Groupe de travail Réseau
Request for Comments : 4552
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Gupta,Tropos Networks
N. Melam, Juniper Networks

juin 2006

Authentification/confidentialité pour OSPFv3

Résumé
Le présent document décrit les moyens et mécanismes pour fournir l'authentification/confidentialité de OSPFv3 en utilisant un en-tête d'extension à l'en-tête d'authentification/encapsulation de charge utile de sécurité (AH/ESP, *Authentication Header/Encapsulating Security Payload*) IPv6.

Table des matières

1. Introduction

OSPF (*Open Shortest Path First*, plus court chemin ouvert en premier) version 2 [RFC2328] définit les champs AuType et Authentication dans son en-tête de protocole pour fournir la sécurité. Dans OSPF pour IPv6 (OSPFv3) [RFC2740], les deux champs d'authentification ont été retirés des en-têtes OSPF. OSPFv3 s'appuie sur l'en-tête d'autentification (AH, *Authentication Header*) IPv6 et sur l'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IPv6 pour fournir l'intégrité, l'authentification, et/ou la confidentialité.

Le présent document décrit comment les en-têtes d'extension AH/ESP IPv6 peuvent être utilisés pour fournir l'authentification/confidentialité à OSPFv3.

On suppose le lecteur familiarisé avec OSPFv3 [RFC2740], AH [RFC4302], ESP [RFC4303], le concept d'associations de sécurité, les modes tunnel et transport de IPsec, et les options de gestion de clé disponibles pour AH et ESP (chiffrement manuel [RFC4301] et échange de clé Internet (IKE, *Internet Key Exchange*) [RFC4306]).

1.1 Conventions utilisées dans ce document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Mode Transport contre mode tunnel

L'association de sécurité (SA, *Security Association*) en mode transport est généralement utilisée entre deux hôtes ou routeurs/passerelles quand ils agissent comme hôtes. La SA doit être en mode tunnel si l'une et l'autre des extrémités de l'association de sécurité est un routeur/passerelle. Deux hôtes PEUVENT établir une SA en mode tunnel entre eux. Les paquets OSPFv3 sont échangés entre les routeurs. Cependant, comme les paquets sont livrés en local, les routeurs assument le rôle d'hôtes dans le contexte des SA en mode tunnel. Toutes les mises en œuvre qui se conforment à la présente spécification DOIVENT prendre en charge les SA en mode transport pour fournir la sécurité IPsec requise aux paquets OSPFv3. Elles PEUVENT aussi prendre en charge les SA en mode tunnel pour fournir la sécurité IPsec requise aux paquets OSPFv3.

3. Authentification

Les mises en œuvre qui se conforment à la présente spécification DOIVENT prendre en charge l'authentification pour OSPFv3.

Pour fournir l'authentification à OSPFv3, les mises en œuvre DOIVENT prendre en charge ESP et PEUVENT prendre en charge AH.

Si ESP en mode transport est utilisée, elle va seulement fournir l'authentification aux paquets de protocole OSPFv3 à l'exclusion de l'en-tête IPv6, des en-têtes d'extension, et des options.

Si AH en mode transport mode est utilisé, il va fournir l'authentification aux paquets de protocole OSPFv3, aux portions choisies de l'en-tête IPv6, aux portions choisies des en-têtes d'extension, et aux options choisies.

Quand l'authentification OSPFv3 est activée,
- o les paquets OSPFv3 qui ne sont pas protégés par AH ou ESP DOIVENT être éliminés en silence.
- o les paquets OSPFv3 qui échouent aux vérifications d'authentification DOIVENT être éliminés en silence.

4. Confidentialité

Les mises en œuvre qui se conforment à la présente spécification DEVRAIENT prendre en charge la confidentialité pour OSPFv3.

Si la confidentialité est fournie, ESP DOIT être utilisé.

Quand la confidentialité OSPFv3 est activée,
- o les paquets OSPFv3 qui ne sont pas protégés par ESP DOIVENT être éliminés en silence.
- o les paquets OSPFv3 qui échouent aux vérifications de confidentialité DOIVENT être éliminés en silence.

