ISAServerFR.org
Le site francophone dédié à Microsoft ISA server et aux problématiques de sécurité.

Comprendre et mettre en oeuvre ISA 2004 en tant que firewall applicatif

Mise en oeuvre des filtres RPC

Difficulté : ★★☆
Auteur : Frédéric ESNOUF
Version : V 1.0
Catégorie : firewall

Information sur ce document

Titre du document	Comprendre et mettre en oeuvre ISA 2004 en tant que firewall applicatif
Fichier	RPC FR.doc
Auteur	Frédéric ESNOUF : frederic@esnouf.net

Version du document

Version	Description	Date
1.0	Version en Anglais publiée sur le site ISAServer.org	15/2/2004
1.1	Traduction de cette version en Français pour ISAServerFR.org	25/2/2004

ATTENTION

Cette documentation est disponible sur le site web ISAServerFR.org à titre d'exemple et dans un but éducatif.

Elle ne constitue en aucun cas une documentation détaillée et il appartient à chaque équipe de valider que sa mise en production ne pose pas de problème de sécurité ou d'exploitation. En aucun cas le site ISAServerFR.org et ses auteurs ne pourraient être tenus pour responsable suite à des problèmes de production.

La sécurité étant un sujet très important pour les entreprises, nous vous invitons à faire appel à des consultants spécialisés dans le cas où vous déterminez que vous ne maîtrisez pas assez ce type d'architecture. Ceci vous permettra d'obtenir le conseil nécessaire durant les phases de design, de mise en œuvre et d'exploitation de ce type d'architecture.

Ne jouez pas avec la sécurité !

Table des matières

I. Convention typographique

Afin de faciliter la lecture de ce document et d'en permette une meilleure compréhension, nous avons décidé d'utiliser des idéogrammes afin de souligner certains aspects.

En voici leur description :

Logo	Explication
	Ce logo indique que nous n'avons pas la réponse à cette question.
	Ce logo indique que nous avons ici un impact direct sur le coût de la solution.
	Ce logo indique que ce point a un impact sur les utilisateurs.
	Ce logo indique que nous avons ici un point important.
	Ce logo indique que nous allons entrer plus en détail dans une technologie.
	Ce logo indique le niveau de technicité de l'article : Simple Moyen Avancé

I.1.Documents & liens associés

Afin de mieux appréhender les concepts de ce document, nous vous recommandons de prendre également en compte ces publications :

- *
- *
- *

II. La problématique

Avec l'arrivée de ISA 2004, Microsoft fournit une nouvelle version de son Firewall comportant de nombreux atouts tant en matière de sécurisation que d'accélération pour le système d'information de l'entreprise.

Si l'on parle sécurité, il est intéressant de noter que le protocole RPC (Remote Procedure Call) qui est utilisé par toutes les applications Microsoft est très souvent méconnu au niveau de son fonctionnement. Il est alors difficile d'en évaluer les 'risques' (il y a des risques comme tous les autres protocoles) et donc de définir une architecture permettant d'y faire face.

Cet article a pour but de décrire les mécanismes RPC, et de montrer comment ISA 2004 à travers son filtre RPC va devenir un allié majeur pour assurer la sécurité des de ces flux au sein de l'entreprise.

A travers un exemple très simple, nous montrerons la méthodologie qui vous permettra de créer vos propres filtres RPC afin de publier de grosses infrastructures à travers ISA 2004, par exemple :

- Protéger des serveurs Exchange,
- Répliquer l'Active Directory entre deux sites distants mais filtrés (cas souvent des fusions acquisitions).

III. Comment ISA répond à cette problématique

A ce jour, de nombreuses équipes sécurité continuent à utiliser des firewalls assurant un filtrage dit de niveau 3 (et 4) du modèle OSI, c'est-à-dire au niveau IP mais également TCP et UDP. Ils procèdent en général par l'ouverture ou la fermeture de ports sur ces équipements. Le problème est que la menace actuelle mais également l'évolution des protocoles (par exemple l'encapsulation de protocoles dans HTTP, tel que le VPN SSL) font que le filtrage de niveau 3 n'est plus du tout suffisant pour assurer la mise en sécurité de l'entreprise. C'est le cas des filtrages RPC (objet de cette documentation, mais de tous les autres protocoles : POP3, http, …). Ceci est valable sur les firewalls connectés à Internet, mais également à ceux installés sur le réseau interne de l'entreprise.

Nous devons donc ouvrir nos flux réseau d'une façon plus intelligente en analysant le contenu des données qui transite. On utilise alors un mécanisme dit de filtrage applicatif (comparé au filtrage IP/TCP/UDP). ISA 2004 est un firewall qui permet de travailler aux deux niveaux et procure de nombreux filtres applicatifs en natif. D'autres optionnels, sont fournit pas des partenaires.

