Groupe de travail Réseau
Request for Comments : 3723
Catégorie : En cours de normalisation
avril 2004
Traduction Claude Brière de L'Isle

B. Aboba, Microsoft
J. Tseng, McDATA Corporation
J. Walker, Intel
V. Rangan, Brocade Communications Systems Inc.
F. Travostino, Nortel Networks

Protocoles de sécurisation de mémorisation de blocs sur IP

Résumé
Le présent document expose comment sécuriser les protocoles de mémorisation de bloc et de découverte des mémorisations qui fonctionnent sous IP (*Protocole Internet*) en utilisant IPsec et l'échange de clé Internet (IKE, *Internet Key Exchange*). Les modèles de menace et les protocoles de sécurité sont développés pour les interfaces de système de petit ordinateur avec le protocole Internet (iSCSI, *Internet Protocol Small Computer System Interface*) le réseautage iFCP (*Internet Fibre Channel Storage Networking*) et FCIP (*Fibre Channel over TCP/IP*), ainsi que pour les protocoles de découverte iSNS (*Internet Storage Name Server*) et SLPv2 (*Service Location Protocol v2*). Les questions de performances et les contraintes de ressource sont analysées.

Table des Matières

1. Introduction

La présente spécification expose l'utilisation de la suite de protocoles IPsec pour la protection des protocoles de mémorisation de bloc sur les réseaux IP (incluant iSCSI, iFCP et FCIP) ainsi que les protocoles de découverte de mémorisation (iSNS et SLPv2).

1.1. Généralités sur iSCSI

iSCSI, décrit dans la [RFC3720], est un protocole de commande/réponse en mode connexion qui fonctionne sur TCP, et est utilisé pour accéder à des disques, des bandes magnétiques et autres appareils. iSCSI est un protocole client-serveur dans lequel les clients (initiateurs) ouvrent des connexions avec les serveurs (cibles) et effectuent une connexion iSCSI.

Le présent document utilise les termes d'initiateur et de cible SCSI pour être clair et éviter la supposition courante que les clients ont considérablement moins de ressources de calcul et de mémoire que les serveurs ; l'inverse est souvent le cas pour SCSI, car les cibles sont couramment des appareils dédiés d'une certaine forme.

Le protocole iSCSI a un mécanisme de négociation fondé sur le texte au titre de sa procédure initiale (de connexion). Le mécanisme est extensible dans ce qui peut être négocié (de nouvelles clés et valeurs de texte peuvent être définies) et aussi dans le nombre de tours de négociation (par exemple, pour s'accommoder de fonctionnalités telles que l'authentification par mise au défi/réponse).

Après la réussite d'une connexion, l'initiateur iSCSI peut produire des commandes SCSI pour exécution par la cible iSCSI, qui retourne une réponse d'état pour chaque commande, sur la même connexion. Une seule connexion est utilisée pour les messages aussi bien de commande/état que de transfert de données ou paramètres de commandes facultatifs. Une session iSCSI peut avoir plusieurs connexions, mais un enregistrement séparé est effectué sur chacune. La session iSCSI se termine lorsque sa dernière connexion est close.

Les initiateurs et cibles iSCSI sont des entités de couche application qui sont indépendantes des accès TCP et des adresses IP. Initiateurs et cibles ont des noms dont la syntaxe est définie dans la [RFC3721]. Les sessions iSCSI entre un initiateur et une cible donnés fonctionnent sur une ou plusieurs connexions TCP entre ces entités. C'est-à-dire que le processus d'enregistrement établit une association entre une session iSCSI et la ou les connexions TCP sur lesquelles sont portés les PDU iSCSI.

Bien que l'enregistrement d'iSCSI puisse inclure l'authentification mutuelle des points d'extrémité iSCSI et la négociation des paramètres de session, iSCSI ne définit pas ses propres mécanismes par paquet d'authentification, de protection de l'intégrité, de la confidentialité ou contre la répétition. Il s'appuie plutôt sur la suite de protocole IPsec pour fournir des services par paquet de confidentialité et intégrité des données et d'authentification, avec IKE comme protocole de gestion de clé. iSCSI utilise TCP pour fournir le contrôle de l'encombrement, la détection d'erreur et la récupération d'erreur.

1.2 Généralités sur iFCP

iFCP, défini dans la [RFC4172], est un protocole de passerelle à passerelle, qui fournit des services de transport à des appareils de fibre optique sur un réseau TCP/IP. iFCP permet l'interconnexion et le réseautage des appareils de fibre optique existants à des vitesse filaires sur un réseau IP. Les mises en œuvre iFCP émulent un tissu de services afin d'améliorer la tolérance aux fautes et l'adaptabilité en tirant pleinement parti de la technologie IP. Chaque connexion TCP est utilisée pour prendre en charge le trafic de mémorisation entre une paire unique de N_PORT de canal de fibre optique.

iFCP n'a pas de mécanisme natif de sécurité dans la bande. Il s'appuie plutôt sur la suite de protocole IPsec pour fournit des services de confidentialité et d'authentification des données, et sur IKE comme protocole de gestion de clé. iFCP utilise TCP pour fournir le contrôle de l'encombrement, la détection d'erreur et la récupération d'erreur.

1.3 Généralités sur FCIP

FCIP, défini dans la [RFC3821], est un pur protocole d'encapsulation de canal Fibre (FC, *Fibre Channel*) qui transporte des trames FC. Le travail de spécification actuel l'a prévu pour l'interconnexion de commutateurs de fibre optique sur des réseaux TCP/IP, mais le protocole n'est pas par lui-même limité à la connexion de commutateurs FC. FCIP diffère de iFCP en ce que aucune interception ou émulation du tissu de services n'est impliqué. Une ou plusieurs connexions TCP sont reliées à une liaison FCIP, qui est utilisée pour réaliser des liaisons inter commutateur (ISL, *Inter-Switch Link*) entre les paires d'entités de canal Fibre. L'encapsulation de trame FCIP est décrite dans la [RFC3643].

FCIP n'a pas de mécanisme de sécurité natif dans la bande. Il s'appuie plutôt sur la suite de protocole IPsec pour fournir des services de confidentialité et d'authentification des données, et sur IKE comme protocole de gestion de clé. FCIP utilise TCP pour fournir le contrôle de l'encombrement, la détection d'erreur et la récupération d'erreur.

1.4 Généralités sur IPsec

IPsec est une suite de protocoles qui est utilisée pour sécuriser la communication à la couche réseau entre deux homologues. La suite de protocoles IPsec est spécifiée dans les documents de l'architecture de sécurité IP [RFC2401], de IKE [RFC2409], [RFC2412], de l'en-tête d'authentification (AH) IPsec [RFC2402] et d'encapsulation de charge utile de sécurité (ESP, *Encapsulating Security Payload*) IPsec [RFC2406]. IKE est le protocole de gestion de clé tandis que AH et ESP sont utilisés pour protéger le trafic IP.

Une SA IPsec est une association de sécurité unidirectionnelle, identifiée de façon univoque par le triplet <indice de paramètre de sécurité (SPI, *Security Parameter Index*) protocole (ESP) et destination IP>. Les paramètres pour une association de sécurité IPsec sont normalement établis par un protocole de gestion de clé. Ils comportent le mode d'encapsulation, le type d'encapsulation, les clés de session et les valeurs de SPI.

IKE est un protocole de négociation en deux phases fondé sur un échange modulaire de messages défini par ISAKMP [RFC2408], et le domaine d'interprétation (DOI, *Domain of Interpretation*) de sécurité IP [RFC2407]. IKE a deux phases, et accomplit les fonctions suivantes :

[1] Protection de la suite de chiffrement et négociation des options – en utilisant des MAC à clés et des mécanismes de chiffrement et d'anti-répétition
[2] Génération de clé maîtresse – comme par des calculs MODP Diffie-Hellman
[3] Authentification des points d'extrémité
[4] Gestion de SA IPsec (négociation de sélecteur, négociation des options, création, suppression, et changement de clé)

Les éléments 1 à 3 sont réalisés dans la phase 1 de IKE, tandis que l'élément 4 est traité dans IKE phase 2.

Une négociation IKE phase 2 est effectuée pour établir les deux associations de sécurité IPsec entrante et sortante. Le trafic à protéger par une SA IPsec est déterminé par un sélecteur qui a été proposé par l'initiateur IKE et accepté par le répondant IKE. Dans le mode transport IPsec, le sélecteur de SA IPsec peut être un "filtre" ou un classeur de trafic, défini comme le quintuplet <adresse IP de source, adresse IP de destination, protocole de transport (UDP/SCTP/TCP), accès de source, accès de destination>. La réussite de l'établissement d'une SA IKE phase-2 résulte en la création de deux SA unidirectionnelles IPsec pleinement qualifiées par le triplet <protocole (ESP/AH), adresse de destination, SPI>.

Les clés de session pour chaque SA IPsec sont déduites d'une clé maîtresse, normalement via un calcul MODP Diffie-Hellman. Le changement de clé d'une paire de SA IPsec existante est accompli par la création de deux nouvelles SA IPsec, par leur activation, et ensuite par la suppression facultative de l'ancienne paire de SA IPsec. Normalement, la nouvelle SA sortante est utilisée immédiatement, et l'ancienne SA entrante est laissée active pour recevoir des paquets pendant une durée définie en local, peut-être 30 secondes ou 1 minute.

1.5 Terminologie

Canal Fibre (FC, *Fibre Channel*)
C'est une technologie de réseautage à des vitesses de l'ordre du gigabit principalement utilisée pour mettre en œuvre des réseaux à zone de mémorisation (SAN, *Storage Area Network*), bien qu'elle puisse aussi être utilisée pour transporter également d'autres types de trame, y compris IP. FC est normalisé par le comité technique TI1 des normes nationales américaines pour les systèmes d'information du comité international pour les normes de technologies de l'information (ANSI-INCITS).

Canal Fibre sur IP (FCIP, *Fibre Channel over IP*)
FCIP est un protocole pour l'interconnexion des îles de canaux Fibre parmi les réseaux IP afin de former un SAN unifié dans un seul tissu de canaux de fibre. Le principal point d'interface FCIP avec le réseau IP est l'entité FCIP. La liaison FCIP représente une ou plusieurs connexions TCP qui existent entre une paire d'entités FCIP.

Adaptateur de bus hôte (HBA, *Host Bus Adapter*)
HBA est un terme générique pour une interface SCSI avec d'autres appareils ; il est en gros analogue au terme carte d'interface réseau (NIC, *Network Interface Card*) pour une interface réseau TCP/IP, excepté que généralement les HBA ont des mises en œuvre de SCSI incorporées, tandis que la plupart des NIC ne mettent pas en œuvre TCP, UDP, ou IP.

Protocole de canal Fibre Internet (iFCP, *Internet Fibre Chanel Protocol*)
iFCP est un protocole de passerelle à passerelle, qui fournit des services de tissu de canaux Fibre aux appareils de fibre optique sur un réseau TCP/IP.

Protocole IP de mémorisation de bloc
Lorsque il est utilisé au sein de ce document, le terme de "protocole IP de mémorisation de bloc" s'applique à tous les protocoles de mémorisation de bloc qui fonctionnent sur IP, y compris iSCSI, iFCP et FCIP.

iSCSI
iSCSI est un protocole client-serveur dans lequel les clients (initiateurs) ouvrent des connexions avec les serveurs (cibles).

iSNS
Le protocole du service de noms de mémorisation sur Internet (iSNS, *Internet Storage Name Server*) assure la découverte et la gestion des appareils de mémorisation iSCSI et canaux Fibre (FCP). Les applications iSNS mémorisent les attributs d'appareils iSCSI et FC et surveillent leur disponibilité et accessibilité, fournissant un répertoire d'informations consolidées pour un réseau intégré de mémorisation de bloc IP. iFCP exige iSNS pour la découverte et la gestion, tandis que iSCSI peut utiliser iSNS pour la découverte, et FCIP n'utilise pas iSNS.

initiateur
L'initiateur iSCSI se connecte à la cible sur l'accès TCP bien connu 3260. L'initiateur iSCSI produit alors des commandes SCSI pour exécution par la cible iSCSI.

cible
La cible iSCSI écoute sur un accès TCP bien connu les connexions entrantes, et retourne une réponse d'état pour chaque commande produite par l'initiateur iSCSI, sur la même connexion.

1.6 Terminologie pour la conformité

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

Noter que les exigences spécifiées dans le présent document ne s'appliquent qu'à l'utilisation de IPsec et IKE avec des protocoles de mémorisation de bloc IP. Donc, ces exigences ne s'appliquent pas aux mises en œuvre de IPsec en général. Le langage des exigences de mise en œuvre devrait donc être supposé se rapporter à la disponibilité des dispositifs à utiliser seulement avec la sécurité de mémorisation de bloc IP.

Bien que les exigences de sécurité dans le présent document soient déjà incorporées dans les documents iSCSI [RFC3720], iFCP [RFC4172] et FCIP [RFC3821] en cours de normalisation, elles sont reproduites ici pour en faciliter la consultation. En cas de divergence, ce sont les documents de normalisation des protocoles individuels qui font foi.

