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, *Layer Two Tunneling Protocol*) peut utiliser IPsec pour assurer l'authentification de tunnel, la protection de la confidentialité, la vérification de l'intégrité et la protection contre la répétition. Les cas de tunnelage volontaire et obligatoire sont tous deux 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 de 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 l'authentification mutuelle des points d'extrémité du tunnel. Cependant, L2TP ne définit pas les mécanismes de protection du tunnel.

IPsec est une suite de protocoles qui est utilisée pour sécuriser la communication à la couche réseau entre deux homologues. Ce protocole se compose du document d'architecture de sécurité IP [RFC2401], de IKE, décrit dans la [RFC2409], de IPsec AH, décrit dans la [RFC2402] et de IPsec ESP, décrit dans la [RFC2406]. IKE est le protocole de gestion de clés 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 requise, il est recommandé que des mécanismes de sécurité supplémentaires tels que IPsec ou TLS [RFC2246] soient utilisés 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 comme mécanisme de transport, le domaine d'application du présent document se limite à L2TP sur les réseaux IP. Les mécanismes exacts pour activer la sécurité pour les réseaux non IP doivent être traités dans les normes appropriées pour L2TP sur les réseaux non IP spécifiques.

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 au serveur de réseau L2TP (LNS, *L2TP Network Server*). Dans le tunnelage volontaire, le NAS n'a pas besoin de prendre L2TP en charge, 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 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 de la part 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 avoir la 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*).

Répondeur : le répondeur 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

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

2. Exigences de sécurité de L2TP

L2TP tunnelle le trafic PPP sur les réseaux publics IP et non IP. Donc, les paquets aussi bien de contrôle que de données du protocole L2TP sont vulnérables aux attaques. Les 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 les paquets (de contrôle et 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 clôturant les connexions PPP ou les tunnels L2TP ;
5 un adversaire peut tenter d'interrompre la négociation PPP ECP afin d'affaiblir ou supprimer la protection de la confidentialité. Autrement, un adversaire peut souhaiter interrompre la négociation de l'authentification PPP LCP afin d'affaiblir le processus PPP d'authentification ou obtenir l'accès aux mots de passe de l'utilisateur.

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

Des 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 les mots de passe du tunnel.

Noter que plusieurs des attaques mentionnées ci-dessus peuvent être effectuées sur des paquets PPP envoyés sur la liaison 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 d'application de la sécurité de L2TP, pour se protéger contre elles, le client DEVRAIT assurer la confidentialité, l'authentification, la protection contre la répétition et de l'intégrité pour les paquets PPP envoyés sur la liaison à numérotation. L'authentification, la protection contre la répétition et de l'intégrité ne sont actuellement pas prises en charge par les méthodes de chiffrement de PPP, décrites dans les [RFC1968], [RFC2419], et [RFC2420].

2.1 Protocole de sécurité 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 fournir 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 fournir une approche adaptable pour la gestion de clés.

Pour satisfaire les exigences mentionnées ci-dessus, toutes les mises en œuvre conformes à la sécurité L2TP DOIVENT mettre en œuvre IPsec ESP pour sécuriser les paquets de contrôle et de données L2TP. Le mode transport DOIT être pris en charge ; le mode tunnel PEUT être pris en charge. Toutes les suites de chiffrement rendues obligatoires par IPsec (décrites dans la [RFC2406] et la [RFC2402]) 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, ce n'est pas un opérateur qui choisit laquelle utiliser. 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 utiliser les mécanismes de protection d'IPsec contre la répétition.

La sécurité L2TP DOIT satisfaire aux exigences de gestion de clé de la suite de protocoles 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*) IPsec [RFC2407].

2.2 Compression et chiffrement sans état

Le chiffrement et/ou la compression sans état sont très souhaitables lorsque L2TP fonctionne sur IP. Comme L2TP est un protocole en mode connexion, l'utilisation de la compression/chiffrement à états pleins est faisable, mais lorsque il fonctionne sur IP, cela n'est pas désirable. Tout en fournissant une meilleure compression, lorsque il est utilisé sans un mécanisme sous-jacent de livraison fiable, 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 de mise en œuvre des schémas de compression/chiffrement à états pleins. Ces considérations ne sont pas aussi importantes lorsque L2TP fonctionne sur un support non IP tels que IEEE 802, ATM, X.25, ou relais de trame, car ces supports garantissent l'ordre et les pertes de paquet sont normalement faibles.