IV. Comprendre RPC

Nous allons maintenant nous focaliser sur le filtre applicatif RPC fournit en standard avec ISA 2004, et pour cela introduire le fonctionnement des flux RPC.

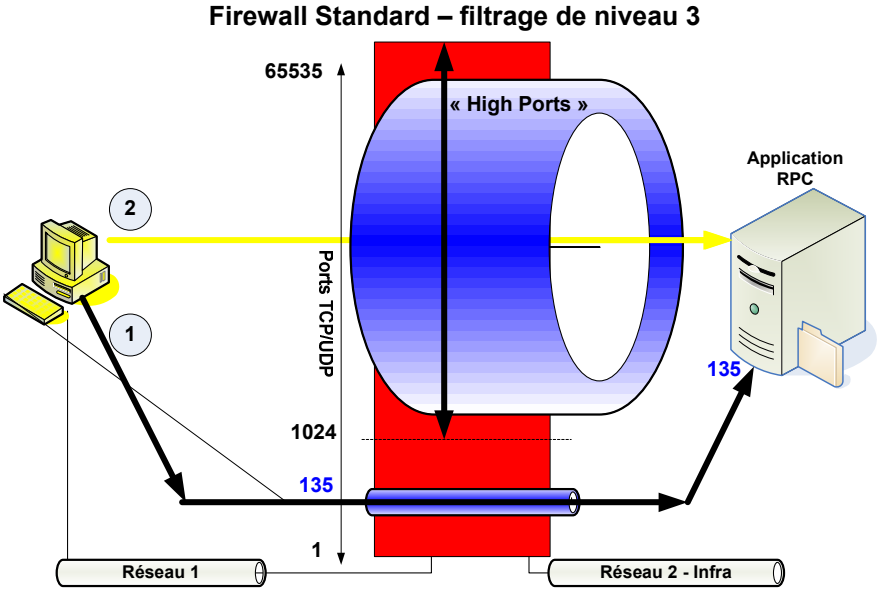
Si vous utilisez un firewall de niveau 3, et si vous souhaitez mettre en oeuvre un filtrage réseau sur RPC, ceci est tout à fait possible. Dans ce cas, vous devez autoriser les machines clientes à discuter avec le serveur hébergeant l'application à travers un certain nombre de ports (les firewall de niveau 3 ne savent qu'ouvrir/fermer des ports). Voici un détail de la règle à mettre en œuvre dans ce cas :

- **Port TCP 135** (le end-port mapper) : Ce service situé sur le serveur distant va être utilisé par l'application RPC cliente (par exemple outlook) pour connaître quel est le port d'écoute du service souhaité (exemple Exchange). Ce end-port mapper va fournir ce port en retour. Ce port d'écoute est donné aléatoirement par la pile IP du serveur et donc se trouver entre les ports TCP 1024 et 65535. La difficulté est que ce port d'écoute change à chaque redémarrage du service serveur et il n'est que dans de très rares cas la possibilité de le fixer.
- **Port de 1024 à 65535** (les high ports): pour les raisons que nous venons de voir, filtrer les accès RPC à l'aide d'un firewall de niveau 3 revient à ouvrir tous les ports au delà de 1024.

Microsoft fournit pour certains de ses services RPC des clefs de registre qui permettent de forcer ceux-ci à utiliser un port précis, ce qui facilite la mise en œuvre de filtrages avec des firewall de niveau 3. Mais cette technique n'est fournie que pour des services d'infrastructure (réplication AD par exemple), est considérée comme une solution de contournement, et donc ne constitue en aucun cas un fonctionnement normal tel que décrit dans les kits de développements (SDK). Ces clefs de registre sont le résultat de la 'bonne volonté' des développeurs, et ne peuvent donc pas être considéré comme 'la' solution universelle pour filtrer les services RPC.

De plus, Microsoft dispose avec ISA 2004 d'un firewall applicatif permettant de filtrer les RPC d'une façon beaucoup plus intelligente. On peut donc raisonnablement se dire qu'à l'avenir, les développeurs ne créeront plus de solutions de contournement de ce type et demanderont aux équipes techniques de filtrer au niveau 7, ce qui est de toute façon de faire la plus universelle et la plus sécurisée.

Voici un schéma qui résume ce que nous venons d'expliquer à travers un diagramme :



Comme vous pouvez le voir sur ce schéma, le firewall de niveau 3 ouvre un nombre impressionnant de ports (le gros tuyau bleu), simplement car il ne peut jamais savoir quel va être le port utilisé par le service RPC distant.

Ce que nous allons faire avec ISA 2004, c'est la publication des mêmes services RPC, mais en filtrant d'une façon plus fine et plus maligne ces flux. Nous allons pour cela utiliser le filtre applicatif RPC fournit par ISA 2004.