2. Sécurité de protocole de mémorisation de bloc

2.1 Exigences de sécurité

Les protocoles de mémorisation de bloc sur IP tels que iSCSI, iFCP et FCIP sont utilisés pour transmettre des commandes SCSI sur les réseaux IP. Donc, les paquets de contrôle et de données de ces protocoles de mémorisation de bloc sur IP sont vulnérables aux attaques. Les exemples d'attaques incluent :

1. un adversaire peut tenter d'acquérir des données et identités confidentielles en espionnant les paquets de données ;
2. un adversaire peut tenter de modifier des paquets qui contiennent des messages de données et de contrôle ;
3. un adversaire peut tenter d'injecter des paquets dans une connexion de mémorisation de bloc IP ;
4. un adversaire peut tenter de capturer une ou des connexions TCP correspondant à une session de mémorisation de bloc IP ;.
5. un adversaire peut lancer des attaques de déni de service contre des appareils de mémorisation de bloc IP , comme en envoyant une réinitialisation TCP ;
6. un adversaire peut tenter d'interrompre un processus de négociation de sécurité, afin d'affaiblir l'authentification, ou d'obtenir l'accès aux mots de passe de l'usager. Cela inclut une interruption de la négociation d'authentification de couche application telle que l'inscription à iSCSI ;
7. un adversaire peut tenter de se faire passer pour une entité légitime de mémorisation de bloc sur IP ;
8. un adversaire peut lancer diverses attaques (modification ou injection de paquet, déni de service) contre le processus de découverte (SLPv2 [RFC2608]) ou de découverte et de gestion (iSNS [RFC4939]). iSCSI peut utiliser SLPv2 ou iSNS. Seul FCIP utilise SLPv2, et seul iFCP utilise iSNS.

Comme les appareils iFCP et FCIP sont la dernière ligne de défense pour toute une île de canaux Fibre, les attaques ci-dessus, si elles réussissent, pourraient compromettre la sécurité de tous les hôtes de canaux Fibre derrière les appareils.

Pour traiter ces menaces, les protocoles de sécurité de mémorisation de bloc sur IP doivent prendre en charge la protection de la confidentialité, l'authentification de l'origine des données, l'intégrité, et le protection contre la répétition paquet par paquet. Les services de confidentialité sont importants car le trafic de mémorisation de bloc IP peut traverser des réseaux publics non sûrs. Les protocoles de sécurité de mémorisation doivent prendre en charge un secret de transmission parfait dans le processus de changement de clés.

L'authentification bidirectionnelle des points d'extrémité de communication DOIT être fournie. Il n'est pas exigé que les identités utilisées pour l'authentification restent confidentielles (par exemple, à un espion passif).

Pour qu'un protocole de sécurité soit utile, la redondance de CPU et la disponibilité du matériel ne doivent pas empêcher la mise en œuvre à 1 Gbit/s aujourd'hui. La faisabilité de mises en œuvre à 10 Gbit/s est très souhaitable, mais peut n'être pas démontrable pour l'instant. Ces niveaux de performances s'appliquent au débit agrégé, et incluent toutes les connexions TCP utilisées entre les points d'extrémité de mémorisation de bloc IP. Les communications de mémorisation de bloc IP impliquent normalement plusieurs connexions TCP. Les questions de performances sont exposées plus en détail à l'Appendice B.

Les réseaux de centre de données d'entreprise sont considérés comme des facilités à la mission critique qui doivent être isolés et protégés de menaces possibles contre la sécurité. De tels réseaux sont souvent protégés par des portails de sécurité, qui fournissent au minimum un bouclier contre les attaques de déni de service. L'architecture de sécurité de mémorisation de bloc IP devrait être capable de démultiplier les services protecteurs de l'infrastructure de sécurité existante, incluant la protection des pare-feu, services de NAT et NAPT, et services de VPN disponibles sur les passerelles de sécurité existantes.

Lorsque des appareils iFCP ou FCIP sont déployés au sein de réseaux d'entreprise, les adresses IP vont être normalement allouées de façon statique comme c'est le cas avec la plupart des routeurs et commutateurs. Par conséquent, la prise en charge de l'allocation dynamique d'adresse IP, comme décrit dans la [RFC3456], ne sera normalement pas exigée, bien qu'elle ne puisse être exclue. De telles facilités seront aussi pertinentes pour les hôtes iSCSI dont les adresses sont allouées de façon dynamique. Il en résulte que les protocoles de sécurité de mémorisation de bloc IP ne doivent pas introduire de faiblesses de sécurité supplémentaires lorsque l'allocation dynamique d'adresse est prise en charge.

Bien que la sécurité de mémorisation de bloc IP soit de mise en œuvre obligatoire, il n'est pas obligatoire de l'utiliser. Les services de sécurité utilisés dépendent de la configuration et des politiques de sécurité mises en place. Par exemple, la configuration va influencer l'algorithme d'authentification négocié lors de l'inscription iSCSI, ainsi que les services de sécurité (confidentialité, authentification de l'origine des données, intégrité, protection anti-répétition) et les transformations négociées lorsque IPsec est utilisé pour protéger les protocoles de mémorisation de bloc IP tels que iSCSI, iFCP et FCIP.

Les mises en œuvre de FCIP peuvent permettre d'activer ou de désactiver des mécanismes de sécurité à la granularité d'une

liaison FCIP. Pour iFCP, la granularité correspond à un portail iFCP. Pour iSCSI, la granularité du contrôle est normalement celle d'une session iSCSI, bien qu'il soit possible d'exercer le contrôle jusqu'à la granularité de l'adresse IP de destination et l'accès TCP.

Noter qu'avec IPsec, les services de sécurité sont négociés à la granularité d'une SA IPsec, de sorte que les connexions de mémorisation de bloc IP qui demandent un ensemble de services de sécurité différents de ceux négociés avec les SA IPsec existantes devront négocier une nouvelle SA IPsec.

Des SA IPsec distinctes sont aussi conseillées lorsque des considérations de qualité de service dictent des traitements différents des connexions de mémorisation de bloc IP. Tenter d'appliquer une qualité de service différente aux connexions traitées par la même SA IPsec peut résulter en un réarrangement, et à sortir de la fenêtre de répétition. Pour un exposé sur ces questions, voir la [RFC2983].

Les protocoles de mémorisation de bloc IP peuvent être supposés transporter des données sensibles et donner accès à des systèmes et données qui requièrent une protection contre les menaces à la sécurité. SCSI et Canal fibre contiennent actuellement peu de mécanismes de sécurité, et s'appuient sur la sécurité physique, administrative, et la configuration correcte des supports de communication et systèmes/appareils qui lui sont rattachés pour leurs propriétés de sécurité.

Pour la plupart des réseaux IP, il est inapproprié de supposer une sécurité physique, une sécurité administrative, et la configuration correcte du réseau et de tous les nœuds rattachés (un réseau physiquement isolé dans un laboratoire d'essais peut être une exception). Donc, l'authentification DEVRAIT être utilisée par les protocoles de mémorisation de bloc IP (par exemple, iSCSI DEVRAIT utiliser un de ses mécanismes d'authentification dans la bande ou l'authentification fournie par IKE) afin de fournir une assurance minimale que les connexions ont été initialement ouvertes avec la contrepartie prévue.

iSNS, décrit dans la [RFC4939], est exigé dans tous les déploiements iFCP. iSCSI peut utiliser iSNS pour la découverte, et FCIP n'utilise pas iSNS. Les applications iSNS mémorisent les attributs d'appareils iSCSI et FC et surveillent leur disponibilité et accessibilité, fournissant un répertoire d'informations consolidées pour un réseau intégré de mémorisation de bloc IP. La spécification iSNS définit les mécanismes pour sécuriser la communication entre un serveur iSNS et ses clients.

2.2. Contraintes de ressources

Les contraintes de ressource et les exigences de performances pour iSCSI sont exposées au paragraphe 3.2 de la [RFC3347]. Les appareils iFCP et FCIP vont normalement être des systèmes déployés sur des étagères dans des locaux de centres de données à air conditionné. De tels systèmes incorporés peuvent inclure des matériels à microplaquettes pour assurer le traitement de chiffrement des données, d'authentification, et de protection de l'intégrité. Donc, les ressources de mémoire et de CPU ne sont généralement pas un facteur contraignant.

iSCSI va être mis en œuvre sur divers systèmes qui vont des grands serveurs qui fonctionnent avec des systèmes d'exploitation non spécialisés jusqu'à des adaptateurs de bus hôte (HBA, *host bus adapter*) incorporés. En général, un adaptateur de bus hôte est le plus contraint des environnements de mise en œuvre d'iSCSI, bien qu'un HBA puisse tirer sur les ressources du système auquel il est rattaché dans certains cas (par exemple, les calculs d'authentification exigés pour l'établissement de la connexion). Plus de ressources devraient être disponibles aux mises en œuvre de iSCSI pour les systèmes d'exploitation incorporés et non spécialisés. Les lignes directrices suivantes indiquent le niveau approximatif de ressources que les fonctions d'authentification, d'établissement de clés, et de changement de clés peuvent raisonnablement s'attendre à consommer :

- Les processeurs à faible puissance avec une petite taille de mot ne sont généralement pas utilisés, car la puissance n'est normalement pas un facteur contraignant, à l'éventuelle exception des HBA, qui peut tirer sur les ressources de calcul du système dans lequel ils sont insérés. De la puissance de calcul devrait être disponible pour effectuer une quantité raisonnable d'exponentiation au titre de l'authentification et de la déduction de clés pour l'établissement de la connexion. La même chose est vraie du changement de clé, bien que la capacité à éviter l'exponentiation pour le changement de clé puisse être souhaitable (mais n'est pas une exigence absolue).

- Les ressources de RAM et/ou flash tendent à être une contrainte dans les mises en œuvre incorporées. 8-10 MB de code et de données pour l'authentification, l'établissement des clés, et le changement de clé est clairement excessif, 800 à 1000 kB est clairement plus que ce qui est souhaitable, mais est tolérable si il n'y a pas d'autre solution de remplacement et 80 à 100 kB devrait être acceptable. Ces tailles sont destinées à donner un grossier ordre de grandeur indicatif, et ne devraient pas être prises comme des cibles ou limites fermes (par exemple, de plus petites tailles de code sont toujours préférables). Les mises en œuvre de logiciels pour des systèmes d'exploitation généralistes peuvent avoir plus de latitude.

Le principal souci de ressources pour la mise en œuvre de mécanismes d'authentification et de changement de clé est la taille du code, car iSCSI suppose que la puissance de calcul pour faire les exponentiations sera disponible.

Il n'y a pas de scénario dominant d'usage iSCSI – les scénarios vont d'une seule connexion contrainte seulement par la bande passante du support à des centaines de connexions d'initiateur à une seule cible ou point d'extrémité de communication. Les sessions SCSI et donc les connexions qu'elles utilisent tendent à être de durée de vie relativement longue ; pour la mémorisation sur disque, un hôte ouvre normalement une connexion SCSI au démarrage et la ferme à la clôture. Une longueur de session de bande tend à se mesurer en heures ou fractions d'heure (c'est-à-dire que des partages rapides du même appareil à bande entre différents initiateurs sont inhabituels) bien que des sessions de contrôle sur un robot à bande puissent être courtes lorsque le robot est partagé entre les pilotes de bandes. D'un autre côté, une bande ne verra pas un grand nombre de connexions d'initiateur à une seule cible ou point d'extrémité de communication, car chaque pilote de bande est dédié à un seul usage à un moment donné, et une douzaine de pilotes de bandes est un gros appareil à bande.

2.3 Protocole de sécurité

2.3.1 Transformations

Toutes les mises en œuvre conformes de sécurité de mémorisation de bloc IP DOIVENT prendre en charge IPsec ESP [RFC2406] pour fournir la sécurité pour les paquets aussi bien de contrôle que de données, ainsi que les mécanismes de protection contre la répétition de IPsec. Lorsque ESP est utilisé, l'authentification de l'origine des données par paquet, la protection de l'intégrité et contre la répétition DOIVENT être utilisées.

Pour fournir la confidentialité avec ESP, ESP avec 3DES en mode CBC [RFC2451], [3DESANSI], DOIT être pris en charge, et AES en mode compteur, comme décrit dans la [RFC3686], DEVRAIT être pris en charge. Pour assurer l'authentification d'origine et l'intégrité des données avec ESP, HMAC-SHA1 [RFC2404] DOIT être pris en charge, et AES en mode MAC CBC avec les extensions XCBC [RFC3566] DEVRAIT être pris en charge. DES en mode CBC NE DEVRAIT PAS être utilisé à cause de sa faiblesse inhérente. ESP avec le chiffrement NUL DOIT être pris en charge pour l'authentification.

2.3.2 Modes IPsec

Les mises en œuvre conformes de protocole de mémorisation de bloc IP DOIVENT prendre en charge ESP [RFC2406] en mode tunnel et PEUVENT mettre en œuvre IPsec avec ESP en mode transport.