5. Distinction de OSPFv3 de OSPFv2

Le type de protocole IP/IPv6 est le même (89) pour OSPFv2 et OSPFv3, et OSPF les distingue sur la base du numéro de version de l'en-tête OSPF. Cependant, les normes actuelles pour IPsec ne permettent pas d'utiliser des champs d'en-tête spécifiques de protocole arbitraires comme sélecteurs. Donc, le champ Version OSPF dans l'en-tête OSPF ne peut pas être utilisé pour distinguer les paquets OSPFv3 des paquets OSPFv2. Comme OSPFv2 est seulement pour IPv4 et OSPFv3 seulement pour IPv6, le champ de version dans l'en-tête IP peut être utilisé pour distinguer les paquets OSPFv3 des paquets OSPFv2.

6. Exigences de IPsec

Afin de mettre en œuvre la présente spécification, les capacités IPsec suivantes sont requises.

Mode transport : IPsec en mode transport DOIT être pris en charge [RFC4301].

Plusieurs bases de données de politique de sécurité (SPD, *Security Policy Database*) : la mise en œuvre DOIT prendre en charge plusieurs SPD avec une fonction de sélection de SPD donnant la capacité de choisir une SPD spécifique sur la base de l'interface [RFC4301].

Sélecteurs : la mise en œuvre DOIT être capable d'utiliser l'adresse de source, l'adresse de destination, le protocole, et la direction comme sélecteurs dans la SPD.

Étiquetage de l'identifiant d'interface : la mise en œuvre DOIT être capable d'étiqueter les paquets entrants avec l'identifiant de l'interface (physique ou virtuelle) via laquelle ils sont arrivés [RFC4301].

Prise en charge de clé manuelle : les clés configurées manuellement DOIVENT être capables de sécuriser le trafic spécifié [RFC4301].

Algorithmes de chiffrement et d'authentification : la mise en œuvre NE DOIT PAS permettre à l'utilisateur de choisir des chiffrements de flux comme algorithme de chiffrement pour sécuriser les paquets OSPFv3 car les chiffrements de flux ne conviennent pas pour les clés manuelles. Sauf quand il y a conflit avec la déclaration ci-dessus, les mots clés "DOIT", "NE DOIT PAS", "EXIGÉ", "DEVRAIT", et "NE DEVRAIT PAS" qui apparaissent dans la [RFC4305] pour les algorithmes à prendre en charge sont à interpréter aussi pour OSPFv3 comme comme décrit dans la [RFC2119].

Configuration dynamique de règle IPsec : le module d'acheminement DEVRAIT être capable de configurer, modifier, et supprimer les règles IPsec à volonté. Ceci est nécessaire principalement pour sécuriser les liaisons virtuelles.

Encapsulation de paquet ESP : l'encapsulation IP des paquets ESP DOIT être prise en charge. Par souci de simplicité, l'encapsulation UDP de paquets ESP NE DEVRAIT PAS être utilisée.

SA différentes pour codets de service différencié (DSCP, *Differentiated Services Code Points*) différents : selon la [RFC4301], la mise en œuvre IPsec DOIT prendre en charge l'établissement et la maintenance de plusieurs SA avec les mêmes sélecteurs entre un envoyeur et un receveur donnés. Cela permet à la mise en œuvre d'associer différentes classes de trafic aux mêmes valeurs de sélecteur pour la prise en charge de la qualité de service (QS).

7. Gestion de clés

OSPFv3 échange des paquets aussi bien en diffusion groupée qu'en envoi individuel. Lorsque OSPFv3 fonctionne sur une interface de diffusion, l'authentification/confidentialité requise est "de un à plusieurs". Comme IKE se fonde sur le protocole d'accord de clé Diffie-Hellman et ne fonctionne que pour deux parties communicantes, il n'est pas possible d'utiliser IKE pour fournir l'authentification/confidentialité "de un à plusieurs" requise. La présente spécification rend obligatoire l'usage du chiffrement manuel avec les mises en œuvre IPsec actuelles. De futures spécifications pourront explorer l'usage de protocoles comme la négociation de clés Kerberos sur Internet (KINK, *Kerberized Internet Negotiation of Keys*) ou le protocole de gestion de clés d'association de groupe sécurisé (GSAKMP, *Group Secure Association Key Management Protocol*) quand ils seront largement disponibles. Dans le chiffrement manuel, les SA sont installées statiquement sur les routeurs et ces SA statiques sont utilisées pour authentifier/chiffrer les paquets.