Le filtrage applicatif consiste à inspecter la donnée de la session TCP/UDP en cours et de s'assurer que celle transportée ne constitue pas une attaque. Ce filtre peut le faire car il ne voit pas la donnée transportée comme « une suite de caractères » mais comme une suite de 'verbes' d'un protocole déterminé.

⚠	Nous décrivons ici le mécanisme de filtrage applicatif pour le protocole RPC, mais l'approche de filtrage applicatif touche tous les protocoles. Dans le cas d'une infrastructure applicative WEB par exemple, il est plus qu'important de mettre en œuvre entre les frontaux WEB et les serveurs SQL des firewall applicatifs permettant de détecter des flux de données de type DROP TABLE.

Le filtre RPC va quant à lui inspecter une partie du dialogue sur le port 135 (le end-port mapper) initié par l'application cliente en direction du serveur. Ce filtre va regarder la trame et extraire un champ appelé l'UUID (Universally Unique IDentifier). Cet UUID représente en fait le nom unique

du service à contacter. Ce dialogue avec le end-port mapper revient pour à un client Outlook à dire « hey serveur, quel est le port d'écoute pour Exchange aujourd'hui ? ».

Voici un exemple de connexion RPC entre une station de travail et un serveur RPC distant (voir le diagramme plus bas) :

① Le PC jaune initie une connexion RPC avec son application jaune distante. Le PC va d'abord se connecter sur le port 135 et demander au serveur distant "hey, quel est le port RPC du service **E1AF8308-5D1F-11C9-91A4-08002B14A0FA**". Cette étrange suite de caractère est en fait l'UUID RPC du service hébergé sur le serveur distant. Ce type de flux arrive à destination car ISA 2004 possède une règle firewall contenant le filtre applicatif RPC. Cette règle indique que cet UUID est autorisé, et que tout autre UUID est refusé. Si un autre UUID était demandé et qu'il n'était pas autorisé, ISA indiquerait au client que ce service n'est pas disponible sans même que le serveur jaune en ai été informé.

② Le serveur RPC a reçu la demande sur son port 135 (end-port mapper), et répond au client que le service RPC demandé écoute par exemple sur le port 2345.

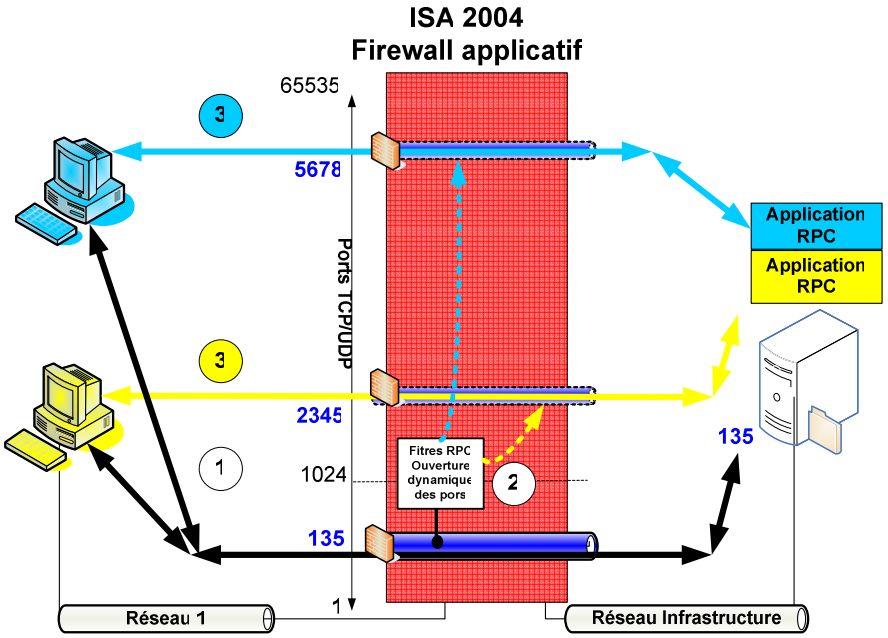
② Maintenant que le flux de localisation RPC a fonctionné, ISA 2004 va dynamiquement ouvrir le port TCP retournée par le serveur jaune (2345) pour ce client. Ceci a été possible car il a inspecté la réponse de ce serveur (en direction du client) et a extrait de la trame RPC le port TCP du service.

③ La station de travail débute une connexion TCP sur le port 2345 et le dialogue RPC démarre entre le logiciel client et l'application serveur. Sur le diagramme nous symbolisons cette ouverture dynamique du port 2345 par un tunnel en pointillé.