2.3.3 IKE

Les mises en œuvre conformes de sécurité de mémorisation de bloc IP DOIVENT prendre en charge IKE [RFC2409] pour l'authentification d'homologues, la négociation des associations de sécurité, et la gestion de clés, en utilisant le DPI IPsec [RFC2407]. La gestion de clés manuelle NE DOIT PAS être utilisée car elle ne fournit pas la prise en charge nécessaire de changement de clés. Les mises en œuvre conformes de sécurité de mémorisation de bloc IP DOIVENT prendre en charge l'authentification d'homologue en utilisant une clé pré partagée, et PEUVENT prendre en charge l'authentification d'homologue fondée sur des certificats en utilisant des signatures numériques. L'authentification d'homologues à l'aide des méthodes de chiffrement à clé publique présentées aux paragraphes 5.2 et 5.3 de IKE [RFC2409] NE DEVRAIENT PAS être utilisées.

Les mises en œuvre conformes de sécurité de mémorisation de bloc IP DOIVENT prendre en charge le mode principal IKE et DEVRAIENT prendre en charge le mode Agressif. Le mode principal IKE avec authentification par clés pré partagées NE DEVRAIT PAS être utilisé quand l'un ou l'autre des homologues utilise une adresse IP allouée de façon dynamique. Bien que le mode principal IKE avec authentification par clés pré partagées offre une bonne sécurité dans de nombreux cas, les situations où sont utilisées des adresses allouées de façon dynamique forcent l'usage d'une clé pré partagée de groupe, ce qui est vulnérable aux attaques par interposition.

Lorsque des signatures numériques sont utilisées pour l'authentification, le mode principal IKE ou le mode agressif IKE PEUVENT être utilisés. Dans tous les cas, l'accès à des informations secrètes mémorisées localement (clé pré partagée, ou clé privée pour signature numérique) doit être convenablement restreint, car la compromission des informations secrètes annule les propriétés de sécurité des protocoles IKE/IPsec.

Lorsque des signatures numériques sont utilisées pour réaliser l'authentification, un négociateur IKE DEVRAIT utiliser une ou des charges utiles de demande de certificat IKE pour spécifier l'autorité (ou les autorités) de certificat qui sont de

confiance en accord avec sa politique locale. Les négociateurs IKE DEVRAIENT vérifier la liste de révocation de certificats (CRL, *Certificate Revocation List*) pertinente avant d'accepter un certificat PKI à utiliser dans des procédures d'authentification de IKE.

Le DOI IPsec [RFC2407] couvre plusieurs types de données d'identification. Au sein de IKE Phase 1, à utiliser au sein des charges utiles IDii et IDir, les mises en œuvre conformes de sécurité de mémorisation de bloc IP DOIVENT prendre en charge les charges utiles d'identité ID_IPV4_ADDR, ID_IPV6_ADDR (si la pile de protocole accepte IPv6) et ID_FQDN. Les mises en œuvre de sécurité iSCSI DEVRAIENT prendre en charge la charge utile d'identité ID_USER_FQDN ; les autres protocoles de mémorisation de bloc IP (iFCP, FCIP) NE DEVRAIENT PAS utiliser la charge utile d'identité ID_USER_FQDN. Les identités autres que ID_IPV4_ADDR et ID_IPV6_ADDR (comme ID_FQDN ou ID_USER_FQDN) DEVRAIENT être employées dans des situations où le mode agressif est utilisé avec des clés pré partagées et où les adresses IP sont allouées de façon dynamique. Les formats sous-réseau IP, gamme d'adresses IP, ID_DER_ASN1_DN, ID_DER_ASN1_GN NE DEVRAIENT PAS être utilisés pour la sécurité de protocole de mémorisation de bloc IP ; la charge utile d'identité ID_KEY_ID NE DOIT PAS être utilisée. Comme décrit dans la [RFC2407], au sein de la phase 1 les champs Accès ID et Protocole DOIVENT être réglés à zéro ou à l'accès UDP 500. Aussi, comme noté dans la [RFC2407] : Quand un échange IKE est authentifié en utilisant des certificats (de tout format) tout identifiant utilisé en entrée de décisions de politique locale DEVRAIT être contenu dans le certificat utilisé dans l'authentification de l'échange.

Les échanges de phase 2 en mode rapide utilisés par les mises en œuvre de protocole de mémorisation de bloc IP DOIVENT porter explicitement les champs Charge utile d'identité (IDci et IDcr). Chaque charge utile de phase 2 IDci et IDcr DEVRAIT porter une seule adresse IP (ID_IPV4_ADDR, ID_IPV6_ADDR) et NE DEVRAIT PAS utiliser les formats sous-réseau IP (*IP Subnet*) ou gamme d'adresse IP *(IP Address Range)*. D'autres formats de charge utile d'identifiant NE DOIVENT PAS être utilisés.

Comme le matériel d'accélération IPsec peut n'être capable de traiter qu'un nombre limité de SA IKE de phase 2 actives, des messages de suppression de phase 2 peuvent être envoyés pour les SA inactives, comme moyen de garder le nombre de SA de phase 2 actives au minimum. La réception d'un message Suppression IKE phase 2 NE DOIT PAS être interprété comme une raison pour supprimer une connexion de mémorisation de bloc IP. Il est plutôt préférable de laisser la connexion vivante, et si du trafic supplémentaire est envoyé dessus, de construire une autre SA IKE phase 2 pour la protéger. Cela évite l'inconvénient de continuellement établir et supprimer les connexions.

2.3.4 Configuration de politique de sécurité

Un des objectifs de la présente spécification est de permettre un haut niveau d'interopérabilité sans exiger de configuration excessive. Ce paragraphe donne des lignes directrices sur le réglage des paramètres IKE afin d'augmenter la probabilité d'une négociation réussie. Il décrit aussi comment les informations sur la configuration de politique de sécurité peuvent être fournies afin d'améliorer encore les chances de succès.

Pour améliorer les perspectives d'interopérabilité, certaines des actions à considérer incluent :

[1] La restriction de transformation.
Comme la prise en charge de 3DES-CBC et HMAC-SHA1 est exigée de toute mise en œuvre, offrir ces transformations améliore la probabilité d'une négociation réussie. Si AES-CTR [RFC3686] avec XCBC-MAC [RFC3566] est pris en charge, cette combinaison de transformations sera normalement préférée, avec 3DES-CBC/HMAC-SHA1 comme offre secondaire.

[2] La restriction de groupe.
Si 3DES-CBC/HMAC-SHA1 est offert, et si des groupes DH sont offerts, il est alors recommandé qu'un groupe DH d'au moins 1024 bits soit offert avec lui. Si AES-CTR/XCBC-MAC est l'offre préférée, et si des groupes DH sont offerts, il est alors recommandé qu'un groupe DH d'au moins 2048 bits soit offert avec lui, comme noté dans [KeyLen]. Si le secret de transmission parfait est exigé en mode rapide, il est alors recommandé que le groupe DH QM PFS soit le même que le groupe DH de IKE Phase 1. Cela réduit le nombre total de combinaisons, améliorant les chances d'interopérabilité.

[3] Les durées de vie de clés.
Si il est offert une durée de vie de clé plus longue que celle désirée, plutôt que de causer l'échec de la négociation IKE, il est recommandé que le répondant considère la durée de vie offerte comme un maximum, et de l'accepter. La clé peut alors utiliser une valeur inférieure pour la durée de vie, et utiliser une Notification de durée de vie afin d'informer l'autre homologue de l'expiration de la durée de vie.

Même lorsque on suit l'avis ci-dessus, il peut encore être utile d'être capable de fournir des informations de configuration

supplémentaires afin d'améliorer les chances de succès, et il est utile d'être capable de gérer la configuration de sécurité sans considération de l'échelle du développement.

Par exemple, il peut être souhaitable de configurer la politique de sécurité d'un appareil de mémorisation de bloc IP. Cela peut se faire manuellement ou automatiquement via un mécanisme de distribution de politique de sécurité. Autrement, il peut être fourni via iSNS ou SLPv2. Si un point d'extrémité de mémorisation de bloc IP peut obtenir la politique de sécurité requise par d'autres moyens (manuels, ou automatiques via un mécanisme de distribution de politique de sécurité) il n'est alors pas besoin de demander ces informations via iSNS ou SLPv2. Cependant, si la configuration de politique de sécurité requise n'est pas disponible via d'autres mécanismes, iSNS ou SLPv2 peuvent être utilisés pour l'obtenir.

Il peut aussi être utile d'obtenir des informations sur les préférences de l'homologue avant d'initier IKE. Bien qu'il soit généralement possible de négocier les paramètres de sécurité au sein d'IKE, il y a des situations dans lesquelles des paramètres incompatibles peuvent causer l'échec de la négociation IKE. Les informations suivantes peuvent être fournies via SLPv2 ou iSNS :

[4] La prise en charge de IPsec ou du texte en clair.
Le minimum de configuration d'homologue requis est si un point d'extrémité de mémorisation de bloc IP exige IPsec ou le texte en clair. Cela ne peut pas être déterminé à partir de la négociation IKE seule sans risquer une longue temporisation, qui est très indésirable pour un protocole à accès par disque.

[5] La prise en charge du secret parfait de transmission (DFS, *Perfect Forward Secrecy*).
Il est utile de savoir si un homologue permet le PFS, car un mode rapide d'IKE Phase 2 peut échouer si un initiateur propose PFS à un répondant qui ne le permet pas.

[6] La préférence pour le mode tunnel.
Bien qu'il soit légal de proposer les deux modes transport et tunnel au sein de la même offre, toutes les mises en œuvre de IKE ne le prennent pas en charge. Il en résulte qu'il est utile de savoir si un homologue préfère le mode tunnel ou le mode transport, afin qu'il soit possible de négocier le mode préféré dès le premier essai.

[7] Prise en charge du mode principal et du mode agressif.
Comme la négociation IKE peut échouer si un mode est proposé à un homologue qui ne le permet pas, il est utile de savoir quels modes permet un homologue, afin qu'un mode permis puisse être négocié dès le premier essai.

Comme iSNS ou SLPv2 peuvent être utilisés pour distribuer la politique de sécurité IPsec et les informations de configuration à utiliser avec les protocoles de mémorisation de bloc IP, ces protocoles de découverte pourraient constituer un 'maillon faible' si ils n'étaient pas sécurisés au moins aussi bien que les protocoles dont ils configurent la sécurité. Comme la vulnérabilité majeure est la modification et la répétition de paquet, lorsque iSNS ou SLPv2 sont utilisés pour distribuer la politique de sécurité ou les informations de configuration, au minimum, l'authentification d'origine des données par paquet, la protection d'intégrité et contre la répétition DOIVENT être utilisées pour protéger le protocole de découverte.

2.4 Authentification iSCSI

2.4.1 CHAP

Les mises en œuvre conformes de iSCSI DOIVENT mettre en œuvre la méthode d'authentification CHAP [RFC1994] (conformément au paragraphe 11.1.4 de la [RFC3720]) qui inclut la prise en charge de l'authentification bidirectionnelle, et l'option d'authentification de la cible.

Lorsque CHAP est effectué sur un canal non chiffré, il est vulnérable à une attaque de dictionnaire hors ligne. Les mises en œuvre DOIVENT prendre en charge les secrets CHAP aléatoires jusqu'à 128 bits, incluant les moyens de générer de tels secrets et de les accepter de la part d'une source de génération externe. Les mises en œuvre NE DOIVENT PAS fournir de moyens de génération (ou d'expansion) de secret autres que la génération aléatoire.

Si CHAP est utilisé avec un secret plus petit que 96 bits, le chiffrement IPsec (conformément aux exigences de mise en œuvre du paragraphe 8.3.2 de la [RFC3720]) DOIT être utilisé pour protéger la connexion. De plus, dans ce cas, l'authentification IKE avec des clés pré partagées de groupe NE DEVRAIT PAS être utilisée. Lorsque CHAP est utilisé avec un secret inférieur à 96 bits, une mise en œuvre conforme NE DOIT PAS continuer la connexion iSCSI à moins qu'elle puisse vérifier que le chiffrement IPsec est utilisé pour protéger la connexion.

Les générateurs NE DOIVENT PAS réutiliser le défi CHAP envoyé par le répondant pour l'autre direction d'une authentification bidirectionnelle. Les répondants DOIVENT vérifier cette condition et clore la connexion iSCSI TCP si elle se produit.

Le même secret CHAP NE DEVRAIT PAS être configuré pour l'authentification de plusieurs initiateurs ou de plusieurs cibles, car cela permet à n'importe lequel d'entre eux de se faire passer pour n'importe lequel d'entre eux, et la compromission de l'un d'eux permet à l'attaquant de se faire passer pour n'importe lequel d'entre eux. Il est recommandé que les mises en œuvre de iSCSI vérifient l'utilisation de secrets CHAP identiques par différents homologues lorsque cette vérification est faisable, et de prendre les mesures appropriées pour avertir les usagers et/ou administrateurs lorsque ceci est détecté. Un seul secret CHAP PEUT être utilisé pour l'authentification d'un initiateur individuel pour plusieurs cibles. De même, un seul secret CHAP PEUT être utilisé pour l'authentification d'une cible individuelle de plusieurs initiateurs.