La discussion qui suit explique qu'il n'est pas adaptable et pratiquement infaisable d'utiliser des associations de sécurité différentes pour le trafic entrant et sortant pour fournir la sécurité de "un à plusieurs" requise. Donc, les mises en œuvre DOIVENT utiliser des clés configurées manuellement avec les mêmes paramètres de SA (indice de paramètre de sécurité (SPI, *Security Parameter Index*) clés, etc.) pour les SA entrantes et sortantes (comme le montre la Figure 3).

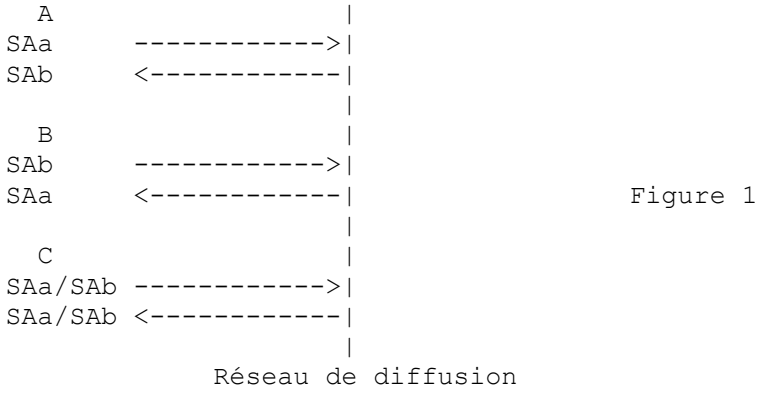

Figure 1

Si on considère la communication entre A et B dans la Figure 1, tout semble aller bien. A utilise des associations de sécurité SAa pour les paquets sortants et B utilise les mêmes pour les paquets entrants et vice versa. Si on inclut maintenant C dans le groupe et si C envoie un paquet en utilisant la SAa, seul A va alors être capable de le comprendre. De même, si C envoie un paquet en utilisant la SAb, seul B va alors être capable de le comprendre. Comme les paquets sont en diffusion groupée et qu'ils vont être traités par A et B, il n'y a pas de SA que C puisse utiliser pour que A et B puissent tous deux les comprendre.

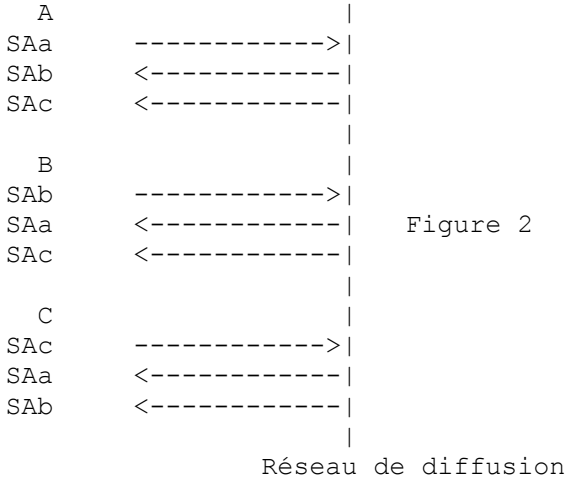

Figure 2

Le problème peut être résolu en configurant des SA pour tous les nœuds sur chaque autre nœud comme le montre la Figure 2. Ainsi A, B, et C vont utiliser respectivement les SAa, SAb, et SAc, pour le trafic sortant. Chaque nœud va chercher la SA à utiliser sur la base de la source (A va utiliser les SAb et SAc pour les paquets reçus de B et C, respectivement). Cette solution n'est pas adaptable et pratiquement infaisable à cause du grand nombre de SA dont la configuration serait nécessaire sur chaque nœud. Aussi, l'ajout d'un nœud dans le réseau de diffusion va exiger l'ajout d'une autre SA sur chaque autre nœud.

