Groupe de travail Réseau
Request for Comments : 3193
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

B. Patel, Intel
B. Aboba, W. Dixon, Microsoft
G. Zorn, S. Booth, Cisco Systems
novembre 2001

Sécuriser L2TP avec IPsec

Résumé
Le présent document expose comment L2TP (Protocole de tunnelage de couche 2) peut utiliser IPsec pour fournir l'authentification de tunnel, la protection de la confidentialité, la vérification de l'intégrité et la protection contre la répétition. Les deux cas du tunnelage volontaire et obligatoire sont exposés.

Table des matières

1. Introduction

L2TP [RFC2661] est un protocole qui tunnelle le trafic PPP sur divers réseaux (par exemple, IP, SONET, ATM). Comme le protocole encapsule PPP, L2TP hérite de l'authentification PPP, ainsi que du protocole de contrôle de chiffrement (ECP, *Encryption Control Protocol*) de PPP (décrit dans la [RFC1968]) et du protocole de contrôle de compression (CCP, *Compression Control Protocol*) (décrit dans la [RFC1962]). L2TP inclut aussi la prise en charge de l'authentification de tunnel, qui peut être utilisée pour authentifier mutuellement les points d'extrémité du tunnel. Cependant, L2TP ne définit pas de mécanisme de protection de tunnel.

IPsec est une suite de protocoles qui est utilisée pour sécuriser la communication entre deux homologues à la couche réseau.

Ce protocole se compose du document sur l'architecture de la sécurité d'IP [RFC2401], IKE, décrit dans la [RFC2409], IPsec AH, décrit dans la [RFC2402] et IPsec ESP, décrit dans la [RFC2406]. IKE est le protocole de gestion de clé tandis que AH et ESP sont utilisés pour protéger le trafic IP.

Le présent document propose l'utilisation de la suite de protocoles IPsec pour protéger le trafic L2TP sur les réseaux IP, et expose comment IPsec et L2TP devraient être utilisés ensemble. Le présent document ne tente pas de normaliser la sécurité de bout en bout. Lorsque la sécurité de bout en bout est exigée, il est recommandé d'ajouter des mécanismes de sécurité supplémentaires (tels qu'IPsec ou TLS [RFC2246]) à utiliser à l'intérieur du tunnel, en plus de la sécurité de tunnel L2TP.

Bien que L2TP ne rende pas obligatoire l'utilisation de IP/UDP pour son mécanisme de transport, le domaine d'application du présent document se limite à L2TP sur les réseaux IP. Le mécanisme exact pour permettre la sécurité pour les réseaux non IP doit être traité dans les normes appropriées spécifiques de L2TP sur les réseaux non IP.

1.1 Terminologie

Tunnelage volontaire
Dans le tunnelage volontaire, un tunnel est créé par l'utilisateur, normalement via l'utilisation d'un client de tunnelage. Il en résulte que le client va envoyer des paquets L2TP au serveur d'accès réseau (NAS, *Network Access Server*) qui va les transmettre jusqu'au serveur réseau L2TP (LNS, *L2TP Network Server)*. En tunnelage volontaire, le NAS n'a pas besoin de prendre en charge L2TP, et le concentrateur d'accès du protocole de tunnelage de couche 2 (LAC, *L2TP Access Concentrator*) réside sur la même machine que le client. Un autre exemple de tunnelage volontaire est le scénario de passerelle à passerelle. Dans ce cas, le tunnel est créé par un appareil du réseau, normalement, un routeur ou un appareil du réseau. Dans ce scénario l'un ou l'autre côté peut lancer le tunnel à la demande.

Tunnelage obligatoire
Dans le tunnelage obligatoire, un tunnel est créé sans aucune action du client et sans permettre aucun choix au client. Il en résulte que le client va envoyer des paquets PPP au NAS/LAC, qui va les encapsuler dans L2TP et les tunneler au LNS. Dans le cas du tunnelage obligatoire, le NAS/LAC doit être à capacité L2TP.

Initiateur
L'initiateur peut être le LAC ou le LNS et c'est l'appareil qui envoie la demande de début de connexion de contrôle (SCCRQ, *Start-Control-Connection-Request*) et reçoit la réponse de début de connexion de contrôle (SCCRP, *Start-Control-Connection-Reply*).

Répondant
Le répondant peut être le LAC ou le LNS et c'est l'appareil qui reçoit la SCCRQ et répond par une SCCRP.

1.2 Langage des exigences

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

2. Exigences de la sécurité de L2TP

L2TP tunnelle le trafic PPP sur les réseaux publics IP et non IP. Donc, les paquets de contrôle et de données du protocole L2TP sont tous deux vulnérables aux attaques. Des exemples d'attaques incluent que :

1. un adversaire peut essayer de découvrir les identités d'utilisateur en espionnant les paquets de données ;
2. un adversaire peut essayer de modifier des paquets (aussi bien de contrôle que de données) ;
3. un adversaire peut essayer de capturer le tunnel L2TP ou la connexion PPP à l'intérieur du tunnel ;
4. un adversaire peut lancer des attaques de déni de service en mettant fin à des connexions PPP, ou à des tunnels L2TP ;
5. un adversaire peut tenter d'interrompre la négociation ECP PPP afin d'affaiblir ou de supprimer la protection de la confidentialité. Autrement, un adversaire peut souhaiter interrompre la négociation de l'authentification du protocole de contrôle de liaison (LCP, *Link Control Protocol*) PPP afin d'affaiblir le processus d'authentification PPP ou d'obtenir l'accès aux mots de passe d'utilisateur.

Pour faire face à ces menaces, le protocole de sécurité L2TP DOIT être capable de fournir l'authentification, la protection de l'intégrité et contre la répétition pour les paquets de contrôle. De plus, il DEVRAIT être capable de protéger la confidentialité pour les paquets de contrôle. Il DOIT être capable de fournir la protection de l'intégrité et contre la répétition des paquets de

données, et PEUT être capable de protéger la confidentialité des paquets de données. Un protocole de sécurité L2TP DOIT aussi fournir une approche adaptable de la gestion de clés.

Le protocole L2TP, et l'authentification et le chiffrement de PPP ne satisfont pas les exigences de sécurité pour L2TP. L'authentification de tunnel L2TP assure l'authentification mutuelle entre le LAC et le LNS à l'origine du tunnel. Donc, il ne protège pas le trafic de contrôle et de données paquet par paquet. Ainsi, l'authentification de tunnel L2TP laisse le tunnel L2TP vulnérable aux attaques. PPP authentifie le client auprès du LNS, mais ne fournit pas d'authentification, de protection de l'intégrité, ou de protection contre la répétition paquet par paquet. Le chiffrement PPP satisfait aux exigences de confidentialité pour le trafic PPP mais ne satisfait pas aux exigences d'authentification, de protection de l'intégrité, de protection contre la répétition, et de gestion de clés. De plus, la négociation ECP de PPP, décrite dans la [RFC1968] ne fournit pas une négociation de chiffrement protégée. Donc, le chiffrement PPP fournit une solution faible de sécurité, et de plus n'aide pas à sécuriser le canal de contrôle L2TP.