Un répondant NE DOIT PAS envoyer sa réponse CHAP si l'initiateur n'a pas réussi à s'authentifier. Par exemple, l'échange suivant :

I->R CHAP_A=<A1,A2,...>
R->I CHAP_A=<A1> CHAP_C=<C> CHAP_I=<I>
I->R CHAP_N=<N> CHAP_C=<C> CHAP_I=<I>

(Où N, (A1,A2), I, C, et R sont respectivement le nom, l'algorithme, l'identifiant, le défi, et la réponse comme définis dans la [RFC1994]) DOIT résulter en ce que le répondant (cible) clôt la connexion iSCSI TCP parce que l'initiateur a échoué à s'authentifier (il n'y a pas de CHAP_R dans le troisième message).

Un secret CHAP utilisé pour l'authentification d'initiateur NE DOIT PAS être configuré pour l'authentification d'une cible, et un secret CHAP utilisé pour l'authentification de cible NE DOIT PAS être configuré pour l'authentification d'un initiateur. Si la réponse CHAP reçue par une extrémité d'une connexion iSCSI est la même que la réponse CHAP que le point d'extrémité receveur aurait généré pour le même défi CHAP, la réponse DOIT être traitée comme un échec d'authentification et causer la clôture de la connexion (cela assure que le même secret CHAP n'est pas utilisé pour l'authentification dans les deux directions). Aussi, si une mise en œuvre iSCSI peut fonctionner à la fois comme initiateur et cible, des secrets et identités CHAP différents DOIVENT être configurés pour ces deux rôles. Voici un exemple des attaques empêchées par les exigences ci-dessus:

Rogue veut se faire passer pour Storage auprès d'Alice, et sait qu'un seul secret est utilisé pour les deux directions d'authentification Storage-Alice.

Rogue convainc Alice d'ouvrir deux connexions avec Rogue, et Rogue s'identifie comme Storage sur les deux connexions.

Rogue produit un défi CHAP sur la connexion 1, attend qu'Alice réponde, et ensuite reflète le défi d'Alice comme défi initial à Alice sur la connexion 2.

Si Alice ne vérifie pas qu'il y a réflexion entre les connexions, la réponse d'Alice sur la connexion 2 permet à Rogue de se faire passer pour Storage sur la connexion 1, même si Rogue ne connaît pas le secret CHAP Alice-Storage.

Noter que RADIUS [RFC2865] ne prend pas en charge l'authentification CHAP bidirectionnelle. Donc, alors qu'une cible agissant comme un client RADIUS est capable de vérifier la réponse de l'initiateur, elle ne sera pas capable de répondre au défi d'un initiateur sauf si elle a accès à un secret partagé approprié par d'autres moyens.

2.4.2 SRP

Les mises en œuvre iSCSI PEUVENT utiliser la méthode d'authentification SRP [RFC2945] (voir au paragraphe 11.1.3 de la [RFC3720]). La force de la sécurité de SRP dépend des caractéristiques du groupe utilisé (c'est-à-dire, du nombre premier modulo N et du générateur g). Comme décrit dans la [RFC2945], il est exigé de N qu'il soit un nombre premier Sophie-German (de la forme N = 2q + 1, où q est aussi premier) le générateur g est une racine primitive de GF(n) [SRPNDSS].

Les groupes bien connus SRP sont inclus dans l'Appendice A et des groupes supplémentaires peuvent être enregistrés auprès de l'IANA. Les mises en œuvre iSCSI DOIVENT utiliser un de ces groupes bien connus. Tous les groupes spécifiés dans l'Appendice A jusqu'à 1536 bits (c'est-à-dire, SRP-768, SRP-1024, SRP-1280, SRP-1536) DOIVENT être pris en charge par les initiateurs et les cibles. Pour garantir l'interopérabilité, les cibles DOIVENT toujours offrir "SRP-1536" comme un des groupes proposés.

2.5 Sécurité de SLPv2

Les protocoles iSCSI et FCIP utilisent tous deux SLPv2 comme moyen de découvrir les entités homologues et les serveurs de gestion. SLPv2 peut aussi être utilisé pour fournir des informations sur la configuration de sécurité de l'homologue.

Lorsque SLPv2 est déployé, les annonces de SA ainsi que les demandes et/ou réponses d'UA sont soumises aux menaces suivantes pour la sécurité :

[1] Un attaquant pourrait insérer ou altérer des annonces de SA ou une réponse à une demande d'UA afin de se faire passer pour l'homologue réel ou lancer une attaque de déni de service.

[2] Un attaquant pourrait avoir connaissance d'une SA ou d'une UA par espionnage, et lancer une attaque contre l'homologue. Étant donnée la valeur potentielle des cibles iSCSI et des entités FCIP, la fuite de telles informations non seulement augmente la possibilité d'une attaque sur le réseau mais il y a aussi le risque d'un vol physique.

[3] Un attaquant pourrait parodier un DAAdvert. Cela pourrait amener les UA et SA à utiliser des DA contrefaits.

Pour contrer ces menaces, les capacités suivantes sont requises :

[a] Les informations de service, telles qu'incluses dans les messages SrvRply, AttrRply, SrvReg et SrvDereg, doivent rester confidentielles.

[b] L'UA doit être capable de distinguer entre informations de service légitimes et illégitimes dans les messages SrvRply et AttrRply. Dans le modèle de sécurité SLPv2, les SA sont de confiance pour signer les données.

[c] Le DA doit être capable de distinguer entre messages SrvReg et SrvDereg légitimes et illégitimes.

[d] L'UA doit être capable de distinguer entre annonces DA légitimes et illégitimes. Cela permet à l'UA d'éviter des DA félons qui retourneraient des données incorrectes ou pas de données du tout. Dans le modèle de sécurité SLPv2, les UA font confiance aux DA pour mémoriser les données, répondre aux questions sur les données et transmettre les données sur les services, mais pas nécessairement pour les générer.

[e] Les SA peuvent avoir à faire confiance aux DA, en particulier si SLPv2 'amélioré par maillage' est utilisé. Dans ce cas, les SA s'enregistrent auprès d'une seule DA et ont confiance que cette DA va transmettre l'enregistrement aux autres.

Par elle-même, la sécurité SLPv2, définie dans la [RFC2608], ne satisfait pas à ces exigences de sécurité. SLPv2 n'assure que l'authentification de bout en bout, mais n'assure pas la confidentialité. Dans l'authentification SLPv2 il n'y a aucun moyen pour authentifier les "réponses à résultat nul". Cela permet à un attaquant de monter une attaque de déni de service en envoyant à des UA des SrvRply ou AttrRply à "résultat nul" comme si elles venaient d'une DA dont l'adresse de source correspond à un DAAdvert légitime.

Dans tous les cas, il y a un potentiel d'attaque de déni de service contre les fournisseur de service du protocole, mais une telle attaque est possible même en l'absence de mécanisme de découverte fondé sur SLPv2.

2.5.1 Protocole SLPv2 de sécurité

Les types de message SLPv2 incluent SrvRqst, SrvRply, SrvReg, SrvDereg, SrvAck, AttrRqst, AttrRply, DAAdvert, SrvTypeRqst, SrvTypeRply, et SAAdvert. SLPv2 exige que les agents d'utilisateur (UA, *User Agent*) et les agents de service (SA, *Service Agent*) prennent en charge SrvRqst, SrvRply, et DAAdvert. Les SA doivent de plus prendre en charge SrvReg, SrvAck, et SAAdvert.

Lorsque il n'existe pas d'agent de répertoire (DA, *Directory Agent*), le SrvRqst est en diffusion groupée, mais la SrvRply est envoyée via UDP en envoi individuel. Les DAAdvert sont aussi en diffusion groupée. Cependant, tous les autres messages SLPv2 sont envoyés en individuel via UDP.

Afin de fournir la fonction de sécurité requise, les mises en œuvre de iSCSI et FCIP qui prennent en charge la sécurité SLPv2 DEVRAIENT protéger les messages SLPv2 envoyés via l'envoi individuel en utilisant IPsec ESP avec une transformation non nulle. Les blocs d'authentification SLPv2 (qui portent des signatures numériques) décrits dans la [RFC2608] PEUVENT aussi être utilisés pour authentifier les messages en envoi individuel et en diffusion groupée.

L'usage de SLPv2 par iSCSI est décrit dans la [RFC4018]. Les initiateurs et cibles iSCSI peuvent activer les mécanismes IKE pour établir les identités. De plus, une connexion iSCSI suivante de session de niveau usager peut protéger la liaison initiateur-cible. Cela va les protéger de toute compromission de la sécurité dans le processus de découverte SLPv2.

L'usage de SLPv2 par FCIP est décrit dans la [RFC3822]. Les entités FCIP supposent qu'une fois que l'identité IKE d'un homologue est établie, le nom d'entité FCIP porté dans la trame courte FCIP est aussi implicitement accepté comme homologue authentifié. Toute association de ce type entre l'identité IKE et le nom d'entité FCIP est établie administrativement.

Pour son utilisation dans la sécurisation de SLPv2, lorsque des signatures numériques sont utilisées pour réaliser l'authentification dans IKE, un négociateur IKE DEVRAIT utiliser une ou des charges utiles Demande de certificat IKE pour spécifier l'autorité (ou les autorités) de certificat qui sont de confiance en conformité avec sa politique locale. Les négociateurs IKE DEVRAIENT vérifier la liste de révocation de certificats (CRL, *Certificate Revocation List*) pertinente avant d'accepter un certificat PKI à utiliser dans la procédure d'authentification d'IKE. Si la gestion de clé des DA SLPv2

n'a pas besoin d'être coordonnée avec les SA et les UA ainsi qu'avec les mises en œuvre de service de protocole, on peut utiliser la gestion de clé fondée sur le certificat, avec une autorité de certificat (CA, *Certificate Authority*) racine partagée.

Une des raisons pour utiliser IPsec pour la sécurité SLPv2 est qu'il est plus probable que des certificats seront déployés pour IPsec que pour SLPv2. Cela simplifie la sécurité SLPv2 et rend tout à la fois plus probable qu'elle sera mise en œuvre de façon interopérable et, plus important, qu'elle sera utilisée. Il en résulte qu'il est désirable qu'il n'en soit pas demandé beaucoup plus pour activer la protection IPsec de SLPv2.

Cependant, le simple fait qu'un certificat soit de confiance pour l'utilisation avec IPsec n'implique pas nécessairement que l'hôte est autorisé à effectuer des opérations SLPv2. Lorsque on utilise IPsec pour sécuriser SLPv2, il peut être souhaitable de distinguer entre les certificats appropriés pour les UA, les SA, et les DA. Par exemple, alors qu'un UA pourrait être autorisé à utiliser tout certificat se conformant à la politique de certificat d'IKE, le certificat utilisé par un SA peut indiquer qu'il est une source légitime d'annonces de service. De même, un certificat de DA peut indiquer qu'il est un DA valide. Cela peut se faire en utilisant des CA spéciaux pour produire des certificats valides utilisés par les SA et les DA ; autrement, on peut employer des autorisations de SA et de DA.

On suppose que la politique de production et distribution des certificats SLPv2 autorisés aux SA et DA les limite aux seuls SA et DA légitimes. Dans ce cas, IPsec est utilisé pour fournir la sécurité SLPv2 comme suit :

[a] Les messages SLPv2 en envoi individuel sont protégés par IPsec, en utilisant ESP avec une transformation non nulle.

[b] Les messages SrvRply et AttrRply provenant d'un DA ou d'un SA sont en envoi individuel aux UA. On suppose que le SA a utilisé un certificat autorisé pour l'annonce de service SLPv2 en établissant la SA IKE phase 1, ou que le DA a utilisé un certificat autorisé pour l'usage du DA, l'UA peut accepter les informations envoyées, même si il n'a pas de bloc d'authentification SLPv2.

Noter que lorsque les messages SrvRqst sont en diffusion groupée, ils ne sont pas protégés. Un attaquant peut tenter d'exploiter cela en falsifiant une SrvRqst en diffusion groupée provenant de l'UA, générant une SrvRply provenant d'un SA du choix de l'attaquant. Bien que la SrvRply soit sécurisée, elle ne correspond pas à une SrvRqst légitime envoyée par l'UA. Pour éviter cette attaque, où les messages SrvRqst sont en diffusion groupée, l'UA DOIT vérifier que les messages SrvRply représentent une réponse légitime à la SrvRqst qui a été envoyée.

[c] Les messages SrvReg et SrvDereg provenant d'un SA sont en envoi individuel aux DA. On suppose que le SA a utilisé un certificat autorisé pour l'annonce de service SLPv2 en établissant la SA IKE phase 1, le DA peut accepter l'enregistrement/désenregistrement même si il n'a pas de bloc d'authentification SLPv2. Normalement, le SA va vérifier l'autorisation du DA avant d'envoyer l'annonce de service.

[d] Les DAAdvert en diffusion groupée peuvent être considérés comme facultatifs. L'UA va tenter de contacter les DA via l'envoi individuel. On suppose que le DA a utilisé un certificat autorisé pour les DAAdvert SLPv2 en établissant la SA IKE phase 1, l'UA peut accepter le DAAdvert même si il n'a pas de bloc d'authentification SLPv2.

[e] Les SA peuvent accepter les DAAdvert comme décrit en [d].

