvelle règle de pu	blication Web	Assistant Nouvelle règle de publication Web	×
Détails de publication inter Indiquez le nom interne du	nes ste Web que vous publiez.	Détails de publication internes Spécifiez le cherrin d'accès interne et les aptions de publication du site Web publé. Yous pouvez publier l'ansemble du site Web ou limiter l'accès à un dossier spécifique.	
Nom de site (ocal : Le nom de site (ocal est le nom d principe, il s'agit du nom entré p. site Web.	ccor5.production5.lan u site Web que vous publez, tel qu'il apparaît en local. En ar les utilisateurs locaux clans leur navigateur pour accèder au	Entrez le nom du ficher ou du dossier que vous souhaitez publier. Pour indure tous les fichiers et tous les sous-dossiers d'un dossier, entrez (*. Par exemple : mon_dossier/*. <u>Chemin d'accès (facultatif) : [</u> Le site Web suivant sera publié en fonction de votre sélection : Site Web : [https://doors.productionS.lan/	1
Si ISA Server ne peut pas rósou ou de l'adresse IP de l'ordinateu	dro le nom de site local, il peut se connecter à l'aide du nom r du serveur qui héberge le site.	Transmettre l'en-tête de l'hôte d'origine plutôt que l'en-tête réel spécifié dans le champ Nom de ste local, sur la page précédente	
🔽 Utiliser un nom ou une adres	se IP d'ordinateur pour se connecter au serveur publé		
<u>N</u> om ou adresse IP de l'ordinate	aur : 192.168.67.5 Pagcourir		
	< Précédent Suivant > Annuier	< <u>Précédent</u> Suivant > Annu	uler

La suite de la règle nous permet de configurer la session entre le client web et le serveur ISA Server 2006.

Il est possible comme avec IIS de filtrer selon le nom DNS (en tête d'hôte).

Dans notre cas, nous configurons la règle pour accepter les connexions avec tout nom de domaine. Il faut ensuite créer un port d'écoute pour configurer les paramètres d'authentification et l'adresse IP externe / le port d'écoute du serveur lsa Server.

Assistant Nouvelle règle de publication Web	Assistant Nouvelle règle de publication Web	×
Informations sur les noms publics Spédifiez le nom complet (FQDN) du domaine ou l'adresse IP que les utilisateurs devront entrer pour accéder au site publié.	Sélectionnez le port d'écoute Le port d'écoute Web spècifie les adresses IP et le port sur lesqueis le serveur ISA reste à l'écoute des demandes Web entrantes.	
Acceptar les demandes pour : Tout nom de domaine Les demandes Web entrantes serent transmises au site Web publié sons vérifier le nom de domaine.	Port d'écoute We <u>b</u> : Propriétée du port d'écoute : Propriétée Valeur	
Chemn d'accès (facuitatif) : Selon vos sélections, les recuétes envoyées à ce site (valeur de l'en-tête hûte) seront acceptées : Site :		
< Prócódent Suivant > Annuler	< <u>Précédent</u> Suivant > Ann	ler

Assistant Nouvelle définition	de port d'écoute Web	Assistant Nouvelle définition de port d'écoute Web
Assistant Nouvelle définition	de port d'écoute Web X Assistant Nouveau port d'écoute Web Dat Assistant vous aide à sider un port d'écoute V/de Les ports d'écoute Vieb spécifient la manière dont ISA Server écoute et authentine les demendes Web provenant des cients. Nem du port d'écoute Web ; port d'écoute 80 Diquez sur Survert pour continuer.	Selected converte centration de port d'écoute web Image: Selection de la converte de convert
	< Présédent Suivant > Annuler	< Bécédent Suivert> Annule

Dans notre cas, le serveur Isa Server 2006 dispose d'une seule adresse IP publique. Si le serveur Isa Server 2006 dispose de plusieurs adresses IP publiques, il est possible de publier le site web que sur cette IP.

Il faut ensuite sélectionner le protocole d'authentification correspondant. Isa Server 2006 permet par exemple une authentification par formulaire.



Le message ci-dessous s'affiche car on va faire de l'authentification en HTTP. Le mot de passe de l'utilisateur va donc passer en clair via Internet. Cela n'est très clairement pas à faire en production. Il faudra passer en HTTPS.



Sélectionner le port d'écoute web que l'on vient de créer.

La capture de droite permet ensuite de définir comment lsa Server 2006 va se connecter au serveur web interne.

Dans notre cas, on sélectionne « Authentification de base » (contrairement à ce qui est indiqué sur la capture).