3. Lignes directrices de l'inter opérabilité L2TP/IPsec

Les lignes directrices suivantes sont établies pour satisfaire aux exigences de sécurité de L2TP en utilisant IPsec dans les situations pratiques.

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

Les mécanismes au sein de PPP et de L2TP fournissent la suppression aussi bien en douceur que non en douceur. Dans le cas de PPP, une séquence TermReq et TermAck de protocole de contrôle des liaisons (LCP, *Link Control Protocol*) correspond à une suppression en douceur. Les messages Garder en vie du LCP et les hellos de tunnel L2TP fournissent la capacité de détecter quand une suppression non en douceur s'est produite. Chaque fois que survient un événement de suppression, causant la clôture 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 des deux homologues, toute SA de phase 1 et phase 2 qui existe encore par suite du tunnel L2TP entre les homologues DEVRAIT être supprimée. Des messages de suppression de phase 1 et de 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 cet événement à L2TP. Si l'état de L2TP est tel qu'un accusé de réception de message de longueur de corps zéro (ZLB, *Zero-Length Body*) a été envoyé en réponse à un STOPCCN, cela peut être supposé être un accusé de réception positif que l'homologue a reçu l'accusé de réception de ce ZLB et a effectué la suppression de tout état de tunnel L2TP associé à l'homologue. L'état du tunnel L2TP et tous filtres associés peuvent maintenant être retirés en toute sécurité.

3.2 Questions de fragmentation

Comme la MRU 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. Un mécanisme qui peut être utilisé pour réduire ce problème est de donner à PPP la valeur de MTU de l'interface d'entrée/sortie du tunnel L2TP/IPsec moins la redondance des en-têtes supplémentaires. Cela pourrait survenir après l'établissement du tunnel L2TP mais avant que commencent les négociations de LCP. Si la valeur de MTU de l'interface entrée/sortie pour le tunnel est inférieure à la MRU par défaut de PPP, elle peut remplacer la valeur utilisée. Cette valeur peut aussi être utilisée comme valeur initiale proposée comme MRU dans la demande de configuration LCP.

Si une PMTU ICMP est reçue par IPsec, cette valeur devrait être mémorisée dans la SA comme proposé dans la [RFC2401]. IPsec devrait aussi donner notification de cet événement à L2TP afin que la nouvelle valeur de MTU puisse être reflétée dans l'interface PPP. Toutes les nouvelles découvertes de PTMU vues à l'interface PPP devraient être confrontées 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. vérifier 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 assuré 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 valeurs d'adresses IP et d'accès UDP dans le paquet correspondent aux informations de la prise qui a été utilisée pour établir le tunnel L2TP. Cette étape empêche des homologues malveillants d'usurper des paquets dans les tunnels des autres.

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

Comme IKE/IPsec ignore les nuances de l'application qu'il protège, aucune intégration n'est normalement nécessaire entre l'application et le protocole IPsec. Cependant, les protocoles qui permettent que le numéro d'accès flotte durant les négociations de protocole (comme 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 répondeur à l'initiateur.

Bien que la spécification L2TP actuelle permette au répondeur d'utiliser une nouvelle adresse IP lorsque il envoie la SCCRP, les mises en œuvre qui exigent la protection de L2TP via IPsec NE DEVRAIENT PAS faire cela. Pour permettre ce comportement quand on utilise L2TP et IPsec, lorsque le répondeur choisit une nouvelle adresse IP, il DOIT envoyer un StopCCN à l'initiateur, avec la paire de valeurs d'attributs (AVP, *attribute value pair*) de 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, le message d'erreur facultatif DOIT être présent et le contenu DOIT comporter l'adresse IP (codée en ASCII) que le répondeur désire utiliser pour la suite de la communication. Seule une 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 des codes de résultat et 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 L2TP pour lier les filtres IPsec et la politique au même homologue.

Les détails du filtrage exigés pour s'accommoder de ce comportement ainsi que les autres mécanismes nécessaires pour protéger L2TP avec IPsec sont exposés dans les sections suivantes.

