Groupe de travail Réseau
Request for Comments : 5386
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

N. Williams, Sun
M. Richardson, SSW

novembre 2008

Sécurité mieux que rien : un mode d'IPsec non authentifié

Résumé
Le présent document spécifie comment utiliser les protocoles d'échange de clé de l'Internet (IKE, *Internet Key Exchange*) comme IKEv1 et IKEv2, pour établir des associations de sécurité (SA, *Security Association*) "non authentifiées" à utiliser avec la charge utile d'encapsulation de sécurité (ESP, *Encapsulating Security Payload*) IPsec et l'en-tête d'authentification (AH, *Authentication Header*) IPsec. Aucun changement des bits du réseau de IKEv2 n'est nécessaire, mais des extensions de la base de données d'autorisation d'homologue (PAD, *Peer Authorization Database*) et de la base de données de politique de sécurité (SPD, *Security Policy Database*) sont spécifiées. IPsec non authentifié est appelé ici par son acronyme populaire, "BTNS" (Better-Than-Nothing Security, *sécurité mieux que rien*).

Table des matières

1. Introduction

On décrit ici comment établir des SA IPsec non authentifiées en utilisant IKEv2 [RFC4306] et des clés publiques non authentifiées. Aucun nouvel élément de protocole de réseau n'est ajouté à IKEv2.

On suppose le modèle de traitement de la [RFC4301].

Le présent document ne définit pas un mode de BSTN opportuniste de IPsec par lequel les nœuds pourraient revenir à IP non protégé quand leurs homologues ne prennent pas en charge IKEv2, ni ne décrit les modes "acte de foi" ou "verrouillage de connexion".

Voir dans la [RFC5387] l'applicabilité et les utilisations de BTNS et la définition de ces termes.

Le présent document décrit BTNS dans les termes des concepts de IKEv2 et de la [RFC4301]. Il n'y a pas de raison que les mêmes méthodes ne puissent pas être utilisées avec IKEv1 [RFC2408], [RFC2409], et [RFC2401] ; cependant, ces spécifications n'incluent pas de concept de PAD, et donc il se peut qu'il ne soit pas possible de mettre en œuvre BTNS sur toutes les mises en œuvre conformes à la RFC2401.

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. BTNS

Le modèle de traitement de IPsec est modifié ici comme suit :

- Un nouveau type d'identifiant est ajouté : "PUBLICKEY". Les identifiants de ce type ont des clé publiques comme valeurs. Ce type d'identifiant n'est pas utilisé sur le réseau.

- Les entrées de PAD qui correspondent à des identifiants PUBLICKEY sont appelés des "entrées de PAD BTNS". Toutes les autres entrées de PAD sont appelées des "entrées de PAD non BTNS".

- Les entrées de PAD BTNS peuvent correspondre à des identifiants PUBLICKEY d'homologue spécifiques (ou empreintes digitale de clé publique) ou à toutes les clés publiques d'homologue. Ces dernières sont appelées des "entrées de PAD BTNS à caractère générique".

- Les entrées de PAD BTNS DOIVENT suivre logiquement (voir ci-dessous) toutes les autres entrées de PAD (la PAD étant une liste ordonnée).

- Une entrée de PAD BTNS à caractère générique peut apparaître dans la PAD, et, si une est présente, DOIT être la dernière entrée dans la PAD (voir ci-dessous).

- Tout homologue qui utilise une méthode IKEv2 AUTH impliquant une signature numérique (faite avec une clé privée à un système de chiffrement à clé publique) peut correspondre à une entrée de PAD BTNS, pourvu qu'elle ne corresponde à aucune entrée de PAD non BTNS. Les méthodes AUTH convenables en août 2007 sont la signature numérique RSA (méthode n° 1) et la signature numérique DSS (méthode n° 3) ; voir le paragraphe 3.8 de la [RFC4306].

- Une mise en œuvre de IPsec capable de BTNS va d'abord chercher dans la PAD des entrées non BTNS correspondant à un identifiant d'homologue. Si aucune entrée de PAD non BTNS correspondante n'est trouvée, alors l'identifiant de l'homologue DOIT être forcé d'être du type "PUBLICKEY" avec la clé publique de l'homologue comme valeur. La recherche dans la PAD est alors refaite pour trouver des entrées de PAD BTNS correspondantes. Cela assure que les entrées de PAD BTNS suivent logiquement les entrées de PAD non BTNS. Une seule recherche de PAD qui préserve cette sémantique est permise.