Assistant Nouvelle règle de publication Web	X Assistant Nouvelle règle de publication Web X
Sélectionnez le port d'écoute Le port d'écoute Web spécifie les adresses IP et le port sur lesquels le serveur ISA reste à l'écoute des demandes Web entrantes.	Délégation de l'authentification ISA Server utilise la méthode de délégation de l'authentification pour authentifier la session qu'il ouvre auprès du site publié.
Port d'écoute Web: port d'écoute 80 Propriétés du port d'écoute : Propriétés Valeur Description Réseaux Externe Port (HTTP) Désativé Méthode d'authentification De base Méthode d'authentification De base	Sélectionnez la méthode utilisée par ISA Server pour s'authentifier auprès du serveur Web publié : Pas de délégation et le client ne peut pas s'authentifier directement Pas de délégation, mais le client peut pas s'authentifier directement Authentification de base Authentification de base Authentifications NTLM Negotiate (Kerberos/NTLM) Délégation Kerberos contrainte
< <u>Précédent</u> Suivant > An	nuler <u>Suivant S</u> Annuler

Sélectionner ensuite « *Tous les utilisateurs* ». Ce mode de configuration va faire que seul le serveur web interne demandera l'authentification (on évite d'avoir deux POPUP d'authentification). On peut aussi utiliser les nouvelles méthodes de « *Délégation Kerberos contrainte* » pour éviter la double authentification.

Assistant	t Nouvelle règle de publication Web	×
Enser Vi pi	mbles d'utilisateurs ous pouvez appliquer cette règle aux demandes de tous les utilisateurs. Vous ouvez également restreindre l'accès à des ensembles d'utilisateurs précis.	
Cette	règle s'applique aux demandes émanant des ensembles d'utilisateurs suivants : lous les utilisateurs	or
	Supprin	imer
Microsof	t Internet Security and Acceleration Server 2006	
1	Le port d'écoute Web sélectionné pour cette règle nécessite l'authentfication. Cepeni sélectionné pour une règle, l'authentification n'a pas lieu. Pour appliquer l'authentifical cocher Exiger que tous les utilisateurs s'authentifient dans la boîte de dialogue Auther Cliquez sur OK pour continuer ou sur Annuler pour modifier votre sélection.	idant, lorsque l'ensemble d'utilisateurs Tous les utilisateurs est ation à cette règle à l'aide de cette configuration, activez la case à entifications avancées du port d'écoute Web.
	OK Annuler	

Cliquer sur Terminer puis aller dans les propriétés de la règle. Par défaut Isa Server 2006 bloque l'authentification HTTP. Il faut donc aller modifier le port d'écoute et cocher la case « *Permettre l'authentification du client via HTTP* ».