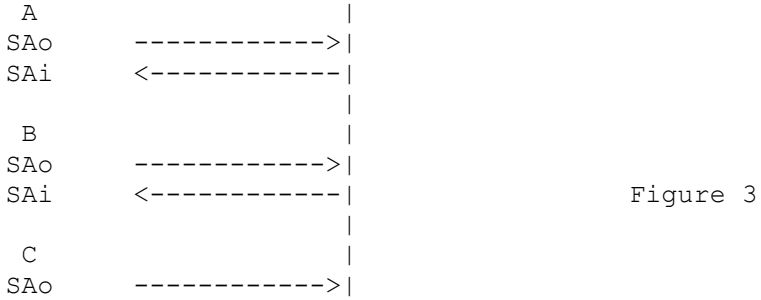

Figure 3

Le problème peut être résolu en utilisant les mêmes paramètres de SA (SPI, clés, etc.) pour les SA entrantes (SAi) et sortantes (SAo) comme montré à la Figure 3.

8. Granularité et sélecteurs de SA

L'utilisateur DEVRAIT avoir le choix de partager la même SA entre plusieurs interfaces ou d'utiliser une unique SA par interface.

OSPFv3 prend en charge le fonctionnement sur plusieurs instances sur une interface en utilisant le champ "Identifiant d'instance" contenu dans l'en-tête OSPFv3. Comme IPsec n'accepte pas que des champs arbitraires soient utilisés dans l'en-tête de protocole comme sélecteurs, il n'est pas possible d'utiliser des SA différentes pour les différentes instances OSPFv3 fonctionnant sur la même interface. Donc, toutes les instances OSPFv3 fonctionnant sur la même interface vont devoir utiliser la même SA. Dans la terminologie de la RFC OSPFv3, les SA sont par liaison et non par interface.

9. Liaisons virtuelles

Une SA différente de la SA de l'interface sous-jacente DOIT être fournie pour les liaisons virtuelles. Les paquets envoyés sur des liaisons virtuelles utilisent des adresses IPv6 en envoi individuel de liaison non locale comme adresses IPv6 de source, tandis que les paquets envoyés sur d'autres interfaces utilisent des adresses de liaison locale en diffusion groupée et en envoi individuel. Cette différence de l'adresse IPv6 de source différencie les paquets envoyés sur des liaisons virtuelles des autres types d'interface OSPFv3.

Comme les adresses IPv6 de point d'extrémité de liaison virtuelle ne sont pas connues, il n'est pas possible d'installer d'entrées de SPD / base de données d'association de sécurité (SAD, *Security Association Database*) au moment de la configuration. Les adresses IPv6 de point d'extrémité de liaison virtuelle sont apprises durant le processus de calcul du tableau d'acheminement. L'échange de paquets sur les liaisons virtuelles ne commence qu'après la découverte des adresses IPv6 de point d'extrémité. Afin de protéger ces échanges, le module d'acheminement doit installer les entrées de SPD/SAD correspondantes avant de commencer ces échanges. Noter que les paramètres de SA manuels sont préconfigurés mais non installés dans la SAD jusqu'à ce que les adresses de point d'extrémité soient connues.

Conformément à la RFC OSPFv3 [RFC2740], l'adresse IP du voisin virtuel est réglée au premier préfixe qui a le "bit LA" établi dans la liste des préfixes des annonces d'état de liaison (LSA, *Link State Advertisement*) de préfixes intra zone générée par le voisin virtuel. Mais quand on en vient à choisir l'adresse de source pour les paquets qui sont envoyés sur la liaison virtuelle, la [RFC2740] suggère simplement d'utiliser une des propres adresses IPv6 mondiales du routeur. Afin d'installer les règles de sécurité requises pour les liaisons virtuelles, l'adresse de source a aussi besoin d'être prévisible. Donc, les routeurs qui mettent en œuvre la présente spécification DOIVENT changer la façon dont les adresses de source et de destination sont choisies pour les paquets échangés sur des liaisons virtuelles quand IPsec est activé.

La première adresse IPv6 avec le "bit LA" établi dans la liste de préfixes annoncés dans les LSA de préfixe intra zone dans la zone de transit DOIT être utilisée comme adresse de source pour les paquets échangés sur la liaison virtuelle. Quand plusieurs LSA de préfixe intra zone sont générés, ils sont considérés comme enchaînés et sont ordonnés par identifiant d'état de liaison ascendant.