2.5.2 Confidentialité des informations de service

Comme les messages SLPv2 peuvent contenir des informations qui peuvent révéler le fabricant de l'appareil ou ses autres caractéristiques associées, la révélation des informations de service constitue un risque pour la sécurité. À titre d'exemple, le nom d'entité FCIP peut révéler un WWN à partir duquel un attaquant peut découvrir des informations potentiellement utiles sur les caractéristiques de l'entité.

Le modèle de sécurité SLPv2 suppose que les informations de service sont publiques, et n'assure donc pas leur confidentialité. Cependant, les appareils de mémorisation représentent une infrastructure critique de mission de valeur substantielle, et donc les mises en œuvre de iSCSI et de sécurité FCIP qui prennent en charge la sécurité SLPv2 DEVRAIENT chiffrer ainsi qu'authentifier et protéger en intégrité les messages SLPv2 en envoi individuel.

En supposant que tous les messages SLPv2 en envoi individuel sont protégés par IPsec, et que la confidentialité est assurée, le risque de divulgation peut alors être limité aux messages SLPv2 envoyés via diffusion groupée, à savoir le SrvRqst et le DAAdvert.

Les fuites d'informations dans une SrvRqst en diffusion groupée dépendent du niveau de détail dans l'interrogation. Si la fuite est un problème, un DA peut alors être fourni. Si ce n'est pas faisable, une interrogation générale peut alors être

envoyés via diffusion groupée, et d'autres détails peuvent ensuite être obtenus des entités qui répondent via des interrogations supplémentaires en envoi individuel, protégées par IPsec.

Les fuites d'informations via une DAAdvert en diffusion groupée posent moins de problèmes que l'authenticité du message, car savoir qu'un DA est présent sur le réseau permet seulement à l'attaquant de savoir que SLPv2 est utilisé, et éventuellement qu'un service de répertoire est aussi présent. Ces informations ne sont pas considérées comme très précieuses.

2.5.3 Implications de SLPv2 pour la sécurité

Par la définition des attributs de sécurité, il est possible d'utiliser SLPv2 pour distribuer des informations sur les réglages de sécurité pour les entités de mémorisation de bloc IP. La distribution par SLPv2 des politiques de sécurité n'est pas nécessaire si les réglages de sécurité peuvent être déterminés par d'autres moyens, tels qu'une configuration manuelle ou la distribution de politique de sécurité IPsec. Si une entité a déjà obtenu sa configuration de sécurité via d'autres mécanismes, elle NE DOIT PAS demander alors la politique de sécurité via SLPv2.

Lorsque SLPv2 est utilisé pour fournir les informations de politique de sécurité à utiliser avec les protocoles de mémorisation de bloc IP, SLPv2 DOIT être protégé par IPsec comme décrit dans le présent document. Lorsque SLPv2 n'est pas utilisé pour distribuer les informations de politique de sécurité, les mises en œuvre PEUVENT utiliser la sécurité SLPv2 comme décrit dans le présent document.

Lorsque SLPv2 est utilisé, mais que la sécurité n'est pas mise en œuvre, les mises en œuvre du protocole de mémorisation de bloc IP DOIVENT prendre en charge une antémémoire négative pour les échecs d'authentification. Cela permet aux mises en œuvre d'éviter de contacter continuellement les points d'extrémité découverts qui ont échoué à l'authentification au sein d'IPsec ou à la couche application (dans le cas de connexion iSCSI). L'antémémoire négative n'a pas besoin d'être entretenue au sein de la mise en œuvre IPsec, mais plutôt au sein de la mise en œuvre de protocole de mémorisation de bloc IP.

Comme le présent document propose que la sécurité bond par bond soit utilisée comme principal mécanisme pour protéger SLPv2, les UA doivent faire confiance aux DA pour relayer précisément les données provenant des SA. C'est un changement au modèle de sécurité SLPv2 décrit dans la [RFC2608]. Cependant, l'authentification SLPv2 telle que définie dans la [RFC2608] ne fournissait pas de moyen d'authentifier les "réponses à résultat nul", laissant SLPv2 vulnérable à une attaque de déni de service. Une telle attaque peut être menée contre un UA en lui envoyant une SrvRply ou AttrRply "résultat nul", envoyée à partir d'une adresse de source correspondant à un DA qui produit une DAAdvert légitime.

De plus, la sécurité SLPv2 telle que définie dans la [RFC2608] ne prend pas en charge la confidentialité. Lorsque IPsec, avec ESP et une transformation non nulle, est utilisé pour protéger SLPv2, non seulement les demandes et réponses en envoi individuel peuvent être authentifiées, mais la confidentialité peut aussi être fournie. Cela inclut les demandes en envoi individuel aux DA et SA ainsi que les réponses. Il est aussi possible de découvrir activement les SA en utilisant la découverte de SA en diffusion groupée, et d'envoyer alors des demandes en individuel aux SA découverts.

Il en résulte que, pour utilisation avec les protocoles de mémorisation de bloc IP, on pense que l'utilisation d'IPsec pour la sécurité est plus appropriée que le modèle de sécurité SLPv2 défini dans la [RFC2608].

Utiliser IPsec pour sécuriser SLPv2 a des implications en termes de performances. Les associations de sécurité établies entre :

- Les UA et les SA peuvent être réutilisées (le client sur l'hôte UA va utiliser le service sur l'hôte SA).
- Les SA et les DA peuvent être réutilisés (les SA vont réenregistrer les services).
- Les UA et les DA ne vont probablement pas être réutilisés (il en résulterait probablement beaucoup d'associations de sécurité inactives, et construites sur le DA).

Lorsque IPsec est utilisé pour protéger SLPv2, il n'est pas nécessairement approprié pour tous les hôtes avec qui une association de sécurité IPsec peut être établie d'être de confiance pour générer des annonces de service SLPv2. C'est particulièrement le cas dans des environnements où il est aisé d'obtenir des certificats valides à utiliser avec IPsec (par exemple, où toute personne qui a accès au réseau peut obtenir un certificat de machine valide pour être utilisé avec IPsec). Si tous les hôtes ne sont pas autorisés à générer des annonces de service, il est alors nécessaire de distinguer entre hôtes autorisés et non autorisés.

Cela peut être accompli par les mécanismes suivants :

[1] Configurer les SA avec les caractéristiques d'identité ou de certificat de DA valides, et configurer les DA avec les identités des SA à qui il est permis d'annoncer des services de mémorisation de bloc IP. Les DA sont alors de

confiance pour appliquer les politiques sur l'enregistrement de service. Cette approche implique une configuration manuelle, mais évite la personnalisation des certificats pour SLPv2.

[2] Restreindre la production des certificats valides à utiliser pour l'annonce de service SLPv2. Alors que tous les certificats d'utilisation admise avec IPsec vont s'enchaîner à une racine de confiance, les certificats pour les hôtes autorisés à générer des annonces de service pourraient être signés par un CA autorisé SLPv2, ou pourraient contenir des autorisations SLPv2 explicites au sein du certificat. Après l'établissement de l'association de sécurité IPsec entre les entités SLPv2, les mises en œuvre SLPv2 peuvent alors récupérer les certificats utilisés dans la négociation afin de déterminer si les entités sont autorisées pour les opérations qui sont à effectuer. Cette approche exige moins de configuration, mais exige une personnalisation des certificats à utiliser avec SLPv2.

2.6 Sécurité de iSNS

Le protocole iSCSI peut utiliser iSNS pour des services de découverte et de gestion, alors que le protocole iFCP est nécessaire pour utiliser iSNS pour de tels services. De plus, iSNS peut être utilisé pour mémoriser et distribuer en toute sécurité des informations de politique et d'autorisation aux appareils iSCSI et iFCP. Lorsque le protocole iSNS est déployé, l'interaction entre serveur iSNS et client iSNS est soumise aux menaces supplémentaires suivantes contre la sécurité :

[1] Un attaquant peut altérer les messages du protocole iSNS, amenant les appareils iSCSI et iFCP à établir des connexions avec des appareils félons, ou affaiblissant la protection IPsec pour le trafic iSCSI ou iFCP.

[2] Un attaquant peut se faire passer pour le serveur iSNS en envoyant de faux messages de vie *(heartbeat)* iSNS. Cela peut tromper les appareils iSCSI et iFCP et les amener à utiliser des serveurs iSNS félons.

[3] Un attaquant peut avoir connaissance des appareils iSCSI et iFCP en espionnant les messages de protocole iSNS. De telles informations pourraient aider un attaquant à monter une attaque directe sur les appareils iSCSI et iFCP, comme une attaque de déni de service ou un vol physique direct.

Pour contrer ces menaces, les capacités suivantes sont nécessaires :

[a] Les messages de protocole iSNS en envoi individuel peuvent devoir être authentifiés. De plus, pour protéger contre la menace [3] ci-dessus, la prise en charge de la confidentialité est souhaitable, et EXIGÉE lorsque certaines fonctions de iSNS sont utilisées.

[b] Les messages de protocole iSNS en diffusion groupée tels que les messages de vie iSNS ont besoin d'authentification. Ces messages n'ont pas besoin d'être confidentiels car ils ne contiennent pas d'informations critiques.

Il n'est pas exigé que les identités des entités iSNS restent confidentielles. Précisément, l'identité et la localisation du serveur iSNS n'ont pas besoin de rester confidentielles.

Pour protéger contre un attaquant qui se ferait passer pour un serveur iSNS, les appareils clients DOIVENT prendre en charge l'authentification des messages en diffusion ou diffusion groupée tels que les messages de vie iSNS. Le bloc d'authentification iSNS (qui est identique en format au bloc d'authentification SLP) PEUT être utilisé à cette fin. Noter que le bloc d'authentification n'est utilisé que pour les messages iSNS en diffusion ou diffusion groupée, et NE DEVRAIT PAS être utilisé dans les messages iSNS en envoi individuel.

Comme iSNS est utilisé pour distribuer des autorisations qui déterminent quels appareils clients peuvent communiquer, l'authentification IPsec et l'intégrité des données DOIVENT être prises en charge. De plus, si iSNS est utilisé pour distribuer la politique de sécurité pour les appareils iFCP et iSCSI, l'authentification, l'intégrité des données, et la confidentialité DOIVENT alors être prises en charge et utilisées.

Lorsque iSNS est utilisé sans sécurité, les mises en œuvre du protocole de mémorisation de bloc IP DOIVENT prendre en charge une antémémoire négative pour les échecs d'authentification. Cela permet aux mises en œuvre d'éviter de continuellement contacter les points d'extrémité découverts qui ont échoué à l'authentification au sein d'IPsec ou à la couche application (dans le cas d'une connexion iSCSI). L'antémémoire négative n'a pas besoin d'être entretenue au sein de la mise en œuvre IPsec, mais plutôt au sein de la mise en œuvre du protocole de mémorisation de bloc IP.

2.6.1 Utilisation de iSNS pour découvrir la configuration de sécurité des appareils homologues

En pratique, au sein d'une seule installation, les appareils iSCSI et/ou iFCP peuvent avoir des réglages de sécurité différents. Par exemple, certains appareils peuvent être configurés pour initier des communications sûres, tandis que

d'autres appareils peuvent être configurés pour répondre à une demande de communication sûre, mais non pour exiger la sécurité. D'autres appareils encore, bien que capables de sécurité, peuvent n'initier ni répondre de façon sécurisée.

En pratique, ces variations de configuration peuvent résulter en ce que des appareils soient incapables de communiquer les uns avec les autres. Par exemple, un appareil qui est configuré pour toujours initier une communication sécurisée va éprouver des difficultés à communiquer avec un appareil qui n'initie ni ne répond de façon sécurisée.

Le protocole iSNS est utilisé pour transférer des informations de dénomination, de découverte, et de gestion entre des appareils iSCSI, des passerelles iFCP, des stations de gestion, et le serveur iSNS. Cela inclut la capacité à activer la découverte des réglages de sécurité utilisés pour les communications via les protocoles iSCSI et/ou iFCP.

Le serveur iSNS mémorise les réglages de sécurité pour chaque interface d'appareil iSCSI et iFCP. Ces réglages de sécurité, qui peuvent être retrouvés par les hôtes autorisés, incluent l'utilisation ou la non utilisation de IPsec, IKE, du mode principal, du mode agressif, de PFS, de clés pré partagées, et de certificats.

Par exemple, IKE peut n'être pas activé pour une interface d'appareil particulier. Si un appareil homologue peut apprendre cela à l'avance en consultant le serveur iSNS, il n'aura pas besoin de perdre du temps et des ressources à tenter d'initier une SA IKE phase 1 avec cette interface d'appareil.

Si iSNS est utilisé pour distribuer une politique de sécurité, les informations minimum qui devrait alors être apprises du serveur iSNS sont l'utilisation ou non de IKE et IPsec par chaque interface d'appareil homologue iFCP ou iSCSI. Ces informations sont codées dans le champ Security Bitmap de chaque portail de l'appareil homologue, et sont applicables interface par interface pour l'appareil homologue. Les interrogations iSNS pour acquérir les données de configuration de sécurité sur les appareils homologues DOIVENT être protégées par l'authentification IPsec/ESP.