On peut voir ici qu'en inspectant le protocole et non en ouvrant un port, ISA 2004 a détecté que cette trame était autorisée car elle contenait une UUID autorisée par des règles firewall.

Sur le diagramme ci-dessous on peut voir que ce même mécanisme est utilisé par la machine bleue ③ qui tente de se connecter sur le même serveur, mais sur l'application RPC bleue. La seule différence dans ce cas est que le client RPC va demander au endport-mapper un UUID différent (bleu non jaune). Par définition, l'application bleue va 'écouter' sur un port différent de l'application jaune, par exemple 5678. Disons que cette application est également autorisée.

Voici un diagramme qui décrit tout ces mécanismes :



Comme nous l'avons vu précédemment, si une application RPC demande à se connecter sur un service non autorisé par ISA (UUID non présente dans la règle), la connexion sera alors impossible et bloquée par ISA dès le dialogue avec le end-point mapper (non transmis au serveur distant).

⚠	Avec cette 'vision' de la sécurité, il est alors possible de n'autoriser que les trafics autorisés, et donc de mettre en œuvre une politique de filtrage applicatif sur le réseau interne de l'entreprise. Ceci permet de protéger ses serveurs d'infrastructures (Exchange, AD, …) de toutes attaque interne (virus, …).

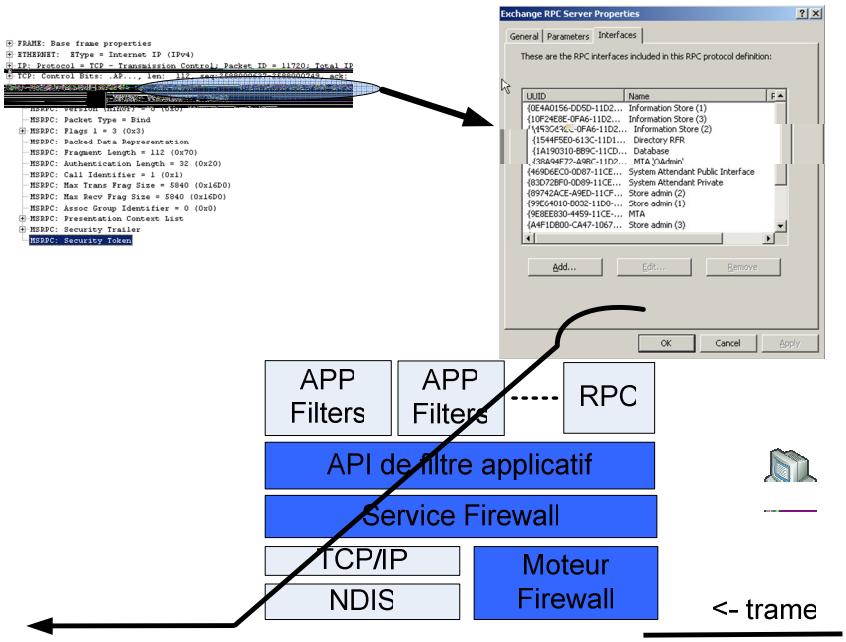
Fonctionnement du filtre RPC

Nous avons vu précédemment comment les filtres RPC fonctionnent. Découvrons maintenant en détail la partie cachée.

Dans le diagramme suivant vous pouvez voir tous les aspects de ce type de filtrage de flux :

- Tout d'abord une capture de **trame** réalisée avec **Microsoft Netmon**. Tout dialogue RPC débute avec une connexion sur le TCP 135 et doit contenir l'UUID du service distant. ISA 2004 va inspecter ce type de trame pour voir si ce flux est autorisé ou interdit. Vous pouvez voir sur ce diagramme l'UUID véhiculée au sein de la trame.

- Le **filtre RPC dans ISA 2004** : si l'UUID n'apparaît pas dans la règle c'est-à-dire dans les propriétés de la règle dans l'interface graphique d'ISA (règle firewall), alors la trame est refusée (le sens interdit sur le diagramme). Pour illustrer l'interface, nous avons ajouté dans ce diagramme la capture écran du filter applicatif RPC pour Exchange qui est fournit en natif averc ISA 2004.



certains services, il n'existe pas de base publique permettant de connaître les UUIDs de tous les services du marché (produits Microsoft ou autre sociétés). Il faut donc apprendre à les découvrir nous-mêmes pour être autonome.

Par exemple, si vous voulez autoriser la réplication entre deux serveurs AD à travers ISA 2004 (c'est un scénario très souvent rencontré lors d'architectures internationales de type 'branch office'), nous devons déterminer les UUIDs de tous les services utilisés (en fait réplication AD, NTFRS…).

Le scénario utilisé pour expliquer cette méthode va consister à autoriser une station d'administration à utiliser la MMC d'administration d'ISA. Si l'on parle RPC, cela revient à autoriser l'UUID utilisée par la MMC ISA pour administrer cette machine.