Les facilités de gestion de clé ne sont pas fournies par le protocole L2TP. Cependant, lorsque on désire l'authentification de tunnel L2TP, il est nécessaire de distribuer des mots de passe de tunnel.

Noter que plusieurs des attaques mentionnées ci-dessus peuvent être portées par des paquets PPP envoyés sur la ligne entre le client et le NAS/LAC, avant l'encapsulation des paquets au sein d'un tunnel L2TP. Bien que, strictement parlant, ces attaques sortent du domaine de la sécurité de L2TP, afin de protéger contre elles, le client DEVRAIT assurer la confidentialité, l'authentification, la protection de l'intégrité et contre la répétition pour les paquets PPP envoyés sur la liaison téléphonique. L'authentification, la protection de l'intégrité et contre la répétition ne sont pas actuellement prises en charge par les méthodes de chiffrement de PPP, décrites dans les [RFC1969]-[RFC2419/2420].

2.1 Protocole de sécurité de L2TP

Le protocole de sécurité L2TP DOIT fournir l'authentification, la protection de l'intégrité et contre la répétition pour les paquets de contrôle. De plus, il DEVRAIT protéger la confidentialité des paquets de contrôle. Il DOIT assurer la protection de l'intégrité et contre la répétition des paquets de données, et PEUT protéger la confidentialité des paquets de données. Un protocole de sécurité L2TP DOIT aussi assurer une approche adaptable de la gestion de clé.

Pour satisfaire ces exigences, toutes les mises en œuvre qui se conforment à la sécurité L2TP DOIVENT appliquer ESP IPsec pour sécuriser aussi bien les paquets de contrôle L2TP que ceux de données. Le mode Transport DOIT être pris en charge ; le mode tunnel PEUT être pris en charge. Toutes les suites de chiffrement obligatoires dans IPsec (décrites dans les [RFC2402] et [RFC2406]) et y compris le chiffrement NUL, DOIVENT être prises en charge. Noter que bien qu'une mise en œuvre DOIVE prendre en charge toutes les suites de chiffrement IPsec, celles qui seront utilisées sont au choix de l'opérateur. Si la confidentialité n'est pas exigée (par exemple, pour le trafic de données L2TP) ESP avec le chiffrement NUL peut être utilisé. Les mises en œuvre DOIVENT appliquer les mécanismes IPsec de protection contre la répétition.

La sécurité L2TP DOIT satisfaire aux exigences de gestion de clé de la suite de protocole IPsec. IKE DEVRAIT être pris en charge pour l'authentification, la négociation d'association de sécurité, et la gestion de clé en utilisant le domaine d'interprétation (DOI, *Domain of Interpretation*) d'IPsec [RFC2407].

2.2 Compression et chiffrement sans état

Le chiffrement et/ou compression sans état est très souhaitable lorsque L2TP fonctionne sur IP. Comme L2TP est un protocole en mode connexion, l'utilisation de compression/chiffrement est faisable, mais lors du fonctionnement sur IP, cela n'est pas souhaitable. Bien que fournissant une meilleure compression, lorsque elles sont utilisées sans un mécanisme de livraison fiable sous-jacent, les méthodes à état plein augmentent les pertes de paquet. Il en résulte qu'elles sont problématiques lorsque elles sont utilisées sur l'Internet où la perte de paquet peut être significative. Bien que L2TP [RFC2661] soit en mode connexion, l'ordre des paquets n'est pas obligatoire, ce qui peut créer des difficultés lors de la mise en œuvre de schémas de compression/chiffrement à états pleins. Ces considérations ne sont pas aussi importantes lorsque L2TP fonctionne sur un support non IP tel que IEEE 802, ATM, X.25, ou de relais de trame, car ces supports garantissent l'ordre, et les pertes de paquets restent normalement faibles.

3. Lignes directrices de l'interfonctionnement L2TP/IPsec

Les lignes directrices suivantes sont établies pour satisfaire aux exigences de la sécurité L2TP en utilisant IPsec dans des situations concrètes.

3.1 Tunnel L2TP et suppression de SA de phase 1 et 2

Les mécanismes au sein de PPP et L2TP assurent la suppression en douceur aussi bien que non en douceur. Dans le cas de PPP, une séquence TermReq et TermAck de LCP correspond à une suppression en douceur. Les messages Garder en vie de LCP et les hellos de tunnel L2TP assurent la capacité de détecter lorsque s'est produite une suppression non en douceur. Chaque fois que surviennent des événements de suppression, causant la fermeture du tunnel, le mécanisme de suppression de connexion de contrôle défini dans la [RFC2661] doit être utilisé. Une fois que le tunnel L2TP est supprimé par l'un ou l'autre homologue, toute SA de phase 1 et phase 2 qui existerait encore par suite du tunnel L2TP entre les homologues DEVRAIT être supprimée. Des messages de suppression de phase 1 et phase 2 DEVRAIENT être envoyés lorsque cela se produit.

Lorsque IKE reçoit un message de suppression de phase 1 ou phase 2, IKE devrait notifier à L2TP que cet événement s'est produit. Si l'état L2TP est tel qu'un accusé de réception de corps de message de longueur zéro (ZLB, *Zero-Length Body*) a été envoyé en réponse à un STOPCCN *(arrêt de connexion)* on peut supposer que c'est un accusé de réception positif, que l'homologue a reçu l'accusé de réception ZLB et a effectué la suppression de tout état de tunnel L2TP associé à l'homologue. L'état de tunnel L2TP et tout filtre associé peut maintenant être retiré en toute sécurité.

3.2 Problèmes de fragmentation

Comme l'unité de réception maximale (MRU, *Maximum Receive Unit*) par défaut pour les connexions PPP est de 1500 octets, la fragmentation peut devenir un problème lorsque on ajoute les en-têtes L2TP et IPsec à une trame PPP. On peut utiliser un mécanisme pour réduire ce problème, qui est de fournir PPP avec la valeur de MTU de l'interface d'entrée/sortie du tunnel L2TP/IPsec moins la redondance des en-têtes supplémentaires. Cela devrait survenir après l'établissement du tunnel L2TP mais avant le début de la négociation LCP. Si la valeur de MTU de l'interface d'entrée/sortie pour le tunnel est inférieure à la MTU par défaut de PPP, elle peut remplacer la valeur utilisée. Cette valeur peut aussi être utilisée comme valeur initiale proposée pour la MRU dans la demande de configuration LCP.

Si un message ICMP PMTU est reçu par IPsec, cette valeur devrait être mémorisée dans la SA comme proposé dans la [RFC2401]. IPsec devrait aussi fournir la notification de cet événement à L2TP afin que la nouvelle valeur de MTU puisse être reflétée dans l'interface PPP. Toutes les découvertes de nouvelles PTMU vues à l'interface PPP devraient être vérifiées par rapport à cette nouvelle valeur et traitées en conséquence.

