Groupe de travail Réseau
Request for Comments: 5619
Catégorie : Sur la voie de la normalisation

Traduction Claude Brière de L'Isle

S. Yamamoto, NICT/KDDI R&D Labs
C. Williams, KDDI R&D Labs
H. Yokota, KDDI R&D Labs
F. Parent, Beon Solutions
août 2009

Analyse et exigences de sécurité pour les passages logiciels

Résumé
Le présent document décrit les lignes directrices de sécurité pour les solutions de passage logiciel de "centres et rayons" *(Hubs and Spokes)* et de "maillage" *(Mesh)*. Avec la discussion des scénarios de déploiement de passages logiciels, la vulnérabilité aux attaques contre la sécurité est analysée pour fournir des mécanismes de protection de la sécurité comme l'authentification, la protection de l'intégrité et de la confidentialité au contrôle de passage logiciel et aux paquets de données.

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet sur la voie de la normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Table des matières

1. Introduction

Le groupe de travail Softwire (passage logiciel) spécifie la normalisation des méthodes de découverte, contrôle, et encapsulation pour connecter des réseaux IPv4 à travers des réseaux IPv6 et des réseaux IPv6 à travers des réseaux IPv4. Le passage logiciel fournit la connexité pour permettre l'accessibilité globale des deux familles d'adresses en réutilisant ou étendant la technologie existante. Le groupe de travail Softwire se concentre sur les deux scénarios qui ont émergé de la discussion de la traversée des réseaux composés de différentes familles d'adresses. Le présent document fournit les lignes directrices de sécurité pour deux espaces de telles solutions de passage logiciel : les scénarios de "centre et rayons" *(Hubs and Spokes)* et de "maillage" *(Mesh)*. Les problèmes de "centre et rayons" et de "maillage" sont décrits dans la [RFC4925], respectivement dans les Sections 2 et 3. Les protocoles choisis pour la connexité de passage logiciel exigent des considérations de sécurité sur des scénarios de déploiement plus spécifiques pour chaque solution. La portée du présent document fournit l'analyse des faiblesses de sécurité pour les scénarios de déploiement et spécifie l'usage approprié des mécanismes de sécurité qui sont appliqués au déploiement de passage logiciel.

Le protocole de tunnelage de couche 2 (L2TPv2, *Layer Two Tunneling Protocol*) est choisi comme protocole de phase 1 à déployer dans l'espace de solution de "centre et rayons". Si L2TPv2 est utilisé dans le réseau non protégé, il va être vulnérable à diverses attaques et DOIT être protégé par un protocole de sécurité approprié, comme IPsec décrit dans la [RFC3193]. Une nouvelle mise en œuvre DEVRAIT utiliser la version 2 du protocole d'échange de clés Internet (IKEv2, *Internet Key Exchange Protocol version 2*) comme protocole de gestion de clés parce que c'est un protocole plus fiable que IKEv1 et qu'il intègre les protocoles exigés dans une seule plate-forme. Le présent document fournit des lignes directrices de mise en œuvre et spécifie l'usage approprié de IPsec comme mécanisme de protection de la sécurité en examinant les faiblesses de la sécurité dans le scénario de "centre et rayons". Le document traite aussi des cas où le protocole de sécurité n'est pas nécessairement obligatoire.

La solution "maillage" de passage logiciel DOIT prendre en charge divers niveaux de mécanismes de sécurité pour protéger les paquets de données transmis sur un tunnel de passage logiciel depuis les réseaux d'accès avec une famille d'adresses à travers le cœur de transit fonctionnant avec une famille d'adresses différente [RFC4925]. Le mécanisme de sécurité pour le plan de contrôle est aussi exigé pour être protégé d'une modification des données de contrôle, d'attaques en usurpation d'identité, etc. Dans la solution "maillage", BGP est utilisé pour distribuer les informations d'acheminement de passage logiciel dans le cœur de transit ; les questions de sécurité pour BGP sont discutées dans d'autres groupes de travail. Le présent document fournit l'utilisation appropriée des mécanismes de sécurité pour les scénarios de déploiement de maillage de passages logiciels.

2. Terminologie

2.1 Abréviations

La terminologie se fonde sur la [RFC4925] "Position du problème du passage logiciel".

AF(i) *(Address Family)* : famille d'adresses, IPv4 ou IPv6. Notation utilisée pour indiquer que les préfixes, un nœud, ou un réseau traitent seulement d'une seule AF IP.

AF(i,j) - Notation utilisée pour indiquer qu'un nœud est double pile ou qu'un réseau est composé de nœuds double pile.

AFBR *(Address Family Border Router)* : routeur bordure de famille d'adresses. Routeur double pile qui interconnecte deux réseaux qui utilisent la même famille d'adresses ou des familles différentes. Un AFBR forme des relations d'échange de trafic avec les autres AFBR, des routeurs de cœur adjacents, et des routeurs rattachés côté client (CE, *Customer Edge*) effectue la découverte et la signalisation de passage logiciel, annonce les informations d'accessibilité de client ASF(i) et encapsule/désencapsule les paquets de client dans les en-têtes de transport de passage logiciel.

CE *(Customer Edge)* : côté client. Routeur situé à l'intérieur d'une île d'accès d'AF qui échange du trafic avec d'autres routeurs CE au sein du réseau de l'île d'accès et avec un ou plusieurs AFBR en amont.

CPE *(Customer Premise Equipment)* : équipement d'installation d'abonné. Équipement, hôte ou routeur, situé dans les locaux d'un abonné et connecté au réseau d'accès d'un transporteur.

PE *(Provider Edge)* : côté fournisseur. Routeur situé à la bordure d'un réseau cœur de transit qui fait l'interface avec le CE dans un îlot d'accès.

SC *(Softwire Concentrator)* : concentrateur de passage logiciel. Nœud qui termine le passage logiciel dans le réseau du fournisseur de service.

SI *(Softwire Initiator)* : initiateur de passage logiciel. Nœud qui initie le passage logiciel au sein du réseau du client.

SW-Encap *(Softwire Encapsulation Set)* : ensemble d'encapsulation de passage logiciel. Il contient les paramètres d'en-tête de tunnel, l'ordre de préférence des types d'en-tête de tunnel, et les types de charge utile attendus (par exemple, IPv4) portés dans le passage logiciel.

SW-NHOP *(Softwire Next_Hop)* : prochain bond de passage logiciel. Cet attribut accompagne les annonces d'accessibilité d'AF de client et est utilisé pour faire référence à un passage logiciel sur l'entrée d'AFBR conduisant aux préfixes spécifiques. Il contient une valeur d'identifiant de passage logiciel et une adresse IP de prochain bond de passage logiciel notées comme adresse <SW ID:SW-NHOP>. Son existence dans la présence des préfixes d'AF de client (dans les annonces ou entrées dans un tableau d'acheminement) implique l'utilisation d'un passage logiciel pour atteindre ce préfixe.

