CONFIGURER LE PARE-FEU POUR SCCM

Mathis SZYDA

I. Création de la GPO avec les règles du firewall.

Sur votre contrôleur de domaine, au sein de la console gestion de stratégie de groupe, créez une nouvelle <u>GPO</u> :



Étant donné qu'elle va contenir les règles du pare-feu qui permettront de pusher le client sur les appareils gérés, on va la nommer "**SCCM - Firewall - Push Client**".

Nouvel objet GPO	>
Nom :	
SCCM - Firewall - Push Client	
Objet Starter GPO source :	

Éditez ensuite la GPO que l'on vient de créer : clic droit puis "Modifier".

Gestion de stratégie de groupe	SCCM - Firewall - Push Client			
 A Forêt : it-connect.local Domaines it-connect.local Default Domain Policy SCCM - Firewall - Push Client 	Étendue Détails Paramètres Délégation Liaisons Afficher les liaisons à cet emplacement :			
> 🛐 Domain Controllers	Modifier			
 Entreprise pfSense Objets de stratégie de groupe Filtres WMI 	Appliqué Lien activé Enregistrer le rapport			

A. Règle "Partage de fichiers et d'imprimantes"

Pour le paramétrage de règles de firewall, il faut accéder à : Configuration ordinateur, Stratégie, Paramètres Windows, Paramètres de sécurité, Pare-feu Windows avec fonctions avancées de sécurité (x2).

Sur "*Règles de trafic entrant*", effectuez un clic droit puis "*Nouvelle règle*".



Choisissez "*Prédéfinie*" comme type de règle et dans la liste sélectionnez "*Partage de fichiers et d'imprimantes*".

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :	
Type de règle	Quel type de règle voulez-vous créer ?
Règles prédéfinies	
Action	Programme Règle qui contrôle les connexions d'un programme. Port Règle qui contrôle les connexions d'un port TCP ou UDP.
	Prédéfinie :
	Partage de fichiers et d'imprimantes
	Règle qui contrôle les connexions liées à l'utilisation de Windows.
	O Personnalisée Règle personnalisée.
	< Précédent Suivant > Annuler

Cochez l'ensemble des règles et poursuivez.

Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Quelles règles suiva sélectionné. Les contenu sera rei Règles : Nom Quelles règles de	oulez-vous créer ? ntes définissent les besoins en conn régles qui sont cochées seront créé riplacé.	ectivité réseau pou es. Si une règle co La règle existe	le groupe pré chée existe dé	idéfini ijà, son
Les règles suiva sélectionné. Les contenu sera res Règles : Nom Partage de	ntes définissent les besoins en conne règles qui sont cochées seront créé mplacé.	ectivité réseau pou es. Si une règle co La règle existe	le groupe pré chée existe de	idéfini ijà, son
sélectionné. Les contenu sera rer Règles : Nom 🖉 Partage de	régles qui sont cochées seront créé nplacé.	es. Si une règle co La règle existe	chée existe de	ijā, son
Nom Partage de		La règle existe	0-4	
Partage de			Profil	Desc
	fichiers et d'imprimantes (LLMNR	Non	Tout	Rèck
Partage de	fichiers et d'imprimantes (Demand	Non	Tout	Les n
Partage de	fichiers et d'imprimantes (Demand	Non	Tout	Les n
Partage de	fichiers et d'imprimantes (Service	Non	Tout	Règk
Partage de	fichiers et d'imprimantes (service S	Non	Tout	Règk
Partage de	fichiers et d'imprimantes (NB-Data	Non	Tout	Règk
Partage de	fichiers et d'imprimantes (NB-Nom	Non	Tout	Règk
Partage de	fichiers et d'imprimantes (SMB-Ent	Non	Tout	Règk
Partage de	fichiers et d'imprimantes (NB-Sessi	Non	Tout	Règk
<				>
	 ✓ Partage de ✓ 	 Partage de fichiers et d'imprimantes (Service Partage de fichiers et d'imprimantes (service S Partage de fichiers et d'imprimantes (NB-Data Partage de fichiers et d'imprimantes (NB-Nom Partage de fichiers et d'imprimantes (SMB-Ent Partage de fichiers et d'imprimantes (NB-Sessi 	Partage de fichiers et d'imprimantes (Service Non Partage de fichiers et d'imprimantes (Service S Non Partage de fichiers et d'imprimantes (NB-Data Non Partage de fichiers et d'imprimantes (NB-Nom Non Partage de fichiers et d'imprimantes (SMB-Ent Non Partage de fichiers et d'imprimantes (NB-Sessi Non Partage de fichiers et d'imprimantes (NB-Sessi Non	Partage de fichiers et d'imprimantes (Service Non Tout Partage de fichiers et d'imprimantes (service S Non Tout Partage de fichiers et d'imprimantes (NB-Data Non Tout Partage de fichiers et d'imprimantes (NB-Nom Non Tout Partage de fichiers et d'imprimantes (SMB-Ent Non Tout Partage de fichiers et d'imprimantes (NB-Sessi Non Tout

Nous souhaitons autoriser ce flux alors sélectionnez "Autoriser la connexion".

Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :	
Type de règle	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?
Règles prédéfinies	Attainstanting
 Action 	Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.
	 Autoriser la connexion si elle est sécurisée Cela comprend uniquement les connexions authentifiées à l'aide du protocole lPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles lPsec du nœud Règle de sécurité de connexion. Performance. Bloquer la connexion
	< Précédent Terminer Annuler

Il va falloir recréer la même règle, mais pour le trafic sortant cette fois-ci, cliquez droit sur "*Règles de trafic sortant*" puis "*Nouvelle règle*".



Sélectionnez "*Prédéfinie*" puis "*Partage de fichiers et d'imprimantes*".

Ť

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :	
Type de règle	Quel type de règle voulez-vous créer ?
Règles prédéfinies	
Action	Programme Règle qui contrôle les connexions d'un programme. Port Règle qui contrôle les connexions d'un port TCP ou UDP.
	Prédéfinie :
	Partage de fichiers et d'imprimantes
	Règle qui contrôle les connexions liées à l'utilisation de Windows.
	Personnalisée Règle personnalisée.
	< Précédent Suivant > Annuler

Cochez tout et continuez.

🔗 Assistant Nouvelle règle de trafic sortant

Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

tapes :				
Type de règle	Quelles règles voulez-vous créer ?			
Règles prédéfinies	Les règles suivantes définissent les besoins en conne	ectivité réseau pou	r le groupe pré	idéfini
Action	sélectionné. Les règles qui sont cochées seront créé contenu sera remplacé. Règles :	es. Si une règle co	chée existe dé	ijā, son
	Nom	La règle existe	Profil	Desc
	Partage de fichiers et d'imprimantes (LLMNR	Non	Tout	Règk
	Partage de fichiers et d'imprimantes (Demand	Non	Tout	Les n
	Partage de fichiers et d'imprimantes (Demand	Non	Tout	Les n
	Partage de fichiers et d'imprimantes (NB-Data	Non	Tout	Règk
	Partage de fichiers et d'imprimantes (NB-Nom	Non	Tout	Règk
	Partage de fichiers et d'imprimantes (SMB-Sor	Non	Tout	Règk
	Partage de fichiers et d'imprimantes (NB-Sessi	Non	Tout	Règk
	<			>

Autorisez la connexion et finalisez la création de cette règle.

Ì



B. Règle "WMI"

Créez une nouvelle règle de trafic entrant :



Cette fois-ci, sélectionnez l'ensemble de règles prédéfinies "Infrastructure de gestion Windows (WMI)".

🔗 Assistant Nouvelle règ	le de trafic entrant	3
Type de règle		
Sélectionnez le type de règle	de pare-feu à créer.	
Étapes :		
 Type de règle 	Quel type de règle voulez-vous créer ?	
Règles prédéfinies		
 Action 	Programme Rècle qui contrôle les connexions d'un programme	
	Règle qui contrôle les connexions d'un port TCP ou UDP.	
	Prédéfinie :	
	Infrastructure de gestion Windows (WMI)	~
	Règle qui contrôle les connexions liées à l'utilisation de Windows.	
	O Personnalisée Règle personnalisée.	
	< Précédent Suivant >	Annuler

Cochez les 3 règles et poursuivez.

Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Quelles règles voulez-vous créer ?			
Les règles suivantes définissent les besoins en conn	ectivité réseau pou	r le groupe pré	idéfini
sélectionné. Les règles qui sont cochées seront créé contenu sera remplacé. Règles :	ies. Si une règle co	chée existe d	éjá, son
Nom	La règle existe	Profil	Desc
Windows Management Instrumentation (ASyn	Non	Tout	Règle
Windows Management Instrumentation (WMI	Non	Tout	Règk
<			>
	Les règles suivantes définissent les besoins en conn sélectionné. Les règles qui sont cochées seront créé contenu sera remplacé. Règles : Windows Management Instrumentation (ASyn Windows Management Instrumentation (WMI Windows Management Instrumentation (DCO	Les règles suivantes définissent les besoins en connectivité réseau pou sélectionné. Les règles qui sont cochées seront créées. Si une règle co contenu sera remplacé.	Les règles suivantes définissent les besoins en connectivité réseau pour le groupe pré sélectionné. Les règles qui sont cochées seront créées. Si une règle cochée existe de contenu sera remplacé.

Autorisez la connexion puis terminez la création de cet ensemble de règles.