3.3 Vérifications de sécurité par paquet

Lorsque un paquet arrive d'un tunnel qui exige la sécurité, L2TP DOIT :

1. S'assurer que le paquet a été déchiffré et/ou authentifié par IPsec. Comme IPsec vérifie déjà que le paquet est arrivé dans la SA correcte, L2TP peut être sûr que le paquet a bien été envoyé par un homologue de confiance et qu'il n'est pas arrivé en clair.
2. Vérifier que les adresses IP et les valeurs d'accès UDP dans le paquet correspondent aux informations sur la prise qui a été utilisée pour établir le tunnel L2TP. Cette étape empêche des homologues malveillants de falsifier des paquets dans d'autres tunnels.

4. Détails du filtrage IPsec lors de la protection de L2TP

Comme IKE/IPsec ignore les nuances de l'application qu'il protège, normalement aucune intégration n'est nécessaire entre l'application et le protocole IPsec. Cependant, les protocoles qui permettent que le numéro d'accès soit flottant durant les négociations de protocole (comme avec L2TP) peuvent causer des problèmes au sein du cadre IKE actuel. La spécification L2TP [RFC2661] déclare que les mises en œuvre PEUVENT utiliser un accès de source UDP alloué de façon dynamique. Ce changement d'accès est reflété dans la SCCRP envoyée du répondant à l'initiateur.

Bien que la spécification L2TP actuelle permette au répondant d'utiliser une nouvelle adresse IP lors de l'envoi de la SCCRP, les mises en œuvre qui exigent la protection de L2TP via IPsec NE DEVRAIENT PAS faire cela. Pour admettre ce comportement lors de l'utilisation de L2TP et IPsec, lorsque le répondant choisit une nouvelle adresse IP, il DOIT envoyer un StopCCN à l'initiateur, avec la paire de valeurs d'attribut (AVP, *attribute value pair*) Code de résultat et d'erreur présente. Le code de résultat DOIT être réglé à 2 (Erreur générale) et le code d'erreur DEVRAIT être réglé à 7 (Essayer une autre fois). Si le code d'erreur est réglé à 7, alors le message d'erreur facultatif DOIT être présent et le contenu DOIT comporter l'adresse IP (codée en ASCII) que le répondant désire utiliser pour les communications suivantes. Seule d'adresse IP codée en ASCII

devrait être présente dans le message d'erreur. L'adresse IP est codée en format décimal séparé par des points pour IPv4 ou dans le format de la [RFC2373] pour IPv6. L'initiateur DOIT analyser les informations de code de résultat et de code d'erreur et envoyer une nouvelle SCCRQ à la nouvelle adresse IP contenue dans le message d'erreur. Cette approche réduit la complexité car maintenant l'initiateur sait toujours précisément l'adresse IP de son homologue. Cela permet aussi un mécanisme contrôlé pour que L2TP lie les filtres et la politique IPsec au même homologue.

Les détails du filtrage exigés pour s'accommoder de ce comportement ainsi que d'autres mécanismes nécessaires pour protéger L2TP avec IPsec sont discutés dans les paragraphes qui suivent.

4.1 Négociations d'IKE phase 1

Selon IKE [RFC2409], lorsque on utilise une authentification par clés prépartagées, une clé doit être présente pour chaque homologue pour lequel une communication sûre est exigée. Lorsque on utilise le mode principal (qui assure la protection de l'identité) cette clé doit correspondre à l'adresse IP pour l'homologue. Lorsque on utilise le mode agressif (qui n'assure pas la protection de l'identité) la clé prépartagée doit se transposer en un des types d'identifiant valides définis dans le DOI IPsec [RFC2407].

Si l'initiateur reçoit un StopCCN avec l'AVP de code de résultat et d'erreur réglée à "essayer une autre fois" et si une adresse IP valide est présente dans le message, il PEUT lier la clé prépartagée originale utilisée par IKE à la nouvelle adresse IP contenue dans le message d'erreur.

On peut souhaiter considérer les implications pour l'adaptabilité de l'utilisation de clés prépartagées comme méthode d'authentification pour la phase 1. À mesure que croît le nombre de points d'extrémité de LAC et LNS, il devient de plus en plus difficile de gérer les clés prépartagées. Chaque fois que possible, l'authentification avec des certificats est préférée.

4.2 Négociations d'IKE phase 2

Durant les négociations de IKE phase 2, les homologues s'accordent sur le trafic à protéger par les protocoles IPsec. Les identifiants de mode rapide représentent le trafic sur lequel les homologues s'accordent à assurer la protection et sont composés d'espaces d'adresses, de protocoles, et d'informations d'accès.

Lorsque on sécurise L2TP avec IPsec, les cas suivants doivent être pris en considération :

Cas :

Accès initiateur	Adresse répondant	Accès répondant
1701	Fixe	1701
1701	Fixe	Dynamique
1701	Dynamique	1701
1701	Dynamique	Dynamique
Dynamique	Fixe	1701
Dynamique	Fixe	Dynamique
Dynamique	Dynamique	1701
Dynamique	Dynamique	Dynamique

En résolvant le cas le plus général des permutations ci-dessus, tous les cas sont couverts. Le cas le plus général est le dernier de la liste. Ce scénario est lorsque l'initiateur choisit un nouveau numéro d'accès et que le répondant choisit une nouvelle adresse et un nouveau numéro d'accès. Le flux de messages L2TP qui survient pour établir cette séquence est le suivant :

----------> IKE phase 1 et phase 2 pour protéger la SCCRQ initiale
SCCRQ -------> (Adresse IP fixe, Numéro fixe d'initiateur)
<------- STOPCCN (Le répondant choisit une nouvelle adresse IP)
-------> Nouveau IKE phase 1 et phase 2 pour protéger la nouvelle SCCRQ
SCCRQ -----> (SCCRQ à la nouvelle adresse IP du répondant)
<------- Nouveau IKE phase 2 pour le changement du numéro d'accès par le répondant
<------- SCCRP (Le répondant choisit un nouveau numéro d'accès)
SCCCN -------> (Achèvement de l'établissement du tunnel L2TP)

Bien que normalement l'initiateur et le répondant ne changent pas les accès de façon dynamique, la sécurité L2TP doit s'accommoder d'applications émergeantes telles que l'équilibrage de charge et la garantie de qualité de service. Cela peut

exiger que l'accès et l'adresse IP flottent durant l'établissement du tunnel L2TP.

Pour la prise en charge du cas général, des mécanismes doivent être conçus dans L2TP et IPsec pour permettre à L2TP d'injecter des filtres dans la base de données des filtres d'IPsec. Cette technique peut être utilisée par toute application qui a des accès flottants et exige la sécurité via IPsec. Elle est décrite dans les paragraphes qui suivent.

Le répondant n'est pas obligé de prendre en charge la capacité de faire flotter son adresse et accès IP. Cependant, l'initiateur DOIT permettre que le répondant fasse flotter son accès et DEVRAIT permettre au répondant de choisir une nouvelle adresse IP (voir au paragraphe 4.2.3).

L'Appendice A donne des exemples des cas qui utilisent le processus décrit ci-dessous.

4.2.1 Définition de la terminologie utilisée pour les déclarations de filtrage

I-Port C'est le numéro d'accès UDP que l'initiateur choisit pour générer/recevoir le trafic L2TP. Ce peut être un accès statique tel que 1701 ou un numéro éphémère alloué par la prise.

