Configuration de IPSEC sur un serveur Windows 2000

Implémentation de IPSEC dans Windows 2000

Le pilote IPSEC se présente sous la forme d'un service matériel, "IPSEC.SYS"[1], automatiquement installé et démarré avec Windows. Toutefois ce service est en mode "transparent" par défaut : il n'a aucun impact sur les communications réseau tant qu'il n'a pas été configuré.

Ses paramètres de configuration lui sont transmis par le service "agent de stratégie IPSEC" (PolicyAgent) qui est quant à lui visible et configurable par l'utilisateur.

Le paramétrage du service IPSEC s'effectue en 4 étapes :

- Création d'une liste de filtres
- Création d'une liste d'actions de filtrage
- Création d'une stratégie IP par assemblage de filtres et d'actions de filtrage
- Attribution de la stratégie

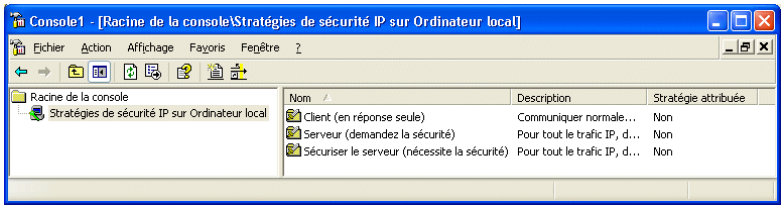
Ce paramétrage peut être rapidement déployé sur les postes contenus dans une ou plusieurs Unités Organisationnelles d'un domaine grâce aux stratégies de groupe de Windows 2000. Dans le cas d'un "home user" ne possédant pas de domaine Windows, celui-ci préférera configurer une stratégie locale sur chacun de ses postes. Dans les deux cas la marche à suivre est la même.

Les stratégies IP de Windows 2000 sont ainsi faites qu'elles regroupent à la fois des règles (port source/destination, adresse source/destination, sous-réseau) et des actions de filtrage (rejeter, accepter ou encapsuler dans IPSEC). Il est donc parfaitement possible d'utiliser une stratégie IP pour mettre en place un firewall rudimentaire sous Windows 2000, sans jamais échanger aucun paquet IPSEC sur le réseau.

Création d'une stratégie IP

Ouvrir l'outil d'administration de la stratégie de sécurité IP. Cet outil est accessible via plusieurs emplacements :

- L'outil d'administration "stratégie de sécurité locale" (localement)
- L'outil d'administration "stratégie de groupe" (pour un domaine)
- La console MMC, snap-in "stratégie de sécurité IP"



Microsoft fournit 3 stratégies prédéfinies : "client", "serveur" ou "sécuriser le serveur". Ces stratégies sont très simples et ne peuvent être utilisées qu'à titre d'exemple.

---

[1] Les services matériels sont normalement invisibles aux utilisateurs, mais peuvent être affichés dans le gestionnaire de périphériques via le menu "affichage / afficher les périphériques cachés".

Nous allons maintenant nous atteler à créer notre propre stratégie, qui comprendra les règles suivantes :

- Autoriser le trafic ICMP en clair
- Autoriser le trafic DNS en clair
- Utiliser ESP sur les accès SMTP à la machine SRV_SMTP
- Utiliser ESP sur les accès HTTP à la machine SRV_SMTP (supposons que cette machine héberge un Webmail car cela permettra plus tard d'aborder un cas particulier intéressant)
- Utiliser ESP sur les accès HTTP à la machine SRV_HTTP
- Utiliser AH sur les accès HTTPS à la machine SRV_HTTP
- Par défaut, refuser le trafic en clair

Création d'une liste de filtres

Dans le menu "Action / Toutes les tâches", 5 actions sont disponibles :

- Créer une stratégie de sécurité
- Gérer les filtres et les actions de filtrage
- Restaurer les stratégies par défaut
- Importer les stratégies
- Exporter les stratégies

Commençons par créer une liste de filtres avec la commande "gérer les filtres et les actions de filtrage". Il nous faut ajouter tous les filtres nécessaires, à savoir :

- Tout le trafic ICMP
- Tout le trafic DNS (UDP/53 et TCP/53)
- Tout le trafic SMTP (TCP/25)
- Tout le trafic HTTP (TCP/80)
- Tout le trafic HTTPS (TCP/443)

Une petite optimisation est possible ici. En effet un filtre peut inclure plusieurs règles : il est donc possible de factoriser les règles de filtrage tant que l'action de filtrage qui leur sera associée reste la même. Dans le cadre de cet exemple, il s'agit typiquement des flux SMTP et HTTP sur la machine SRV_SMTP qui sont tous deux protégés par ESP.