- Un homologue qui correspond à une entrée de PAD BTNS est appelé un "homologue BTNS". Un tel homologue est "authentifié" en vérifiant la signature dans sa charge utile IKEv2 AUTH avec la clé publique provenant de la charge utile CERT de l'homologue.

- Bien sûr, si aucune entrée de PAD correspondante n'est trouvée, alors la SA IKE est rejetée comme il est normal.

- Un nouveau fanion pour les entrées de SPD : "BTNS_OK". Le trafic de/vers les homologues qui correspondent à l'entrée de PAD BTNS vont correspondre seulement aux entrées de SPD qui ont le fanion BTNS_OK établi. Le SPD

peut être cherché par adresse ou par identifiant (de type PUBLICKEY pour les homologues BTNS) conformément au modèle de traitement IPsec de la [RFC4301]. La recherche par identifiant dans ce cas exige la création d'entrées de SPD qui sont liées aux valeurs de clé publique. Cela pourrait être utilisé pour construire un comportement "d'acte de foi" [RFC5387] (voir le paragraphe 4.2) par exemple.

Les nœuds DOIVENT rejeter les propositions de SA IKE provenant d'homologues qui correspondent à des entrées de PAD non BTNS mais échouent à s'authentifier correctement.

Les nœuds qui souhaitent être traités comme des nœuds BTNS par leurs homologues DOIVENT inclure des charges utiles CERT de clé publique nues. Actuellement seules des charges utiles CERT de clé publique RSA nues sont définies, ce qui signifie que BTNS fonctionne seulement avec des clés publiques RSA pour l'instant (voir "Clé RSA brute" au paragraphe 3.6 de la [RFC4306]). Les nœuds PEUVENT aussi inclure tout nombre de certificats qui lient la même clé publique. Ces certificats n'ont pas besoin d'être pré-partagés avec leurs homologues (par exemple, parce qu'éphémères, auto-signés). Les clés RSA à utiliser dans BTNS peuvent être générées à tout moment, mais le verrouillage de connexion [RFC5660] exige qu'elles restent constantes entre les échanges IKEv2 qui sont utilisés pour établir les SA pour les connexions verrouillées.

Pour préserver la signification standard du contrôle d'accès IPsec :
- o les entrées de PAD BTNS DOIVENT suivre logiquemet toutes les entrées de PAD non BTNS,
- o l'entrée de PAD BTNS à caractère générique DOIT être la dernière entrée logique de la PAD, et
- o l'entrée de PAD BTNS à caractère générique DOIT avoir des contraintes d'identifiant qui ne se chevauchent pas logiquement avec celles des autres entrées de la PAD.

Comme décrit ci-dessus, les exigences d'ordre logique de la PAD peuvent facilement être mises en œuvre par une double recherche dans la PAD au moment de l'authentification de l'homologue : une fois en utilisant l'identifiant affirmé par l'homologue, et si cela échoue, une fois en utilisant la clé publique de l'homologue comme un identifiant PUBLICKEY. Une mise en œuvre à une seule passe qui satisfait cette exigence est permise.

La contrainte de non chevauchement de l'identifiant d'entrée de BTNS peut facilement être mise en œuvre en cherchant deux fois dans la PAD : une fois quand les homologues BTNS s'authentifient, et encore une fois quand les homologues BTNS négocient les SA filles. Dans la première passe, on recherche dans la PAD une entrée de PAD correspondante comme décrit ci-dessus. Dans la seconde, on cherche pour s'assurer que les sélecteurs de trafic de la SA fille affirmés des homologues BTNS ne sont pas en conflit avec des entrées de PAD non BTNS. Des mises en œuvre à une seule passe qui préservent cette sémantique sont faisables.

3. Scénarios d'usage

Afin d'expliquer les règles ci-dessus, un certain nombre de scénarios vont être examinés. Le but ici est de persuader le lecteur que ces règles sont à la fois suffisantes et nécessaires.

Cette section est seulement pour information.