4.1 Négociation IKE phase 1

Selon IKE [RFC2409], lorsque on utilise l'authentification par clé pré partagée, une clé doit être présente pour chaque homologue avec lequel une communication sûre est requise. 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 ne fournit pas la protection de l'identité) la clé pré partagée doit se transposer en un des types d'identifiants 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 pré partagée d'origine 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 pré partagée comme méthode d'authentification pour la phase 1. Lorsque le nombre de points d'extrémité de LAC et de LNS augmente, les clés pré partagée deviennent de plus en plus difficiles à gérer. Chaque fois que possible, l'authentification avec des certificats est préférée.

4.2 Négociation IKE phase 2

Durant les négociations de IKE phase 2, les homologues se mettent d'accord sur le trafic qui est à protéger par les protocoles IPsec. Les identifiants du mode rapide représentent le trafic que les homologues s'accordent à protéger et se composent des informations d'espace d'adresse, de protocole, et d'accès.

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

Accès de l'initiateur	Adresse du répondeur	Accès du répondeur
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 répondeur choisit une nouvelle adresse et un nouveau numéro d'accès. Le flux de messages L2TP qui se produit pour établir cette séquence est le suivant :

--> IKE phase 1 et phase 2 pour protéger la SCCRQ initiale
SCCRQ --> (adresse IP fixe, accès d'initiateur dynamique)
<-- STOPCCN (le répondeur choisit une nouvelle adresse IP)
--> Nouvelle IKE phase 1 et phase 2 pour protéger la nouvelle SCCRQ
SCCRQ --> (SCCRQ à la nouvelle adresse IP du répondeur)
<-- Nouvelle IKE phase 2 pour changer le numéro d'accès par le répondeur
<-- SCCRP (le répondeur choisit un nouveau numéro d'accès)
SCCCN --> (l'établissement du tunnel L2TP est achevé)

Bien que normalement l'initiateur et le répondeur 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 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 qui permettent à L2TP d'injecter des filtres dans la base de données de filtres de IPsec. Cette technique peut être utilisée par toute application qui fait flotter les accès et exige la sécurité via IPsec, et elle est décrite dans les paragraphes qui suivent.

Le répondeur n'est pas obligé de prendre en charge la capacité de faire flotter son adresse IP et son accès. Cependant, l'initiateur DOIT permettre au répondeur de faire flotter son accès et DEVRAIT permettre au répondeur 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 Définitions de terminologie utilisées pour les déclarations de filtrage

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

R-Port numéro de l'accès UDP que le répondeur choisit 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 répondeur utilise après avoir reçu la SCCRQ initiale.

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

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

R-IPAddr adresse IP que le répondeur utilise 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 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 envoyée par l'homologue durant les négociations IKE phase 2. Cette seule adresse peut être formatée comme une seule adresse IP, une adresse Netmask IP avec le Netmask réglé à 255.255.255.255, et une gamme d'adresses IP avec la gamme étant 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 la valeur d'accès dans les identifiants de mode rapide négociés durant IKE phase 2.

Les filtres définis dans les paragraphes qui suivent figurent dans l'ordre décroissant de priorité.

4.2.2 Filtres initiaux nécessaires pour protéger la SCCRQ

Le filtre initial établi sur l'initiateur et le répondeur est nécessaire pour protéger la SCCRQ envoyée par l'initiateur pour ouvrir le tunnel L2TP. L'initiateur et le répondeur doivent tous deux être pré configurés pour ces filtres, ou L2TP doit avoir une méthode pour injecter ces informations dans la base de données de filtrage 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 du répondeur : sortant-1 : aucun. Ils devraient être créés de façon dynamique par IKE à la réussite de l'achèvement de la phase 2.
entrant-1 :de Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Filtres de l'initiateur : sortant-1 : de I-IPAddr, à R-IPAddr1, UDP, src I-Port, dst 1701
entrant-1 : de R-IPAddr1, àI-IPAddr, UDP, src 1701, dst I-Port
entrant-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 de filtre IPsec, une fois que son numéro d'accès de source est connu. Si l'initiateur utilise un accès fixe de 1701, ces filtres PEUVENT être définis de façon statique.

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

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 la SA ne peut pas être établie pour une raison quelconque, le paquet DOIT être éliminé.