R-Por C'est le numéro d'accès UDP que choisit le répondant pour générer/recevoir le trafic L2TP. Ce peut être le numéro d'accès 1701 ou un numéro éphémère alloué par la prise. C'est le numéro d'accès que le répondant utilise après avoir reçu la SCCRQ initiale.

R-IPAddr1 C'est l'adresse IP sur laquelle le répondant écoute pour la SCCRQ initiale. Si le répondant ne choisit pas une nouvelle adresse IP, cette adresse sera utilisée pour tout le trafic L2TP ultérieur.

R-IPAddr2 C'est l'adresse IP que le répondant choisit à réception de la SCCRQ. Cette adresse est utilisée pour envoyer la SCCRP et tout le trafic ultérieur de tunnel L2TP est envoyé et reçu à cette adresse.

R-IPAddr C'est l'adresse IP qu'utilise le répondant pour envoyer et recevoir les paquets L2TP. C'est soit la valeur initiale de R-IPAddr1, soit une nouvelle valeur de R-IPAddr2.

I-IPAddr C'est l'adresse IP qu'utilise l'initiateur pour communiquer avec le tunnel L2TP.

Any-Addr La présence de Any-Address définit que IKE devrait accepter toute adresse seule proposée dans l'adresse locale des identifiants de mode rapide envoyés par l'homologue durant les négociations IKE de phase 2. Cette seule adresse peut être formatée comme une seule adresse IP, une adresse IP Netmask avec le Netmask réglé à 255.255.255.255, et une gamme d'adresses IP dont la gamme est 1, ou un nom d'hôte qui peut se résoudre en une adresse. Se reporter à la [RFC2407] pour plus d'informations sur le format des identifiants de mode rapide.

Any-Port La présence de Any-Port définit que IKE devrait accepter une valeur de 0 ou une valeur d'accès spécifique pour valeur d'accès dans les identifiants de mode rapide négociés durant IKE phase 2.

Les filtres définis dans les paragraphes qui suivent sont énumérés de la plus forte priorité à la plus faible.

4.2.2 Filtres initiaux nécessaires pour protéger le SCCRQ

Le filtre initial établi sur l'initiateur et le répondant est nécessaire pour protéger la SCCRQ envoyée par l'initiateur pour ouvrir le tunnel L2TP. L'initiateur et le répondant doivent tous deux soit être préconfigurés pour ces filtres, soit L2TP doit avoir une méthode pour injecter ces informations dans la base de données de filtrage d'IPsec. Dans l'un et l'autre cas, ce filtre DOIT être présent avant que les messages d'établissement du tunnel L2TP commencent à s'écouler.

Filtres de répondant :
Sortie-1 : Aucun. Ils devraient être créés de façon dynamique par IKE après la réussite de l'achèvement de la phase 2.

Entrée-1 : De Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Filtres d'initiateur :
Sortie-1 : De I-IPAddr, à R-IPAddr1, UDP, src I-Port, dst 1701

Entrée-1 : De R-IPAddr1, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-2 : De R-IPAddr1, à I-IPAddr, UDP, src Any-Port, dst I-Port

Lorsque l'initiateur utilise des accès dynamiques, L2TP doit injecter les filtres dans la base de données des filtres IPsec, une

fois que le numéro d'accès de source est connu. Si l'initiateur utilise l'accès fixe de 1701, ces filtres PEUVENT être définis de façon statique.

La définition Any-Port dans la déclaration de filtre entrant-2 de l'initiateur est nécessaire pour traiter le changement potentiel d'accès qui pourrait survenir par suite du changement de son numéro d'accès par le répondant.

Si un faisceau de SA de phase 2 n'est pas déjà présent pour protéger la SCCRQ, l'envoi d'une SCCRQ par l'initiateur DEVRAIT causer l'établissement par IKE des SA nécessaires pour protéger ce paquet. Autrement, L2TP peut aussi demander à IKE d'établir le faisceau de SA. Si pour une raison quelconque, la SA ne peut être établie, le paquet DOIT être abandonné.

Les numéros d'accès dans les identifiants de mode rapide envoyés par l'initiateur DOIVENT contenir les numéros d'accès spécifiques utilisés pour identifier la prise UDP. Les numéros d'accès vont être soit I-Port/1701, soit 1701/1701 pour la SCCRQ initiale. Les identifiants de mode rapide envoyés par l'initiateur seront un sous ensemble du filtre Entrée-1 chez le répondant. Il en résulte que l'échange de mode rapide va finir et que IKE devrait injecter un ensemble de filtres spécifique dans la base de données des filtres IPsec et associer cet ensemble de filtres à la SA de phase 2 établie entre les homologues. Ces filtres devraient persister tant qu'existe le tunnel L2TP. Le nouvel ensemble de filtres chez le répondant sera :

Filtres du répondant :
Sortie-1 : De R-IPAddr1, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-1 : De I-IPAddr, à R-IPAddr1, UDP, src I-Port, dst 1701
Entrée-2 : De Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Des mécanismes DEVRAIENT exister entre L2TP et IPsec afin que L2TP ne retransmette pas la SCCRQ alors que la SA est en cours d'établissement. Les mécanismes de retransmission du canal de contrôle de L2TP devraient commencer une fois que la SA a été établie. Cela va aider à éviter les fins de temporisation qui peuvent survenir par suite de lenteurs de l'établissement de SA.

Une fois que la SA de phase 2 a été établie entre les homologues, la SCCRQ devrait être envoyée de l'initiateur au répondant.

Si le répondant ne choisit pas une nouvelle adresse IP ou un nouveau numéro d'accès, le tunnel L2TP peut maintenant procéder à son établissement.

4.2.3 Choix d'une nouvelle adresse IP par le répondant

Cette étape décrit le processus qui devrait être suivi lorsque le répondant choisit une nouvelle adresse. La seule opportunité pour que le répondant change son adresse IP est après avoir reçu la SCCRQ mais avant d'envoyer une SCCRP.

La nouvelle adresse que le répondant choisit d'utiliser DOIT être reflétée dans l'AVP de code de résultat et d'erreur d'un message STOPCCN. Le code de résultat DOIT être réglé à 2 (Erreur générale) et le code d'erreur DOIT être réglé à 7 (Essayer une autre fois). Le message d'erreur facultatif DOIT être présent et le contenu DOIT comporter l'adresse IP (codée en ASCII) que le répondant désire utiliser pour les communications ultérieures. Seule l'adresse IP codée en ASCII devrait être présente dans le message d'erreur. L'adresse IP est codée en format décimal séparé par des points pour IPv4 ou en format de la [RFC2373] pour IPv6.

Le message STOPCCN DOIT être envoyé en utilisant les mêmes informations d'adresse et d'accès UDP qu'utilisées par l'initiateur pour envoyer la SCCRQ. Ce message va protéger en utilisant l'établissement de faisceau de SA initial pour protéger la SCCRQ.