Pour expliquer les scénarios, un diagramme de référence décrivant un exemple de réseau est utilisé. C'est le suivant :

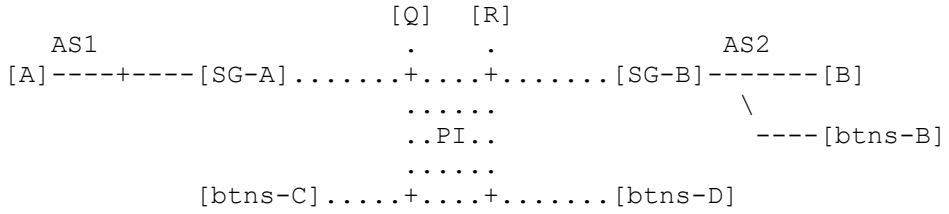

Figure 1 : Diagramme de réseau de référence

Dans ce diagramme, il y a huit systèmes. Six systèmes sont des nœuds d'extrémité (A, B, C, D, Q, et R). Deux sont des passerelles de sécurité (SG-A, SG-B) protégeant les réseaux sur lesquels résident [A] et [B]. Le nœud [Q] est à capacité IPsec et BTNS. Le nœud [R] est un nœud simple, sans capacité IPsec ni BTNS. Les nœuds[C] et [D] sont à capacité BTNS.

Les nœuds [C] et [Q] ont des adresses fixes. Le nœud [D] a une adresse non fixe.

On va examiner comment ces divers nœuds communiquent avec le nœud [SG-A] et/ou comment [SG-A] rejette les communications avec certains de ces nœuds. Dans le premier exemple, on examine le point de vue de [SG-A]. Dans le second exemple, on examine le point de vue de [Q]. Dans le troisième exemple, on regarde le point de vue de [C].

PI est l'Internet public ("la jungle").

3.1 Exemple n° 1 : passerelle de sécurité

La machine sur laquelle on va se concentrer dans cet exemple est [SG-A], un appareil de pare-feu d'une espèce quelconque qu'on souhaite configurer pour répondre aux connexions en BTNS provenant de [C].

[SG-A] a les entrées de PAD et de SPD suivantes :

Règle	ID distant	SA fille, ID permis	Recherche de SPD par
1	<ID de B>	<réseau de B>	IP
2	<ID de Q>	<hôte de Q>	IP
3	PUBLICKEY:any	ANY	IP

La dernière entrée est l'entrée de BTNS.

Figure 2 : Tableau de PAD de [SG-A]

Noter que l'entrée de PAD de [SG-A] a une et une seule entrée de PAD à caractère générique : l'entrée de PAD fourre-tout de BTNS à la dernière entrée, comme décrit à la Section 2.

<Identifiants de SA filles permis> et <recherche de SPD par> sont tirés de la [RFC4301], paragraphe 4.4.3.

Règle	Adr. locale	Adr. distante	Protocole de couche suivante	BTNS	Action acceptées
1	[A]	[R]	ANY	N/A	BYPASS
2	[A]	[Q]	ANY	non	PROTECT(ESP, tunnel, AES, SHA256)
3	[A]	réseau B	ANY	non	PROTECT(ESP, tunnel, AES, SHA256)
4	[A]	ANY	ANY	oui	PROTECT(ESP ,transport, integr+conf)

Figure 3 : Tableau de SPD de [SG-A]

Le traitement par [SG-A] des tentatives d'établissement de SA par les divers homologues est le suivant :

- [Q] ne correspond pas à l'entrée de PAD n° 1 mais correspond à l'entrée de PAD n° 2. Le traitement de la PAD s'arrête, puis la recherche est faite dans la SPD par l'identifiant de [Q] pour trouver l'entrée n° 2. Les SA filles ont alors la permission d'avoir les adresses de [SG-A] et de [Q] comme adresses de point d'extrémité.

- [SG-B] correspond à l'entrée de PAD n° 1. Le traitement de la PAD s'arrête, puis la recherche est faite dans la SPD par l'identifiant de [SG-B] pour trouver l'entrée n° 3 de la SPD. Les SA filles ont alors la permission d'avoir les adresses de [SG-A] et toute adresse provenant du réseau de B comme adresse de point d'extrémité.

- [R] n'initie aucune SA IKE ; son trafic pour [A] est outrepassé par l'entrée de SPD n° 1.

- [C] ne correspond pas aux entrées de PAD n° 1 ou 2 mais correspond à l'entrée de PAD n° 3, l'entrée de PAD de BTNS à caractère générique. La recherche dans la SPD est faite par l'adresse de [C], l'entrée de SPD n° 4 correspond. Les SA filles ont alors la permission d'avoir l'adresse de [SG-A] et l'adresse de [C] comme adresses de point d'extrémité, pourvu que l'adresse de [C] ne soit ni celle de [Q] ni aucune de [B] (voir la Section 2). Voir le dernier alinéa ci-dessous.

