Groupe de travail Réseau
Request for Comments : 5566
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

L. Berger, LabN
R. White, Cisco Systems
E. Rosen, Cisco Systems
juin 2009

Attribut BGP Encapsulation de tunnel IPsec

Résumé
L'identifiant de famille d'adresses suivante (SAFI, *Subsequent Address Family Identifier*) d'encapsulation BGP fournit une méthode d'échange dynamique des informations d'encapsulation et d'indication des types de protocole d'encapsulation à utiliser pour les différents prochains bonds. Actuellement, la prise en charge des types de tunnel d'encapsulation générique d'acheminement (GRE, *Generic Routing Encapsulation*) du protocole de tunnelage de couche 2 (L2TPv3, *Layer 2 Tunneling Protocol*) et de IP dans IP est définie. Le présent document définit la prise en charge des types de tunnel IPsec.

Table des matières

1. Introduction

L'identifiant de famille d'adresses suivante (SAFI, *Subsequent Addresse Family Identifier*) d'encapsulation BGP [RFC4271] permet la communication des informations de tunnel et l'association de ces informations à un prochain bond BGP. Le SAFI

d'encapsulation peut être utilisé pour prendre en charge la transposition de préfixes aux prochains bonds et tunnels de la même famille d'adresses, de préfixes IPv6 en prochains bonds IPv4 et tunnels en utilisant la [RFC4798], et des préfixes IPv4 en prochains bonds IPv6 et tunnels en utilisant la [RFC5549]. Le SAFI d'encapsulation peut aussi être utilisé pour prendre en charge la transposition de préfixes de VPN en tunnels quand les préfixes de VPN sont annoncés selon les [RFC4364] ou [RFC4659]. La [RFC5565] donne un utile contexte pour l'utilisation du SAFI d'encapsulation.

Le SAFI d'encapsulation est défini dans la [RFC5512]. La [RFC5512] définit aussi la prise en charge des types de tunnel GRE [RFC2784], L2TPv3 [RFC3931], et IP dans IP [RFC2003]. Le présent document s'appuie sur la [RFC5512] et définit la prise en charge des tunnels IPsec. La prise en charge est définie pour l'en-tête d'authentification IP (AH, *Authentication Header*) en mode tunnel [RFC4302] et pour l'encapsulation de charge utile de sécurité IP (ESP, *Encapsulating Security Payload*) en mode tunnel [RFC4303]. L'architecture IPsec est définie dans la [RFC4301]. La prise en charge de IP dans IP [RFC2003] et de MPLS dans IP [RFC4023] protégée par le mode transport IPsec est aussi définie.

Le format d'encapsulation des informations d'accessibilité de couche réseau (NLRI, *Network Layer Reachability Information*) n'est pas modifié par le présent document.

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. Types d'encapsulation de tunnel

Conformément à la [RFC5512], le type de tunnel est indiqué dans l'attribut Encapsulation de tunnel. Le présent document définit les valeurs de type de tunnel suivantes :

- Point d'extrémité d'émission de tunnel : type = 3
- IPsec en mode tunnel : type = 4 [RFC4302], [RFC4303]
- Tunnel avec mode de transport IPsec : type = 5 [RFC2003], [RFC4303]
- Tunnel MPLS dans IP avec mode de transport IPsec : type = 6 [RFC4023]

Note : voir au paragraphe 4.3 de la [RFC5512] une discussion sur l'annonce et l'utilisation de plusieurs types de tunnel.

Note : la spécification de la [RFC4023] pour les tunnels MPLS dans IP avec mode de transport IPsec s'applique aussi aux tunnels IP dans IP.

Le présent document ne spécifie pas l'utilisation des types de sous TLV définis dans la [RFC5512] avec ces types de tunnel. Voir ci-dessous la définition d'un sous TLV spécifique à utiliser avec les types de tunnel définis.

3. Utilisation des types de tunnel IPsec

Les types de tunnel IPsec sont définis ci-dessus avec les valeurs 4, 5, et 6. Si R1 est un locuteur BGP qui reçoit une mise à jour de SAFI d'encapsulation provenant d'un autre locuteur BGP, R2, alors si R1 a des paquets de données pour lesquels R2 est le prochain bond BGP, R1 DOIT initier une association de sécurité (SA, *Security Association*) IPsec du "type de tunnel" spécifié, et tous ces paquets de données DOIVENT être envoyés à travers cette SA.

Soit R1 et R2 deux locuteurs BGP qui peuvent envoyer des paquets de données à travers R3, de telle façon que les paquets de données de R1 et de R2 puissent être reçus par R3 sur la même interface. Dans ce cas, quand R3 envoie un SAFI d'encapsulation qui indique un type de tunnel IPsec à R2, alors R3 DEVRAIT aussi envoyer une mise à jour spécifiant un SAFI d'encapsulation avec un type de tunnel IPsec à R1. C'est-à-dire, sur une interface donnée, si IPsec est exigé pour un paquets de données, il DEVRAIT être exigé pour tous. Cela élimine la dépendance aux mécanismes de sélecteur IPsec pour distinguer correctement le trafic qui a besoin d'être protégé du trafic qui n'en a pas besoin.