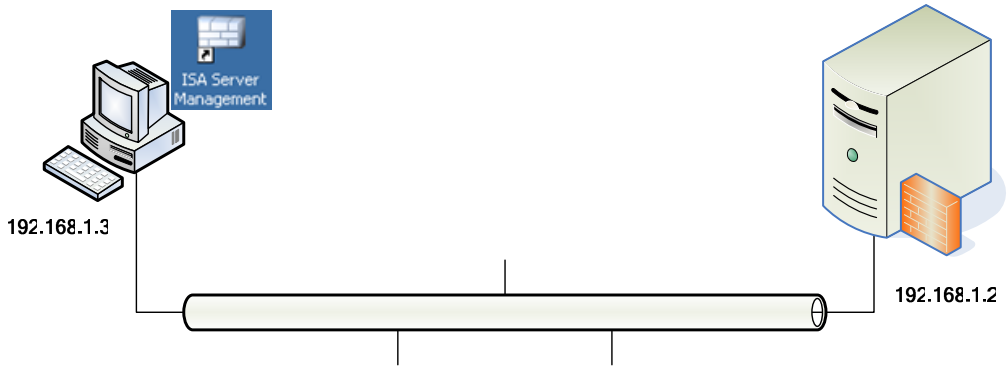
V. Le challenge : découvrir les UUID(s)

Nous avons vu précédemment pourquoi ouvrir tous les ports de 1024 à 65535 n'était pas une bonne solution. Nous allons donc le faire d'une façon plus précise en utilisant les filtres RPC.

Le problème est que pour créer une règle d'autorisation de flux, il faut connaître la ou les UUIDs utilisées par l'application RPC cliente (MMC ISA dans notre exemple).

Pour découvrir les UUIDs de cette MMC ISA, nous avons créé un laboratoire de test relativement simple. En voici la description:

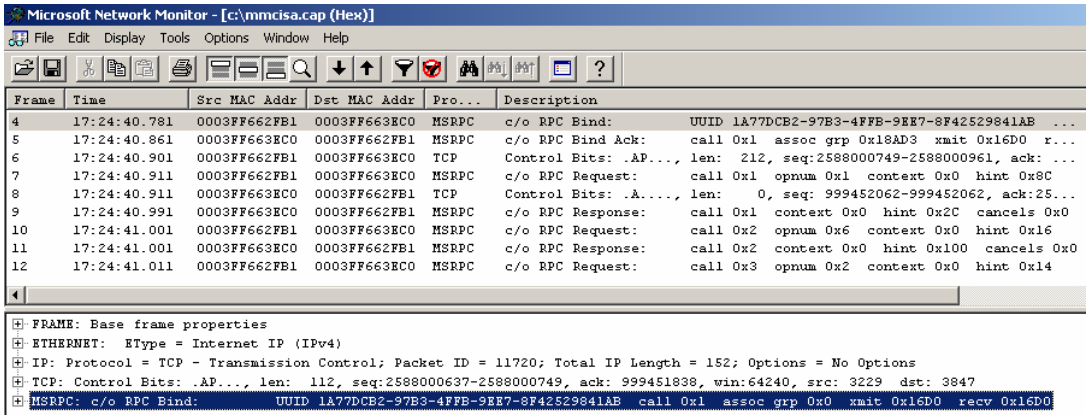
- Une station d'administration qui va lancer la MMC ISA,
- Un serveur ISA 2004.



Pour analyser ce trafic, nous avons d'abord créé une règle autorisant tous les types de flux depuis la station d'administration en direction d'ISA sur son réseau 'Local Host'.

Nous avons ensuite lancé le Microsoft Network Monitor sur le serveur ISA 2004 et avons précisé dans la règle de capture de ne prendre que le trafic venant de l'IP de la machine d'administration.

Voici le résultat de cette capture :



En regardant cette capture, on voit clairement apparaître le dialogue sur le port 135 (RPC Bind) visant à déterminer le port utilisé par le service distant. On identifie alors clairement l'UUID utilisée par la MMC ISA :

En analysant le reste de la trame nous avons détecté lors de nos tests qu'il n'y a pas d'autres UUID utilisé par la console. Ceci ne signifie en aucun cas que toutes les MMC n'utilisent qu'un seul UUID, et il est donc dans le cas d'une analyse de regarder l'ensemble des trames.