La première adresse IPv6 avec le "bit LA" établi dans la liste de préfixes reçue dans les LSA de préfixe intra zone du voisin virtuel dans la zone de transit DOIT être utilisée comme adresse de destination pour les paquets échangés sur la liaison virtuelle. Quand plusieurs LSA de préfixe intra zone sont reçus, ils sont considérés comme enchaînés et sont ordonnés par identifiant d'état de liaison ascendant.

Cela rend prévisibles les adresses de source et de destination des paquets échangés sur la liaison virtuelle quand IPsec est activé.

10. Changement de clés

Pour conserver la sécurité d'une liaison, les valeurs de clé d'authentification et de chiffrement DEVRAIENT être changées périodiquement.

10.1 Procédure de changement de clés

La procédure en trois étapes suivante DEVRAIT être suivie pour changer les clés des routeurs sur une liaison sans éliminer de paquets du protocole OSPFv3 ou interrompre l'adjacence.

(1) Pour chaque routeur sur la liaison, créer une SA entrante supplémentaire pour l'interface dont les clés sont changées en utilisant un nouveau SPI et la nouvelle clé.

(2) Pour chaque routeur sur la liaison, remplacer la SA sortante d'origine par une qui utilise les nouvelles valeurs de SPI et de clés. L'opération de remplacement de SA devrait être atomique par rapport à l'envoi de paquets OSPFv3 sur la liaison afin qu'aucun paquet OSPFv3 ne soit envoyé sans authentification/chiffrement.

(3) Pour chaque routeur sur la liaison, supprimer la SA entrante d'origine.

Noter que tous les routeurs sur la liaison doivent achever l'étape 1 avant qu'aucun ne commence l'étape 2. De même, tous les routeurs sur la liaison doivent achever l'étape 2 avant qu'aucun ne commence l'étape 3.

Une façon de contrôler la progression de l'étape une à la suivante est que chaque routeur ait une constante de temps configurable KeyRolloverInterval. Après que le routeur a commencé l'étape 1 sur une certaine liaison, il attend pendant cet intervalle de temps et ensuite passe à l'étape 2. De même, après être passé à l'étape 2, il attend pendant cet intervalle de temps et passe ensuite à l'étape 3.

Afin de réaliser une transition de clés en douceur, tous les routeurs sur une liaison devraient utiliser la même valeur de KeyRolloverInterval et devraient initier le processus de changement de clé dans cette période de temps.

À la fin de cette procédure, tous les routeurs sur la liaison vont avoir une seule SA entrante et sortante pour OSPFv3 avec les nouvelles valeurs de SPI et de clés.

10.2 KeyRolloverInterval

La valeur configurée de KeyRolloverInterval devrait être assez longue pour permettre à l'administrateur de changer les clés sur tous les routeurs OSPFv3. Comme cette valeur peut varier de façon significative selon la mise en œuvre et le déploiement, il appartient à l'administrateur de choisir la valeur appropriée.

10.3 Intervalle de changement de clés

Ce paragraphe analyse la sécurité fournie par le changement de clés manuel et recommande que les clés de chiffrement et d'authentification DEVRAIENT être changées au moins tous les 90 jours.

La plus faible sécurité fournie par les mécanismes de sécurité discutés dans la présente spécification est quand le chiffrement NUL (pour ESP) ou pas de chiffrement (pour AH) est utilisé avec l'authentification HMAC-MD5. Toutes les autres combinaisons d'algorithmes vont au moins être aussi dures à casser que celles mentionnées ci-dessus. Ceci est montré par les hypothèses raisonnables suivantes :

- Le chiffrement NUL et l'authentification HMAC-SHA-1 vont être plus sûres que HMAC-SHA-1 car il est considéré comme étant plus sûr que HMAC-MD5.

- La combinaison du chiffrement NON NUL et de l'authentification NULLE n'est pas applicable car cette spécification rend l'authentification obligatoire quand la sécurité OSPFv3 est activée.

- Le chiffrement de la sécurité de chiffrement des données (DES, *Data Encryption Security*) et l'authentification HMAC-MD5 va être plus sûr à cause de la sécurité supplémentaire fournie par DES.

o D'autres algorithmes de chiffrement comme 3DES et la norme de chiffrement évolué (AES, *Advanced Encryption Standard*) vont être plus sûrs que DES.

La [RFC3562] analyse les exigences de changement de clés pour l'option de signature TCP MD5. L'analyse fournie dans la RFC 3562 est aussi applicable à la présente spécification car elle est indépendante des schéma de données.

