

Lab 3: Sécurité IPsec

Objectif:
Sécuriser les liaisons sans fil

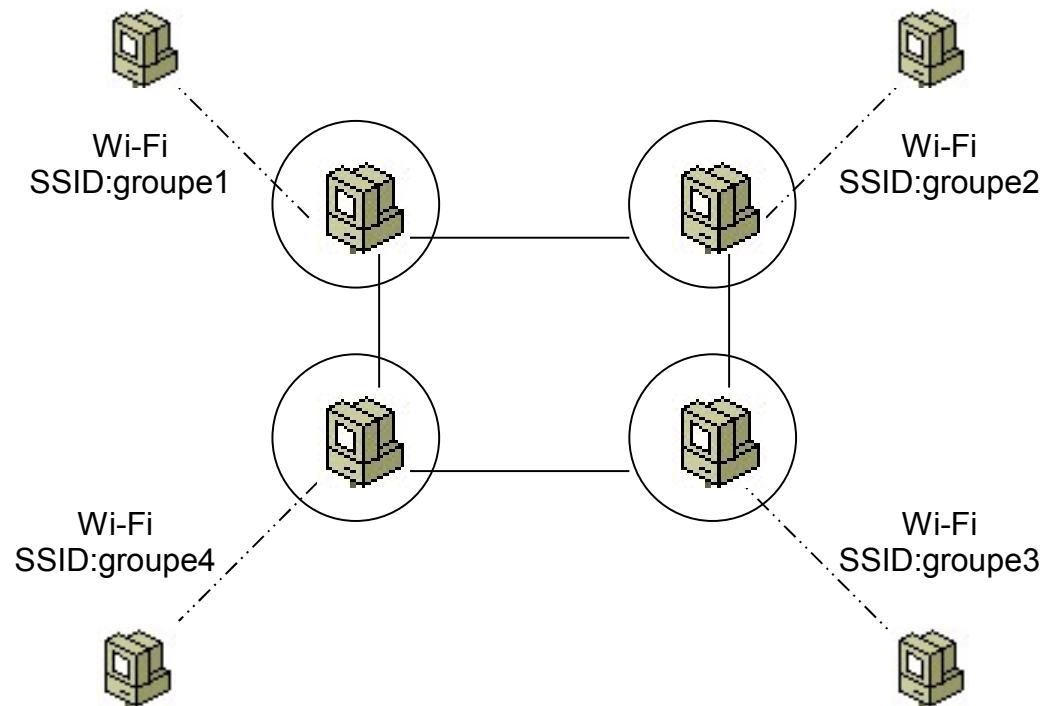
ipsec6

- L'utilitaire Ipsec6.exe vous permet de configurer les associations de sécurité et les stratégies IPsec.
- Ipsec6.exe possède plusieurs commandes, chacune dotée de son propre jeu de paramètres.
- **ipsec6 sp** [*Interface*] // security policies
Affiche les stratégies de sécurité actives. Peut également afficher les stratégies de sécurité actives d'une interface spécifique.
- **ipsec6 sa** // security associations
Affiche les associations de sécurité actives.
- **ipsec6 l** *NomFichierSansExtension* // load
Charge les stratégies de sécurité à partir de *NomFichier.spd* et les associations de sécurité à partir de *NomFichier.sad*.
- **ipsec6 s** *NomFichierSansExtension* // save
Enregistre les stratégies de sécurité actuelles dans *NomFichier.spd* et les associations de sécurité actuelles dans *NomFichier.sad*. Cette commande vous permet de créer des fichiers afin de configurer les stratégies de sécurité et les associations de sécurité. En l'absence de stratégie ou d'association de sécurité, cette commande crée *NomFichier.spd* pour les stratégies de sécurité et *NomFichier.sad* pour les associations de sécurité. Vous pouvez utiliser ces fichiers comme modèles de configuration des stratégies et associations de sécurité en les modifiant avec un éditeur de texte.
- **ipsec6 d** [**sp** | **sa**] [*Index*] // delete
Supprime les stratégies de sécurité (utilisation du paramètre **sp**) ou les associations de sécurité (utilisation du paramètre **sa**) de la liste des stratégies et associations de sécurité actives sur la base du numéro d'index spécifié. Vous pouvez utiliser **ipsec6 sp** ou **ipsec6 sa** pour afficher le numéro d'index.
- **ipsec6 m** [**on** | **off**] // mobile
 - Spécifie si les mises à jour de liaison utilisées pour les protocoles IPv6 mobiles sont protégés par la sécurité IP. Cette protection est activée par défaut.