Assistant Nouvelle règle	de trafic entrant	Ì
Action		
Spécifiez une action à entreprer	ndre lorsqu'une connexion répond aux conditions spécifiées dans la règle.	
Étapes :	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?	
 Règles prédéfinies 	Autoriser la connexion	
 Action 	Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.	
	 Autoriser la connexion si elle est sècurisée Cela comprend uniquement les connexions authentifiées à l'aide du protocole lPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles lPsec du nœud Règle de sécurité de connexion. Prostructure Bloquer la connexion 	
	< Précédent Terminer Annuler	r

Il n'est pas nécessaire de refaire cette règle en trafic sortant, seulement en entrant c'est suffisant.

La GPO est terminée, il suffira de l'appliquer à l'ensemble des ordinateurs que vous gérez avec SCCM. Sur vos postes clients, il faudra réaliser l'habituel "**gpupdate /force**" pour forcer l'actualisation des GPO.

III. Ouverture des ports pour SQL Server

Étant donné que cette ouverture de ports concerne uniquement le serveur SQL, on va opérer directement depuis celui-ci. Je vous invite à aller dans le panneau de configuration, puis dans Parefeu Windows. Sur la gauche, cliquez sur "*Paramètres avancés*".



Créez une nouvelle règle de trafic entrant :

Pare-feu Windows avec fonct	tions avancées de sécurit	é C	2
Fichier Action Affichage	?		
🗢 🤿 🙍 📷 🗟 🖬			
Pare-feu Windows avec fonct	tions avancées de sée Ré	ègles	de
Règles de trafic entrant Règles de trafic sortant	Nouvelle règle		1
Règles de sécurité de c	Houvene regien.		ire
> 🛃 Analyse	Filtrer par profil	>	i r
	Filtrer par éta <u>t</u>	>	ni
	Filtrer par groupe	>	se
	Affic <u>h</u> age	>	se

Nous n'allons pas utiliser de règle prédéfinie cette fois-ci, car elle n'existe pas. Nous allons indiquer directement les ports que l'on souhaite ouvrir, sélectionnez "*Port*".

PAssistant Nouvelle règle de trafic entrant	
Type de règle	
Sélectionnez le type de règle de pare-feu à créer.	

Etapes : Type de règle	Quel type de règle voulez-vous créer ?
 Protocole et ports Action Profil Nom 	Programme Règle qui contrôle les connexions d'un programme. Port Règle qui contrôle les connexions d'un port TCP ou UDP.
	O Prédéfinie :
	Accès réseau COM+
	Règle qui contrôle les connexions liées à l'utilisation de Windows. O Personnalisée Règle personnalisée.
	< Précédent Suivant > Annuler

63

Cette règle s'applique au protocole "TCP" et la liste de ports est la suivante : 1433 et 4022.

Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

Type de règle	Cette règle s'applique t-elle à TCP ou UD	P?	
Protocole et ports	TCP		
Action	O UDP		
Profil			
Nom	Cette rècle s'annique t elle à tous les pou	te locario ou à des porte loca	ur enéctiones ?
	Cerre regre a appriçõe r eire a rous res por		ny shoraidhos t
	O Tous les ports locaux		
	Ports locaux spécifiques :	1433, 4022	
		Exemple : 80, 443, 50	00-5010

Nous allons autoriser la connexion sur ces deux ports.

Assistant Nouvelle regi	e de tranc entrant	^
Action		
Spécifiez une action à entrepre	endre lorsqu'une connexion répond aux conditions spécifiées dans la règle.	
Étapes :		
Type de règle	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?	
Protocole et ports	Autoriser la connexion	٦
Action	Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui	
 Profil 	ne le sont pas.	
THOM	Cela comprend uniquement les connexions authentifiées à l'aide du protocole lPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles lPsec du nœud Règle de sécurité de connexion. Perconsaluer. O Bloquer la connexion	
	< Précédent Suivant > Annuler	

Pas besoin d'appliquer cette règle sur les profils privé et public, vous pouvez laisser seulement "Domaine". Comme ceci :

Profil

Spécifiez les profils auxquels s'applique cette règle.

Étapes :	
Type de règle	Quand cette règle est elle appliquée ?
Protocole et ports	
Action	Domaine
Profil	Lors de la connexion d'un ordinateur à son domaine d'entreprise.
Nom	Privé
	Lors de la connexion d'un ordinateur à un emplacement réseau privé, par exemple à domicile ou au bureau.
	Public
	Lors de la connexion d'un ordinateur à un emplacement public.
	< Précédent Suivant > Annuler

63

Nommez la règle, par exemple : SCCM - SQL Ports 1433 et 4022

Assistant Nouvelle règle	de trafic entrant	ම
Nom		
Spécifier le nom et la description	de cette règle.	
Étapes :		
Type de règle		
Protocole et ports		
Action		
Profil	Nom :	
Nom	SCCM - SQL Ports 1433 et 4022	
	Description (facultatif) :	
	< Précédent Tau	miner Annuler

Tout est prêt sur le firewall