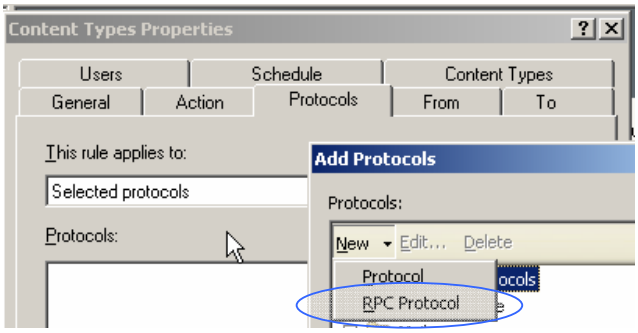
VI. Mise en œuvre du filtre RPC

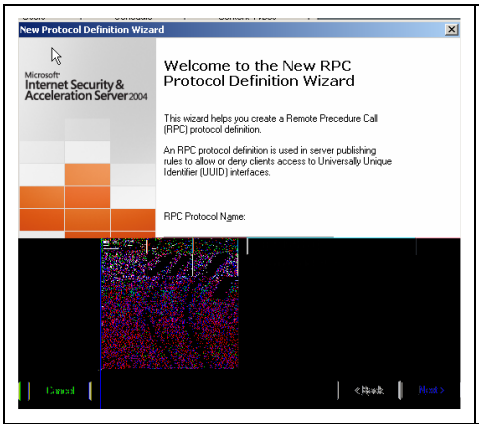
Nous connaissons maintenant l'UUID utilisé par la MMC ISA

Nous allons donc maintenant créer notre propre **« définition de protocole RPC »**, ce qui signifie créer un objet ISA auquel nous allons donner un nom et ajouter à celui-ci la liste des UUIDs autorisés. Ensuite nous allons utiliser cette définition au sein d'une règle firewall précise.

Pour réaliser cette création de définition, nous allons commencer par créer la future règle firewall (le menu de création d'une définition est accessible à travers le menu de définition d'une règle).

Une fois créée, aller dans l'onglet protocoles, puis sélectionner l'option « Add Protocols ». Cliquer ensuite sur « New » et sélectionner 'RPC Protocol' :



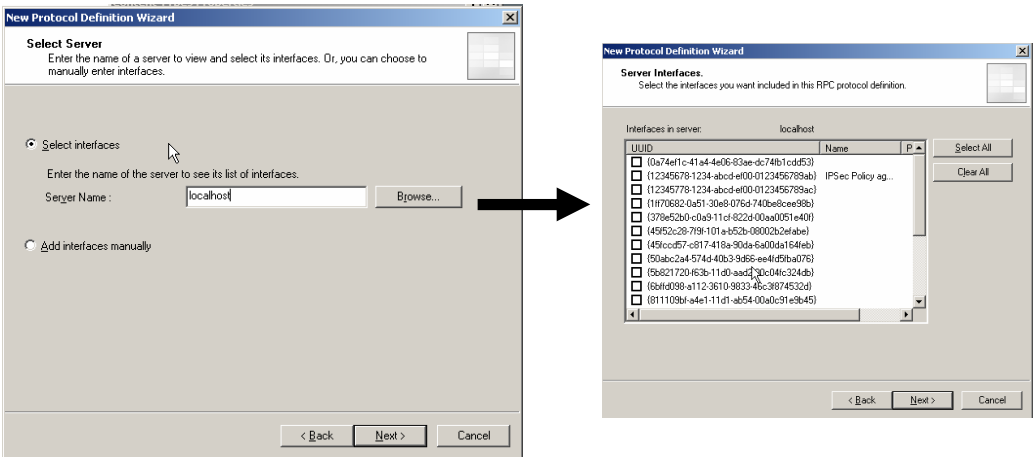


Un assistant démarre alors. Il s'agit de l'assistant de création de 'définition de protocole RPC'.

Petit conseil : utilisez une convention de nommage vous permettant de faire la différence entre vos propres protocoles (Ici FE-rpc-isammc commencant par mes initiales) et les protocoles fournit par Microsoft.

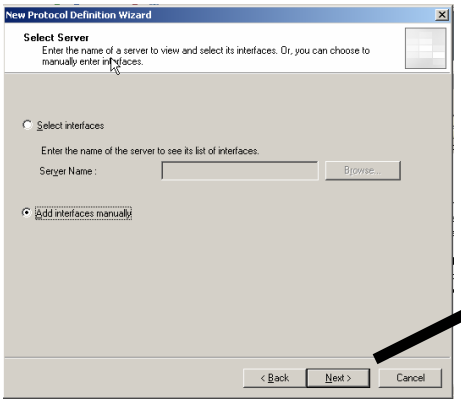
Sur l'écran ci-dessous vous avez deux options possibles :

- **Option 1 - select interfaces**: cette option va vous permettre de lister tous les services RPC exécutés sur la machine ISA elle-même. Vous pourrez alors cocher les UUIDs que vous voulez ajouter à votre définition. Dans notre cas cette option pourrait être utile car le servce à publier est sur cette machine. Mais sans pouvoir expliquer pourquoi, l'UUID que nous avons détecté en utilisant netmon n'apparaît pas dans la liste. Egalement, cette option n'est pas utilisée si le serveur RPC à atteindre n'est pas la machine ISA elle-même:

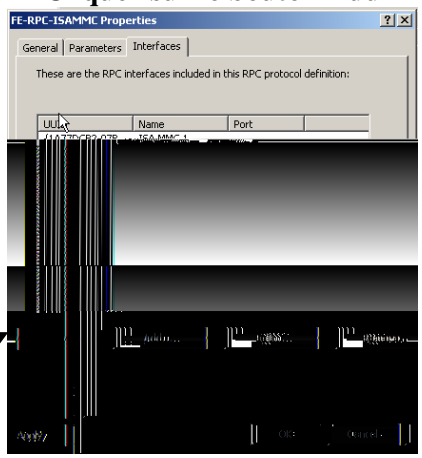


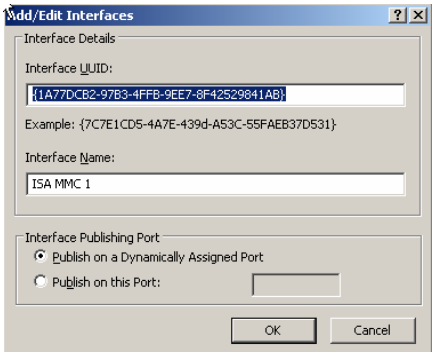
- **Option 2 - add interfaces manually** : Cette option nous propose une interface dans laquelle il faut saisir une par une les UUIDs à ajouter à notre définition. Pour réaliser cette opération, procéder ainsi :

Sélectionner 'Add interfaces » et cliquer sur next.



Cliquer sur le bouton Add



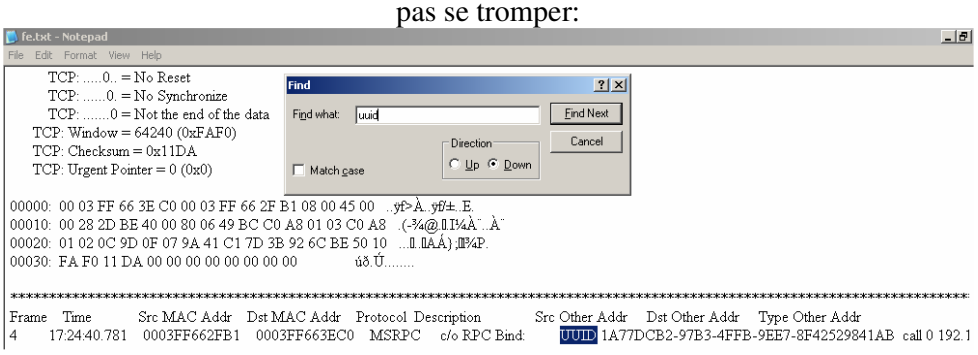


Un fois cliqué sur Add button, vous obtenez cet écran.

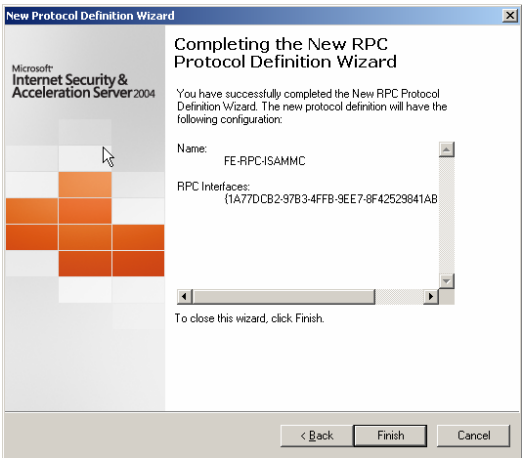
Il suffit alors de taper dans la zone 'interface UUID' l'UUID du service à publier, et indiquer dans la zone 'interface Name' le nom que vous souhaitez lui donner.

Laisser le bouton radio sur 'publish'.

Afin de ne pas se tromper dans la saisie de l'UUID, une astuce peut être utilisée. Installez sur le serveur ou se trouve netmon l'imprimante 'text only'. Imprimez ensuite l'ensemble de la capture dans un fichier texte et localisez la trame à l'aide de la fonction 'edit/find. Il ne reste plus qu'à faire un copier coller pour ne pas se tromper:



Pour cet article nous avons utilisé un scénario simple qui après investigation avec netmon nous indique que nous avons besoin dans notre définition que d'un seul UUID. Si dans votre scénario de production vous avez besoin de plus d'une UUID pour votre définition pour autoriser la communication, répéter cette opération pour chaque UUID.