Etape 1

Chaque équipe crée une association de sécurité IPSec entre deux hôtes d'un même sous-réseau. L'association de sécurité exécute l'authentification à l'aide de l'en-tête d'authentification (AH, *Authentication Header*) et de l'algorithme de hachage MD5 (Message Digest 5). Dans cet exemple, la configuration sécurise tout le trafic entre deux hôtes voisins. L'hôte 1 possède l'adresse lien-local FE80::2AA:FF:FE53:A92C, et l'hôte 2 l'adresse lien-local FE80::2AA:FF:FE92:D0F1.

Sur l'hôte 1, créez des fichiers vides d'association de sécurité (.sad) et de stratégie de sécurité (.spd) à l'aide de la commande **ipsec6 s**. Dans cet exemple, la commande Ipsec6.exe est **ipsec6 s test**. Elle crée deux fichiers dont les entrées vides permettent de configurer manuellement les associations de sécurité (Test.sad) et les stratégies de sécurité (Test.spd).



Etape 2

Sur l'hôte 1, modifiez le fichier .spd, en ajoutant une stratégie de sécurité qui sécurise tout le trafic entre l'hôte 1 et l'hôte 2.

Le tableau suivant illustre l'entrée de stratégie de sécurité ajoutée à Test.spd avant la première entrée (la première entrée de Test.spd n'est pas modifiée) :

Nom de champ du fichier .spd	Valeur exemple
Policy	2
RemoteIPAddr	- FE80::2AA:FF:FE92:D0F1
LocalIPAddr	- *
Protocol	- *
RemotePort	- *
LocalPort	- *
IPSecProtocol	AH
IPSecMode	TRANSPORT
RemoteGWIPAddr	*
SABundleIndex	NONE
Direction	BIDIRECT
Action	APPLY
InterfaceIndex	0

Tapez un point-virgule à la fin de l'entrée configurant cette stratégie de sécurité. Les entrées de stratégie doivent être placées en ordre numérique décroissant.

Etape 3

Sur l'hôte 1, modifiez le fichier .sad, en ajoutant des entrées d'association de sécurité afin de sécuriser tout le trafic entre l'hôte 1 et l'hôte 2. Deux associations de sécurité doivent être créées, l'une pour le trafic en direction de l'hôte 2, l'autre pour le trafic en provenance de l'hôte 2.

Le tableau suivant illustre la première entrée d'association de sécurité ajoutée à Test.sad (pour le trafic vers l'hôte 2) :

Nom de champ du fichier .sad	Valeur exemple
SAEntry	2
SPI	3001
SADestIPAddr	FE80::2AA:FF:FE92:D0F1
DestIPAddr	POLICY
SrcIPAddr	POLICY
Protocol	POLICY
DestPort	POLICY
SrcPort	POLICY
AuthAlg	HMAC-MD5
KeyFile	Test.key
Direction	OUTBOUND
SecPolicyIndex	2

Tapez un point-virgule à la fin de l'entrée configurant cette association de sécurité.

Etape 3 (cont.)

Le tableau suivant illustre la seconde entrée d'association de sécurité ajoutée à Test.sad (pour le trafic en provenance l'hôte 2) :

Nom de champ du fichier .sad	Valeur exemple
SAEntry	1
SPI	3000
SADestIPAddr	FE80::2AA:FF:FE53:A92C
DestIPAddr	POLICY
SrcIPAddr	POLICY
Protocol	POLICY
DestPort	POLICY
SrcPort	POLICY
AuthAlg	HMAC-MD5
KeyFile	Test.key
Direction	INBOUND
SecPolicyIndex	2

Tapez un point-virgule à la fin de l'entrée configurant cette association de sécurité. Les entrées d'association de sécurité doivent être placées en ordre numérique décroissant.

Etape 4

Sur l'hôte 1, créez un fichier contenant les données utilisées pour la création et la validation du hachage MD5 (Message Digest 5) appliqué à chaque paquet à protection IPSec échangé avec l'hôte 2. Dans cet exemple, un fichier texte est utilisé. Test.key est créé avec le contenu **Ceci est un test**. Il n'y a aucun caractère, espace ou ligne supplémentaire.

Le protocole IPv6 de Windows XP prend uniquement en charge la configuration manuelle des clés pour les associations de sécurité en mode rapide (également appelées associations de sécurité IPSec ou Phase II), car la négociation du mode principal par le biais d'IKE (Internet Key Exchange) n'est pas effectuée. La configuration des clés manuelles repose sur la création de fichiers contenant leurs données texte ou binaires. Dans cet exemple, la même clé pour les associations de sécurité est utilisée dans les deux directions. Vous pouvez utiliser différentes clés pour les associations de sécurité entrantes et sortantes en créant différents fichiers de clés et en les référençant avec le champ **KeyFile** du fichier .sad.