Assistant Nouvelle règle de	aublication Web	4						- 22 		NI517 SF		_
	Elo do l'Assistant Nouvoau Rògio	a nare-feu (*	Strateg	ié de pare-les	<u>u</u>		T. constant	1	-	1.50	T	7
Microsoft	de publication Web	ivés virtuels	Ordre -	Stratègie	Rom	-	Action	Protocoles	De / Port d'écoub	: A	Condition	Description
Internet Security & Acceleration Server 2005		cn FS	Règles de stratégie d'entreprise appliquées avant la stratégie de pare-feu de groupe									
	L'Assistant Nouveau Règle de publication Web est terminé.	e.			AND							
	Le nouveau Regie de publication web présentera la configuration suivance :	6	Règles de	stratégie de	pare-feu		19422-0023-002	1210100000000				
		5	1	Groupe	publication	i serveur DVS 192	🧭 Autorisei	r 🕼 Serveur DNS	Externe	192, 168, 67, 10	6	
	Non :		2 2	Groupe	publication	Prgariëtës	- Calubration	HITP	e tuccelo troc 🌉	0 📄 deor5.produc	. 🏫 Tous les utris.	
	Action :		₿ 💽 3	Groupe	eutorseti	Sypprimer		U FTP	📥 Interne	Sterne 🌑	🖓 Taus les utilis.	
	Type de publication					Copier		HTTES				
	Connectes le seiveur Vieb publié au moyen du protocol					Exporter le sél	ection					
	<u> </u>		Règles de	stratègie d'e	entreprise a	Tobortes gave	la selección	bare-feu de gr	oupe			
	Cliques sur Terminer pour fermer l'Assistent.		💽 Der	Entreprise	Règle par	Monter		🖁 Tout le trefic	성 Tous les rèse .	🐴 Tous les réser.	. 🦓 Taus les utilis	Règle d'accè
						Désagtiver						
						Configurer HT1	rp.					
Texter la rècle	- Brénédert Tarman Ormán	7										
iese siege	K Gerener Jennes Minne											
Propriétés de publi	ation site web 192.168.67.105	? X	Prop	riótóc do	port d'é	coute 90				2 1		
			rrop	fietes de	porcue	couce oo						
Chemins d'accès	Pontage Utilisateurs Planification Traductio	n de liens		Général) F	léseaux	Conr	nexions	Certificats			
Délégation de l'	authentification Paramètres de l'applie	ation		Authen	ntification		Formulai	ires	550	i i		
Général Action	De À Trafic Port d'écoute N	om public	_	المغلم الم	huthantifi	ration du dia				1		
Cette règle s'ann	lique aux requêtes reques sur le port d'écoute su	ivant	I N	rieu ioue u : Iéthode d'a	authentifi	ation aunrès	niu E dia 150 Se	arvar i				
	ique dus requetes regues sur le port à cooute se	ir dine.			addriendin	acion adpres	5 GC 15A 50	л чог ,		_		
				Authentific	ation HTT:	Р						
port d'écoute 80		tés	L I	Z De base			F	🗌 Inté	arée			
Propriétés du po	t d'écoute : Nouve	au	1	00 000	·	, <u>D</u> igos	`	1 2100	groo			
Propriété	Valeur											
Description												
Réseaux Ban (UTTD)	Externe											
Port (HTTP) Port (HTTPS)	80 Désactivé			4éthode de	e validatio	n de l'auther	htification -					
Méthode d'auti	nentification De base		I	5A Server	valide les	informations	d'identifica	ation du clien	t via :			
Toujours authe	ntifier Non			Window	vs (Active	Directory)						
					nctive Dire	ctory)						
					-	secory)						
				C RADIOS	, ,							
			1	O Mot de	passe à u	sage unique	d'authenti	fication pour	serveur RADII	15		
La modification d	a propriétée du port d'écoute offecte toutes les	àalaa		O RSA Se	cyrID	G	onfigurer le	es serveurs d	e validation			
utilisant ce port d	écoute.	egies										
Aide sur les ports	d'écoute Web								Avancé			
			Ai	de sur <mark>les</mark> i	paramètre	es d'authenti	fication					
Tester la règle	OK Annuler /	ppliquer					ОК	Annuler	Appliqu	ier		
Options d'authentif	ration avancées	2 ¥	1									
Préférences d'authe	ntification											
□ Paramètres de cor	figuration du client											
	ungen ekkenn der einer ne											



On peut maintenant appliquer la règle et la tester (nouveauté du SP1).

Propriétés de Publication site web 192.168.67.1	Résultats des tests de la Règle de publication Web
Chemins d'accès Pontage Utilisateurs Planification Traduction de liens Délégation de l'authentification Paramètres de l'application Général Action De À Trafic Port d'écoute Nom public Cette règle s'applique à ce site publié :	Isagm40.production40.lan Image: 192.168.67.1 Image: 192.1
Demandes du proxy au site publié Indiquez comment le pare-feu traite par proxy les demandes au serveur publié : C Les demandes semblent émaner du serveur ISA C Les demandes semblent émaner du glient d'origine Aide sur <u>le transfert des demandes</u>	Test terminé Le test a correctement exécuté la vérification des paramètres de cette URL sur le serveur
Tester la règle OK Annuler Appliquer	<u>Arrêter</u>

6.6.3 Configuration des règles de publication web HTTPS et des règles pour publier Outlook Web Access, ActiveSync et Outlook Anywhere :

De nombreux site web expliquent comment publier un site web via un pontage SSL (deux connexions HTTPS) :

- <u>http://www.isaserver.org/tutorials/Publishing-Exchange-2007-OWA-Exchange-ActiveSync-</u> <u>RPCHTTP-2006-ISA-Firewall-Part6.html</u>
- <u>http://technet.microsoft.com/en-us/library/bb794751.aspx</u>
- <u>http://technet.microsoft.com/fr-fr/library/aa998934(EXCHG.80).aspx</u>
- <u>http://technet.microsoft.com/fr-fr/library/bb201695(EXCHG.80).aspx</u>
- http://www.msexchange.org/tutorials/Outlook-Anywhere-2007-ISA-Server-2006.html

Si votre client est en train de migrer d'Exchange 2003 vers Exchange 2007, appliquer la procédure suivante pour publier Outlook Web Access et ActiveSync du serveur Exchange 2003 et Exchange 2007 avec le même serveur ISA et une seule adresse IP publique :

<u>http://msreport.free.fr/?p=164</u>

6.7 Configuration de la mise en cache avec lsa Server 2006 :

Isa Server 2006 permet de mettre en cache le contenu des sites web HTTP, HTTPS et FTP. Par défaut la mise en cache avec Isa Server 2006 est désactivée.