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 seront 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 entrant-1 chez le répondeur. 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 de filtre IPsec et associer cet ensemble de filtres avec la SA de phase 2 établie entre les homologues. Ces filtres devraient persister tant que le tunnel L2TP existe. Le nouvel ensemble de filtres chez le répondeur sera :

Filtres de répondeur : sortant-1 : de R-IPAddr1, à I-IPAddr, UDP, src 1701, dst I-Port
entrant-1 : de I-IPAddr, à R-IPAddr1, UDP, src I-Port, dst 1701
entrant-2 : de Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Des mécanismes DEVRAIENT exister entre L2TP et IPsec pour que L2TP ne retransmette pas la SCCRQ pendant l'établissement de la SA. Les mécanismes de retransmission de canal de contrôle de L2TP devraient débuter une fois que la SA a été établie. Cela va aider à éviter des fins de temporisations qui pourraient survenir par suite de lenteurs dans l'établissement de la SA.

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

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

4.2.3 Le répondeur choisit une nouvelle adresse IP

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

La nouvelle adresse que le répondeur 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 répondeur désire utiliser pour la suite de la communication. Seules les adresses IP codées en ASCII devraient être présentes 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.

Le message STOPCCN DOIT être envoyé en utilisant les mêmes informations d'adresse et accès UDP que l'initiateur a utilisé pour envoyer la SCCRQ. Ce message sera protégé en utilisant l'établissement initial de faisceau de SA pour protéger la SCCRQ.

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

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

En supposant que le tunnel initial a été supprimé et que les filtres ont eu besoin de créer le tunnel supprimé, les nouveaux filtres pour l'initiateur et le répondeur seront :

Filtres de l'initiateur : sortant-1 : de I-IPAddr, à R-IPAddr2, UDP, src I-Port, dst 1701
entrant-1 : de R-IPAddr2, à I-IPAddr, UDP, src 1701, dst I-Port
entrant-2 : de R-IPAddr2, à I-IPAddr, UDP, src Any-Port, dst I-Port

Une fois la phase 2 IKE achevée, le nouvel ensemble de filtres chez le répondeur sera :
Filtres du répondeur : sortant-1 : de R-IPAddr2, à I-IPAddr, UDP, src 1701, dst I-Port
entrant-1 : de I-IPAddr, à R-IPAddr2, UDP, src I-Port, dst 1701
entrant-2 : de Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

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

4.2.4 Le répondeur choisit un nouveau numéro d'accès

Le répondeur PEUT choisir un nouvel accès UDP de source pour le trafic du tunnel L2TP. Cette décision DOIT être prise avant d'envoyer la SCCRP. Si un nouveau numéro d'accès est choisi, L2TP doit alors injecter de nouveaux filtres dans la base de données de filtres IPsec. Le répondeur doit commencer de nouvelles négociations IPsec de phase 2 avec l'initiateur.

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

Filtres d'initiateur :

sortant-1 : de I-IPAddr, à R-IPAddr, UDP, src I-Port, dst R-Port
sortant-2 : de I-IPAddr, à R-IPAddr, UDP, src I-Port, dst 1701
entrant-1 : de R-IPAddr, à I-IPAddr, UDP, src R-Port, dst I-Port
entrant-2 : de R-IPAddr, à I-IPAddr, UDP, src 1701, dst I-Port
entrant-3 : de R-IPAddr, à I-IPAddr, UDP, src Any-Port, dst I-Port

Le filtre entrant-1 pour l'initiateur sera injecté par IKE à la réussite de l'achèvement des négociations de phase 2 initiées par l'homologue.

Filtres du répondeur :

sortant-1 : de R-IPAddr, à I-IPAddr, UDP, src R-Port, dst I-Port
sortant-2 : de R-IPAddr, à I-IPAddr, UDP, src 1701, dst I-Port
entrant-1 : de I-IPAddr, à R-IPAddr, UDP, src I-Port, dst R-Port
entrant-2 : de I-IPAddr, à R-IPAddr, UDP, src I-Port, dst 1701
entrant-3 : de Any-Addr, à R-IPAddr1, UDP, src Any-Port, dst 1701

Une fois les négociations achevées, la SCCRP est envoyée et le tunnel L2TP peut termines son établissement. Après l'établissement du tunnel L2TP, toutes les SA résiduelles et leurs filtres associés peuvent être supprimés.