À réception du STOPCCN, l'initiateur DOIT analyser l'adresse IP provenant de l'AVP Code de résultat et d'erreur et effectuer les vérifications de bonne santé nécessaires pour vérifier que c'est une adresse correctement formatée. Si aucune erreur n'est trouvée, L2TP devrait injecter un nouvel ensemble de filtres dans la base de données de filtres IPsec. Si on utilise l'authentification par clés prépartagées, L2TP PEUT demander à IKE de lier la nouvelle adresse IP à la clé prépartagée qui a été utilisée pour l'adresse IP originale.

Comme l'adresse IP du répondant a changé, une nouvelle SA de phase 1 et de phase 2 doit être établie entre les homologues avant d'envoyer la nouvelle SCCRQ.

En supposant que le tunnel initial a été supprimé et que les filtres nécessaires pour créer le tunnel ont été retirés, les nouveaux filtres pour l'initiateur et le répondant seront :

Filtres d'initiateur :
Sortie-1 : De I-IPAddr, à R-IPAddr2, UDP, src I-Port, dst 1701

Entrée-1 : De R-IPAddr2, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-2 : De R-IPAddr2, à I-IPAddr, UDP, src Any-Port, dst I-Port

Une fois que IKE phase 2 s'est achevé, le nouvel ensemble de filtres chez le répondant sera :

Filtres de répondant :
Sortie-1 : De R-IPAddr2, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-1 : De I-IPAddr, à R-IPAddr2, UDP, src I-Port, dst 1701
Entrée-2 : De Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Si le répondant choisit de ne pas passer à un nouveau numéro d'accès, l'établissement du tunnel L2TP peut maintenant s'achever.

4.2.4 Choix d'un nouveau numéro d'accès par le répondant

Le répondant PEUT choisir un nouvel accès UDP de source à utiliser pour le trafic t du tunnel L2TP. Cette décision DOIT être prise avant d'envoyer la SCCRP. Si un nouveau numéro d'accès est choisi, alors L2TP doit injecter de nouveaux filtres dans la base de données de filtres d'IPsec. Le répondant doit lancer une nouvelle négociation IKE phase 2 avec l'initiateur.

L'ensemble final de filtres chez l'initiateur et le répondant est le suivant .

Filtres de l'initiateur :
Sortie-1 : De I-IPAddr, à R-IPAddr, UDP, src I-Port, dst R-Port
Sortie-2 : De I-IPAddr, à R-IPAddr, UDP, src I-Port, dst 1701
Entrée-1 : De R-IPAddr, à I-IPAddr, UDP, src R-Port, dst I-Port
Entrée-2 : De R-IPAddr, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-3 : De R-IPAddr, à I-IPAddr, UDP, src Any-Port, dst I-Port

Le filtre Entrée-1 pour l'initiateur sera injecté par IKE à l'achèvement réussi de la négociation de phase 2 initiée par l'homologue.

Filtres du répondant :
Sortie-1 : De R-IPAddr, à I-IPAddr, UDP, src R-Port, dst I-Port
Sortie-2 : De R-IPAddr, à I-IPAddr, UDP, src 1701, dst I-Port
Entrée-1 : De I-IPAddr, à R-IPAddr, UDP, src I-Port, dst R-Port
Entrée-2 : De I-IPAddr, à R-IPAddr, UDP, src I-Port, dst 1701
Entrée-3 : De Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Une fois achevées les négociations, la SCCRP est envoyée et le tunnel L2TP peut terminer son établissement. Après l'établissement du tunnel L2TP, toute SA résiduelle et ses filtres associés peuvent être supprimés.

4.2.5 Considérations d'accès de sortie de passerelle à passerelle et de L2TP

Dans le scénario de passerelle à passerelle ou dans le scénario à numérotation L2TP, l'un ou l'autre côté peut initier L2TP. Le processus décrit dans les étapes précédentes devrait être suivi avec un ajout. L'ensemble de filtres initial des deux côtés DOIT inclure le filtre suivant :

Filtre entrant :
1 : De Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Lorsque l'un ou l'autre homologue décide de lancer un tunnel, L2TP devrait injecter les filtres entrant et sortant nécessaires pour protéger la SCCRQ. L'établissement de tunnel se déroule alors exactement comme mentionné dans les paragraphes précédents.

5. Considérations pour la sécurité

5.1 Questions d'authentification

La négociation IKE d'IPsec DOIT négocier une méthode d'authentification spécifiée dans IKE [RFC2409]. En plus de l'authentification IKE, les mises en œuvre de L2TP utilisent les méthodes d'authentification de PPP, telles que celles décrites dans les [RFC1994]-[RFC2284]. Dans la présente section, on expose les problèmes d'authentification.

5.1.1 Différences entre authentification IKE et PPP

Bien que PPP assure l'authentification initiale, il n'assure pas l'authentification par paquet, ni la protection de l'intégrité ou contre la répétition. Cela implique que l'identité vérifiée dans l'authentification PPP initiale n'est ensuite pas vérifiée à réception de chaque paquet.

Avec IPsec, lorsque l'identité affirmée dans IKE est authentifiée, les clés déduites résultantes sont utilisées pour assurer l'authentification par paquet, et la protection de l'intégrité et contre la répétition. Il en résulte que l'identité vérifiée dans la conversation IKE est ensuite vérifiée à réception de chaque paquet.

Supposons que l'identité revendiquée dans PPP soit une identité d'utilisateur, tandis que l'identité revendiquée au sein de IKE est une identité de machine. Comme seule l'identité de machine est vérifiée paquet par paquet, il n'y a aucun moyen de vérifier que seul l'usager authentifié au sein de PPP utilise le tunnel. En fait, les mises en œuvre de IPsec qui ne prennent en charge que l'authentification de machine n'ont normalement aucun moyen d'appliquer une ségrégation du trafic. Il en résulte que lorsque l'authentification de machine est utilisée, une fois qu'un tunnel L2TP/IPsec est ouvert, tout utilisateur sur une machine multi-utilisateurs va normalement être capable d'envoyer du trafic dans le tunnel.

Si la mise en œuvre IPsec prend en charge l'authentification d'utilisateur, ce problème peut être évité. Dans ce cas, l'identité de l'utilisateur affirmée dans IKE sera vérifiée paquet par paquet. Afin d'assurer la ségrégation du trafic entre les usagers lorsque l'authentification d'utilisateur est activée, le client DOIT s'assurer que seul le trafic provenant de cet usager particulier est envoyé sur le tunnel L2TP.

5.1.2 Authentification de certificat dans IKE

Lorsque l'authentification de certificat X.509 est choisie au sein de IKE, le LNS est supposé utiliser une charge utile de demande de certificat (CRP, *Certificate Request Payload*) IKE pour demander de la part du client un certificat produit par une autorité de certificat particulière, ou peut utiliser plusieurs CRP si plusieurs autorités de certificat sont de confiance et configurées dans sa politique d'authentification IKE d'IPsec.

Le LNS DEVRAIT être capable de faire confiance à plusieurs autorités de certificat afin de permettre aux points d'extrémité de client de tunnel de s'y connecter en utilisant leurs propres accréditifs de certificat provenant de leur infrastructure de clés publiques (PKI, *Public-Key Infrastructure*) choisie. La vérification côté client et côté serveur des listes de révocation de certificat PEUT être activée autorité de certificat par autorité de certificat, car des différences de vérification de liste de révocation existent entre différents fournisseurs de PKI.