Indépendamment du fait que les impacts sur les performances d'une telle optimisation sont totalement inconnus mais probablement marginaux, il reste que la stratégie IP obtenue au final risque d'être moins lisible : utiliser cette optimisation avec parcimonie ...

La création des filtres ne devrait normalement pas poser de problèmes vu la simplicité des interfaces. Les protocoles IP supportés par Windows (avec leur identifiant numérique) sont :

- "any" (*),
- "user-defined" (?),
- EGP (8), HMP (20), ICMP (1), RAW (255), RDP (27), RVD (66), TCP (6), UDP (17) et XNS (22).

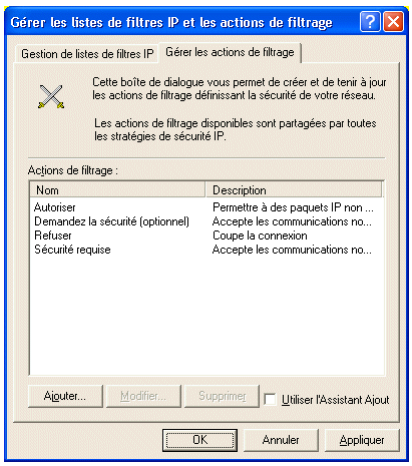
Ceci étant le support de ces protocoles est très limité puisque à part les ports source et destination sur TCP et UDP, aucune autre option protocolaire n'est gérée ...

L'option "image miroir" rend la même règle valable pour des paquets ayant une adresse IP source et destination inversée. En général il est souhaitable de la laisser cochée, mais comme on le verra par la suite, cette option n'a que peu d'intérêt puisque la règle par défaut du filtre est "accepter".

Création d'une liste d'actions de filtrage

Passons maintenant à l'onglet "actions de filtrage". Là encore il nous faut définir toutes les actions que nous allons utiliser à savoir :

- Autoriser en clair
- Refuser
- Exiger ESP
- Exiger AH



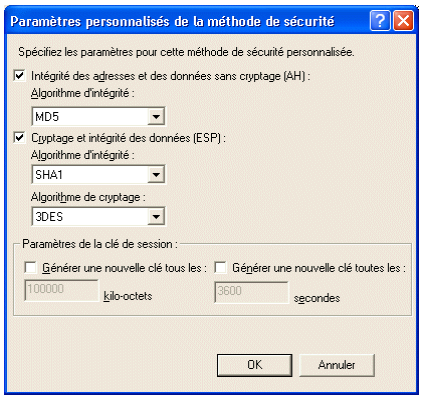
Ici aussi on appréciera la simplicité des interfaces graphiques de configuration.

Windows propose les options suivantes :

- Autoriser
- Refuser
- Négocier la sécurité

On voit donc (comme annoncé) que les stratégies IP permettent à peu de frais de mettre en place des règles de "firewalling" sur Windows 2000, même si on ne souhaite pas chiffrer/signer le trafic IP.

Windows 2000 permet d'utiliser IPSEC en mode AH, ESP ou les deux. Les algorithmes supportés sont tout ce qu'il y a de plus traditionnels : MD5, SHA1, DES, 3DES.



Bien que les algorithmes cryptographiques ci-dessus soient réputés robustes, activer les options de renouvellement de la clé de session permet d'augmenter encore le niveau de sécurité vis-à-vis d'un attaquant collectant le trafic réseau, sans réel impact sur la performance (les paramètres par défaut indiquent au pilote IPSEC de renouveler la clé de session tous les 100 Mo de trafic ou toutes les heures, ce qui est marginal).