2.2 Langage des exigences

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

3. Lignes directrices pour la sécurité des noyaux et rayons

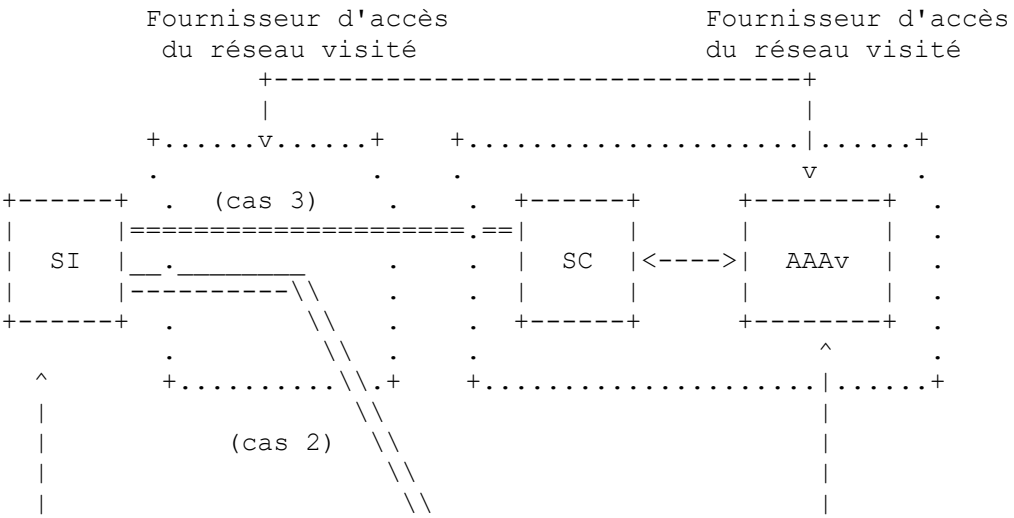
3.1 Scénarios de déploiement

Pour fournir les lignes directrices de sécurité, la discussion du scénario possible de déploiement et la relation de confiance dans le réseau est importante.

L'initiateur de passage logiciel (SI) réside toujours dans le réseau client. Le nœud dans lequel réside le SI peut être l'appareil d'accès du CPE, un autre routeur CPE dédié derrière l'appareil d'accès de CPE d'origine, ou toute sorte d'appareil hôte, comme un ordinateur individuel une application, un détecteur, etc.

Cependant, l'appareil hôte ne peut pas toujours avoir un accès direct à son réseau transporteur de rattachement, auquel l'utilisateur s'est abonné. Par exemple, le SI dans l'ordinateur individuel portable peut accéder à divers réseaux d'accès comme des points d'accès Wi-Fi, des réseaux d'entreprise visités, etc. C'est le cas du nomadisme, que le passage logiciel DEVRAIT prendre en charge.

Comme modèle de déploiement de passage logiciel, les trois cas suivants montrés dans la Figure 1 devraient être examinés. Les cas 2 et 3 sont typiques d'un mode nomade, mais sont aussi applicables à un nœud stationnaire. Afin de connecter en toute sécurité l'un à l'autre un SI et un SC légitimes, le processus d'authentification entre SI et SC est normalement effectué en utilisant des serveurs d'authentification, autorisation, et comptabilité (AAA).



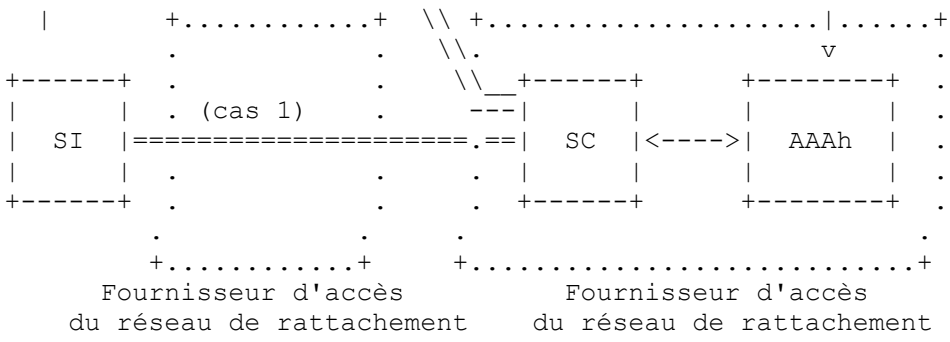


Figure 1 : Modèle d'authentification pour centre et rayons

Le serveur AAA montré à la Figure 1 interagit avec le SC, qui agit comme client AAA. L'AAA peut consister en plusieurs serveurs AAA, et le mandataire AAA peut être intermédiaire entre le SC et les serveurs AAA. Le présent document se réfère au serveur AAA dans le fournisseur de service de réseau de rattachement comme serveur AAA de rattachement (AAAh) et à celui du fournisseur de service de réseau visité comme au serveur AAA visité (AAAv).

La [RFC4925] "Position du problème du passage logiciel" déclare que la solution de passage logiciel doit être capable de s'intégrer aux solutions d'AAA actuellement déployées. L2TPv2 utilisé dans le passage logiciel prend en charge les authentifications PPP et L2TP qui peuvent être intégrées avec des serveurs AAA courants.

Quand le passage logiciel est utilisé dans un réseau non protégé, un processus d'authentification plus fort est exigé (par exemple, IKEv2). Le choix approprié des processus d'authentification est discuté au paragraphe 3.4 à l'égard des diverses menaces pour la sécurité.

Cas 1 : le SI se connecte au SC qui appartient au fournisseur de service du réseau de rattachement via le réseau du fournisseur d'accès de rattachement qui fonctionne avec une famille d'adresses différente. On suppose que le réseau du fournisseur d'accès de rattachement et le fournisseur de service du réseau de rattachement pour le SC sont sous le même système administratif.

Noter que l'adresse IP de l'appareil hôte, dans lequel le SI réside, est statique ou dynamique selon le service souscrit. La découverte du SC peut être automatique. Mais dans ce document, les informations sur le SC, par exemple, le nom dans le DNS ou l'adresse IP, sont supposées être configurées à l'avance par l'utilisateur ou le fournisseur du SI.

Cas 2 : le SI se connecte au SC qui appartient au fournisseur de service du réseau de rattachement via le réseau d'accès visité. Dans le cas de nomadisme, le SI/utilisateur ne s'abonne pas au fournisseur d'accès visité. Pour l'accès réseau par le réseau public, comme des points d'accès Wi-Fi, le fournisseur de service du réseau de rattachement n'a pas de relation de confiance avec le réseau d'accès.

Noter que l'adresse IP de l'appareil hôte, dans lequel le SI réside, peut être changée périodiquement du fait de la politique du fournisseur de service du réseau de rattachement.

Cas 3 : le SI se connecte au SC qui appartient au fournisseur de service du réseau visité via le réseau d'accès visité. C'est typique du cas d'accès nomade. Quand le SI est mobile, il peut circuler du FAI de rattachement qui fournit le réseau d'accès de rattachement, au réseau d'accès visité, par exemple, le réseau de point d'accès de Wi-Fi fourni par le FAI différent. Le SI ne se connecte pas au SC dans le réseau de rattachement, par exemple, pour des raisons géographiques. Le SI/utilisateur ne s'abonne pas au fournisseur de service du réseau visité, mais le fournisseur de service du réseau visité a un accord d'itinérance avec le fournisseur de service du réseau de rattachement.

Noter que l'adresse IP de l'hôte, dans lequel réside le SI, est fournie avec la politique du fournisseur de service du réseau visité.

3.2 Relation de confiance

L'établissement d'une relation de confiance entre le SI et le SC est différent dans trois cas. Les considérations de sécurité doivent être prises en compte pour chaque cas.

Dans le cas 1, le SC et le serveur AAA de rattachement dans le même fournisseur de service réseau DOIVENT avoir une

relation de confiance et les communications entre eux DOIVENT être sécurisées. Quand le SC s'authentifie auprès du SI, le SC transmet le message de demande d'authentification au serveur AAA de rattachement et obtient le message d'acceptation avec la paire d'attribut-valeur pour l'authentification du SI. Comme le SI est dans le réseau du fournisseur de service, le fournisseur peut prendre des mesures pour protéger les entités (par exemple, le SC, les serveurs AAA) contre un certain nombre de menaces pour la sécurité, y compris les communications entre eux.

Dans le cas 2, quand le SI est mobile, l'accès au fournisseur de service du réseau de rattachement à travers le fournisseur du réseau d'accès visité est permis. La relation de confiance entre le SI et le SC dans le réseau de rattachement DOIT être établie. Quand le réseau d'accès visité est un réseau public, diverses attaques doivent être considérées. En particulier pour que le SI se connecte au SC légitime, l'authentification du SI au SC DOIT être effectuée avec celle du SC au SI.