11. Barrière de protection IPsec et SPD

La barrière de protection IPsec DOIT être autour du protocole OSPF. Donc, tout le trafic OSPF entrant et sortant passe par le traitement IPsec.

La fonction de sélection de SPD DOIT retourner une SPD avec les règles suivantes pour toutes les interfaces qui ont l'authentification/confidentialité OSPFv3 désactivée.

N°.	source	destination	protocole	action
1	toutes	toutes	OSPF	outrepasser

La fonction de sélection de SPD DOIT retourner une SPD avec les règles suivantes pour toutes les interfaces qui ont l'authentification/confidentialité OSPFv3 activée.

N°.	source	destination	protocole	action
2	fe80::/10	toutes	OSPF	protéger
3	fe80::/10	toutes	ESP/OSPF ou AH/OSPF	protéger
4	src/128	dst/128	OSPF	protéger
5	src/128	dst/128	ESP/OSPF ou AH/OSPF	protéger

Pour les règles 2 et 4, l'action "protéger" signifie chiffrer/calculer la valeur de vérification d'intégrité (ICV, *Integrity Check Value*) et l'ajout d'un en-tête ESP ou AH. Pour les règles 3 et 5, l'action "protéger" signifie de déchiffrer/authentifier les paquets et supprimer les en-têtes ESP ou AH.

La règle 1 va outrepasser les paquets OSPFv3 sans aucun traitement IPsec sur les interfaces qui ont l'authentification/confidentialité OSPFv3 désactivée.

Les règles 2 et 4 vont éliminer les paquets OSPFv3 entrants qui n'ont pas été sécurisés avec les en-têtes ESP/AH.

ESP/OSPF ou AH/OSPF dans les règles 3 et 5 signifie qu'il y a un paquet OSPF sécurisé avec ESP ou AH.

Les règles 2 et 3 sont destinées à sécuriser les paquets OSPF en envoi individuel et en diffusion groupée qui ne sont pas échangés sur les liaisons virtuelles.

Les règles 4 et 5 sont destinées à sécuriser les paquets échangés sur les liaisons virtuelles. Ces règles sont installées après avoir appris les adresses IPv6 de point d'extrémité de la liaison virtuelle. Ces règles DOIVENT être installées dans la SPD pour les interfaces qui sont connectées à la zone de transit pour la liaison virtuelle. Ces règles PEUVENT autrement être installées sur toutes les interfaces. Si ces règles ne sont pas installées sur toutes les interfaces, des paquets OSPFv3 en clair ou malveillants avec les mêmes adresses de source et de destination que le point d'extrémité de la liaison virtuelle vont être livrées à OSPFv3. Bien que OSPFv3 élimine ces paquets car ils n'ont pas été reçus sur la bonne interface, OSPFv3 reçoit des paquets en clair ou malveillants même quand la sécurité est activée. Installer ces règles sur toutes les interfaces assure que OSPFv3 ne reçoit pas ces paquets en clair ou malveillants quand la sécurité est activée. Par ailleurs, installer ces règles sur toutes les interfaces augmente les frais généraux de traitement sur les interfaces alors qu'il n'y a pas d'autre traitement IPsec. La décision d'installer ou non ces règles sur toutes les interfaces ou sur juste les interfaces qui sont connectées à la zone de transit est une décision privée et n'affecte en aucune façon l'interopérabilité. Donc c'est un choix de mise en œuvre.

12. Entropie des clés manuelles

Les mises en œuvre DOIVENT permettre à l'administrateur de configurer les clés de chiffrement et d'authentification en format hexadécimal plutôt que de le restreindre à un sous ensemble de caractères ASCII (lettres, nombres, etc.). Un jeu de caractères restreint va réduire significativement l'entropie de clé comme exposé dans [OSPFsec].

13. Protection contre la répétition

Comme il n'est pas possible d'utiliser les normes actuelles pour fournir une protection complète contre la répétition tout en utilisant le chiffrement manuel, la solution proposée ne va pas fournir de protection contre les attaques en répétition.