Les mises en œuvre de L2TP PEUVENT utiliser des accès alloués de façon dynamique pour les deux accès de source et de destination si la sécurité pour chaque combinaison d'accès de source et de destination peut être négociée avec succès par IKE.

5.1.3 Authentification de certificat de machine ou d'utilisateur dans IKE

Les accréditifs de certificat fournis par le client L2TP durant la négociation IKE PEUVENT être ceux de la machine ou ceux de l'utilisateur L2TP. Lorsque l'authentification de la machine est utilisée, le certificat de machine est normalement mémorisé sur le LAC et le LNS durant un processus d'inscription. Lorsque des certificats d'utilisateur sont utilisés, le certificat d'utilisateur peut être mémorisé soit sur la machine, soit sur une carte à mémoire.

Comme la valeur d'un certificat de machine est inversement proportionnelle à la facilité avec laquelle un attaquant peut en obtenir un sous un faux semblant, il est conseillé que le processus d'inscription de certificat de machine soit strictement contrôlé. Par exemple, seuls les administrateurs ont la capacité d'inscrire une machine avec un certificat de machine.

Bien que la mémorisation de certificat sur une carte à mémoire diminue la probabilité d'une compromission de la clé privée, les cartes à mémoire ne sont pas nécessairement souhaitables dans toutes les situations. Par exemple, certaines organisations qui déploient des certificats de machine les utilisent de façon à restreindre l'utilisation de matériels non approuvés. Comme l'authentification de l'utilisateur peut être fournie au sein de PPP (en gardant en mémoire les faiblesses décrites

précédemment) la prise en charge de l'authentification de machine dans IPsec rend possible d'authentifier la machine aussi bien que l'usager.

Dans des circonstances où cette double assurance est considérée comme valable, permettre le déplacement du certificat de machine d'une machine à une autre, comme ce serait possible si le certificat de machine était mémorisé sur une carte à mémoire, peut être indésirable.

De même, lorsque les certificats d'utilisateur sont déployés, il est conseillé que le processus d'inscription de l'usager soit strictement contrôlé. Si par exemple, un mot de passe d'utilisateur peut être directement utilisé pour obtenir un certificat (temporaire ou à plus long terme) alors ce certificat n'offre pas plus de valeur de sécurité que le mot de passe. Pour limiter la capacité d'un attaquant à obtenir un certificat d'utilisateur à partir d'un mot de passe volé, la période d'inscription peut être limitée, après quoi l'accès du mot de passe sera terminé. Une telle politique empêchera un attaquant qui a obtenu le mot de passe d'un compte inutilisé d'obtenir une certificat d'utilisateur une fois expirée la période d'inscription.

5.1.4 Clés prépartagée dans IKE

L'utilisation de clés prépartagées dans le mode principal d'IKE est vulnérable aux attaques par interposition *(man-in-the-middle attacks)* lorsque on se trouve dans des situations d'accès distant. En mode principal, il est nécessaire d'utiliser SKEYID_e avant la réception de la charge utile d'identification. Donc la sélection de la clé pré partagée ne peut que se fonder sur les informations contenues dans l'en-tête IP. Cependant, dans les situations d'accès distant, l'allocation dynamique d'adresse IP est normale, de sorte qu'il n'est souvent pas possible d'identifier la clé prépartagée requise sur la base de l'adresse IP.

Donc, lorsque des clés prépartagées sont utilisées dans des scénarios d'accès distant, la même clé prépartagée est partagée par un groupe d'usagers et n'est plus capable de fonctionner comme un secret partagé efficace. Dans cette situation, ni le client ni le serveur ne s'identifient durant IKE phase 1 ; on sait seulement que les deux parties sont membres du groupe qui a connaissance de la clé prépartagée. Cela permet à n'importe qui d'accéder à la clé prépartagée du groupe et d'agir comme un agresseur interposé.

Cette faiblesse ne se présente pas en mode agressif car la charge utile d'identité est envoyée plus tôt dans l'échange, et donc la clé prépartagée peut être choisie sur la base de l'identité. Cependant, lorsque le mode agressif est utilisé, l'identité de l'usager est exposée et cela est souvent considéré comme indésirable.

Il en résulte que lorsque le mode principal est utilisé avec des clé prépartagées, sauf si PPP effectue l'authentification mutuelle, le serveur n'est pas authentifié. Cela permet à un serveur félon en possession de la clé prépartagée du groupe de se faire passer avec succès pour le LNS et de monter une attaque de dictionnaire sur les méthodes d'authentification traditionnelles telles que CHAP [RFC1994]. Une telle attaque aurait le potentiel de compromettre de nombreux mots de passe en un instant. Cette faiblesse est présente dans certaines mises en œuvre existantes de mode tunnel IPsec.

Pour éviter ce problème, les mises en œuvre de L2TP/IPsec NE DEVRAIENT PAS utiliser une clé partagée de groupe pour l'authentification IKE auprès du LNS. Les valeurs de clé d'authentification prépartagée IKE DEVRAIENT être protégées d'une manière similaire à celle du mot de passe de compte d'usager utilisé par L2TP.

5.2 Interactions de sécurité entre IPsec et PPP

Lorsque L2TP est protégé avec IPsec, les services de sécurité de PPP et d'IPsec sont tous deux disponibles. Les services qui sont négociés dépendent de si le tunnel est obligatoire ou volontaire. Une analyse détaillée des scénarios de tunnelage volontaire et obligatoire figure ci-après. Ces scénarios ne sont pas normatifs et ne créent pas d'exigence pour qu'une mise en œuvre soit conforme à la sécurité L2TP.

Dans les scénarios ci-dessous, on suppose que les clients et serveurs L2TP sont tous deux capables d'établir et d'obtenir les propriétés des associations de sécurité IPsec, ainsi que d'influencer les services de sécurité IPsec négociés. De plus, on suppose que les clients et serveurs L2TP sont capables d'influencer le processus de négociation pour le chiffrement et la compression PPP.

5.2.1 Tunnel obligatoire

Dans le cas d'un tunnel obligatoire, le client envoie des trames PPP au LAC, et ne saura normalement pas que les trames sont tunnelées, ni ne connaîtra aucun des services de sécurité en place entre le LAC et le LNS. Au LNS, un paquet de données va arriver, incluant une trame PPP encapsulée dans L2TP, qui est lui-même encapsulé dans un paquet IP. En obtenant les propriétés de l'association de sécurité établie entre le LNS et le LAC, le LNS peut obtenir des informations sur les services de

sécurité en place entre lui-même et le LAC. Donc, dans le cas de tunnelage obligatoire, le client et le LNS ont une connaissance inégale des service s de sécurité en place entre eux.