4.2.5 Considérations de passerelle à passerelle et de L2TP numéroté

Dans le scénario de passerelle à passerelle ou de 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 filtre initial DOIT des deux côtés 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 des homologues décide de commencer un tunnel, L2TP devrait injecter les filtres entrants et sortants nécessaires pour protéger la SCCRQ. L'établissement de tunnel se déroule alors exactement comme décrit dans les paragraphes précédents.

5. Considérations sur la sécurité

5.1 Problèmes d'authentification

La négociation IKE d'IPsec DOIT négocier la méthode d'authentification spécifiée dans la [RFC2409]. En plus de l'authentification IKE, les mises en œuvre de L2TP utilisent les méthodes d'authentification de PPP, comme celles décrites dans les [RFC1994]-[RFC2284]. Dans cette section, on discute des questions d'authentification.

5.1.1 Différences d'authentification entre IKE et PPP

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

Avec IPsec, lorsque l'identité affirmée dans IKE est authentifiée, les clés déduites résultantes sont utilisées pour assurer l'authentification, la protection de l'intégrité et contre la répétition paquet par paquet. 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 d'IKE est une identité de machine. Comme seule l'identité de machine est vérifiée paquet par paquet, il n'y a pas de moyen

de vérifier que seul l'utilisateur 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 de mettre en application la ségrégation du trafic. Il en résulte que lorsque l'authentification de machine est utilisée, une fois qu'un tunnel L2TP/IPsec est ouvert, tout usager sur une machine multi-utilisateur va normalement être capable d'envoyer du trafic sur le tunnel.

Si la mise en œuvre IPsec prend en charge l'authentification de l'utilisateur, ce problème peut être écarté. Dans ce cas, l'identité d'utilisateur revendiquée au sein de IKE sera vérifiée paquet par paquet. Afin d'assurer la ségrégation des trafics entre les usagers lorsque l'authentification de l'utilisateur est effectuée, le client DOIT s'assurer que seul le trafic provenant de cet utilisateur particulier est envoyé sur le tunnel L2TP.

5.1.2 Authentification de certificat dans IKE

Lorsque est choisie l'authentification par certificat X.509 au sein de IKE, le LNS est supposé utiliser une charge utile de demande de certificat (CRP, *Certificate Request Payload*) IKE pour demander au client un certificat produit par une autorité de certificat particulière ou peut utiliser plusieurs CRP si plusieurs autorités de certificat sont de confiance et sont configurées dans sa politique d'authentification IKE 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 leur propre accréditif de certificat provenant de l'infrastructure de clés publiques (PKI, *Public-Key Infrastructure*) de leur choix. La vérification de la liste de révocation de certificat du côté client et serveur PEUT être activée sur la base de l'autorité de certification (CA, *Certification Authority*) car des différences de vérification de liste de révocation existent entre les différents fournisseurs de PKI.

Les mises en œuvre de L2TP ne PEUVENT utiliser des accès alloués de façon dynamique pour les accès de source et de destination que 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 machine contre usager 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'engagement. Lorsque les certificats d'usager sont utilisés, le certificat d'usager 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 de faux prétextes, il est conseillé que le processus d'engagement du certificat de machine soit strictement contrôlé. Par exemple, seuls les administrateurs peuvent avoir la capacité d'engager une machine avec un certificat de machine.

Bien que la mémorisation du certificat sur une carte à mémoire diminue la probabilité de 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'usage de matériels non approuvés. Comme l'authentification d'utilisateur peut être fournie au sein de PPP (en se souvenant des faiblesses décrites plus haut) 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 dans lesquelles cette double assurance est considérée comme valable, permettre le mouvement 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 c'est un certificat d'utilisateur qui est utilisé, il est conseillé que le processus d'engagement de l'utilisateur 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) ce certificat n'a alors 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'engagement peut être limitée, après quoi l'accès par le mot de passe sera bloqué. Une telle politique empêche un attaquant qui a obtenu le mot de passe d'un compte inutilisé d'obtenir un certificat d'utilisateur une fois que la période d'engagement est expirée.