Les administrateurs des sites web peuvent spécifier les paramètres de mise en cache de leurs sites web à l'aide des balises META. Pour plus d'informations, voir :

http://www.commentcamarche.net/forum/affich-17721-balise-meta

Si le site web change très souvent de contenu, la mise en cache peut être problématique et doit donc être désactivée. L'administrateur du site web renseigne alors la balise META dans ce sens. Isa Server permet de d'activer / désactiver / configurer la mise en cache des sites web et FTP à l'aide :

- Des règles de cache.
- Des règles de téléchargement planifiées.

Pour plus d'informations :

- http://www.isaserver.org/tutorials/ISA-Firewall-Web-Caching-Capabilities.html
- http://www.isaserver.org/tutorials/Understanding-Web-Caching-Concepts-ISA-Firewall.html
- http://www.isaserver.org/tutorials/ISA-2006-Web-Caching.html

6.7.1 Activer le cache sur le serveur lsa Server 2006 :

Tout d'abord, il est nécessaire d'activer le cache Isa Server 2006. Pour cela, appliquer la procédure cidessous. Il est alors nécessaire de redémarrer le service pare feu (attention arrêt de production).



6.7.2 Configurer les règles de cache :

Il est ensuite possible de configurer les règles de cache pour empêcher la mise en cache de certains sites web ou de modifier les paramètres par défaut de la mise en cache.

Configuration	V recreations regime A Rediez	ue cacile Visues us	celarinargement de concern
5erveurs	Ordre 🔺 Nom		Á
👍 Réseaux	💽 1 🛛 Règie de	cathe Microsoft Update	ij e
🐏 Cache 🗇 Add-Ins	💽 Dernier 🔋 Rêgle par	défaut	\$1
🚹 Général	Propriétés de Règle de cac	he Microsoft Update	<u>? ×</u>
	Général À Stock	age et récupération des	données dans le cache
	HTTP	FTP	Avancé
	🔽 Activer la mise en cache	HITP	
	Si aucun délai d'expiration n sont mis à jour en fonction d	'est spédifié par la sourc de ces paramètres de du	e, les objets du cache réa de vie :
	La durée de vie est la durée le cache, avant qu'il n'expire la création ou la modification	pendant laquelle le coni s. L'âge du contenu est l n d'un objet.	enu reste valide dans s temps écoulé depuis
	Définir la durée de vie des o contenu) :	bjets (% de l'âge du	20
	Limites de durée de vie :		
	Pas moins de :	15	Minutes 💌
	Pasplus d <u>e</u> :	1	Jours 💌
	 Appliquer également ces spécifient une expiration 	limites de durée de vie 1	aux sources qui

La mise en cache FTP est configuré par exemple sur 1 journée ce qui peut être problématique dans certains cas.

6.7.3 Création de tâches de téléchargement de contenu :

Isa Server permet de télécharger le contenu de site web en heure creuse afin d'accélérer la navigation en heure pleine.

😂 Ré] 🏠 Co	seaux privés virtuels (Vf onfiguration Serveurs	Lecteurs de cache Règles de cache Ai i <u>aches de téléchargement de contenu</u>
	Réseaux	Tâches de téléchargement de contenu
····	Add-ins	Les tâches de téléchargement de contenu définissent le contenu Web que ISA Server doit précharger, et planifient la mise en cache du conter
🖬	Général	Pour créer une tâche de téléchargement de contenu, ouvrez le volet des tâches, cliquez sur Planifier une tâche de téléchargement de contenu
Activer le	es tâches de téléchargement de	e contenu planifiées 🛛 🔀
⚠	Les tâches de téléchargement plar Le réseau dhôte local est configur Le groupe de configuration des têx	flées ne s'exécuteront qu'aux conditions suivantes : é de manifère à rester à l'écoute de demandes provemant de clients Web Proxy. Thes de bléchangement plantières est activé (de tradegie du système).
	Youlez-vous configurer ces paramé Yous devez appliquer ces modifical	itros ? jions à la configuration .
		ii Ilin Ade

Pour que la règle de téléchargement planifiée fonctionne, il faut autoriser le serveur lsa Server à accéder au site web et donc modifier la stratégie système.