Dans le cas 3, si le SI passe sur le domaine administratif d'un fournisseur de service réseau différent, le serveur AAA visité communique avec le serveur AAA de rattachement pour obtenir les informations pour l'authentification du SI. Le serveur AAA visité DOIT avoir une relation de confiance avec le serveur AAA de rattachement et la communication entre eux DOIT être sécurisée afin d'effectuer de façon appropriée les services d'itinérance qui ont été acceptés dans des conditions spécifiées.

Noter que le chemin pour les communications entre le serveur AAA de rattachement et le serveur AAA visité peut consister en plusieurs mandataires AAA. Dans ce cas, le modèle de menaces de mandataire AAA DEVRAIT être considéré [RFC2607]. Un mandataire AAA malveillant peut lancer des attaques passives ou actives contre la sécurité. La fiabilité des mandataires dans les chaînes de mandataires AAA va s'affaiblir quand le compte de bonds de la chaîne de mandataires est plus long. Par exemple, les informations de comptabilité échangées parmi les mandataires AAA sont attirantes pour un adversaire. La communication entre un serveur AAA de rattachement et un serveur AAA visité DOIT être protégée.

3.3 Scénarios de menaces pour la sécurité des passages logiciels

Le passage logiciel peut être utilisé pour connecter des réseaux IPv6 à travers des réseaux publics IPv4 et des réseaux IPv4 à travers des réseaux IPv6 publics. Les paquets de contrôle et de données utilisés durant la session de passage logiciel sont vulnérables à des attaques contre la sécurité.

Une analyse complète des menaces sur le passage logiciel exige l'examen des protocoles utilisés pour l'établissement du passage logiciel, de la méthode d'encapsulation utilisée pour transporter la charge utile, et des autres protocoles utilisés pour la configuration (par exemple, les annonces de routeur, DHCP).

La solution de passage logiciel utilise un sous ensemble des fonctionnalités du protocole de tunnelage de couche deux (L2TPv2, *Layer Two Tunneling Protocol*) ([RFC2661], [RFC5571]). Dans le modèle "centre et rayons" de passage logiciel, L2TPv2 est utilisé seulement dans un modèle volontaire de tunnel. Le SI agit comme un concentrateur d'accès L2TP (LAC, *L2TP Access Concentrator*) et un point d'extrémité PPP. Le tunnel L2TPv2 est toujours initié par le SI.

L'analyse générique de menace faite pour L2TP en utilisant IPsec [RFC3193] est applicable aux déploiement de "centre et rayons" de passage logiciel. Les analyses de menaces pour d'autres protocoles tels que IPv6 mobile (MIPv6, *Mobile IPv6*) [RFC4225], le protocole de transport d'authentification et d'accès au réseau (PANA, *Protocol for Carrying Authentication for Network Access*) [RFC4016], les prochaines étapes de la signalisation (NSIS, *Next Steps in Signaling*) [RFC4081], et les protocoles d'acheminement [RFC4593] sont applicables ici aussi et devraient être utilisées comme références.

D'abord, le SI qui réside sur le réseau client envoie un paquet de demande de début de connexion de contrôle (SCCRQ, *Start-Control-Connection-Request*) au SC pour initier le passage logiciel. L2TPv2 offre un système facultatif d'authentification de tunnel (similaire à celui du protocole d'authentification par dialogue à énigme (CHAP, *Challenge Handshake Authentication Protocol*) durant l'établissement de la connexion de contrôle. Cela exige un secret partagé entre le SI et le SC et aucune gestion de clé n'est offerte pour ce L2TPv2.

Quand la connexion de contrôle L2TPv2 est établie, le SI et le SC entrent facultativement dans la phase d'authentification après avoir achevé la négociation du protocole de contrôle de liaison (LCP, *Link Control Protocol*) PPP. L'authentification PPP accepte l'authentification CHAP unidirectionnelle ou bidirectionnelle, et peut renforcer l'infrastructure AAA existante. L'authentification PPP n'assure pas l'authentification par paquet.

Le chiffrement PPP est défini mais la négociation du protocole de contrôle de chiffrement (ECP, *Encryption Control Protocol*) PPP n'assure pas une négociation de suite de chiffrement protégée. Le chiffrement PPP fournit une solution de sécurité faible [RFC3193]. Une mise en œuvre ECP de PPP ne peut pas être attendue. L'authentification PPP ne fournit pas non plus de gestion de clé adaptable.

Une fois la configuration du tunnel L2TPv2 et de PPP établies, le SI est connecté et peut commencer à utiliser la connexion.

Ces étapes sont vulnérables à des attaques par interposition (MITM, *man-in-the-middle*), déni de service (DoS), et vol de service, qui sont causées par les actions suivantes de l'adversaire.

Les attaques d'adversaires sur le passage logiciel incluent :

1. Un adversaire peut essayer de découvrir les identités et autres informations confidentielles en espionnant les paquets de données.

2. Un adversaire peut essayer de modifier les paquets de contrôle et de données. Ce type d'attaque implique des violations de l'intégrité.

3. Un adversaire peut essayer d'espionner et collecter les messages de contrôle. En répétant ces messages, un adversaire peut réussir à capturer le tunnel L2TP ou la connexion PPP à l'intérieur du tunnel. Un adversaire pourrait monter des attaques de MITM, de DoS, et de vol de service.

4. Un adversaire peut inonder le nœud de passage logiciel avec des messages de signalisation bogués pour causer des attaques de DoS en terminant les tunnels L2TP ou les connexions PPP.

5. Un adversaire peut tenter de perturber la négociation de passage logiciel afin d'affaiblir ou supprimer la protection de la confidentialité.

6. Un adversaire peut souhaiter perturber la négociation d'authentification de LCP PPP.

Quand des serveurs AAA sont impliqués dans l'établissement d'un tunnel de passage logiciel, les attaques contre la sécurité peuvent être montées sur la communication associée à des serveurs AAA. Précisément, pour le cas 3 mentionné au paragraphe 3.2, un adversaire peut espionner les paquets entre des serveurs AAA dans le réseau de rattachement et visité et compromettre les données d'authentification. Un adversaire peut aussi perturber la communication entre les serveurs AAA, causant un déni de service. La sécurité des communications de serveur AAA sort du domaine d'application du présent document.

Dans des environnements où la liaison est partagée sans protection cryptographique et où une authentification faible ou unidirectionnelle est utilisée, ces attaques contre la sécurité peuvent être montées sur les paquets de contrôle et de données de passage logiciel.

Quand il n'y a pas de relation de confiance préalable entre le SI et le SC, tout nœud peut prétendre être un SC. Dans ce cas, un adversaire peut se faire passer pour le SC pour intercepter le trafic (par exemple, un concentrateur de passage logiciel "félon").

Le SC félon peut introduire une attaque de déni de service en mettant les paquets provenant du SI dans un trou noir. Le SC félon peut aussi espionner tous les paquets envoyés du ou vers le SI. Les menaces sur la sécurité d'un SC félon sont similaires à celles d'un routeur compromis.

Le déploiement d'un filtrage d'entrée est capable de contrôler l'accès d'utilisateurs malveillants [RFC4213]. Sans vérifications spécifiques de filtrage d'entrée dans le désencapsuleur chez le SC, il serait possible à un attaquant d'injecter un faux paquet, laissant le système vulnérable à des attaques comme le DoS. En utilisant un filtrage d'entrée, des adresses internes invalides peuvent être rejetées. Sans filtrage d'entrée des adresses internes, une autre sorte d'attaque peut se produire. Les utilisateurs malveillants d'un autre FAI pourraient commencer en utilisant son infrastructure de tunnelage pour obtenir une connexité gratuite aux adresses internes, transformant effectivement le FAI en un fournisseur de transit d'adresse internes.