- Un nœud BTNS félon qui tente d'affirmer les adresses de [Q] ou de [B] va correspondre aux entrées de PAD pour [Q] ou [B] et échouer à s'authentifier comme [Q] ou [B], et dans ce cas sera rejeté, ou il va correspondre à l'entrée de PAD n° 3 mais il ne lui sera pas permis de créer des SA filles avec les adresses de [Q] ou [B] comme sélecteurs de trafic.

- Un nœud BTNS félon qui tente d'établir une SA par laquelle il affirme l'adresse de [C] va réussir à établir une telle SA. La protection de [C] exige des liens supplémentaires de l'identifiant BTNS spécifique de [C] (c'est-à-dire, sa clé publique) pour que son trafic s'écoule à travers la connexion verrouillée et le lien de canal ou à travers un acte de foi,

dont aucun n'est décrit ici.

3.2 Exemple n° 2 : système d'extrémité mixte

[Q] est un serveur NFSv4.

[Q] est une mise en œuvre IPsec native, et sa mise en œuvre de NFSv4 est à capacité IPsec.

[Q] veut protéger tout le trafic avec [A]. [Q] veut aussi protéger le trafic NFSv4 avec tous les homologues. Sa PAD et sa SPD sont configurées comme suit :

Règle	ID distant	SA fille, ID permis	Recherche de SPD par
1	<Identifiant de [A]>	<adresse de [A]>	IP
2	PUBLICKEY:any	ANY	IP

La dernière entrée est l'entrée de BTNS.

Figure 4 : Tableau de PAD de [Q]

Règle	Adr. locale	Adr. distante	Protocole de couche suivante	BTNS	Action acceptées
1	[Q]	[A]	ANY	non	PROTECT(ESP, tunnel, AES, SHA256)
2	[Q] accès 2049	ANY	ANY	oui	PROTECT(ESP, transport, integr+conf)

Figure 5 : Tableau de SPD de [Q]

La même analyse que montrée au paragraphe 3.1 s'applique ici à l'égard de [SG-A], [C], et des homologues félons. La seconde entrée de SPD permet à tout nœud à capacité BTNS de négocier une SA spécifique de l'accès à l'accès 2049, l'accès sur lequel fonctionne NFSv4. De plus, [SG-B] est traité comme un homologue BTNS car il n'est pas connu de [Q], et donc tout hôte derrière [SG-B] peut accéder au service NFSv4 sur [Q]. Comme [Q] n'a pas de relation formelle avec [SG-B], les nœuds félons peuvent se faire passer pour [B] (c'est-à-dire, affirmer les adresses de [B]).

3.3 Exemple n° 3 : Système BTNS seul

[C] prend seulement en charge BTNS et veut utiliser BTNS pour protéger le trafic NFSv4. Sa PAD et sa SPD sont configurées comme suit :

Règle	ID distant	SA fille, ID permis	Recherche de SPD par
1	PUBLICKEY:any	ANY	IP

La dernière (et seule) entrée est l'entrée de BTNS.

Figure 6 : Tableau de PAD de [Q]

Règle	Adr. locale	Adr. distante	Protocole de couche suivante	BTNS	Action acceptées
1	[C]	ANY avec accès 2049	ANY	oui	PROTECT(ESP, transport, integr+conf)
2	[C]	ANY	ANY	N/A	BYPASS

Figure 7 : Tableau de SPD de [SG-A]

L'analyse du paragraphe 3.1 s'applique comme suit :

- La communication avec [Q] sur l'accès 2049 correspond à l'entrée de SPD numéro 1. Cela est cause que [C] initie un échange IKEv2 avec [Q]. L'entrée de PAD sur [C] fait qu'il ne se soucie pas de l'identité qu'affirme [Q]. Plus d'authentification (et de lien de canal) pourrait se produire au sein du protocole NFSv4.
- La communication avec [A], [B], ou toute autre machine Internet (y compris [Q]) se fait en clair, tant que ce n'est pas sur l'accès 2049.
- Toute l'analyse sur les nœuds BTNS félons s'applique, mais ils peuvent seulement affirmer des SA pour l'accès 2049.