Les protocoles sont négociés dans l'ordre d'affichage. Les options globales de la règle permettent de contrôler l'action de filtrage en cas d'échec de la négociation :

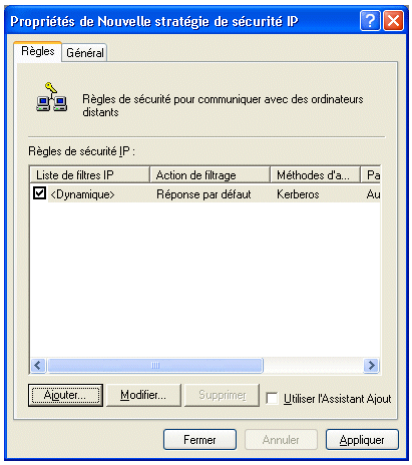
- "Accepter les communications non sécurisées mais toujours répondre en utilisant IPSEC" permet de répondre aux machines qui ne sont pas configurées pour utiliser IPSEC en priorité, tout en ne sacrifiant pas la sécurité

- "Autoriser une communication non sécurisée avec un ordinateur qui n'utilise pas IPSEC" ne devrait pas être activée puisque cette option établit une règle de réponse par défaut non sécurisée !

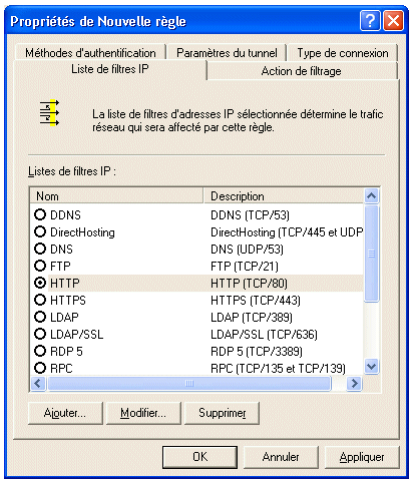
- "Session de clé principale PFS" permet de renégocier la clé principale avant chaque négociation de clé de session : le déchiffrement d'une session TCP par un attaquant ne met alors pas en danger les autres communications qu'il a pu capturer (*Perfect Forward Secrecy*), mais ce au prix d'une charge réseau et CPU considérablement accrue !

Assemblage de la stratégie

Il nous reste maintenant à assembler les listes de filtres et les listes d'action pour décrire la stratégie de sécurité IP que nous voulons mettre en œuvre dans cet exemple : pour cela il nous faut créer une nouvelle stratégie IP dans la console "stratégie de sécurité IP" toujours ouverte.



Si tous les filtres et toutes les actions de filtrage ont été correctement saisis, cette étape ne devrait pas poser de problème : il suffit d'ajouter les correspondances une à une via le bouton "ajouter".



On remarquera que chaque "règle" (qui représente en fait une association entre un filtre et une action de filtrage) possède des méta-paramètres :

- "Type de connexion" permet de définir si la règle s'applique à une connexion locale, une connexion RAS, ou les deux.

- "Paramètres du tunnel" permet de définir le point de sortie d'un tunnel IPSEC, inutile dans notre cas[2].

- "Méthode d'authentification" permet de définir la méthode utilisée lors de la négociation de la clé principale.

  Les méthodes disponibles sont les mêmes que sous Unix (à savoir secret pré-partagé ou certificat X.509), à l'exception de la méthode "Kerberos" qui utilise comme secret la clé de session Kerberos, lue dans le ticket d'authentification du poste dans son domaine : cette méthode très souple n'est donc disponible que lorsque tous les équipements communiquant appartiennent à un domaine Windows 2000.

[2] Seul le mode transport est présenté dans cette fiche.

Comme il est possible là encore de définir plusieurs méthodes d'authentification par ordre de préférence, la méthode "Kerberos" peut être utilisée en conjonction avec une méthode plus standard.

La règle de réponse par défaut s'applique aux communications qui ne rentrent pas dans le cadre des filtres précédents.

On notera d'ailleurs avec intérêt que les actions "refuser" sont prioritaires sur les actions "accepter", mais que le filtre par défaut est associé à une action "négocier, accepter le trafic en clair en cas d'échec" (la règle de réponse par défaut). Nous ne sommes donc pas en présence d'un "vrai" firewall, et il serait très mal avisé d'ajouter une règle "refuser" sur tout le trafic IP car cette règle serait prioritaire sur toutes les autres !

L'onglet "général" permet de paramétrer le protocole IKE (échange de clés). Là encore il s'agit d'une liste d'algorithmes par ordre de préférence, qui ne présente pas de difficultés de compréhension particulières.