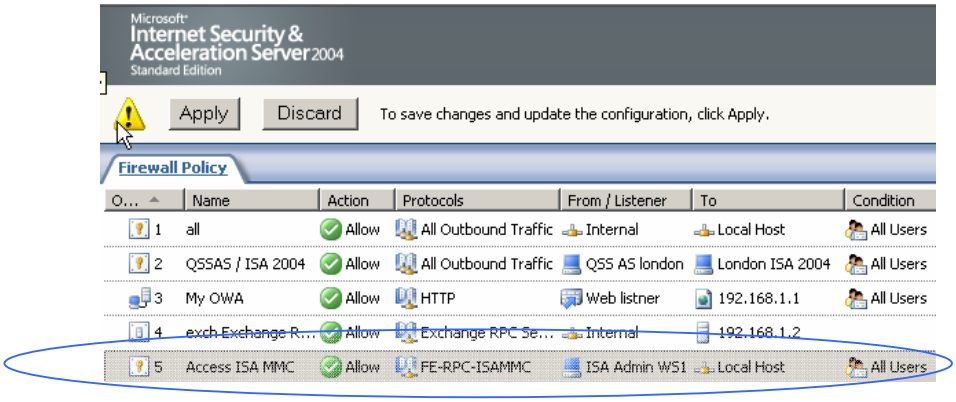
Lorsque vous avez entré toutes les UUIDs nécessaires, à la fin de la procédure d'ajout d'UUID sur une nouvelle définition de protocole RPC, cliquez sur Finish.

A ce niveau votre nouvelle 'définition' d'UUIDs est disponible dans la liste des définitions d'ISA et vous pouvez l'associer aux règles firewall.

VII. Finaliser la règle firewall d'autorisation

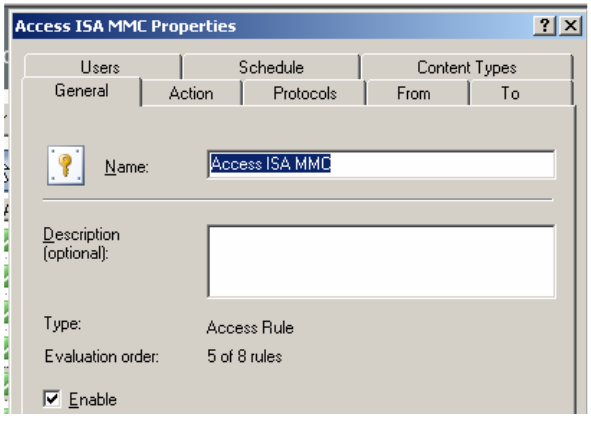
Nous venons dans le chapitre de créer notre propre définition de protocole RPC, nous allons maintenant l'utiliser au sein d'une règle firewall.

Voici le détail de la règle pour autoriser notre poste de travail à dialoguer en RPC avec ISA (réseau LocalHost). Le cercle bleu indique notre nouvelle règle. On y voit la 'définition - protocoles' (ce que nous avons créé dans le chapitre précédant), la source (ISA Admin WS1 – identifié par son adresse IP) et LocalHost qui indique le réseau interne de la machine ISA.

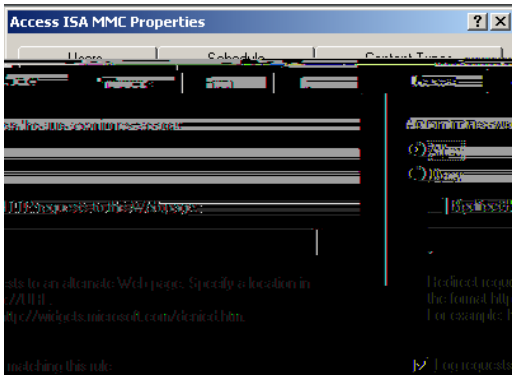


Voici maintenant le détail de chaque TAB de la règle firewall

Nom de la règle firewall



Règle de type autorise (Allow)



Difficulté :

IX. Conclusion

La mise en œuvre de firewalls applicatifs est quasiment incontournable sur l'Internet (ceci est valable pour tous les types de protocoles), mais également sur le réseau interne de l'entreprise. Les filtres RPC d'ISA 2004 est un atout majeur pour faire face aux attaques internes sur les réseaux d'infrastructure.

La mise en œuvre de ce type d'architecture permet de garantir qu'une attaque de ce type de pourra se propager sur les serveurs d'entreprise. Les statistiques tant françaises qu'étrangères montrent bien que les attaques internes représentent un coût très important, et on ne peut donc pas les prendre en compte lors d'une réflexion sur un design.

ISA 2004 possède un filtrage RPC très complet qui permet de monter le niveau de sécurité à un niveau bien plus haut que la simple ouverture de ports.