3.4 Commentaires divers

Si [SG-A] n'avait pas la capacité BTNS, il n'aurait alors pas les entrées de PAD et de SPD respectivement n° 3 et 4, dans l'exemple n° 1. Ensuite [C] serait rejeté comme normal dans le modèle IPsec standard [RFC4301].

De façon similaire, si [Q] n'avait pas la capacité BTNS, il n'aurait alors pas les entrées de PAD et de SPD n° 2 dans l'exemple n° 2. Alors [C] serait rejeté comme normal dans le modèle IPsec standard [RFC4301].

4. Considérations sur la sécurité

La négociation d'associations de sécurité non authentifiées est sujette à des attaques par interposition (MITM, *man-in-the-middle*) et devrait être utililée avec précaution. Lorsque il n'y a pas d'infrastructure de sécurité, cela peut bien sûr être mieux que rien.

L'utilisation avec des applications qui lient l'authentification à des couches de réseau supérieures pour sécuriser les canaux aux couches inférieures peut fournir un moyen sûr d'utiliser IPsec non authentifié, mais cela n'est pas spécifié ici.

L'entrée de PAD BTNS doit être la dernière et les contraintes d'identifiant de SA fille doivent être sans chevauchement avec toute autre entrée de PAD, comme décrit à la Section 2. Cela va assurer qu'aucun homologue BTNS ne peut se faire passer pour un autre homologue IPsec non BTNS.

4.1 Verrouillage de connexion et lien de canal

BTNS est sujet aux attaques MITM. Une façon de s'en protéger suite aux communications initiales est d'utiliser le "verrouillage de connexion" [RFC5660]. Dans le verrouillage de connexion, des protocoles de couche supérieure (ULP, *Upper Layer Protocol*) coopèrent avec IPsec pour lier des flux de paquets discrets à des séquences de SA similaires. Le verrouillage de connexion exige une mise en œuvre native de IPsec.

Les attaques MITM peuvent être détectées en utilisant des cadres et/ou mécanismes d'authentification de couche application, tels que GSS-API [RFC2743], avec lien de canal [RFC5056]. Les "canaux" IPsec ne sont rien d'autre que des connexions verrouillées.

4.2 Acte de foi pour BTNS

Acte de foi (LoF, *Leap of Faith*) est le terme généralement utilisé quand un utilisateur accepte l'assertion qu'une certaine clé identifie un homologue sur la première communication (en dépit d'un manque de preuve forte de cette assertion) et ensuite se souvient de cette association pour de futures communications. Spécifiquement c'est un mode de fonctionnement courant pour les clients de Secure Shell [RFC4251]. Quand un serveur est rencontré pour la première fois, le client Secure Shell peut demander à l'utilisateur si il accepte la clé publique du serveur. Si il l'accepte, le client enregistre le nom du serveur (tel que donné par l'utilisateur) et la clé publique dans une base de données.

L'acte de foi peut fonctionner de façon similaire pour les nœuds BTNS, mais il est actuellement encore en cours de conception et de spécification par le groupe de travail BTNS de l'IETF.

5. Remerciements

Merci à notre relecteur, Stephen Kent.

6. Références

6.1 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)

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

6.2 Références pour information

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Protocole Internet d'association de sécurité et gestion de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2409] D. Harkins et D. Carrel, "L'échange de clés Internet (IKE)", novembre 1998. *(Obsolète, voir la* RFC4306)

[RFC2743] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2, mise à jour 1", janvier 2000. (*MàJ par* RFC5554)

[RFC4251] T. Ylonen et C. Lonvick, "Architecture du protocole Secure Shell (SSH)", janvier 2006. *(P.S. ; MàJ par* RFC8308)

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC7296)

[RFC5056] N. Williams, "Sur l'utilisation des liaisons de canaux pour sécuriser les canaux", novembre 2007. *(P.S.)*

[RFC5387] J. Touch et autres, "Problème et déclaration d'applicabilité pour la sécurité mieux que rien (BTNS)", novembre 2008. *(Info.)*

[RFC5660] N. Williams, "Canaux IPsec : verrouillage de connexion**",** octobre 2009. *(P.S.)*

Adresse des auteurs

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US
mél : Nicolas.Williams@sun.com

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA
mél : mcr@sandelman.ottawa.on.ca
URI : http://www.sandelman.ottawa.on.ca/