6.7.4 Gestion du contenu du cache :

L'utilitaire *Cache Directory Tool for Internet Security and Acceleration (ISA) Server 2006* permet de gérer le contenu du cache et de marquer une page en cache comme expirée. Pour plus d'informations sur cet outil, voir :

http://www.microsoft.com/downloads/details.aspx?familyid=b9ecfcd3-c13f-4447-83edadd9a8ea45db&displaylang=en

6.8 Configuration de la découverte automatique :

Isa Server peut être configuré pour permettre au client proxy web et pare feu de découvrir automatiquement le serveur Isa Server. Pour plus d'informations, voir :

<u>http://www.isaserver.org/tutorials/Configuring-WPAD-Support-ISA-Firewall-Web-Proxy-Firewall-Clients.html</u>

6.9 Configuration de la détection d'intrusion :

Isa Server intègre des outils (très limité) dé détection et de prévention d'intrusion. Très clairement, je préconise de désactiver les mesures de prévention contre les attaques par saturation. En effet, rien n'empêche un attaquant de générer des très nombreuses trames en usurpant l'IP d'une partenaire de la société. Hors dans ce cas les « mesures de prévention contre les attaques par saturation » risque de faire plus de mal qu'autres choses (bloquer du trafic légitime d'une entreprise partenaire de la votre...).

Stratégie de sécurité supplémentaire	
Activer la détection d'intrusions et la détection d'attaques DNS	Définir les paramètres de prévention des attaques par Saturation
Configurer la protection IP	

Dans tous les cas préférer loguer les attaques et éviter de couper le flux automatiquement en cas de détection d'attaque.

Le module IDS d'Isa Server 2006 gère surtout d'ancienne attaque qui sont maintenant nativement géré par les piles TCP/IP modernes. Un des modules intéressant dans l'IDS est la détection des attaques DNS.

Prévention des attaques par saturation	? ×	Détection des intrusions	<u>?</u> ×
Prévention des attaques par saturation Exceptions IP		Attaques communes Attaques DNS	
Mesures de prévention contre les attaques par saturation et la propagation de ver Définissez les limites des mesures préventives pour ces attaques potentielles : Nombre maximal de demandes de connexion TCP		 Activer la détection d'intrusions Activer la détection des attaques sélectionnées : Attaque de type « Windows out-of-band (WinNuke) » 	
par minute, par adresse IP	<u> </u>	Attaque de type « Land »	
Nombre maximal de connexions TCP simultanées Modifier		Attaque de type « Ping of death »	
Nombre maximal de connexions TCP semi-ouvertes Affichers		Attaque de type « <u>U</u> PP bomb »	
Nombre maximal de demandes HTTP par minute, Modifier.		Attaque de type « Port scan » Détection après ce nombre d'attaques de type « Port scan » :	
Nombre maximal de nouvelles sessions non-TCP Modifier		Ports connus : 10	
Nombre maximal de sessions UDP simultanées Modifier.		Lous les ports : 20	
Spécifier le nombre de paquets refusés pour Modifiers.		Enregistrer les paguets perdus	
Consigner le trafic bloqué par les paramètres de prévention des attaques par saturation		Pour configurer les notifications d'attaques, modifiez les définitions d'alertes pour ces attaques.	
		Aide sur <u>les alertes</u>	
OK Annuler Appl	liquer	OK Annuler Applic	quer



6.10 Mise en œuvre du filtrage applicatif avec Isa Server 2006 :

Le gros point fort d'Isa Server 2006 est sa capacité à effectuer du filtrage au niveau 7 de la couche OSI. On parle dans ce cas de filtrage applicatif.

Isa Server 2006 intègre de nombreux filtre applicatif.