Comme le LNS est capable de savoir si la protection de la confidentialité, l'authentification, et la protection de l'intégrité et contre la répétition sont en place entre lui-même et le LAC, il peut utiliser cette connaissance afin de modifier son comportement durant la négociation PPP ECP [RFC1968] et CCP [RFC1962]. Supposons que la politique de confidentialité du LNS peut être décrite par un des termes suivants : "Chiffrement exigé", "Chiffrement permis" ou "Chiffrement interdit". Si les services de confidentialité IPsec sont en place, alors un LNS qui met en œuvre une politique de "Chiffrement interdit" va agir comme si la politique avait été violée. De même, un LNS qui met en œuvre une politique "Chiffrement exigé" ou "Chiffrement permis" va agir comme si ces politiques étaient satisfaites, et ne va pas rendre obligatoire l'utilisation du chiffrement ou de la compression PPP. Ce n'est pas la même chose que d'insister pour que le chiffrement et la compression PPP soient désactivées, car la décision va dépendre de la politique du client.

Comme le client n'a pas connaissance des services de sécurité en place entre le LAC et le LNS, et comme il peut ne pas faire confiance au LAC ou au réseau entre lui-même et le LAC, le client va normalement vouloir s'assurer d'une sécurité suffisante par l'utilisation d'IPsec de bout en bout ou du chiffrement/compression PPP entre lui-même et le LNS.

Un client qui souhaite s'assurer des services de sécurité sur le chemin entier du voyage ne va pas modifier ce comportement même si il n'a aucune connaissance des services de sécurité en place entre le LAC et le LNS. Le client négocie les services de confidentialité entre lui-même et le LNS afin de fournir la confidentialité sur le réseau entre lui-même et le LAC. Le client négocie la sécurité de bout en bout entre lui-même et la station d'extrémité afin d'assurer la confidentialité dans la portion du chemin entre le LNS et la station d'extrémité.

Le client ne va normalement pas faire confiance au LAC et va négocier les services de confidentialité et de compression de son propre chef. Il en résulte que le LAC peut seulement souhaiter négocier IPsec ESP avec chiffrement nul avec le LNS, et le LNS va demander la protection contre la répétition. Cela va assurer que les services de confidentialité et de compression ne seront pas dupliqués sur le chemin entre le LAC et le LNS. Il en résulte une meilleure adaptabilité pour le LAC, car le chiffrement sera traité par le client et le LNS.

Le client peut satisfaire son désir de services de confidentialité d'une de deux façons. Si il sait que les stations d'extrémité avec lesquelles il va communique sont à capacité IPsec (ou si il refuse de parler à des stations d'extrémité sans capacité IPsec) il peut alors refuser de négocier le chiffrement /compression PPP et à la place négocier IPsec ESP avec les stations d'extrémité. Si le client ne sait pas que toutes les stations d'extrémité qu'il contacte sont à capacité IPsec (le cas le plus probable) il va alors négocier le chiffrement/compression PPP. Il peut en résulter une duplication de compression/chiffrement qui ne peut être éliminer que si la compression/chiffrement PPP peut être désactivée paquet par paquet. Noter que comme le LNS sait que les paquets du client sont tunnelés mais que le client ne le sait pas, le LNS peut s'assurer que la compression/chiffrement sans état est utilisée en offrant des méthodes de compression/chiffrement sans état si il en est de disponibles dans les négociations ECP et CCP.

5.2.2 Tunnel volontaire

Dans le cas d'un tunnel volontaire, le client va envoyer des paquets L2TP au NAS, qui va les acheminer au LNS. Sur une liaison à numérotation téléphonique, ces paquets L2TP seront encapsulés dans IP et PPP. En supposant qu'il est possible au client de restituer les propriétés de l'association de sécurité entre lui-même et le LNS, le client aura connaissance de tous les services de sécurité négociés entre lui et le LNS. Il aura aussi connaissance des services de chiffrement/compression PPP négociés entre lui-même et le NAS.

De son point de vue, le LNS va noter une trame PPP encapsulée dans L2TP, qui est lui-même encapsulé dans un paquet IP. Cette situation est identique à celle du cas du tunnelage obligatoire. Si le LNS restitue les propriétés de l'association de sécurité établie entre lui et le client, il peut être informé des services de sécurité en place entre eux. Donc, dans le cas du tunnelage volontaire, le client et le LNS ont une connaissance symétrique des services de sécurité en place entre eux.

Comme le LNS est capable de savoir si la confidentialité, l'authentification, la vérification d'intégrité ou la protection contre la répétition sont en place entre le client et lui-même, il est capable d'utiliser cette connaissance pour modifier sa position de négociation ECP et CCP PPP. Si la confidentialité IPsec est en place, le LNS peut se comporter comme si une directive "chiffrement exigé" avait été satisfaite, ne rendant pas obligatoire l'utilisation du chiffrement ou de la compression PPP. Normalement, le LNS ne va pas insister pour que le chiffrement/compression PPP soit désactivé, laissant plutôt cette décision au client.

Comme le client a connaissance des services de sécurité en place entre lui et le LNS, il peut agir comme si une directive "chiffrement exigé" avait été satisfaite si IPsec ESP avait déjà été en place entre lui et le LNS. Donc, il peut demander que le chiffrement et la compression PPP ne soient pas négociés. Si les services de compression IP ne peuvent pas être négociés, il

sera normalement souhaitable de désactiver la compression PPP si aucune méthode sans état n'est disponible, due aux effets indésirables de la compression PPP à états pleins.

Donc, dans le cas du tunnelage volontaire, le client et le LNS vont normalement être capables d'éviter d'utiliser le chiffrement et la compression PPP, négociant plutôt la confidentialité, l'authentification, et les services de protection d'intégrité d'IPsec, ainsi que la compression IP, si elle est disponible.

Il peut en résulter une duplication du chiffrement si le client communique avec une station d'extrémité à capacité IPsec. Afin d'éviter la duplication du chiffrement/compression, le client peut négocier deux associations de sécurité avec le LNS, une avec ESP en chiffrement nul, et une avec confidentialité/compression. Les paquets qui vont à une station d'extrémité à capacité IPsec vont passer sur l'ESP avec l'association de sécurité à chiffrement nul, et les paquets pour une station d'extrémité sans capacité IPsec vont passer sur l'autre association de sécurité. Noter que de nombreuses mises en œuvre IPsec ne peuvent pas prendre en charge cela sans permettre aux paquets L2TP sur le même tunnel d'être générés de multiples accès UDP. Cela exige des modifications à la spécification L2TP.

Noter aussi que le client peut souhaiter mettre en place des services de confidentialité pour des paquets non tunnelés qui voyagent entre lui et le NAS. Cela va protéger le client contre l'espionnage sur le réseau entre lui et le NAS. Par suite, il peut souhaiter négocier le chiffrement et la compression PPP avec le NAS. Comme dans le tunnelage obligatoire, il va en résulter une duplication du chiffrement, et éventuellement de la compression, sauf si la compression/chiffrement PPP peut être désactivée sur la base du paquet.

6. Références

[RFC1661] W. Simpson, éditeur, "Protocole point à point (PPP)", STD 51, juillet 1994. *(MàJ par la* RFC2153)

[RFC1962] D. Rand, "Protocole de contrôle de compression en PPP (CCP)", juin 1996.

[RFC1968] G. Meyer, "Protocole de contrôle de chiffrement en PPP (ECP)", juin 1996. *(P.S.)*

[RFC1969] K. Sklower, G. Meyer, "Protocole de chiffrement en DES sur PPP (DESE)", juin 1996. (*Obsolète, voir* RFC2419)

[RFC1994] W. Simpson, "Protocole d'authentification par mise en cause de la prise de contact en PPP (CHAP)", août 1996.