Attribution de la stratégie

La dernière étape consiste à attribuer la stratégie, ce qui a pour effet de la rendre active immédiatement. Les modifications de stratégie sont ensuite prises en compte périodiquement (par défaut toutes les 3 heures, mais cette valeur est réglable dans les propriétés de la stratégie).

Une seule stratégie peut être attribuée à la fois à un poste donné.

Bien entendu avant tout déploiement de stratégie IP en "grandeur nature", il est fortement recommandé de réaliser des tests exhaustifs, Windows ayant tendance à ouvrir beaucoup plus de ports qu'on ne le croit (l'exemple le plus connu et le plus honni des administrateurs réseau étant les ports RPC dynamiques). Si vous déployez dans un domaine une stratégie bloquante pour les communications avec le contrôleur de domaine, il vous faudra mettre à jour la stratégie "à la main" sur tous les postes …

Quelques remarques sur l'implémentation de IPSEC dans Windows

La mise en place d'une stratégie IP dans un domaine Windows 2000 s'effectue normalement sans douleur dans un réseau très homogène (postes Windows 2000 SP2 ou mieux).

Cette relative simplicité ne doit pas faire oublier les problèmes de compatibilité inévitablement rencontrés lors de tentatives de communications avec du logiciel non-Microsoft, par forcément d'ailleurs par non respect de la RFC, mais plus par le traitement des cas aux limites, tels que le rétablissement d'un tunnel après un "timeout".

Windows n'est néanmoins pas exempt de tout reproche, quant on sait que les versions françaises de Windows 2000 antérieures au SP2 utilisent "silencieusement" l'algorithme DES en lieu et place de l'algorithme 3DES pour des raisons de législation sur la cryptographie … Voilà le genre de problème qui prend un certain temps à dépanner !

Les outils disponibles en cas de problème sont le journal d'événement, dans lequel les pilotes ISAKMP et IPSEC enregistrent leurs messages, et l'outil IPSECMON (maintenant intégré à l'Admin Pack pour Windows 2003 sous forme de snap-in "moniteur de la sécurité IP").

Dernier détail : par défaut le trafic TCP et UDP ayant un port source de 88 ou 500 outrepasse toutes les stratégies IP en place … Il faut le savoir ! Pour remédier à ce désagrément il est nécessaire de mettre à 1 la valeur suivante en base de registre :

HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt (REG_DWORD)

Cette clé ne corrige pas tous les cas d'exception puisque les négociations IKE, les Broadcasts et les Multicasts restent exemptés de stratégie IP, mais c'est déjà mieux. Les choses se sont améliorées avec Windows 2003, pour plus d'informations je vous invite à vous reporter aux articles suivants :

http://support.microsoft.com/?kbid=254728
http://support.microsoft.com/?kbid=810207

La face Nord : IPSECPOL

Il existe également des outils de configuration en ligne de commande pour IPSEC, mais leur usage devrait être réservé aux fanatiques du script ou au dépannage de dernier recours (le mode sans échec en ligne de commande).

Ces outils sont :

- IPSECPOL sous Windows 2000
- IPSECCMD sous Windows XP (disponible dans les Support Tools)
- L'infâme NETSH sous Windows 2003

Conclusion

La mise en place du protocole IPSEC en mode transport dans un réseau purement Windows 2000 SP2 ou ultérieur peut être qualifiée de triviale et permet d'améliorer considérablement la sécurité des protocoles historiquement "faibles" tels que FTP, POP, SMTP ou HTTP.

L'interaction avec d'autres systèmes d'exploitation est plus hasardeuse mais reste possible au prix d'un effort de mise en œuvre important.

Enfin la mise en place de règles IPSEC sur un serveur Windows 2000 ne le protège pas contre les attaques directes (scan de ports) à cause des trous béants introduits volontairement dans le filtrage réseau : le gain sécuritaire obtenu ne s'applique qu'aux communications réseau et leurs traditionnelles vulnérabilités (écoute, rejeu, altération, "man-in-the-middle").

Nicolas RUFF
Consultant Sécurité, Expert Windows
EdelWeb / Groupe ON-X

Merci à
Patrick CHAMBET
EdelWeb / Groupe ON-X