Pour plus d'informations, voir http://technet.microsoft.com/en-us/library/bb794732.aspx

Microsoft Internet Security and Acceleration	Server 2006								
Eichier Action Affichage ?									
⇔ → 🖻 🖬 😰 🗷 🔄									
Microsoft Internet Security and Acceleration Server D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D D	200 Internet Security & Acceleration Server 20 Enterprise Edition	01 Microsoft [*] Internet Security & Serveur de stockage de configurations : isagm40.production40.lan Acceleration Server 2006 Serveur de stockage de configurations : isagm40.production40.lan Enterprise Edition							
Stratégie par défaut	(i) <u>Cliquez ici pour en savoir</u>	plus sur le Programme d'amélioration du produi	<u>t.</u>						
Add-ins d'entreprise	Filtres d'application Filtre	Filtres d'application Filtres Web							
Groupes Jagm40 Jurveillance Stratégie de pare-feu (isagm40) Stratégie virtuels (VPN) Configuration	Nom 🔺	Description	Fournisseur						
	📲 Filtre d'accès FTP	Active les protocoles FTP (client et serveur)	Microsoft (R) Corporation	4.0					
	🖅 Filtre de détection d'intrusion Recherche les attaques par dépassement de ta Microsoft (R) Corporation 4.0								
	«) Filtre de proxy Web	Active le proxy et le cache HTTP	Microsoft (R) Corporation	4.0					
Réseaux	Filtre DNS	Filtre le trafic DNS	Microsoft (R) Corporation	4.0					
	Hiltre H.323	Active le protocole H.323	Microsoft (R) Corporation	4.0					
Général	M Filtre MMS	Active le protocole de flux de média Microsoft	Microsoft (R) Corporation	4.0					
	N Filtre PNM	Active le protocole de diffusion multimédia en c	Microsoft (R) Corporation	4.0					
	N Filtre PPTP	Active le tunnel PPTP via ISA Server	Microsoft (R) Corporation	4.0					
	Sa Filtre RPC	Active la publication des serveurs RPC	Microsoft (R) Corporation	4.0					
	Hiltre RTSP	Active le protocole de flux en temps réel	Microsoft (R) Corporation	4.0					
	iltre SMTP	Filtre le trafic SMTP	Microsoft (R) Corporation	4.0					
	™ Filtre SOCKS V4	Active les communications SOCKS 4	Microsoft (R) Corporation	4.0					

Microsoft Internet Security and Acceleration Ser	ver 2006					_ 8
Eichier Action Affichage ?						
Microsoft Internet Security and Acceleration Server 20(Entroprise Strotógies d'ontroprise Entrotógies d'ontroprise Entrotógies d'ontroprise Entrotógies d'ontroprise	Microsoft Intern Accele Enterprise	et Security & Pration Server 2006 Serv	eur de stockage de configurations : isagm4	40.production40.lan		Add-ins
Stratégie par défaut	(i) <u>Cliquez</u>	ici pour en savoir plus sur l	le Programme d'amélioration du produit.			
Add-ins d'entreprise	Filtres d'ap	pication Filtres Web			_	
isagm40	Ordre 🔺	Nom	Description	Sens	Version	Fourni
Surveillance	M 🔁 1	Filtre DiffServ	Active le balisage DiffServ du trafic Web en fo	. Les deux	4.0	Microsof D
	• 2	Filtre d'équilibrage de la cha.	. Permet la publication de batteries de serveurs	. Demandes Web entrantes	4.0	Microsof V
Configuration	• 3	Filtre de compression	Active la compression HTTP/HTTPS	Les deux	4.0	Microsof c
	v 🗐 +	Filtre de délégation de l'aut	. Permet de déléguer l'authentification aux serv	. Demandes Web entrantes	4.0	Microsof a
	ە 🗐 5	Filtre d'authentification par	. Active l'authentification par formulaires (cooki	Demandes Web entrantes	4.0	Microsof C
Général	0 — 6	Filtre d'authentfication RA	Active l'authentification RADIUS	Les deux	4.0	Microsofr.
‱ ≣ ¶ Dépannage	• 7	Filtre d'authentification LDAP	Propose l'authentification LDAP	Demandes Web entrantes	4.0	Microsof la
	۰ 8	Filtre de traduction de liens	Active la traduction de liens pour les serveurs	. Demandes Web entrantes	4.0	Microsof L
	• 🗐 9	Filbre HTTP	Filtre le trafic HTTP et applique la stratégie HT	. Les deux	4.0	Microsof⊢
	•🔳 10	Filtre de cache de contenu	. Active la mise en cache du contenu HTTP com	Les deux	4.0	Microsof c

Les filtres applicatifs peuvent être gérés à deux niveaux :

- Au niveau du filtre (cas du filtre SMTP).
- Au niveau d'une règle d'accès (cas du filtre HTTP).

6.10.1 Présentation du filtre applicatif SMTP

Le filtre SMTP va nous permettre de bloquer certaines méthodes / commandes SMTP qui ne sont pas par exemple utilisés par les serveurs SMTP autorisés.