La politique de sécurité a la granularité de locuteur BGP à locuteur BGP. Les politiques de sécurité requises doivent être configurées dans les locuteurs BGP. Les politiques pour chaque SA vont normalement être établies en utilisant IKEv2 (échange de clé Internet) [RFC4306], avec authentification par clé publique ou par clé pré-partagée. La SA PEUT aussi être configurée via des techniques manuelles. La spécification et les considérations de configuration manuelle sont définies dans les [RFC4301], [RFC4302], et [RFC4303] (et incluent des clés, des numéros d'indice de paramètre de sécurité (SPI, *Security Parameter Index*) le protocole IPsec, les algorithmes d'intégrité/chiffrement, et le mode de numéro de séquence).

4. Sous TLV Authentifiant de tunnel IPsec

Le présent document définit un nouveau sous TLV à utiliser avec l'attribut Encapsulation de tunnel défini dans la [RFC5512]. Le nouveau sous TLV est appelé "sous TLV Authentificateur de tunnel IPsec", et un ou plusieurs de ces sous TLV PEUVENT être inclus dans toutes NLRI de SAFI d'encapsulation [RFC5512] indiquant un type de tunnel défini dans le présent document. La prise en charge du sous TLV Authentificateur de tunnel IPsec DOIT être mise en œuvre chaque fois que les types de tunnel définis dans le présent document sont mis en œuvre. Cependant, cette utilisation est FACULTATIVE, et est une affaire de politique.

Le type de sous TLV du sous TLV Authentificateur de tunnel IPsec est 3. La longueur du sous TLV est variable. La structure du sous TLV est comme suit :

- Type d'authentificateur : deux octets : Le présent document définit le type d'authentificateur 1, "Hachage SHA-1 de clé publique", comme défini au paragraphe 3.7 de la RFC 4306.
- Valeur (variable) : valeur utilisée pour authentifier le locuteur BGP qui a généré ces NLRI. La longueur de ce champ n'est pas codée explicitement, mais peut être calculée comme (Longueur de sous TLV - 2).

Dans le cas de l'authentificateur de type 1, ce champ contient les 20 octets de la valeur du hachage.

Un locuteur BGP qui envoie le sous TLV Authentificateur de tunnel IPsec avec le type d'authentificateur 1 DOIT être configuré avec une paire de clés privée/publique, la clé publique étant la clé dont le hachage est envoyé dans le champ Valeur du sous TLV. Le locuteur BGP DOIT soit (a) être capable de générer un certificat auto signé pour la clé publique, soit autrement (b) être configuré avec un certificat pour la clé publique.

Quand le sous TLV Authentificateur de tunnel IPsec est utilisé, il est fortement RECOMMANDÉ que l'intégrité de la session BGP elle-même soit protégée. Ceci est généralement fait en utilisant l'option TCP MD5 [RFC2385].

4.1 Utilisation du sous TLV Authentifiant de tunnel IPsec

Si un sous TLV Authentificateur de tunnel IPsec avec le type d'authentificateur 1 est présent dans la mise à jour de SAFI d'encapsulation, alors R1 (comme défini à la Section 3) DOIT utiliser IKEv2 [RFC4306] pour obtenir un certificat de R2 (comme défini à la Section 3) et R2 DOIT envoyer un certificat pour la clé publique dont le hachage s'est produit dans le champ Valeur du sous TLV Authentificateur de tunnel IPsec. R1 NE DOIT PAS tenter d'établir une SA avec R2 SAUF si le hachage de la clé publique dans le certificat a la même valeur qui se produit dans un des sous TLV Authentificateur de tunnel IPsec.

R2 DOIT aussi effectuer le traitement réciproque. Précisément, quand il établit une SA à partir de R1 et que R1 a annoncé les sous TLV Authentificateur de tunnel IPsec avec le type d'authentificateur 1, R2 DOIT utiliser IKEv2 [RFC4306] pour obtenir un certificat de R1, et R1 DOIT envoyer un certificat pour la clé publique dont le hachage s'est produit dans le champ Valeur du sous TLV Authentificateur de tunnel IPsec. R2 NE DOIT PAS tenter d'établir une SA avec R1 SAUF si le hachage de la clé publique dans le certificat a la même valeur qui se produit dans un des sous TLV Authentificateur de tunnel IPsec.

Noter que le type de tunnel "point d'extrémité d'émission du tunnel" (valeur = 3) peut être utilisé par un locuteur BGP qui ne veut pas être le point d'extrémité receveur d'un tunnel IPsec mais seulement le point d'extrémité émetteur.

5. Considérations sur la sécurité

Le présent document utilise les technologies de tunnel fondées sur IP pour prendre en charge le transport de plan des données. Par conséquent, les considérations sur la sécurité de ces technologies de tunnel s'appliquent. Le présent document définit la prise en charge de IPsec AH [RFC4302] et ESP [RFC4303]. Les considérations sur la sécurité de ces documents

ainsi que de la [RFC4301] s'appliquent aux aspects de plan des données du présent document.