Le filtrage d'entrée ne fournit pas une protection complète dans le cas où une usurpation d'adresse s'est produite. Afin de fournir une meilleure protection contre l'usurpation d'adresse, l'authentification avec lien entre l'adresse légitime et l'identité authentifiée DOIT être mise en œuvre. Cela peut être mis en œuvre entre le SC et le SI en utilisant IPsec.

3.4 Lignes directrices pour la sécurité des passages logiciels

Sur la base de l'analyse des menaces sur la sécurité du paragraphe 3.3 du présent document, le protocole de sécurité du passage logiciel DOIT prendre en charge les protections suivantes :

1. Les messages de contrôle de passage logiciel entre SI et SC DOIVENT être protégés contre les espions et les attaques d'usurpation d'identité.

2. Le protocole de sécurité de passage logiciel DOIT être capable de se protéger contre des attaques en répétition.

3. Le protocole de sécurité de passage logiciel DOIT être capable de protéger l'identifiant d'appareil contre l'usurpation d'identité quand il est échangé entre le SI et le SC.

4. Le protocole de sécurité de passage logiciel DOIT être capable lier de façon sûre la session authentifiée à l'identifiant d'appareil du client, pour empêcher le vol de service.

5. Le protocole de sécurité de passage logiciel DOIT être capable de protéger les messages contre la déconnexion et la révocation.

L'exigence du protocole de sécurité de passage logiciel est comparable à celle de la [RFC3193].

Pour les paquets de contrôle de passage logiciel, l'authentification, la protection de l'intégrité et contre la répétition DOIVENT être prises en charge, et la confidentialité DEVRAIT être prise en charge.

Pour les paquets de données de passage logiciel, l'authentification, la protection de l'intégrité et contre la répétition DEVRAIENT être prises en charge, et la confidentialité PEUT être prise en charge.

La [RFC4925] "Déclaration du problème du passage logiciel" fournit des exigences pour la solution de "centre et rayons" qui sont prises en compte pour définir les mécanismes de protection de la sécurité.

1. Le plan de contrôle et/ou de données DOIT être capable de fournir une pleine sécurité de la charge utile quand elle est désirée.

2. La technologie déployée DOIT être examinée très attentivement.

Cette protection supplémentaire de la sécurité doit être séparable du mécanisme de tunnelage du passage logiciel.

Noter que la portée de cette sécurité est sur le tunnel L2TP entre SI et SC. Si une sécurité de bout en bout est exigée, un protocole de sécurité DEVRAIT être utilisé dans les paquets de charge utile. Mais ceci sort du domaine d'application du présent document.

3.4.1 Authentification

Le protocole de sécurité de passage logiciel DOIT prendre en charge l'authentification d'utilisateur dans le plan de contrôle afin d'autoriser l'accès au service et fournir un enregistrement adéquat de l'activité. Bien que plusieurs protocoles d'authentification soient disponibles, les menaces sur la sécurité doivent être examinées pour le choix du protocole.

Par exemple, considérons un SI/utilisateur qui se sert d'un accès par le protocole d'authentification par mot de passe (PAP, *Password Authentication Protocol*) au SC avec un mot de passe en clair. Dans de nombreuses circonstances, cela représente un grand risque pour la sécurité. L'adversaire peut se faire passer pour un utilisateur légitime en utilisant le mot de passe volé. Le protocole d'authentification par défi à énigme (CHAP, *Challenge Handshake Authentication Protocol*) [RFC1994] chiffre un mot de passe avec un "défi" envoyé du SC. Le vol du mot de passe peut être atténué. Cependant, comme CHAP prend seulement en charge l'authentification unidirectionnelle, le risque d'une interposition ou d'un SC félon ne peut pas être écarté. Le protocole d'authentification extensible de sécurité de la couche transport (EAP-TLS, *Extensible Authentication Protocol-Transport Layer Security*) [RFC5216] rend obligatoire l'authentification mutuelle et évite les SC félons.

Quand le SI a établi une connexion au SC par un public réseau, le SI peut vouloir prouver l'identité du SC. Le passage logiciel DOIT prendre en charge l'authentification mutuelle pour permettre un tel scénario.

Dans certaines circonstances cependant, le fournisseur de service peut décider de permettre une connexion non authentifiée

[RFC5571]. Par exemple, quand le client est déjà authentifié par d'autres moyens, comme des réseaux fermés, des réseaux cellulaires à la couche 2, etc., le fournisseur de service peut décider de désactiver l'authentification. Si aucune authentification n'est effectuée sur une couche, le SC agit comme une passerelle pour des connexions anonymes. Le fonctionnement d'un tel service DOIT être configurable par l'administrateur du SC et le SC DEVRAIT prendre des mesures de sécurité, comme un filtrage d'entrée et un enregistrement adéquat de l'activité. On devrait noter que le service de connexion anonyme ne peut pas fournir les fonctions de sécurité décrites dans le présent document (par exemple, la protection de l'intégrité, contre la répétition, et la confidentialité).

L2TPv2 choisi comme protocole de phase 1 de passage logiciel prend en charge l'authentification PPP et L2TPv2. L'authentification PPP et L2TPv2 subissent diverses menaces sur la sécurité, comme déclaré au paragraphe 3.3. Elles vont être utilisées dans les conditions limitées décrites dans les paragraphes qui suivent.

3.4.1.1 Authentification PPP

PPP peut fournir l'authentification mutuelle entre le SI et le SC en utilisant CHAP [RFC1994] durant la phase d'établissement de la connexion (via le protocole de contrôle de liaison, LCP). L'authentification CHAP de PPP peut être utilisée quand le SI et le SC sont sur un réseau IP de confiance, non public.

Comme CHAP ne fournit pas d'authentification, de protection d'intégrité ou contre la répétition, par paquet PPP, l'authentification CHAP NE DOIT PAS être utilisée non protégée sur un réseau IP public. Si d'autres mécanismes protégés appropriés ont déjà été appliqués, l'authentification CHAP PPP PEUT être utilisée.

Facultativement, d'autres méthodes d'authentification comme PAP, MS-CHAP, et EAP PEUVENT être acceptées.

3.4.1.2 Authentification L2TPv2

L2TPv2 fournit une authentification facultative de tunnel de style CHAP durant l'établissement de la connexion de contrôle [RFC2661], paragraphe 5.1.1. L'authentification L2TPv2 NE DOIT PAS être utilisée non protégée sur un réseau IP public, la même restriction étant appliquée à l'authentification CHAP PPP.

3.4.2 Protocole de sécurité de passage logiciel

Pour satisfaire les exigences ci-dessus, toutes les mises en œuvre qui se conforment à la sécurité de passage logiciel DOIVENT mettre en œuvre les protocoles de sécurité suivants.

IPsec ESP [RFC4303] en mode transport est utilisé pour sécuriser les paquets de contrôle et de données de passage logiciel. Le protocole d'échange de clé Internet (IKE, *Internet Key Exchange*) [RFC4306] DOIT être pris en charge pour l'authentification, la négociation d'association de sécurité, et la gestion de clés pour IPsec. L'applicabilité des différentes versions de IKE est discutée au paragraphe 3.5.

Le protocole de sécurité de passage logiciel DOIT prendre en charge la traversée de NAT. L'encapsulation UDP de paquets ESP IPsec [RFC3948] et la négociation de la traversée de NAT dans IKE [RFC3947] DOIVENT être supportées quand IPsec est utilisé.

3.5 Lignes directrices pour l'usage de IPsec dans les passages logiciels

Quand la solution de passage logiciel "centre et rayons" mise en œuvre par L2TPv2 est utilisée dans un réseau qui n'est pas de confiance, le passage logiciel DOIT être protégé par des protocoles de sécurité appropriés, comme IPsec. Ce paragraphe fournit des lignes directrices pour l'usage de IPsec dans les passages logiciels fondés sur L2TPv2.