Propr	iétés de Filtr	e SMTP		? ×
Gén	iéral Commar	ndes SMTP		
		1		1
	(Commendae		- I
	Activer		Longueur maxim	-
	X I	BDAT	20	
	l 🎽 👘	DATA	6	
	l 🍝 👘	EHLO	71	
	lŏ –	EXPN	71	
	l 🖉 👘	HELO	71	
	Ö	HELP	6	
	I	MAIL FROM:	266	-
		NOOP	6	
	 🖉 👘	QUIT	6	
		RCPT TO:	266	.
		RSET	6	-
	Ajou <u>t</u> er	Supprimer	Modifier	
		OK	Annuler Ap	pliquer

6.10.2 Présentation du filtre applicatif HTTP :

Le filtre HTTP d'Isa Server 2006 permet de filtrer les trames http :

- Selon la taille de l'entête
- La charge utile des requêtes : une requête GET contient généralement une URL et a donc une taille très faible. Le trafic web est logiquement très asymétrique (on reçoit plus qu'on envoie). Voici une technique très simple pour détecter les tunnels HTTP.
- Selon le type de méthode HTTP (GET, POST…).
- Selon une siganture.



Pour plus d'informations sur le filtre HTTP :

- http://windowsitpro.itpro.fr/Dossiers-par-Theme/suivante/1/8/050382915-1.1-Les-limitationsinherentes-aux-regles-d-acces.htm#R1
- http://www.laboratoire-microsoft.org/articles/server/Filtre-HTTP/3-le-filtre-http/

7 Les tâches d'administration courante d'Isa Server :

7.1 Sauvegarder son serveur Isa Server :

Pour sauvegarder son serveur ISA, on peut exporter toute la configuration. Pour cela, appliquer la procédure ci-dessous :

Microsoft Internet Security and Acceleration Server 2006	Assistant Exportation
Eichier Action Affichage ?	Préférences pour l'exportation Choissea les données facultatives que vous souhaitez inclure dans le fichier exporté.
← → III 😫 II 2 → ⊙ Microsoft Internet Security and Acceleration Server 2006	Exporter des informations configentielles Si cette option est sélectionnée, les mots de passe utilisateurs, les secrets RADIUS
En Actualiser	partagis et autros informations confidentellas seront exportés. Les informations seront cryptées à l'aide du mot de passe spécifié. Mot de passe
Exporter (sanvegarder) Importer (restaurer)	(au moins <u>8</u> caractères) : Confirmer le mot de passe :
<u>Connecter au serveur de stockage de configuration</u>	Exporter les paramètres d'autorisations utilisateurs Si cette option est sélectionnée, les rôles d'administration délégués aux utilisateurs et aux groupes serret exportés.
Se déconnecter de l'entreprise Image: Se déconnecter de l'entreprise	Alde Sur l <u>es informations conficient elles spécificies au serveur</u>
Aide	< Brécédent Sulvant > Annuler

Il faut aussi penser à exporter tous les certificats web installés sur le serveur lsa au format PFX (clé publique et clé privée). Pour plus d'informations sur l'exportation de certification, voir :

<u>http://technet.microsoft.com/fr-fr/library/cc738545(WS.10).aspx</u>

Pour plus d'informations sur la sauvegarde Isa Server, voir :

http://www.isaserver.org/tutorials/ISA-Server-2006-Backup-Restore-Capabilities.html

7.2 Mise en œuvre de la délégation d'administration avec lsa Server 2006 :

Une Best Practice est de créer des comptes d'administration nominatifs Isa Server et d'activer le suivi des modifications (nécessite installation du SP1 d'Isa Server 2006). Pour plus d'informations : <u>http://www.isaserver.org/tutorials/Role-based-administration-ISA-Server-2006.html</u>

7.3 Configuration de rapports avec lsa Server 2006 :

Les rapports permettent de déterminer entre autres comment est utilisée la connexion Internet. Attention les rapports lsa Server ne peuvent pas être générés pour la journée en cours, seulement pour la veille.

Par défaut, toutes les connexions effectuées à travers lsa Server sont journalisés dans une base de données MSDE (une base pour chaque journée par défaut).