5.1.4 Clés pré partagées dans IKE

L'utilisation de clés pré partagées dans le mode principal de IKE est vulnérable aux attaques par interposition lorsque utilisées dans des situations d'accès à distance. Dans le mode principal, il est nécessaire que SKEYID_e soit utilisé avant la

réception de la charge utile d'identification. Donc, le choix de la clé pré partagée ne peut se fonder que sur les informations contenues dans l'en-tête IP. Cependant, dans les situations d'accès à distance, l'allocation dynamique d'adresse IP est normal, de sorte qu'il est souvent impossible d'identifier la clé pré partagée requise sur la base de l'adresse IP.

Donc, lorsque des clés pré partagées sont utilisées dans des scénarios d'accès à distance, la même clé pré partagée est partagée par un groupe d'utilisateurs et ne peut plus 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 pré partagée Cela permet à tous ceux qui ont accès à la clé pré partagée du groupe d'agir comme attaquant interposé.

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

Il en résulte que lorsque le mode principal est utilisé avec des clés pré partagées, sauf si PPP effectue l'authentification mutuelle, le serveur n'est pas authentifié. Cela permet à un serveur pirate en possession de la clé pré partagée de 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 pourrait éventuellement compromettre de nombreux mots de passe en une seule fois. Cette vulnérabilité est présente dans certaines mises en œuvre existantes d'IPsec en mode tunnel.

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

5.2 Interactions de sécurité IPsec/PPP

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

Dans les scénarios ci-dessous, on suppose que les clients et serveurs L2TP sont tous deux capables d'établir et 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 de PPP.

5.2.1 Tunnel obligatoire

Dans le cas d'un tunnel obligatoire, le client envoie des trames PPP au LAC, et va normalement ne pas savoir si les trames vont être tunnelées, ni si des services de sécurité sont en place entre le LAC et le LNS. Au LNS, un paquet de données va arriver, qui comporte 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 du tunnelage obligatoire, le client et le LNS ont une connaissance inégale des services de sécurité en place entre eux.

Comme le LNS est capable de savoir si la protection de la confidentialité, de l'intégrité, l'authentification, et la protection 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 puisse être décrite par un des termes suivants : "Chiffrement exigé," "Chiffrement permis" ou "Chiffrement interdit". Si les services de confidentialité IPsec sont en place, un LNS qui met en œuvre une politique de "Chiffrement interdit" va alors agir comme si la politique avait été violée. De même, un LNS qui met en œuvre une politique de "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. Ceci n'est pas la même chose que d'insister pour que le chiffrement et la compression PPP soient désactivés, car cette 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 ne peut 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 de 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 su le chemin entier ne va pas modifier ce comportement même si il a 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 de s'assurer de la confidentialité sur la portion du chemin entre le LNS et la station terminale.

Normalement, le client ne va pas faire confiance au LAC et va négocier les services de confidentialité et de compression de son côté. Il en résulte que le LAC peut seulement souhaiter négocier IPsec ESP avec le 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 des deux façons suivantes. Si il sait que toutes les stations terminales avec lesquelles il communique sont capables de mettre en œuvre IPsec (ou si il refuse de parler aux stations terminales qui n'ont pas la capacité IPsec) il peut alors refuser de négocier le chiffrement/compression PPP et négocier à la place IPsec ESP avec les stations terminales. Si le client ne sait pas si toutes les stations terminales qu'il va contacter ont la capacité IPsec (le cas le plus probable) il va alors négocier le chiffrement/compression PPP. Il peut en résulter une duplication de la compression/chiffrement qui ne peut être éliminée que si la compression/chiffrement PPP peut être désactivée paquet par paquet. Noter que comme le LNS sait que les paquets du client vont être 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 de 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, ces paquets L2TP vont être 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-même et le LNS. Il aura aussi connaissance des services de chiffrement/compression PPP négociés entre lui-même et le NAS.

Du point de vue du LNS, on va noter une trame PPP encapsulée dans L2TP, qui est lui-même encapsulé dans un paquet IP. Cette situation est identique au cas du tunnelage obligatoire. Si le LNS restitue les propriétés de l'association de sécurité établie entre lui-même 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 de l'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 de 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-même et le LNS, il peut agir comme si une directive "Chiffrement exigé" avait été satisfaite si IPsec ESP était déjà en place entre lui-même 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 va normalement être souhaitable de désactiver la compression PPP si aucune méthode sans état n'est disponible, à cause des 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 les services de confidentialité, d'authentification, et de protection de l'intégrité IPsec à la place, ainsi que la compression IP, si elle est disponible.