La [RFC3193] discute de la façon dont L2TP peut utiliser IKE [RFC2409] et IPsec [RFC2401] pour fournir l'authentification de tunnel, la protection de la confidentialité, la vérification de l'intégrité, et la protection contre la répétition. Depuis la publication de la [RFC3193], des révisions des protocoles IPsec ont été publiées (IKEv2 [RFC4306], ESP [RFC4303], traversée de NAT pour IKE [RFC3947] et ESP [RFC3948]).

Étant donné que la technologie déployée doit être très fortement considérée [RFC4925] pour que la solution réponde aux besoins du marché, la [RFC3193] DOIT être prise en charge. Cependant, une nouvelle mise en œuvre DEVRAIT utiliser IKEv2 [RFC4306] pour IPsec parce que il a de nombreux avantages sur IKE [RFC2409]. Dans les nouveaux déploiements,

IKEv2 DEVRAIT être utilisé aussi.

Bien que la [RFC3193] puisse être appliquée dans la solution "centre et rayons" de passage logiciel, des exigences de passage logiciel telles que la traversée de NAT, la traversée de NAT pour IKE [RFC3947] et ESP [RFC3948] DOIVENT être prises en charge.

Pendant ce temps, IKEv2 [RFC4306] intègre la traversée de NAT. IKEv2 prend aussi en charge l'authentification EAP, avec l'authentification qui utilise des secrets partagés (clé pré-partagée) ou une signature (certificat) à clé publique.

Le choix de clé pré-partagée ou de certificat dépend de l'état du réseau pour lequel le passage logiciel va être déployé, comme décrit au paragraphe 3.5.2. Cependant, les clés pré-partagées et les certificats acceptent seulement l'authentification de la machine. Quand l'authentification de la machine et de l'utilisateur sont exigées comme, par exemple, dans le cas de nomadisme, EAP DEVRAIT être utilisé.

Avec EAP, IKEv2 [RFC4306] prend en charge les méthodes d'authentification traditionnelles qui peuvent être utiles dans des environnements où l'authentification fondée sur le nom d'utilisateur et le mot de passe est déjà déployée.

IKEv2 est un protocole plus fiable que IKE [RFC2409] en termes de capacité de protection contre la répétition, de mécanisme de protection activés contre le DoS, etc. Donc, les nouvelles mises en œuvre DEVRAIENT utiliser IKEv2 plutôt que IKE.

Les paragraphes qui suivent vont discuter de l'utilisation de IPsec pour protéger L2TPv2 comme appliquée dans le modèle "centre et rayons" de passage logiciel. Sauf mention contraire, IKEv2 et la nouvelle architecture IPsec [RFC4301] sont supposées.

3.5.1 Problèmes d'authentification

Une mise en œuvre de IPsec utilisant IKE prend seulement en charge l'authentification de la machine. Elle n'a pas de moyen de vérifier l'identité d'un utilisateur et de discriminer le trafic de tunnel parmi les utilisateurs d'un environnement de machine multi utilisateurs. IKEv2 peut prendre en charge l'authentification d'utilisateur avec charge utile EAP en s'appuyant sur l'infrastructure existante d'authentification et de base de données d'accréditifs. Cela permet la ségrégation du trafic parmi les utilisateurs quand l'authentification d'utilisateur est utilisée en combinaison avec l'authentification traditionnelle. L'identité d'utilisateur affirmée dans IKEv2 va être vérifiée paquet par paquet.

Si le serveur AAA est impliqué dans l'établissement d'association de sécurité entre le SI et le SC, une clé de session peut être déduite de l'authentification entre le SI et le serveur AAA. Des échanges EAP réussis au sein de IKEv2 courent entre le SI et le serveur AAA pour créer une clé de session, qui est transférée de façon sûre au SC à partir du serveur AAA. La relation de confiance entre les entités impliquées suit le paragraphe 3.2 du présent document.

3.5.2 Clés IPsec pré partagées pour l'authentification

Avec IPsec, quand 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, par paquet. Par suite, l'identité vérifiée dans IKE est ensuite vérifiée à réception de chaque paquet.

L'authentification en utilisant des clés pré-partagées peut être utilisée quand le nombre de SI et SC est petit. Lorsque le nombre de SI et SC croît, les clés pré-partagées deviennent de plus en plus difficiles à gérer. Un protocole de sécurité de passage logiciel DOIT fournir une approche adaptable à la gestion de clé. Chaque fois que possible, l'authentification avec certificats est préférée.

Quand des clés pré-partagées sont utilisées, des clés pré-partagées de groupe NE DOIVENT PAS être utilisées parce que elles sont vulnérables aux attaques par interposition ([RFC3193], paragraphe 5.1.4).

3.5.3 Lignes directrices pour l'inter-opérabilité

L'inter-opérabilité L2TPv2/IPsec concernant la suppression de tunnel, la fragmentation, et les vérifications de sécurité par paquet donnée à la Section 3 de la [RFC3193] doit être prise en compte.

Bien que la spécification de L2TP permette à celui qui répond (le SC dans le passage logiciel) d'utiliser une nouvelle

adresse IP ou de changer le numéro d'accès quand il envoie la réponse à la demande de début de connexion de contrôle (SCCRP, *Start-Control-Connection-Request-Reply*) une mise en œuvre de concentrateur de passage logiciel NE DEVRAIT PAS faire cela ([RFC3193], Section 4).

Cependant, pour certaines raisons, par exemple, "équilibrage de charge" entre les SC, le changement d'adresse IP est exigé. Pour signaler un changement d'adresse IP, le SC envoie un message StopCCN au SI en utilisant l'AVP Résultat et Code d'erreur dans un message L2TPv2. Une nouvelle SA IKE et SA fille DOIT être établie à la nouvelle adresse IP.

Comme ESP en mode transport est utilisé, l'en-tête UDP qui porte le paquet L2TP va avoir une somme de contrôle incorrecte due au changement de parties de l'en-tête IP durant le transit. Le paragraphe 3.1.2 de la [RFC3948] définit trois procédures qui peuvent être utilisées pour corriger la somme de contrôle. Une mise en œuvre de passage logiciel NE DOIT PAS utiliser la "mise à jour incrémentaire de somme de contrôle" (option 1 décrite dans la [RFC3948]) parce que IKEv2 n'a pas les informations exigées (charge utile NAT-OA) pour calculer cette somme de contrôle. Comme ESP fournit déjà la validation sur le paquet L2TP, une approche simple est d'utiliser l'approche "ne pas vérifier" (option 3 dans la [RFC3948]).

3.5.4 Détails du filtrage IPsec

Si les anciennes architectures de IPsec [RFC2401] et IKE [RFC2409] sont utilisées, des exemples de base de données de politique de sécurité (SPD, *security policy database*) de la [RFC3193], Appendice A peuvent être appliqués au modèle de passage logiciel. Dans ce cas, l'initiateur est toujours le client (SI), et celui qui répond est le SC. Des exemples de SPD IPsec pour IKE [RFC2409] sont aussi donnés dans l'Appendice A du présent document.

L'architecture IPsec révisée de la [RFC4301] a redéfini les entrées de SPD pour donner plus de souplesse (plusieurs sélecteurs par entrée, liste de gammes d'adresses, base de données d'authentification d'homologue (PAD, *Peer Authentication Database*) fanion "remplir à partir du paquet" (PFP) etc.). L'échange de clé Internet (IKE, *Internet Key Exchange*) a aussi été révisé et simplifié dans IKEv2 [RFC4306]. Les paragraphes qui suivent donnent des exemples de SPD pour l'utilisation par les passages logiciels des architectures révisée de IPsec et IKEv2.