2.6.2 Utilisation de iSNS pour distribuer les politiques de sécurité iSCSI et iFCP

Une fois que la communication entre les clients iSNS et le serveur iSNS est sécurisée par l'utilisation de IPsec, les clients iSNS ont la capacité de découvrir les réglages de sécurité exigés pour la communication via les protocoles iSCSI et/ou iFCP. L'utilisation de iSNS pour la distribution des politiques de sécurité offre la possibilité de réduire la charge de la configuration manuelle des appareils, et diminue la probabilité d'échecs de communications dus à des politiques de sécurité incompatibles. Si iSNS est utilisé pour distribuer les politiques de sécurité, l'authentification IPsec, l'intégrité des données, et la confidentialité DOIVENT alors être utilisées pour protéger tous les messages de protocole iSNS.

La configuration IKE/IPsec complète de chaque appareil iFCP et/ou iSCSI peut être mémorisée dans le serveur iSNS, y compris les politiques qui sont utilisées pour les négociations IKE phase 1 et phase 2 entre les appareils clients. Le format de charge utile IKE inclut une série d'une ou plusieurs propositions que l'appareil iSCSI ou iFCP va utiliser lors de la négociation de la politique IPsec appropriée à utiliser pour protéger le trafic iSCSI ou iFCP.

Noter que la distribution de politique de sécurité par iSNS n'est pas nécessaire si les réglages de sécurité peuvent être déterminés par d'autres moyens, tels que la configuration manuelle ou la distribution de politique de sécurité par IPsec. Si une entité a déjà obtenu sa configuration de sécurité via d'autres mécanismes, elle NE DOIT PAS demander alors la politique de sécurité via iSNS.

Pour plus de détails sur la façon de mémoriser et restituer les propositions de politique d'IKE dans le serveur iSNS, voir la [RFC4939].

2.6.3 Interaction iSNS avec IKE et IPsec

Lorsque la sécurité IPsec est activée, chaque client iSNS qui est enregistré dans la base de données iSNS entretient au moins une association de sécurité de phase 1 et une de phase 2 avec le serveur iSNS. Tous les messages de protocole iSNS entre les clients iSNS et le serveur iSNS sont à protéger par une association de sécurité de phase 2.

2.6.4 Exigences de mise en œuvre de serveur iSNS

Toutes les mises en œuvre iSNS DOIVENT prendre en charge le mécanisme de protection contre la répétition d'IPsec. ESP en mode tunnel DOIT être mis en œuvre, et IPsec avec ESP en mode transport PEUT être mis en œuvre.

Pour fournir l'authentification d'origine des données et la protection de l'intégrité avec ESP, HMAC-SHA1 DOIT être pris en charge, et AES en mode MAC CBC avec les extensions XCBC [RFC3566] DEVRAIT être pris en charge. Lorsque la confidentialité est mise en œuvre, 3DES en mode CBC DOIT être pris en charge, et AES en mode Compteur, comme décrit dans la [RFC3686], DEVRAIT être pris en charge. DES en mode CBC NE DEVRAIT PAS être utilisé à cause de sa

faiblesse inhérente. Si la confidentialité n'est pas exigée mais si l'authentification d'origine des données et la protection de l'intégrité sont activées, ESP avec chiffrement NUL DOIT être utilisé.

Les mises en œuvre iSNS conformes DOIVENT prendre en charge IKE pour l'authentification, la négociation des associations de sécurité, et la gestion de clés, en utilisant le DOI IPsec, décrit dans la [RFC2407]. On peut s'attendre à ce que les protocoles de mémorisation de bloc IP envoient de forts volumes de données, ce qui exige des changements de clés. Comme la gestion de clés manuelle n'assure pas la prise en charge du changement de clés, son utilisation est interdite avec les protocoles de mémorisation de bloc IP. Bien que iSNS n'envoie pas un fort volume de données, et que donc le changement de clés ne soit pas un souci majeur, le changement de clés manuel NE DEVRAIT PAS être utilisé. Cela dans un souci de cohérence, car la prise en charge du changement dynamique de clés est déjà exigé des mises en œuvre de sécurité de mémorisation IP.

Les mises en œuvre conformes de la sécurité d'iSNS DOIVENT prendre en charge l'authentification en utilisant une clé prépartagée, et PEUVENT prendre en charge l'authentification de l'homologue fondée sur le certificat en utilisant des signatures numériques. L'authentification de l'homologue en utilisant les méthodes de chiffrement à clé publique exposées aux paragraphes 5.2 et 5.3 de la [RFC2409] NE DEVRAIT PAS être utilisée.

Les mises en œuvre iSNS conformes DOIVENT prendre en charge le mode principal IKE et DEVRAIENT prendre en charge le mode agressif. Le mode principal IKE avec l'authentification par clés pré partagées NE DEVRAIT PAS être utilisé lorsque l'un ou l'autre des homologues utilise des adresses IP allouées de façon dynamique. Bien que le mode principal avec authentification par clés pré partagées offre une bonne sécurité dans de nombreux cas, les situations où les adresses allouées de façon dynamique sont utilisées forcent l'usage d'une clé prépartagée de groupe, qui est vulnérable à l'attaque par interposition.

Lorsque les signatures numériques sont utilisées pour l'authentification, le mode principal IKE ou le mode agressif IKE PEUVENT l'un ou l'autre être utilisés. Dans tous les cas, l'accès aux informations secrètes mémorisées localement (clé prépartagée ou clé privée pour signature numérique) DOIT être convenablement restreint, car la compromission des informations secrètes annule les propriétés de sécurité des protocoles IKE/IPsec.

Lorsque des signatures numériques sont utilisées pour réaliser l'authentification, un négociateur IKE DEVRAIT utiliser une ou des charges utiles Demande de certificat IKE pour spécifier l'autorité (ou les autorités) de certificat qui sont de confiance en conformité avec sa politique locale. Les négociateurs IKE DEVRAIENT vérifier la liste de révocation de certificats (CRL, *Certificate Revocation List*) pertinente avant d'accepter un certificat PKI à utiliser dans les procédures d'authentification de IKE.

3. Lignes directrices d'interopérabilité pour la sécurité dans iSCSI

Les lignes directrices suivantes sont établies pour satisfaire aux exigences de sécurité d'iSCSI en utilisant IPsec dans la pratique.

3.1 Questions de sécurité dans iSCSI

iSCSI fournit l'identifiant iSCSI, présenté dans la [RFC3720], qui inclut la prise en charge de l'authentification de couche application. Cette authentification est logiquement entre l'initiateur iSCSI et la cible iSCSI (par opposition à entre les points d'extrémité de communication TCP/IP). L'intention du concept iSCSI est que l'initiateur et la cible représentent les systèmes (par exemple, hôte et dispositif de disque ou système de bande magnétique) participant à la communication, par opposition aux interfaces ou points d'extrémité de communication réseau.

Le protocole iSCSI et l'authentification d'amorçage iSCSI ne satisfont pas aux exigences de sécurité pour iSCSI. L'authentification d'amorçage iSCSI assure l'authentification mutuelle entre l'initiateur et la cible iSCSI à l'origine de la connexion, mais ne protège pas le trafic de contrôle et de données paquet par paquet, laissant la connexion iSCSI vulnérable aux attaques. L'authentification d'amorçage iSCSI authentifie l'initiateur auprès de la cible, mais ne fournit pas par elle-même d'authentification, de protection de l'intégrité, de la confidentialité ou contre la répétition, paquet par paquet. De plus, l'authentification d'amorçage iSCSI n'assure pas une négociation protégée de suite de chiffrement. Donc, l'amorçage iSCSI donne une solution de sécurité faible.

3.2 Interaction entre iSCSI et IPsec

Une session iSCSI [RFC3720], comportant une ou plusieurs connexions TCP, est identifiée par le couple constitué par l'identifiant défini par l'initiateur et celui défini par la cible, <ISID, TSIH>. Chaque connexion dans une session donnée

reçoit une identification de connexion (CID, *Connection Identification*) univoque. La connexion TCP est identifiée par le quintuplé <adresse IP de source, adresse IP de destination, protocole (TCP), accès de source, accès de destination>. Une SA IPsec de phase 2 est identifiée par le triplet <protocole (ESP), adresse de destination, SPI>.

Les informations de session iSCSI et de connexion sont portées dans les commandes d'amorçage iSCSI, et transportées sur TCP. Comme un initiateur iSCSI peut avoir plusieurs interfaces, les connexions iSCSI au sein d'une session iSCSI peuvent être initiées à partir d'adresses IP différentes. De même, plusieurs cibles iSCSI peuvent exister derrière une seule adresse IP, de sorte qu'il peut y avoir plusieurs sessions iSCSI entre une certaine paire <adresse IP de source, adresse IP de destination>.

Lorsque plusieurs sessions iSCSI sont actives entre une certaine paire <initiateur, cible>, l'ensemble de connexions TCP utilisé par une certaine session iSCSI doit être disjoint de celui utilisé par toutes les autres sessions iSCSI entre la même paire <initiateur, cible>. Donc, une connexion TCP peut être associée à une session iSCSI et seulement une.

Les relations entre les sessions iSCSI, les connexions TCP et les SA IKE phase 1 et phase 2 sont les suivantes :

[1] Un initiateur ou une cible iSCSI peut avoir plus d'une interface, et donc avoir plusieurs adresses IP. Aussi, plusieurs initiateurs et cibles iSCSI peuvent exister derrière une seule adresse IP. Il en résulte qu'une session iSCSI peut correspondre à plusieurs associations de sécurité IKE phase 1, bien que normalement une seule association de sécurité IKE phase 1 existera pour un couple <adresse IP d'initiateur, adresse IP de cible>.

[2] Chaque connexion TCP au sein d'une session iSCSI est protégée par une SA IKE phase 2. Les sélecteurs peuvent être spécifique de cette connexion TCP ou peuvent couvrir plusieurs connexions. Alors que chaque SA IKE phase 2 peut protéger plusieurs connexions TCP, chaque connexion TCP est transportée sur seulement une SA IKE phase 2.

Cela étant, toutes les informations nécessaires pour la liaison iSCSI/IPsec sont contenues dans les messages iSCSI Login des l'initiateur et la cible iSCSI. Cela inclut le lien entre une SA IKE phase 1 et les sessions iSCSI correspondantes, ainsi que le lien entre une connexion TCP, une SA IKE phase 2, et l'identifiant de connexion iSCSI.

3.3 Initier une nouvelle session iSCSI

Afin de créer une nouvelle session iSCSI, si il n'existe pas déjà une SA IKE phase 1, elle est alors établie par un initiateur qui met en œuvre la sécurité iSCSI. Les connexions iSCSI suivantes établies au sein de la session iSCSI vont normalement être protégées par des SA IKE phase 2 déduites de cette SA IKE phase 1, bien que des SA IKE phase 1 supplémentaires puissent aussi être établies.

Les mises en œuvre d'initiateur et de cible achèvent avec succès les négociations de IKE phase 1 et phase 2 avant que l'initiateur iSCSI contacte la cible sur l'accès TCP bien connu 3260, et envoie la commande iSCSI Login sur la connexion TCP. Les mises en œuvre IPsec configurées avec les politiques correctes (par exemple, utilisant ESP avec une transformation non nulle pour tout le trafic destiné à l'accès TCP bien connu 3260) vont traiter cela automatiquement.

L'initiateur remplit le champ ISID, et laisse le champ TSIH réglé à zéro, pour indiquer que c'est le premier message d'un nouvel échange d'établissement de session. L'initiateur remplit aussi une valeur de CID, qui identifie la connexion TCP sur laquelle la commande Login est échangée. Lorsque la cible iSCSI répond par sa commande Login, les deux appareils iSCSI vont connaître le TSIH, et donc l'identifiant de session iSCSI <ISID, TSIH>.

Un seul identifiant de session iSCSI peut avoir plusieurs SA IKE phase 1 associées, et chaque SA IKE phase 1 peut correspondre à plusieurs identifiants de session iSCSI. Chaque connexion iSCSI (identifiée par l'identifiant de connexion) correspond à une seule connexion TCP (identifiée par le quintuplet). Chaque SA IKE phase 2 est identifiée par la combinaison <Protocole (ESP), adresse de destination, SPI>. Une SA de phase 2 peut protéger plusieurs connexions TCP, et correspondre à une seule SA IKE phase 1.

Au sein de IKE, chaque rafraîchissement de clé exige qu'une nouvelle association de sécurité soit établie. En pratique, il y a un intervalle de temps durant lequel une vieille SA, sur le point d'expirer, et une SA nouvellement établie vont être toutes deux valides. La mise en œuvre IPsec va choisir quelle association de sécurité utiliser sur la base de la politique locale, et les problèmes de iSCSI ne jouent aucun rôle dans ce processus de sélection.

3.4 Fermeture en douceur de iSCSI

Des mécanismes au sein de iSCSI assurent la fermeture aussi bien en douceur que non en douceur des sessions iSCSI ou des connexions TCP individuelles au sein d'une session. La commande iSCSI Logout est utilisée pour effectuer la suppression en douceur. Cette commande permet à l'initiateur iSCSI de demander que :

[a] la session soit close,
[b] une connexion spécifique au sein de la session soit close,
[c] une connexion spécifique soit marquée pour récupération.

Lorsque la mise en œuvre iSCSI souhaite fermer une session, elle utilise la commande iSCSI appropriée pour accomplir cela. Après les échanges de messages de contrôle iSCSI appropriés pour la clôture de session, la mise en œuvre de sécurité iSCSI va normalement initier une demi clôture de chaque connexion TCP au sein de la session iSCSI.