Etape 5

Sur l'hôte 2, créez des fichiers vides d'association de sécurité (.sad) et de stratégie de sécurité (.spd) à l'aide de la commande **ipsec6 s**. Dans cet exemple, la commande Ipsec6.exe est **ipsec6 s test**. Elle crée deux fichiers dont les entrées vides permettent de configurer manuellement les associations de sécurité (Test.sad) et les stratégies de sécurité (Test.spd).

Dans un souci de simplicité, les mêmes noms pour les fichiers .sad et .spd sont utilisés sur l'hôte 2. Vous pouvez utiliser des noms de fichier différents sur chaque hôte.

Sur l'hôte 2, modifiez le fichier .spd, en ajoutant une stratégie de sécurité qui sécurise tout le trafic entre l'hôte 2 et l'hôte 1.

Le tableau suivant illustre l'entrée de stratégie de sécurité ajoutée à Test.spd avant la première entrée (la première entrée de Test.spd n'est pas modifiée) :

Nom de champ du fichier .spd	Valeur exemple
Policy	2
RemoteIPAddr	- FE80::2AA:FF:FE53:A92C
LocalIPAddr	- *
Protocol	- *
RemotePort	- *
LocalPort	- *
IPSecProtocol	AH
IPSecMode	TRANSPORT
RemoteGWIPAddr	*
SABundleIndex	NONE
Direction	BIDIRECT
Action	APPLY
InterfaceIndex	0

Tapez un point-virgule à la fin de l'entrée configurant cette stratégie de sécurité. Les entrées de stratégie doivent être placées en ordre numérique décroissant.

Etape 6

Sur l'hôte 2, modifiez le fichier .sad, en ajoutant des entrées d'association de sécurité afin de sécuriser tout le trafic entre l'hôte 2 et l'hôte 1. Deux associations de sécurité doivent être créées : l'une pour le trafic en direction de l'hôte 1, l'autre pour le trafic en provenance de l'hôte 1.

Le tableau suivant illustre la première entrée d'association de sécurité ajoutée à Test.sad (pour le trafic vers l'hôte 1) :

Nom de champ du fichier .sad	Valeur exemple
SAEntry	2
SPI	3001
SADestIPAddr	FE80::2AA:FF:FE53:A92C
DestIPAddr	POLICY
SrcIPAddr	POLICY
Protocol	POLICY
DestPort	POLICY
SrcPort	POLICY
AuthAlg	HMAC-MD5
KeyFile	Test.key
Direction	OUTBOUND
SecPolicyIndex	2

Tapez un point-virgule à la fin de l'entrée configurant cette association de sécurité.

Etape 6 (cont.)

Le tableau suivant illustre la seconde entrée d'association de sécurité ajoutée à Test.sad (pour le trafic en provenance l'hôte 1) :

Nom de champ du fichier .sad	Valeur exemple
SAEntry	1
SPI	3000
SADestIPAddr	FE80::2AA:FF:FE92:D0F1
DestIPAddr	POLICY
SrcIPAddr	POLICY
Protocol	POLICY
DestPort	POLICY
SrcPort	POLICY
AuthAlg	HMAC-MD5
KeyFile	Test.key
Direction	INBOUND
SecPolicyIndex	2

Tapez un point-virgule à la fin de l'entrée configurant cette association de sécurité. Les entrées d'association de sécurité doivent être placées en ordre numérique décroissant.

Etape 7

Sur l'hôte 2, créez un fichier texte contenant une chaîne de caractères utilisée pour authentifier les associations de sécurité créées avec l'hôte 1. Dans cet exemple, Test.key est créé et contient la chaîne **Ceci est un test**. Il n'y a aucun caractère, espace ou ligne supplémentaire.

Sur l'hôte 1, utilisez la commande **ipsec6 I** pour ajouter, à partir des fichiers .spd et .sad, les stratégies de sécurité et les associations de sécurité configurées. Dans cet exemple, la commande **ipsec6 I test** est exécutée sur l'hôte 1.

Sur l'hôte 2, utilisez la commande **ipsec6 I** pour ajouter, à partir des fichiers .spd et .sad, les stratégies de sécurité et les associations de sécurité configurées. Dans cet exemple, la commande **ipsec6 I test** est exécutée sur l'hôte 2.

Sur l'hôte 2, adressez la commande **ping6** à l'hôte 1.

Si vous utilisez le Moniteur réseau pour capturer le trafic, vous devez apercevoir l'échange des messages de requête et de réponse d'écho ICMPv6, avec un en-tête d'authentification (AH, *Authentication Header*) entre l'en-tête IPv6 et l'en-tête ICMPv6.