3.5.4.1 Exemple de passage logiciel IPv6 sur IPv4 L2TPv2 pour IKEv2

Si IKEv2 est utilisé comme protocole de gestion de clés, la [RFC4301] fournit les directives pour les entrées de SPD. Dans IKEv2, on peut utiliser le fanion PFP pour spécifier la SA, et le numéro d'accès peut être choisi avec la charge utile de sélecteur de trafic répondeur (TSr, *Traffic Selector - Responder*) durant CREATE_CHILD_SA. On décrit ci-après les entrées de PAD, respectivement sur le SI et le SC. Les entrées de PAD sont seulement des exemples de configuration. L'entrée de PAD sur le SC correspond aux identités d'utilisateur de l'entrée de SDP L2TP. Ceci est fait en utilisant un type de nom symbolique spécifié dans la [RFC4301].

PAD de SI :
- Si identité_distante = identité_SI
  Alors authentifier (secret partagé/certificat/)
  et autoriser la SA_fille pour l'adresse distante SC_adresse

PAD de SC :
- Si identité_distante = utilisateur_1
  Alors authentifier (secret partagé/certificat/EAP)
  et autoriser les SA_filles pour le nom symbolique "l2tp_spd_entry"

On décrit ensuite les entrées de SPD pour, respectivement, le SI et le SC. Noter que le trafic IKEv2 et ESP DOIT être permis (bypass). Cela inclut le protocole IP 50 et les accès UDP 500 et 4500.

Le format de paquet IPv4 quand ESP protège et que L2TPv2 porte un paquet IPv6 est montré au Tableau 1, qui est similaire au Tableau 1 de la [RFC4891].

Composants (du premier au dernier)	**Contient**
En-tête IPv4	(src = IPv4-SI, dst = IPv4-SC)
En-tête ESP	
En-tête UDP	(src port=1701, dst port=1701)
En-tête L2TPv2	
En-tête PPP	

En-tête IPv6
(charge utile)
ICV ESP

Tableau 1 : Format de paquet pour L2TPv2 avec ESP portant un paquet IPv6

SPD pour l'initiateur de passage logiciel :
SPD-S d'initiateur de passage logiciel
- Si adresse_locales=IPv4-SI
  adresse_distante=IPv4-SC
  Protocole de prochaine couche=UDP
  accès_local=1701
  accès_distant=ANY (PFP=1)
  Alors utiliser une SA ESP en mode transport
  Initier en utilisant IDi = utilisateur_1 à l'adresse IPv4-SC

SPD pour le concentrateur de passage logiciel :
SPD-S de concentrateur de passage logiciel
- Si nom="l2tp_spd_entry"
  adresse_locale=IPv4-SC
  adresse_distante=ANY (PFP=1)
  Protocole de prochaine couche=UDP
  accès_local=1701
  accès_distant=ANY (PFP=1)remote_port=ANY (PFP=1)
  Alors utiliser une SA ESP en mode transport

3.5.4.2 Exemple de passage logiciel IPv4 sur IPv6 L2TPv2 pour IKEv2

Les entrées de PAD pour le SI et le SC sont montrées en exemple. Ces exemples de configuration sont similaires à ceux du paragraphe 3.5.4.1 du présent document.

PAD SI :
- Si identité_distante = identité_SI
  Alors authentifier (secret partagé/certificat/)
  et autoriser la SA_fille pour l'adresse distante SC_address

PAD SC :
- Si identité_distante = utilisateur_2
  Alors authentifier (secret partagé/certificat/EAP)
  et autoriser les SA_filles pour le nom symbolique "l2tp_spd_entry"

On décrit ensuite les entrées de SPD pour, respectivement le SI et le SC. Dans cet exemple, le SI et le SC sont notés avec les adresses IPv6, respectivement IPv6-SI et IPv6-SC. Noter que le trafic IKEv2 et ESP DOIT être permis (bypass). Cela inclut le protocole IP 50 et les accès UDP 500 et 4500.

Le format de paquet IPv6 quand ESP protège et que L2TPv2 porte un paquet IPv4 est montré au Tableau 2, qui est similaire au Tableau 1 de la [RFC4891].

Composants (du premier au dernier)	**Contient**
En-tête IPv6	(src = IPv6-SI, dst = IPv6-SC) |
En-tête ESP	
En-tête UDP	(src port=1701, dst port=1701) |
En-tête L2TPv2	
En-tête PPP	
En-tête IPv4	
(charge utile)	
ICV ESP	

Tableau 2 : Format de paquet pour L2TPv2 avec ESP portant un paquet IPv4

SPD pour l'initiateur de passage logiciel :
SPD-S d'initiateur de passage logiciel
- Si adresse_locale = IPv6-SI
  adresse_distante = IPv6-SC
  Protocole de prochaine couche=UDP
  accès_local=1701
  accès_distant=ANY (PFP=1)
  Alors utiliser une SA ESP en mode transport
  Initier en utilisant IDi = utilisateur_2 à l'adresse IPv6-SC

SPD pour le concentrateur de passage logiciel :
SPD-S de concentrateur de passage logiciel
- Si nom="l2tp_spd_entry"
  adresse_locale=IPv6-SC
  adresse_distante=ANY (PFP=1)
  Protocole de prochaine couche=UDP
  accès_local=1701
  accès_distant=ANY (PFP=1)
  Alors utiliser une SA ESP en mode transport

4. Lignes directrices pour la sécurité de maillage

4.1 Scénario de déploiement

Dans la solution "maillage" de passage logiciel ([RFC4925], [RFC5565]) il est exigé d'établir la connexité pour accéder aux îles de réseau d'un type de famille d'adresses à travers un cœur de transit d'un type différant de famille d'adresses. Pour assurer l'accessibilité à travers le cœur de transit, des AFBR sont installés entre l'île de réseau d'accès et le cœur de réseau de transit. Ces AFBR peuvent fonctionner comme des routeurs côté fournisseur (PE, *Provider Edge*) au sein d'un système autonome ou effectuer de l'échange de trafic à travers les systèmes autonomes. Les AFBR établissent et encapsulent les passages logiciels dans un maillage aux autres îles à travers le cœur de réseau de transit. Le cœur de réseau de transit consiste en un ou plusieurs fournisseurs de service.

Dans la solution de "maillage" de passage logiciel, une paire de routeurs PE (des AFBR) utilise BGP pour échanger les informations d'acheminement. Les nœuds AFBR dans le réseau de transit sont des locuteurs BGP internes et vont échanger du trafic les uns avec chaque autre directement ou via un réflecteur de chemin pour échanger des ensembles SW-encap, effectuer la signalisation de passage logiciel, et annoncer les informations d'accessibilité aux îles d'accès d'AF et les informations de prochain bond de passage logiciel (SW-NHOP). Si ces informations sont annoncées au sein d'un système autonome, le nœud AFBR qui les reçoit des autres AFBR ne les transmet pas aux autres nœuds AFBR. Pour échanger les informations entre les AFBR, la connexité de maillage complet va être établie.

La connexité entre les routeurs CE et PE inclut des circuits physiques dédiés, des circuits logiques (comme de relais de trame et ATM) et un accès partagé au support (comme l'accès fondé sur Ethernet).

Quand les AFBR sont des routeurs PE situés à la bordure des réseaux cœurs du fournisseur, cette architecture est similaire à celle de L3VPN décrite dans la [RFC4364]. La connexité entre un routeur CE dans une île d'accès réseau et un routeur PE dans un réseau de transit est établie de façon statique. Les îles d'accès sont des réseaux d'entreprise traités par des routeurs PE dans le réseau de transit du fournisseur. Dans ce cas, les îles de réseaux d'accès sont administrées par le système autonome du fournisseur.

Les AFBR peuvent avoir plusieurs connexions au cœur de réseau, et peuvent aussi avoir des connexions à plusieurs réseaux d'accès clients. Les réseaux d'accès clients peuvent se connecter à chaque autre par des réseaux privés ou par l'Internet. Quand les réseaux d'accès clients ont leur propre numéro d'AS, un routeur CE situé à l'intérieur des îles d'accès forme un échange de trafic BGP privé avec un AFBR. De plus, un AFBR peut avoir besoin d'échanger des informations d'acheminement Internet complètes avec chaque réseau auquel il se connecte.