Lorsque la mise en œuvre de sécurité iSCSI souhaite fermer une connexion TCP individuelle tout en laissant active la session iSCSI parente, elle devrait faire une demi clôture de la connexion TCP. Après l'expiration de la temporisation TIME_WAIT, la connexion TCP est close.

3.5 Fermeture iSCSI non en douceur

Si une certaine connexion TCP a une défaillance inattendue, la connexion iSCSI associée est supprimée. Il n'y a pas d'exigence qu'une suppression d'IKE phase 2 suive immédiatement la suppression de la connexion iSCSI ou la suppression de phase 1. Comme une SA IKE phase 2 peut correspondre à plusieurs connexions TCP, une telle suppression peut être inappropriée. De même, si la mise en œuvre IKE reçoit un message Supprimer phase 2 pour une association de sécurité qui correspond à une connexion TCP, cela n'implique pas nécessairement que la connexion TCP ou iSCSI soit à supprimer.

Si une séquence commande/réponse Logout marque une connexion comme à supprimer de la session iSCSI, alors, après que l'homologue iSCSI a exécuté un processus de suppression iSCSI pour la connexion, la connexion TCP sera close. L'état de la connexion iSCSI peut alors être retiré en toute sécurité.

Comme une SA IKE phase 2 peut être utilisée par plusieurs connexions TCP, une mise en œuvre iSCSI ne devrait pas dépendre de la réception du message Supprimer IPsec phase 2 comme confirmation que l'homologue iSCSI a exécuté un processus de suppression iSCSI pour la connexion.

Comme le matériel d'accélération IPsec peut n'être seulement capable de traiter qu'un nombre limité de SA IKE phase 2 actives, les messages Suppression phase 2 peuvent être envoyés pour des SA inactives comme moyen de garder au minimum le nombre de SA de phase 2 actives. La réception d'un message Supprimer IKE phase 2 NE DOIT PAS être interprété comme une raison pour supprimer la connexion iSCSI correspondante si aucune commande/réception Logout n'a été exécutée sur la connexion. Il est plutôt préférable de laisser la connexion iSCSI établie, et si du trafic supplémentaire est envoyés dessus, d'amener une autre SA IKE phase 2 pour le protéger. Cela évite d'éventuellement activer et désactiver continuellement les connexions iSCSI.

3.6 CRC de couche application

La détection et récupération d'erreur iSCSI suppose que les sommes de contrôle TCP et IP fournissent une protection d'intégrité inadéquate pour les communications à haut débit. Comme décrit dans [CRCTCP], lorsque on fonctionne à haut débit, la somme de contrôle TCP de 16 bits [RFC793] ne va pas nécessairement détecter toutes les erreurs, ce qui peut résulter en une corruption des données. iSCSI [RFC3720] incorpore donc un CRC de 32 bits pour protéger ses en-têtes et données.

Lorsque une vérification de CRC échoue (c'est-à-dire, lorsque le CRC calculé chez le receveur ne correspond pas au CRC reçu) la PDU iSCSI couverte par ce CRC est éliminée. Comme vraisemblablement l'erreur n'a pas été détectée par la somme de contrôle TCP, une retransmission TCP ne va pas intervenir et donc ne peut pas aider à récupérer de l'erreur. iSCSI contient des mécanismes de renvoi à la fois des données et des commandes pour traiter les situations qui en résultent, y compris SNACK, la capacité à réitérer les commandes R2T, et le bit réessayer (X) pour les commandes.

IPsec offre une protection contre un attaquant qui tente de modifier des paquets en transit, ainsi que contre des modifications involontaires de paquet causées par des dysfonctionnements du réseau ou d'autres erreurs. En général, les transformations d'authentification IPsec autorisent une plus forte protection d'intégrité que la somme de contrôle TCP de 16 bits et le CRC de 32 bits de couche application spécifié pour l'utilisation avec iSCSI. Comme la protection d'intégrité IPsec survient en dessous de TCP, si une erreur est découverte, le paquet sera alors éliminé et la retransmission TCP va se produire, de sorte qu'aucune action de récupération n'a besoin d'être entreprise à la couche iSCSI.

3.6.1 Simplification de la logique de récupération

Lorsque il est connu que la protection d'intégrité IPsec est en place de bout en bout entre les points d'extrémité iSCSI (ou la portion qui requiert une protection d'intégrité supplémentaire) les portions de iSCSI peuvent être simplifiées. Par

exemple, les mécanismes pour récupérer des échecs de vérification de CRC ne sont pas nécessaires.

Si le CRC iSCSI est négocié, la logique de récupération peut être simplifiée pour regarder tout échec de vérification de CRC comme fatal (par exemple, générer une SCSI CHECK CONDITION sur une erreur de données, clôt la connexion TCP correspondante sur erreur d'en-tête) parce qu'il sera très rare que les erreurs non détectées par la protection d'intégrité IPsec soient détectées par le CRC iSCSI.

3.6.2 Omission du CRC iSCSI

Dans certaines situations où IPsec est employé, le CRC iSCSI ne va pas apporter de protection supplémentaire et peut être omis.

Par exemple, lorsque le traitement IPsec est chargé avec la somme de contrôle TCP et la vérification de CRC iSCSI au sein du NIC, chacune de ces vérifications sera effectuée avant de transférer les données à travers le bus, de sorte que les erreurs suivantes ne seront pas détectées par ces mécanismes. Il en résulte que lorsque le traitement IPsec est chargé sur le NIC, le CRC iSCSI n'est pas nécessaire et que les mises en œuvre peuvent souhaiter ne pas le négocier.

Cependant, dans d'autres circonstances, la somme de contrôle TCP et le CRC iSCSI vont assurer une couverture d'erreur supplémentaire parce qu'ils sont calculés et vérifiés à des points différents dans la pile de protocoles ou dans des appareils différents de ceux qui mettent en œuvre les vérifications d'intégrité d'IPsec. La couverture résultante d'erreurs supplémentaires possibles rend souhaitable de négocier l'utilisation du CRC iSCSI même lorsque la protection d'intégrité IPsec est utilisée. Des exemples de ces situations incluent lorsque :

[1] IPsec, TCP et iSCSI sont mis en œuvre purement dans le logiciel. Là, des modes de défaillance supplémentaires peuvent être détectés par la somme de contrôle TCP et/ou le CRC iSCSI. Par exemple, après la réussite de la vérification IPsec d'intégrité du message, le segment est copié au titre du traitement TCP, et une erreur de mémoire durant de processus peut causer l'échec de la vérification de la somme de contrôle TCP ou du CRC iSCSI.

[2] La mise en œuvre est un mandataire ou une passerelle iSCSI-iSCSI. Ici, le CRC iSCSI peut être propagé d'une connexion iSCSI à une autre. Dans ce cas, le CRC iSCSI est utile pour protéger les données iSCSI contre les erreurs de mémoire, bus, ou logiciel au sein du mandataire ou passerelle, et le demander est souhaitable.

[3] IPsec est fourni par un appareil externe à l'appareil iSCSI réel. Ici, les CRC d'en-tête et de données iSCSI peuvent être conservés à travers la partie de la connexion qui n'est pas protégée par IPsec. Par exemple, la connexion iSCSI pourrait traverser un autre bus, une carte d'interface, un réseau, une carte d'interface, et un bus entre l'appareil iSCSI et l'appareil qui fournit IPsec. Dans ce cas, le CRC iSCSI est souhaitable, et la mise en œuvre iSCSI derrière l'appareil IPsec peut le demander.

Noter que si les deux extrémités de la connexion sont sur le même segment, alors le trafic sera effectivement protégé par le CRC de couche 2, de sorte que la négociation du CRC iSCSI n'est pas nécessaire pour protéger contre les erreurs de NIC et de réseau, bien qu'elle puisse être désirable pour d'autres raisons (par exemple, les cas [1] et [2] ci-dessus).

4. Questions de sécurité de iFCP et FCIP

4.1 Exigences d'authentification de iFCP et FCIP

iFCP et FCIP ont des protocoles d'homologue à homologue. Les sessions iFCP et FCIP peuvent être initiées par l'une ou l'autre des passerelles homologues ou par les deux. Par conséquent, l'authentification bidirectionnelle des passerelles homologues DOIT être fournie.

iFCP et FCIP sont des protocoles de transport qui encapsulent les trames SCSI et canal fibre sur IP. Donc, les identités de canal fibre, de système d'exploitation, et d'utilisateur sont transparentes aux protocoles iFCP et FCIP.

Les passerelles iFCP utilisent les informations de découverte de domaine obtenues du serveur iSNS pour déterminer si le N_PORT du canal fibre initiateur devrait se voir accorder l'accès au N_PORT de la cible. Les identités N_PORT utilisées dans le processus Port Login (PLOGI) seront considérées comme authentifiées pourvu qu'elles soient reçues sur une connexion dont la sécurité se conforme à la politique locale de sécurité.

Il n'est pas exigé que les identités utilisées dans l'authentification restent confidentielles.

4.2 Interaction d'iFCP avec IPsec et IKE

Un portail iFCP conforme est capable d'établir une ou plusieurs associations de sécurité IKE phase-1 avec un portail iFCP homologue. Une SA de phase 1 peut être établie lorsque un portail iFCP est initialisé, ou peut être différée jusqu'à

l'établissement de la première connexion TCP avec des exigences de sécurité.

Une SA IKE phase-2 protège une ou plusieurs connexions TCP au sein du même portail iFCP. Plus précisément, la réussite de l'établissement d'une SA IKE phase 2 résulte en la création de deux SA IPsec unidirectionnelles pleinement qualifiées par le triplet <SPI, adresse IP de destination, ESP>. Ces SA protègent le processus d'établissement des connexions TCP sous-jacentes et de tout leur trafic TCP ultérieur. Chacune des connexions TCP protégée par une SA est soit dans l'état non lié, soit liée à une session iFCP spécifique.

En résumé, à tout moment :
[1] il existe 0..M SA IKE phase-1 entre les portails iFCP homologues,
[2] chaque SA IKE phase 1 a 0..N SA IKE phase 2,
[3] chaque SA IKE phase 2 protège 0..Z connexions TCP.

La création d'une SA IKE phase 2 peut être déclanchée par des règles de politique de sécurité récupérées sur un serveur iSNS. Autrement, la création d'une SA peut être déclanchée par des règles de politique configurées à travers une interface de gestion, reflétant les règles de politique qui résident dans iSNS. De la même façon, l'utilisation d'une charge utile Échange de clé en mode rapide pour le secret de transmission parfait peut être conduite par des règles de politique de sécurité récupérées auprès su serveur iSNS, ou établies à travers une interface de gestion.

Si une mise en œuvre iFCP fait usage de connexions TCP non liées, et que de telles connexions appartiennent à un portail iFCP avec des exigences de sécurité, alors les connexions non liées DOIVENT être protégées par une SA à tout moment tout comme les connexions liées.

À réception d'un message Supprimer IKE phase 2, il n'y a pas d'exigence de terminer les connexions TCP protégées ou de supprimer la SA IKE phase 1 associée. Comme une SA IKE phase 2 peut être associée à plusieurs connexions TCP, clore de telles connexions pourrait en fait être inapproprié et prématuré.

Pour minimiser le nombre de SA actives de phase 2, les messages Supprimer IKE phase 2 peuvent être envoyés pour les SA de phase 2 dont les connexions TCP n'ont pas traité de trafic de données depuis un certain temps. Pour minimiser l'utilisation de ressources de SA lorsque les connexions TCP associées sont au repos, la création d'une nouvelle SA devrait être différée jusqu'à ce que de nouvelles données soient à envoyer sur les connexions.

4.3 Interaction de FCIP avec IPsec et IKE

Les entités FCIP établissent des tunnels avec les autres entités FCIP afin de transférer les trames FC encapsulées dans IP. Chaque tunnel est une liaison FCIP séparée, et peut encapsuler plusieurs connexions TCP. Le lien des connexions TCP à une liaison FCIP est effectué en utilisant le nom mondial de canal fibre (WWN, *Fibre Channel World Wide Name*) des deux entités FCIP.

Les entités FCIP peuvent avoir plus d'une interface et adresse IP, et il est possible à une liaison FCIP de contenir plusieurs connexions TCP dont les adresses IP de point d'extrémité FCIP sont différentes. Dans ce cas, une SA IKE phase 1 est normalement établie pour chaque paire d'adresse IP de point d'extrémité FCIP. Pour les besoins de l'établissement d'une SA IKE phase 1, des adresses IP statiques sont normalement utilisées pour l'identification.

Chaque connexion TCP au sein d'une liaison FCIP correspond à une SA IKE phase 2 (mode rapide). Elle est établie avant d'envoyer le paquet SYN TCP initial et s'applique à toute la vie de la connexion. La négociation de phase 2 est aussi exigée pour le changement de clés, afin de protéger contre les attaques en répétition.

Les mises en œuvre FCIP PEUVENT fournir la gestion administrative de l'utilisation de la confidentialité. Ces interfaces de gestion DEVRAIENT être fournies de manière sûre, de façon à empêcher un attaquant de subvertir le processus de sécurité en attaquant l'interface de gestion.