Comme avec la [RFC5512], toute modification des informations utilisées pour former les en-têtes d'encapsulation, pour choisir un type de tunnel, ou pour choisir un tunnel particulier pour un type particulier de charge utile peut conduire à une mauvaise direction, une mauvaise livraison et/ou l'élimination des paquets de données d'utilisateur. La mauvaise livraison est moins un problème quand IPsec est utilisé, car une telle mauvaise livraison va probablement résulter en un échec d'authentification ou de déchiffrement chez le receveur. De plus, dans les environnements où l'authentification des locuteurs BGP est désirée, le sous TLV Authentificateur de tunnel IPsec défini dans la Section 4 peut être utilisé.

Plus largement, les considérations sur la sécurité pour le transport des informations d'accessibilité IP en utilisant BGP sont discutées dans les [RFC4271] et [RFC4272], et sont également applicables pour les extensions décrites dans le présent document.

Si l'intégrité de la session BGP n'est pas elle-même protégée, alors un imposteur pourrait monter une attaque de déni de service en établissant de nombreuses sessions BGP et en forçant la création de SA IPsec pour chacune. Cependant, comme un tel imposteur pourrait mettre à mal le système d'acheminement entier, cette sorte d'attaque particulière n'est probablement pas d'une importance particulière.

On devrait noter qu'une session BGP peut elle-même être transportée sur un tunnel IPsec. De tels tunnels IPsec peuvent fournir plus de sécurité à une session BGP. La gestion de ces tunnels IPsec sort du domaine d'application du présent document.

6. Considérations relatives à l'IANA

L'IANA administre l'allocation de nouveaux espaces de noms et de nouvelles valeurs pour les espaces de noms définis dans le présent document et revues dans cette section.

L'IANA a fait les allocations suivantes dans le registre "Types de tunnel d'attribut d'encapsulation de tunnel BGP".

Valeur	Nom	Référence
3	Point d'extrémité d'émission de tunnel	[RFC5566]
4	IPsec en mode tunnel	[RFC5566]
5	Tunnel IP dans IP avec IPsec en mode transport	[RFC5566]
6	Tunnel MPLS dans IP avec IPsec en mode transport	[RFC5566]

L'IANA a fait les allocations suivantes dans le registre "Sous TLV d'attribut d'encapsulation de tunnel BGP".

Valeur	Nom	Référence
3	Authentificateur de tunnel IPsec	[RFC5566]

7. Références

7.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212, RFC9072)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, 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.)*

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

[RFC5512] P. Mohapatra, E. Rosen, "Identifiant de famille d'adresse suivante (SAFI) d'encapsulation BGP et attribut d'encapsulation de tunnel de BGP", avril 2009. *(P. S.)*

7.2 Références pour information

[RFC2003] C. Perkins, "Encapsulation de IP dans IP", octobre 1996. (*MàJ par* RFC 3168, RFC 6864, Errata) *(P.S.)*

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S. ; MàJ par la* RFC6691) *; remplacée par* RFC5925)

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", DOI 10.17487/RFC2784, mars 2000.

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", DOI 10.17487/RFC3931, mars 2005. *(P.S.)*

[RFC4023] T. Worster et autres, "Encapsulation de MPLS dans IP ou encapsulation d'acheminement générique (GRE)", mars 2005. (*MàJ par* RFC5332) *(P.S.)*

[RFC4272] S. Murphy, "Analyse des faiblesses de la sécurité de BGP", janvier 2006. *(Information)*

[RFC4364] E. Rosen et Y. Rekhter, "Réseaux privés virtuels IP BGP/MPLS", février 2006. (*P.S., MàJ par* RFC4577, RFC4684)

[RFC4659] J. De Clercq et autres, "Extension de réseau privé virtuel (VPN) IP BGP-MPLS pour VPN IPv6", septembre 2006. *(P.S.)*

[RFC4798] J. De Clercq et autres, "Connexion d'îlots IPv6 sur MPLS IPv4 avec des routeurs de bordure IPv6 de fournisseur (6PE)", février 2007. *(P.S.)*

[RFC5549] F. Le Faucheur, E. Rosen, "Annonce des informations d'accessibilité de couche réseau IPv4 avec un prochain bond IPv6", mai 2009. *(P. S. ; remplacée par* RFC8950*)*

[RFC5565] J. Wu, Y. Cui, C. Metz, E. Rosen, "Cadre de maillage de passage logiciel", juin 2009. *(P. S.)*

8. Remerciements

Les auteurs souhaitent remercier Sam Hartman et Tero Kivinen de leur aide sur les questions relatives à la sécurité.

Adresse des auteurs

Lou Berger
LabN Consulting, L.L.C.
mél : lberger@labn.net

Russ White
Cisco Systems
mél : riw@cisco.com

Eric C. Rosen
Cisco Systems, Inc.
mél : erosen@cisco.com