4.2 Relation de confiance

Tous les nœuds AFBR dans le cœur de transit DOIVENT avoir une relation de confiance ou un accord avec chaque autre pour établir des passages logiciels. Quand le cœur de transit consiste en un seul domaine administratif, on suppose que tous

les nœuds (par exemple, AFBR, PE, ou réflecteur de chemin, si applicable) sont de confiance pour chaque autre.

Si le cœur de transit consiste en plusieurs domaines administratifs, les routeurs intermédiaires entre les AFBR peuvent ne pas être de confiance.

Il DOIT y avoir une relation de confiance entre le PE dans le cœur de transit et le CE dans l'île correspondante, bien que la ou les liaisons entre le PE et le CE puissent n'être pas protégées.

4.3 Scénarios de menaces pour la sécurité des passages logiciels

Comme l'architecture de passage logiciel dans la solution de maillage est très similaire à celle du VPN provisionné par le fournisseur (PPVPN, *Provider-Provisioned VPN*). Les considérations de menaces sur la sécurité du fonctionnement de PPVPN sont applicables à celles de la solution de maillage de passage logiciel [RFC4111].

Des exemples d'attaques des paquets de données transmis sur un tunnel de passage logiciel incluent :

1. Un adversaire peut essayer de découvrir des informations confidentielles en espionnant les paquets de passage logiciel.

2. Un adversaire peut essayer de modifier le contenu des paquets de passage logiciel.

3. Un adversaire peut essayer de falsifier des paquets de passage logiciel qui n'appartiennent pas aux domaines autorisés et d'insérer des copies de paquets enregistrés qui ont été légitimes et sont répétés.

4. Un adversaire peut lancer des attaques de déni de service (DoS) en supprimant le trafic de données du passage logiciel. Les attaques de DoS du type épuisement de ressources peuvent être montées contre le plan des données en injectant une grande quantité de données non authentifiées dans le passage logiciel depuis l'extérieur du tunnel de passage logiciel.

5. Un adversaire peut essayer d'espionner les paquets du passage logiciel et d'examiner leurs aspects ou méta-aspects qui peuvent être visibles même quand les paquets eux-mêmes sont chiffrés. Un attaquant pourrait gagner d'utiles informations fondées sur la quantité et le rythme du trafic, les tailles de paquet, les adresses de source et destination, etc.

Les attaques contre la sécurité peuvent être montées aussi sur le plan de contrôle. Dans la solution de maillage de passage logiciel, l'encapsulation de passage logiciel va être établie en utilisant BGP. Comme décrit dans la [RFC4272], BGP est vulnérable à diverses menaces contre la sécurité comme la violation de la confidentialité, des attaques en répétition, en insertion, suppression, et modification de messages BGP, des attaques par interposition, et des attaques de déni de service.

4.4 Applicabilité du mécanisme de protection de la sécurité

Étant donné que la sécurité est généralement un compromis entre coût et risque, il est aussi utile de considérer la probabilité des différentes attaques. Il y a au moins une différence perceptible entre la probabilité de la plupart des types d'attaques montées avec succès dans les différents déploiements.

La relation de confiance entre les utilisateurs dans les réseaux d'accès, de fournisseur de cœur de transit, et les autres parties de réseaux, décrite au paragraphe 4.2, est un élément clé pour déterminer l'applicabilité du mécanisme de protection de la sécurité pour le déploiement spécifique de maillage de passage logiciel.

4.4.1 Mécanisme de protection de la sécurité pour le plan de contrôle

La [RFC4925] "Position du problème du passage logiciel" déclare que le mécanisme d'établissement du maillage de passage logiciel pour annoncer l'encapsulation de passage logiciel DOIT prendre en charge l'authentification, mais que le fournisseur du cœur de transit peut décider de le désactiver dans certaines circonstances.

Le mécanisme d'authentification BGP est spécifié dans la [RFC2385]. Le mécanisme défini dans la [RFC2385] est fondé sur une fonction de hachage unidirectionnelle (MD5) et l'utilisation d'une clé secrète. La clé est partagée entre une paire de routeurs homologues et est utilisée pour générer des valeurs de code d'authentification de message de 16 octets qui ne sont pas facilement calculées par un attaquant qui n'a pas accès à la clé.

Cependant, le mécanisme de sécurité pour le transport BGP (par exemple, TCP-MD5) est inadéquat dans certaines circonstances et exige aussi une interaction de l'opérateur pour maintenir un niveau de sécurité respectable. Les déploiements actuels de TCP-MD5 montrent quelques insuffisances à l'égard de la gestion de clé, comme décrit dans la [RFC3562].

La gestion de clé peut être particulièrement incommode pour les opérateurs. Le nombre de clés exigé et la maintenance des clés (produire/révoquer/renouveler) a eu un effet cumulatif comme barrière au déploiement. Donc, des moyens automatisés de gestion des clés, pour réduire la charge opérationnelle, sont disponibles dans le système de sécurité de BGP ([BGP-SEC], [RFC4107]).

L'utilisation de IPsec contrecarre les attaques d'insertion, suppression, et modification de message, ainsi que les attaques par interposition par des intrus. Si la confidentialité des données d'acheminement est désirée, l'utilisation de IPsec ESP pourrait assurer ce service. Si des attaques d'espionnage sont identifiées comme une menace, ESP peut être utilisé pour assurer la confidentialité (chiffrement) l'intégrité, et l'authentification de la session BGP.

4.4.2 Mécanisme de protection de la sécurité pour le plan des données

Pour transporter les paquets de données à travers le cœur de transit, la solution de maillage définit plusieurs encapsulations: L2TPv3, IP dans IP, MPLS (fondé sur LDP et fondé sur RSVP-TE) et GRE. Pour transporter en toute sécurité de tels paquets de données, le passage logiciel DOIT prendre en charge le tunnel IPsec.

IPsec peut assurer l'authentification et l'intégrité. La mise en œuvre DOIT prendre en charge ESP avec chiffrement nul [RFC4303] ou autrement AH (en-tête d'authentification IP) [RFC4302]. Si une partie du réseau de cœur de transit n'est pas de confiance, ESP avec chiffrement PEUT être appliqué.

Comme les passages logiciels sont créés dynamiquement par BGP, la distribution automatique de clés DOIT être effectuée par IKEv2 [RFC4306] avec clé pré-partagée ou gestion de clé publique. Pour la création dynamique de tunnel IPsec de passage logiciel, la clé pré-partagée va être la même dans tous les routeurs. À savoir, la clé pré-partagée indique ici "clé de groupe" au lieu de clé "partagée par paire".

Si la politique de sécurité exige une gestion de clé plus forte, la clé publique DEVRAIT être utilisée. Si une infrastructure de clé publique n'est pas disponible, le sous TLV Authentification de tunnel IPsec spécifié dans la [RFC5566] DOIT être utilisé avant l'établissement de la SA.

Si la ou les liaisons entre le site de l'utilisateur et le PE du fournisseur ne sont pas de confiance, le chiffrement PEUT alors être utilisé sur la ou les liaisons PE-CE.

Avec la protection cryptographique de la sécurité, la technique de contrôle d'accès réduit l'exposition aux attaques provenant de l'extérieur des réseaux du fournisseur de service (réseaux de transit). La technique de contrôle d'accès inclut le contrôle d'accès paquet par paquet ou flux de paquets par flux de paquet au moyen de filtres ainsi qu'en admettant une session à un protocole de contrôle/signalisation/gestion utilisé pour mettre en œuvre le maillage de passage logiciel.

La technique de contrôle d'accès est une protection importante contre les attaques de DoS, etc., et un ajout nécessaire à la force cryptographique dans l'encapsulation. Les paquets qui satisfont les critères associés à un filtre particulier peuvent être éliminés ou recevoir un traitement particulier pour empêcher une attaque ou atténuer l'effet d'une future attaque possible.