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

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2284] L. Blunk, J. Vollbrecht, "Protocole extensible d'authentification (EAP) en PPP", mars 1998. (*Obs., voir* RFC3748) *(P.S.)*

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC4291) *(PS)*

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

[RFC2402] S. Kent et R. Atkinson, "En-tête d'authentification IP", novembre 1998. (*Obsolète, voir* RFC4302, 4305)

[RFC2406] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", novembre 1998. *(Obsolète, voir* RFC4303*)*

[RFC2407] D. Piper, "Le domaine d'interprétation de sécurité IP de l'Internet pour ISAKMP", novembre 1998. *(Obsolète, voir* RFC4306*)*

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

[RFC2419] K. Sklower, G. Meyer, "Protocole de chiffrement par DES dans PPP, version 2 (DESE-bis)", septembre 1998. *(P.S.)*

[RFC2420] H. Kummert, "Protocole de chiffrement Triple-DES sur PPP (3DESE)", septembre 1998. *(P.S.)*

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2

"L2TP"", *(P.S.)*

Remerciements

Merci à Gurdeep Singh Pall, David Eitelbach, Peter Ford, et Sanjay Anand de Microsoft, à John Richardson de Intel et à Rob Adams de Cisco pour les utiles discussions de cette gamme de problèmes.

Adresse des auteurs

Baiju V. Patel
Intel Corp
2511 NE 25th Ave
Hillsboro, OR 97124
téléphone : +1 503 702 2303
mél : baiju.v.patel@intel.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 706-6605
mél : bernarda@microsoft.com

William Dixon
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 703 8729
mél : wdixon@microsoft.com

Glen Zorn
Cisco Systems, Inc.
500 108th Avenue N.E., Suite 500
Bellevue, Washington 98004
téléphone : +1 425 438 8218
mél : gwz@cisco.com

Skip Booth
Cisco Systems
7025 Kit Creek Road
RTP, NC 27709
téléphone : +1 919 392 6951
mél : ebooth@cisco.com

Appendice A Exemple de filtre IPsec réglé pour l'établissement de tunnel L2TP

Cette section donne des exemples de filtres IPsec réglés pour l'établissement de tunnel L2TP. Bien que les exemples d'ensembles de filtres soient pour IPv4, des exemples similaires seraient aussi facilement construits pour IPv6.

A.1 Initiateur et répondant utilisent des adresses et accès fixes

C'est le plus simple des cas car rien ne change durant l'établissement de tunnel L2TP. Comme l'initiateur ne sait pas si le répondant va changer son numéro d'accès, il doit toujours être prêt pour ce cas. Dans cet exemple, l'initiateur va utiliser une adresse IPv4 de 1.1.1.1 et le répondant va utiliser une adresse IPv4 de 2.2.2.1.

Les filtres pour ce scénario sont :

A.1.1 Protéger le SCCRQ

Filtres d'initiateur :
Sortie-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
Entrée-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
Entrée-2 : De 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondant :
Sortie-1 : Aucun, injecté de façon dynamique lorsque IKE phase 2 s'achève
Entrée-1 : De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

Après l'achèvement de IKE phase 2, les filtres chez l'initiateur et le répondant seront :

Filtres d'initiateur :
Sortie-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
Entrée-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
Entrée-2 : De 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondant :
Sortie-1: De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
Entrée-1: De 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
Entrée-2: De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

A.2 Scénario de passerelle à passerelle où l'initiateur et le répondeur utilisent des accès dynamiques

Dans ce scénario, l'un et l'autre côté peut initier le tunnel. Comme des accès dynamiques seront utilisés, une négociation de phase 2 supplémentaire doit se faire pour protéger la SCCRP envoyée du répondant à l'initiateur. En dehors de l'établissement de la phase 2 additionnelle, la seule autre différence est que L2TP chez le répondant doit injecter un filtre supplémentaire dans la base de données IPsec une fois que le nouveau numéro d'accès est choisi.
Cet exemple montre aussi le filtre additionnel nécessaire à l'initiateur qui permet à l'un et l'autre côté de commencer le tunnel. Dans le scénario de numérotation ou dans celui de passerelle à passerelle, ce filtre supplémentaire est exigé.

Pour cet exemple, on suppose que l'accès dynamique donné à l'initiateur est 5000 et que son adresse IP est 1.1.1.1. Le répondant va utiliser une adresse IP de 2.2.2.1 et un numéro d'accès de 6000.

Les filtres pour ce scénario sont :

A.2.1 Filtres initiaux pour permettre à l'un et l'autre côté de répondre aux négociations

Dans ce cas, les deux homologues doivent être capables d'accepter les négociations de phase 2 de et vers les homologues L2TP. My-IPAddr est défini comme toute adresse IP que l'appareil veut accepter pour les négociations L2TP.

Filtres de répondant présents chez les deux homologues :
Entrée-1 : De Any-Addr, à My-IPAddr, UDP, src Any-Port, dst 1701

Note : La source IP dans le filtre Entrée-1 ci-dessus pour les tunnels de passerelle à passerelle peut être spécifique de IP, comme 1.1.1.1, et non nécessairement Any-Addr.

A.2.2 Protéger la SCCRQ, un homologue étant l'initiateur

Filtres d'initiateur :
Sortie-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
Entrée-2 : De 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 5000
Entrée-3 : De Any-Addr, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondant :
Sortie-1 : Aucun, injecté de façon dynamique lors de l'achèvement de IKE phase 2
Entrée-1 : De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

Après l'achèvement de IKE phase 2, les filtres chez l'initiateur et chez le répondant seront :

Filtres d'initiateur :
Sortie-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
Entrée-2 : De 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 5000
Entrée-3 : De Any-Addr, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondant :
Sortie-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
Entrée-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-2 : De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

A.2.3 Protéger la SCCRP après le changement d'accès

À ce point, le répondant sait quel numéro d'accès il va utiliser. Les nouveaux filtres devraient être injectés par L2TP pour refléter cette nouvelle allocation d'accès.

Le nouvel ensemble de filtres chez le répondant est :

Filtres de répondant :
Sortie-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000

Sortie-2 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000

Entrée-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 6000
Entrée-2 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-3 : De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

La seconde phase 2 va commencer une fois que L2TP envoie la SCCRP. Une fois que les négociations de phase 2 sont achevées, le nouvel ensemble de filtres chez l'initiateur et chez le répondant sera :

Filtres d'initiateur :
Sortie-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 6000
Sortie-2 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000
Entrée-2 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
Entrée-3 : De 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondant :
Sortie-1 : De 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000
Sortie-2 : De 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
Entrée-1 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 6000
Entrée-2 : De 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
Entrée-3 : De Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

Une fois que l'établissement du tunnel L2TP est réussi, la phase 2 d'origine peut être supprimée. Cela permet aux déclarations des filtres Entrée-2 et Sortie-2 d'être également supprimées.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Déclaration complète de droits de reproduction

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.