Une analyse détaillée des diverses vulnérabilités des protocoles d'acheminement et d'OSPF en particulier est discutée dans la [RFC4593] et [OSPFsec]. La conclusion est que la répétition des paquets OSPF peut causer l'interruption des adjacences, ce qui peut conduire à une attaque de DoS sur le réseau. Elle peut aussi causer un fonctionnement en continu du processus d'échange de la base de données causant ainsi une surcharge de CPU ainsi que des micro boucles dans le réseau.

14. Considérations sur la sécurité

Le présent mémoire discute de l'utilisation des en-têtes IPsec AH et ESP pour assurer la sécurité de OSPFv3 pour IPv6. Donc, les questions de sécurité imprègnent tout le document.

L'analyse des faiblesses de la sécurité d'OSPF [OSPFsec] identifie les vulnérabilités d'OSPF dans deux scénarios – un sans authentification ou avec une authentification par un simple mot de passe, et l'autre avec une authentification cryptographique. La solution décrite dans la présente spécification fournit une protection contre toutes les vulnérabilités identifiées pour les scénarios avec authentification cryptographique avec les exceptions suivantes :

Limitations de clé manuelle :
Cette spécification rend obligatoire l'usage de clés manuelles. Les limitations connues à l'usage de clés manuelles sont les suivantes :

- Comme les numéros de séquence ne peuvent pas être négociés, la protection contre la répétition ne peut être fournie. Cela laisse OSPF non sûr contre les attaques qui peuvent être effectuées en répétant des paquets OSPF.
- Les clés manuelles sont généralement de longue durée (les changer souvent est une tâche fastidieuse). Cela donne à un attaquant assez de temps pour découvrir les clés.
- Comme l'administrateur configure manuellement les clés, il y a une chance que les clés configurées soient faibles (il y a au moins des clés faibles connues pour DES/3DES).

Attaques d'usurpation d'identité :
L'usage de la même clé sur tous les routeurs OSPF connectés à une liaison les met tous dans une position non sûre contre des attaques d'usurpation d'identité si un des routeurs OSPF est compromis, fonctionne mal, ou est mal configuré.

Une analyse détaillée des diverses vulnérabilités des protocoles d'acheminement est discutée dans la [RFC4593].

15. Références

15.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2328] J. Moy, "OSPF version 2", STD 54, avril 1998. *(MàJ par la* RFC6549, RFC8042)

[RFC2740] R. Coltun, D. Ferguson, J. Moy, "OSPF pour IPv6", décembre 1999. (*Obsolète, voir* RFC5340) *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4304] S. Kent, "Addendum du numéro de séquence étendu (ESN) au domaine d'interprétation IPsec (DOI) pour le protocole d'associations de sécurité et de gestion de clé Internet (ISAKMP)", décembre 2005. *(P.S.)*

[RFC4305] D. Eastlake 3rd, "Exigences de mise en œuvre d'algorithme cryptographique pour l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)", décembre 2005. *(P.S. ; Obsolète, voir* RFC4835)

15.2 Références pour information

[OSPFsec] Jones, E. et O. Moigne, "OSPF Security Vulnerabilities Analysis", Work in Progress.

[RFC3562] M. Leech, "Considérations sur la gestion de clés pour l'option de signature MD5 dans TCP", juillet 2003. *(Information)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4593] A. Barbir et autres, "Menaces génériques contre les protocoles d'acheminement", octobre 2006. *(Info.)*

Remerciements

Les auteurs tiennent à exprimer leurs sincères remerciements à Marc Solsona, Janne Peltonen, John Cruz, Dhaval Shah, Abhay Roy, Paul Wells, Vishwas Manral, et Sam Hartman qui ont fourni d'utiles informations et critiques sur ce mémoire. Des remerciements particuliers sont dus à Acee Lindem pour ses nombreuses corrections éditoriales.

Nous tenons aussi à remercier les membres des groupes de travail IPsec et OSPF qui ont fourni de précieux commentaires de relecture.

Adresse des auteurs

Mukesh Gupta
Tropos Networks
555 Del Rey Ave
Sunnyvale, CA 94085
téléphone : 408-331-6889
mél : mukesh.gupta@tropos.com

Nagavenkata Suresh Melam
Juniper Networks
1194 N. Mathilda Ave
Sunnyvale, CA 94089
téléphone : 408-505-4392
mél : nmelam@juniper.net

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administatif (IASA) de l'IETF.