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

Noter aussi que le client peut souhaiter mettre en place des services de confidentialité pour les paquets non tunnelés qui passent à travers lui-même et le NAS. Cela va protéger le client contre l'espionnage sur le réseau entre lui-même et le NAS. Il en résulte qu'il peut souhaiter négocier le chiffrement et la compression PPP avec le NAS. Comme dans le tunnelage obligatoire, cela va donner 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) *(Info.)*

[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, John Richardson de Intel et Rob Adams de Cisco pour les utiles discussions de cet espace deproblème.

Adresses 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 d'ensemble de filtres IPsec pour l'établissement de tunnel L2TP

Cette section donne des exemples d'ensembles de filtres IPsec pour l'établissement de tunnel L2TP. Bien que l'exemple d'ensemble de filtres soit pour IPv4, des exemples similaires pourraient tout aussi facilement être construits pour IPv6.

A.1 L'initiateur et le répondeur utilisent des adresses et accès fixés

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

sortant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
entrant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
entrant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondeur :

sortant-1 : aucun, injection dynamique lorsque s'achève IKE phase 2
entrant-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 répondeur seront :

Filtres d'initiateur :

sortant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
entrant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
entrant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondeur :

sortant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 1701
entrant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 1701, dst 1701
entrant-2 : de Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

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

Dans ce scénario, il est permis à l'un et l'autre côté d'initier le tunnel. Comme on va utiliser des accès dynamiques, une négociation de phase 2 supplémentaire doit avoir lieu pour protéger la SCCRP envoyée du répondeur à l'initiateur. À part l'établissement de la phase 2 supplémentaire, la seule autre différence est que L2TP chez le répondeur doit injecter un filtre supplémentaire dans la base de données IPsec une fois choisi le nouveau numéro d'accès.

Cet exemple montre aussi le filtre supplémentaire nécessaire pour l'initiateur qui permet que l'un ou l'autre côté commence le tunnel. Que ce soit dans le scénario à numérotage ou dans celui de passerelle à passerelle, ce filtre supplémentaire est nécessaire.

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

Pour ce scénario, les filtres sont :

A.2.1 Les filtres initiaux permettent aux deux côtés 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 sur laquelle l'appareil va accepter les négociations L2TP.

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

Note : l'adresse IP de source dans le filtre entrant-1 ci-dessus pour les tunnels de passerelle à passerelle peut être spécifique de IP, comme 1.1.1.1, et pas nécessairement Any-Addr.

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

Filtres d'initiateur :
sortant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
entrant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
entrant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 5000
entrant-3 : de Any-Addr, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondeur :
sortant-1 : aucun, injection dynamique à l'achèvement de IKE phase 2.
entrant-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 répondeur seront :

Filtres d'initiateur :
sortant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
entrant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
entrant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 5000
entrant-3 : de Any-Addr, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondeur :
sortant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
entrant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
entrant-2 : de Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

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

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

Le nouvel ensemble de filtres chez le répondeur est :

Filtres de répondeur :
sortant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000
sortant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
entrant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 6000
entrant-2 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
entrant-3 : de Any-Addr, à 2.2.2.1, UDP, src Any-Port, dst 1701

La seconde phase 2 va débuter une fois que L2TP aura envoyé la SCCRP. À l'achèvement des négociations de phase 2, le nouvel ensemble de filtres chez l'initiateur et le répondeur sera :

Filtres d'initiateur :
sortant-1 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 6000
sortant-2 : de 1.1.1.1, à 2.2.2.1, UDP, src 5000, dst 1701
entrant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000
entrant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000
entrant-3 : de 2.2.2.1, à 1.1.1.1, UDP, src Any-Port, dst 1701

Filtres de répondeur :
sortant-1 : de 2.2.2.1, à 1.1.1.1, UDP, src 6000, dst 5000
sortant-2 : de 2.2.2.1, à 1.1.1.1, UDP, src 1701, dst 5000

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

Une fois réussi l'établissement du tunnel L2TP, la phase 2 d'origine peut être supprimée. Cela permet aussi de retirer les déclarations de filtre entrant-2 et sortant-2.

Déclaration de propriété intellectuelle

Déclaration complète de droits de reproduction

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