Propriétés de Tâches de rapport	Assistant Nouvelle tâche de	rapport X
Tâches de rapport		Assistant Nouvelle tâche de rapport
Tâche de rapport Période	Nicrosoft Internet Security & Acceleration Server 2006	
		Cet Assistant vous aide à créer une tâche de rapport. Une tâche de rapport génère des rapports récurrents en fonction de la planification définie.
		rapport journaliere total
		Cliquez sur Suivant pour continuer.
Ajouter Modifier Supprimer Exécuter		
OK Annuler Appliquer		< Erécédent Suvant > Annuler
Assistant Nouvelle tâche de rapport	Assistant Nouvelle tâche de	rapport 🔀
Contenu du rapport Un rapport inclut le contenu spécifié ici.	Spécifiez la planification tâche de rapport s'exèc	rapporc en déterminant à quelle fréquence, et à quel mament, la utera.
Sélectionnez le contenu à inclure dans ce rapport :	Exécuter cette täche de ra	ipport :
I⊽ <u>Résumé</u>	Tous les jours	
🔽 Utilisation du <u>W</u> eb	Ioutes les semeines, le	s jours spécifiés :
✓ <u>U</u> tilisation des applications	r ⊻endredi	E Semedi E Dimanche
V Traffic et u tilisetion	Pour générer un rap;	ort couvrant une sempine entière, ne spécifiez qu'un jour-
	🔿 Tous les mois, à cette d	date chague mois :
tal peñare	Pour être sûr que le raj susceptible de ne pas o rapports couvrant un n	sport soit généré tous les mois, n'utilises pas de date xister certains mois (29, 30 ou 31). Pour générer des nois entier, entrez « 1 » dans le champ Dete.
	Par défaut, les rapports s	ont générés à L'heure du math. Vous pouvez modifier la
	tatile de repport dans les	proprietes des teulles de replants.
< Précédent Suvant > Annule	er	< Précédent Suivant > Annuler
Assistant Nouvelle talche de rapport 2 Envoyer la notification par messagerie 2 Aeris quiun rapport à té à printér, une notification de rapport peut être envoyée automatiquement au destinatare spécifié. 2	×	
Envoyer une notification per courrier électrorique pour les rapports terminés		
Serveur SMTP : Parcoyrin		
Qe:		
<u>A</u> :		
Service : Message : CErbrez le nessage pour le corps du message électronique :>		
Endure un ien vers ie report, final dans ie message Tester		
< Précédent Suvant > Annuler	1	

Pour plus d'informations sur la mise en œuvre de rapport avec lsa Server 2006 : <u>http://www.isaserver.org/tutorials/Logging-Reporting-ISA-Server-2006.html</u>

7.4 Troubleshouting avec l'onglet Surveillance\Journalisation :

Il est possible de monitoirer toutes les connexions en cours sur le serveur et les filtrer entre autres selon l'adresse IP source / cible.

Pour chaque connexion, il est possible de connaître la règle Isa Server qui s'est appliquée et de savoir si la connexion a été acceptée ou refusée.



odifier le filtre			?
Afficher uniquement les ent	trées qui réponder	nt à ces conditions :	
Filtrer par	Condition	Valeur	
💷 Type d'enregistrem	Est égal à	Filtre de pare-feu ou	de proxy Web
💷 Heure du journal	Live		
Action	Différent de	État de la connexion	
	Epi	registrer le filtre	Charger le filtre
Spécifiez les critères de filtr	age des données	:	
Filtr <u>e</u> r par	<u>C</u> ondition	<u>Valeur</u>	
	<u>-</u>	v	
Su	Ipprimer	Mettre à jour	Ajo <u>u</u> ter à la liste

8 Mise en œuvre des VPN :

Isa Server 2006 supporte deux types de VPN :

- PPTP
- L2TP

Isa Server ne fait qu'intégrer dans son interface les fonctionnalités du service RRAS de Windows 2003 Server (simplification de l'interface).

Pour plus d'informations sur la prise en charge des VPN par lsa Server 2006 :

http://technet.microsoft.com/en-us/library/bb794723.aspx

8.1.1 Configuration d'Isa Server comme serveur VPN L2TP :

Appliquer la procédure ci-dessous :

http://www.laboratoire-microsoft.org/articles/server/ISA2004/6/

Pour plus d'informations :

- http://www.isaserver.org/tutorials/2004dhcprelay.html
- http://support.microsoft.com/kb/837355/en-us
- http://207.46.16.252/en-us/magazine/2007.11.isavpn.aspx

8.1.2 Pour créer des connexions VPN site à site :

Pour plus d'informations, voir :

- http://www.labo-microsoft.com/whitepapers/20588/
- http://www.isaserver.org/tutorials/Implementing-IPSEC-Site-to-Site-VPN-between-ISA-Server-2006-Beta-Cisco-PIX-501.html