5. Considérations sur la sécurité

Le présent document discute des diverses menaces sur la sécurité pour les paquets de contrôle et de données de passage logiciel dans les solutions de mise sur le marché de "centre et rayons" et de "maillage". Avec ces discussions, les mises en œuvre de protocole de sécurité de passage logiciel sont fournies en référençant la [RFC4925] "Position du problème du passage logiciel", la [RFC3193] "Sécuriser L2TP en utilisant IPsec", la [RFC4111] "Cadre de sécurité pour les PPVPN", et la [RFC5406] "Lignes directrices pour spécifier l'utilisation de IPsec". Les lignes directrices pour l'emploi du protocole de sécurité sont aussi données en considérant le contexte spécifique du déploiement.

Noter que le présent document discute de la protection de la sécurité du tunnel de passage logiciel et ne traite pas de la protection de bout en bout.

6. Remerciements

Les auteurs tiennent à remercier Tero Kivinen de sa relecture du document et Francis Dupont pour ses suggestions substantielles. Nos remerciements à Jordi Palet Martinez, Shin Miyakawa, Yasuhiro Shirasaki, et Bruno Stevant pour leurs retours.

Nous voulons aussi remercier les auteurs du document cadre du déploiement de passage logiciel de centre et rayons [RFC5571] pour la fourniture du texte concernant la sécurité.

7. Références

7.1 Références normatives

[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. DOI 10.17487/RFC2119, *(MàJ par* RFC8174)

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

[RFC2661] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2 "L2TP"", DOI 10.17487/RFC2661, *(P.S.)*

[RFC3193] B. Patel et autres, "Sécuriser L2TP avec IPsec", novembre 2001. *(P.S.)*

[RFC3947] T. Kivinen et autres, "Négociation de traversée de NAT dans IKE", janvier 2005. *(P.S.)*

[RFC3948] A. Huttunen et autres, "Encapsulation UDP de paquets ESP d'IPsec", janvier 2005. *(P.S.)*

[RFC4107] S. Bellovin, R. Housley, "Lignes directrices pour la gestion des clés de chiffrement", juin 2005, DOI 10.17487/RFC4107, (BCP0107)

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", DOI 10.17487/RFC4301, décembre 2005. *(P.S.) (Remplace la* RFC2401)

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

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

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

7.2 Références pour information

[BGP-SEC] Christian, B. and T. Tauber, "BGP Security Requirements", Travail en cours, novembre 2008.

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

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

[RFC2607] B. Aboba, J. Vollbrecht, "Chaînage de mandataire et mise en œuvre de politique dans l'itinérance", juin 1999. *(Info.)*

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

[RFC4016] M. Parthasarathy, "Analyse des menaces et exigences de sécurité pour le protocole de transport d'authentification et d'accès au réseau (PANA)", mars 2005. *(Information)*

[RFC4081] H. Tschofenig et autres, "Menaces pour la sécurité des prochaines étapes de la signalisation (NSIS)", juin 2005. *(Info.)*

[RFC4111] L. Fang, éd., "Cadre de sécurité pour les réseaux privés virtuels approvisionnés par le fournisseur (PPVPN)", juillet 2005. *(Information)*

[RFC4213] E. Nordmark, R. Gilligan, "Mécanismes de transition de base pour hôtes et routeurs IPv6", octobre 2005. *(P.S.)*

[RFC4225] P. Nikander et autres, "Fondements des concepts de sécurité de l'optimisation de l'acheminement d'IPv6 mobile", décembre 2005. *(Information)*

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

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

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

[RFC4891] R. Graveman et autres, "Utilisation d'IPsec pour sécuriser les tunnels IPv6 dans IPv4" mai 2007. *(Info.)*

[RFC4925] X. Li et autres, "Position du problème du passage logiciel", juillet 2007. *(Information)*

[RFC5216] D. Simon, B. Aboba, R. Hurst, "Protocole d'authentification EAP-TLS", mars 2008.*(P.S. ; remplace* RFC2716 ; *MàJ par* RFC9190*)*

[RFC5406] S. Bellovin, "Lignes directrices pour spécifier l'utilisation de IPsec version 2", février 2009. (BCP0146)

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

[RFC5566] L. Berger, R. White, E. Rosen, "Attribut d'encapsulation de tunnel IPsec pour BGP", juin 2009. *(P. S.)*

[RFC5571] B. Storer et autres, "Cadre de déploiement de centre et rayons de passage logiciel avec la version 2 du protocole de tunnelage de couche deux (L2TPv2)", juin 2009. *(P. S.)*

Appendice A. Exemples

Si l'ancienne architecture de IPsec [RFC2401] et de IKE [RFC2409] est utilisée, les exemples de SPD de la [RFC3193] sont applicables au modèle "centre & rayons". Dans ce modèle, l'initiateur est toujours le client (SI), et celui qui répond est le SC.

A.1 Exemple de passage logiciel IPv6 sur IPv4 avec L2TPv2 pour IKE

Les adresses IPv4 de l'initiateur et du concentrateur de passage logiciel sont notées respectivement par IPv4-SI et IPv4-SC. Si la traversée de NAT est utilisée dans IKE, les accès UDP de source et destination sont 4500. Dans cette entrée SPD, IKE se réfère à l'accès UDP 500. * note un caractère générique et indique un accès ou adresse "ANY".

Local	**Distant**	**Protocole**	**Action**
IPV4-SI	IPV4-SC	ESP	BYPASS
IPV4-SI	IPV4-SC	IKE	BYPASS
IPv4-SI	IPV4-SC	UDP, src 1701, dst 1701	PROTECT(ESP, transport)
IPv4-SC	IPv4-SI	UDP, src * , dst 1701	PROTECT(ESP, transport)

SPD d'initiateur de passage logiciel

Distant	Local	Protocole	Action
*	IPV4-SC	ESP	BYPASS
*	IPV4-SC	IKE	BYPASS
*	IPV4-SC	UDP, src *, dst 1701	PROTECT(ESP, transport)

SPD de concentrateur de passage logiciel

A.2 Exemple de passage logiciel IPv4 sur IPv6 avec L2TPv2 pour IKE

Les adresses IPv6 de l'initiateur et du concentrateur de passage logiciel sont notées respectivement IPv6-SI et IPv6-SC. Si la traversée de NAT est utilisée dans IKE, les accès UDP de source et de destination sont 4500. Dans cette entrée de SPD, IKE se réfère à l'accès UDP 500. * note un caractère générique et indique un accès ou adresse ANY.

Local	Distant	Protocole	Action
IPV6-SI	IPV6-SC	ESP	BYPASS
IPV6-SI	IPV6-SC	IKE	BYPASS
IPv6-SI	IPV6-SC	UDP, src 1701, dst 1701	PROTECT(ESP, transport)
IPv6-SC	IPv6-SI	UDP, src *, dst 1701	PROTECT(ESP, transport)

SPD d'initiateur de passage logiciel

Distant	Local	Protocole	Action
*	IPV6-SC	ESP	BYPASS
*	IPV6-SC	IKE	BYPASS
*	IPV6-SC	UDP, src * , dst 1701	PROTECT(ESP, transport)

SPD de concentrateur de passage logiciel

Adresse des auteurs

Shu Yamamoto
NICT/KDDI R&D Labs
1-13-16 Hakusan, Bunkyo-ku
Tokyo 113-0001
Japan
mél : shu@nict.go.jp

Carl Williams
KDDI R&D Labs
Palo Alto, CA 94301
USA
téléphone : +1-650-279-5903
mél : carlw@mcsr-labs.org

Hidetoshi Yokota
KDDI R&D Labs
2-1-15 Ohara
Fujimino, Saitama 356-8502
Japan
mél : yokota@kddilabs.jp

Florent Parent
Beon Solutions
Quebec, QC
Canada
mél : Florent.Parent@beon.ca