Les entités FCIP n'exigent aucune authentification de niveau utilisateur, car toutes les entités FCIP participent à une fonction tunnel de niveau machine. FCIP utilise SLP pour la découverte, mais pas pour distribuer les politiques de sécurité.

5. Considérations pour la sécurité

5.1 Mode transport contre mode tunnel

Par rapport aux protocoles de mémorisation de blocs, les différences majeures entre le mode tunnel IPsec et le mode transport sont les suivantes :

[1] Considérations de MTU
Le mode tunnel introduit un en-tête IP supplémentaire dans le datagramme qui se reflète dans une diminution correspondante de la MTU de chemin vue par les paquets qui traversent le tunnel. Il peut en résulter une diminution de la taille maximum de segment des connexions TCP qui passent à travers le tunnel.

[2] Allocation d'adresse et configuration
Dans le mode tunnel IPsec, il est nécessaire que les adresses de source internes et externes soient configurées, et que les adresses de destination internes et externes soient découvertes. Au sein du mode transport, il est seulement nécessaire de découvrir une seule adresse de destination et de configurer une seule adresse de source. Les considérations d'usage des adresses d'IPsec en mode tunnel sont exposées plus en détails ci-dessous.

[3] Traversée de NAT
Comme on l'a noté dans la [RFC3715], ESP en mode tunnel IPsec peut traverser un NAT dans des circonstances limitées, tandis que ESP en mode transport ne peut pas traverser un NAT. Pour permettre la traversée de NAT dans le cas général, la fonctionnalité de traversée de NAT par IPsec décrite dans les [RFC3715], [RFC3947] et [RFC3948] peut être mise en œuvre. Le paragraphe suivant donne plus de détails.

[4] Traversée de pare-feu
Lorsque un protocole de mémorisation de bloc doit traverser des domaines administratifs, l'administrateur de pare-feu peut désirer vérifier l'intégrité et l'authenticité de chaque paquet en transit, plutôt que d'ouvrir un trou dans le pare-feu pour le protocole de mémorisation de bloc. Le mode tunnel IPsec se prête à de telles vérifications, car le pare-feu peut terminer la connexion en mode tunnel tout en permettant encore aux points d'extrémité de communiquer de bout en bout. Si c'est désiré, les points d'extrémité peuvent de plus utiliser le mode transport IPsec pour la sécurité de bout en bout, afin qu'ils puissent aussi vérifier l'authenticité et l'intégrité de chaque paquet par eux-mêmes.

À l'opposé, effectuer cette vérification avec le mode transport IPsec est plus complexe, car le pare-feu aura besoin de clore la connexion en mode transport IPsec et aura besoin d'agir comme une passerelle iSCSI, iFCP ou FCIP, ou un mandataire TCP, générant une nouvelle connexion en mode transport IPsec à partir du pare-feu jusqu'au point d'extrémité interne. Une telle mise en œuvre ne peut pas fournir la protection de bout en bout de l'authenticité ou de l'intégrité, et un CRC de couche application (iSCSI) ou la transmission du CRC de la trame canal fibre (iFCP et FCIP) est nécessaire pour protéger contre les erreurs introduites par le pare-feu.

[5] Intégration IPsec-application
Lorsque IPsec et le protocole de couche application sont mis en œuvre sur le même appareil ou hôte, il est possible d'activer une étroite intégration entre eux. Par exemple, la couche application peut demander que les connexions soient protégées par IPsec et vérifier qu'elles le sont, et peut obtenir les attributs de l'association de sécurité IPsec. Alors que dans les mises en œuvre de mode transport, les mises en œuvre d'IPsec et de protocole d'application résident normalement sur le même hôte, avec le mode tunnel IPsec ils peuvent résider sur des hôtes différents. Lorsque IPsec est mis en œuvre sur une passerelle externe, l'intégration entre l'application et IPsec n'est normalement pas possible. Cela limite la capacité de l'application à contrôler et vérifier le comportement IPsec.

5.1.1 Considérations sur l'adressage IPsec en mode tunnel

Les tunnels IPsec incluent à la fois des adresses de source et de destination internes et externes.

Lorsque elle est utilisée avec les protocoles de mémorisation de bloc IP, l'adresse de destination interne représente l'adresse de l'homologue de protocole de mémorisation de bloc IP (par exemple, la destination ultime du paquet). L'adresse de destination interne peut être découverte en utilisant SLPv2 ou iSNS, ou peut être résolue à partir d'un FQDN via DNS, de sorte qu'obtenir cette adresse n'est normalement pas un problème.

L'adresse de destination externe représente l'adresse de la passerelle de sécurité IPsec utilisée pour atteindre l'homologue. Plusieurs mécanismes ont été proposés pour découvrir la passerelle de sécurité IPsec utilisée pour atteindre un homologue particulier. La [RFC2230] expose l'utilisation des enregistrements de ressource (RR, *Resource Record*) KX pour la découverte de passerelle IPsec. Cependant, alors que les RR KX sont pris en charge par de nombreuses mises en œuvre de serveur DNS, ils n'ont pas encore été largement déployés. Autrement, les SRV DNS de la [RFC2782] peuvent être utilisés à cette fin. Lorsque le DNS est utilisé pour la localisation de passerelle, des mécanismes de sécurité du DNS tels que DNSSEC ([RFC2535], [RFC2931]), TSIG [RFC2845], et Mise à jour dynamique simple [RFC3007] sont conseillés.

Lorsque elle est utilisée avec les protocoles de mémorisation de bloc IP, l'adresse de source externe est configurée soit de façon statique, soit dynamique, en utilisant des mécanismes tels que DHCPv4 [RFC2131], DHCPV6 [RFC3315], ou l'autoconfiguration d'adresse sans état [RFC2373].

L'adresse de source interne DEVRAIT être incluse dans la charge utile Identifiant de mode rapide lorsque l'homologue établit une SA en mode tunnel avec la passerelle de sécurité IPsec. Cela active la passerelle de sécurité IPsec pour acheminer correctement les paquets vers l'homologue distant. L'adresse de source interne peut être configurée via divers mécanismes, selon le scénario. Lorsque les homologues de mémorisation de bloc IP sont localisés au sein du même domaine administratif, il est normalement possible que les adresses de source interne et externe soient les mêmes. Cela va fonctionner parce que l'adresse de source externe est supposée être allouée à partir d'un préfixe alloué au domaine administratif, et est donc acheminable au sein du domaine. En supposant que la passerelle de sécurité IPsec est au courant de l'adresse de source interne utilisée par l'homologue qui se connecte et qu'elle sonde un chemin d'hôte sur elle, les paquets qui arrivent à la passerelle de sécurité IPsec destinés à cette adresse peuvent alors être correctement encapsulés et envoyés sur le tunnel correct.

Lorsque les homologues de mémorisation de bloc IP sont localisés au sein de domaines administratifs différents, il peut être nécessaire que l'adresse de source interne soit allouée par la passerelle de sécurité IPsec, "joignant" effectivement l'hôte distant au LAN rattaché à la passerelle de sécurité IPsec. Par exemple, si l'hôte distant devait utiliser son adresse de source (externe) allouée comme adresse de source interne, un certain nombre de problèmes pourraient résulter :

[1] les systèmes de détection d'intrusion qui surveillent le LAN derrière la passerelle de sécurité IPsec remarqueraient que les adresses de source ont leur origine en dehors du domaine administratif ;

[2] les paquets de réponse pourraient ne pas atteindre leur destination, car la passerelle de sécurité IPsec n'annonce normalement pas le chemin par défaut, mais plutôt seulement le préfixe d'où il alloue les adresses. Comme l'adresse de l'homologue distant n'a pas pour origine un préfixe natif du domaine administratif, il est probable que les routeurs au sein du domaine n'auront pas de chemin pour lui, et vont envoyer le paquet au routeur qui annonce le chemin par défaut (peut-être un routeur frontière) au lieu de la passerelle de sécurité IPsec.

Pour ces raisons, pour l'utilisation inter-domaines, l'allocation des adresses de sources internes peut être nécessaire. Ce n'est pas à présent un scénario très courant ; cependant, si l'allocation d'adresse est fournie alors l'allocation d'adresse fondée sur DHCP au sein du mode tunnel IPsec [RFC3456] DOIT être prise en charge. Noter que ce mécanisme n'est pas encore largement déployé dans les passerelles de sécurité IPsec ; les serveurs existants de mode tunnel IPsec mettent normalement en œuvre cette fonctionnalité via des extensions propriétaires à IKE.

5.2 Traversée de NAT

Comme noté dans la [RFC3715], ESP en mode tunnel peut traverser un NAT dans un ensemble de circonstances limité. Par exemple, si il y a seulement un point d'extrémité de protocole derrière un NAT, des sélecteurs de "TOUT à TOUT" sont négociés, et si le receveur n'effectue pas de validation d'adresse de source, alors ESP en mode tunnel peut réussir à traverser les NAT. Comme ignorer la validation d'adresse de source introduit une nouvelle vulnérabilité pour la sécurité, et que la négociation de sélecteurs spécifiques est souhaitable afin de limiter le trafic qui peut être envoyé sur le tunnel, ces conditions peuvent ne pas nécessairement s'appliquer, et la traversée de NAT en mode tunnel ne va pas toujours être possible.

TCP porté au sein d'ESP en mode transport ne peut pas traverser de NAT, même si ESP lui-même n'inclut pas de champ d'en-tête IP dans sa vérification d'intégrité de message. Cela parce que la somme de contrôle de TCP à 16 bits est calculée sur la base d'un "pseudo en-tête" qui inclut les champs d'en-tête IP, et que la somme de contrôle est protégée par la vérification d'intégrité de message ESP IPsec. Il en résulte, que la somme de contrôle TCP sera toujours invalidée par un NAT situé entre les deux points d'extrémité.

Comme le calcul et la vérification de la somme de contrôle TCP est obligatoire dans IPv4 et dans IPv6, il n'est pas possible d'omettre la vérification de la somme de contrôle tout en restant conforme aux normes. Afin de permettre la traversée des NAT existants tout en restant conforme, les mises en œuvre de sécurité iSCSI, iFCP ou FCIP peuvent utiliser la traversée de NAT d'IPsec/IKE, telle que décrite dans les [RFC3715], [RFC3948], et [RFC3947].

Les spécifications de traversée de NAT de IKE [RFC3947] et IPsec [RFC3948] permettent que l'encapsulation UDP de IPsec soit négociée si un NAT est détecté dans le chemin. En déterminant l'adresse IP du NAT, la somme de contrôle TCP peut être calculée sur la base d'un pseudo en-tête incluant l'adresse et les accès ajustés au NAT. Si cela est fait avant de calculer la vérification d'intégrité du message IPsec, la vérification de la somme de contrôle TCP n'échouera pas.

5.3 Problèmes de IKE

Il y a des situations où il est nécessaire que IKE soit mis en œuvre dans le matériel. Dans de telles situations, il est important de garder la taille des mises en œuvre de IKE dans des limites strictes. Une limite supérieure de la taille d'une mise en œuvre de IKE pourrait être considérée comme étant de 800 kbit, 80 kbit permettant une mise en œuvre dans une large gamme de situations.

Comme noté au Tableau 5.3-1 de la page suivante, il existe des mises en œuvre IKE qui satisfont à ces exigences. Donc, bien que le retrait de fonctionnalités IKE rarement utilisées (comme les méthodes d'authentification de nom occasionnel) réduirait la complexité, les mises en œuvre ne vont normalement pas exiger cela afin de tenir dans le budget de taille du code.

5.4 Problèmes de changement de clés

On s'attend à ce que les mises en œuvre de mémorisation de bloc IP aient besoin de fonctionner à grande vitesse. Par exemple, les mises en œuvre qui fonctionnent à 1 Gbit/s sont actuellement en préparation, avec des mises en œuvre à 10 Gbit/s qui vont bientôt suivre. À ces vitesses, une seule SA IPsec pourrait rapidement parcourir le cycle de l'espace de numéros de séquence de 32 bits d'IPsec.

Par exemple, une seule SA fonctionnant à 1 Gbit/s de taux de ligne et qui envoie des paquets de 64 octets épuiserait l'espace de numéros de séquence de 32 bits en 2200 secondes, ou 37 minutes. Avec des paquets de 1518 octets, l'épuisement surviendrait en 14,5 heures. À 10 Gbit/s, l'épuisement surviendrait en 220 secondes ou 3,67 minutes. Avec des paquets de 1518 octets, cela se produirait en 1,45 heures.

À l'avenir, il pourrait être souhaitable pour les mises en œuvre fonctionnant à des vitesses de 1 Gbit/s ou plus de mettre en œuvre une extension de numéro de séquence IPsec, décrite dans la [RFC4303]. Noter que selon la transformation utilisée, il est possible que le changement de clés soit nécessaire avant l'épuisement de l'espace de numéros de séquence.

Dans les chiffrements en mode CBC, le texte chiffré d'un bloc dépend du texte en clair de ce bloc aussi bien que du texte chiffré du bloc précédent. Cela implique que si le texte chiffré de deux blocs est identique, et si le teste en clair du prochain bloc est aussi identique, le texte chiffré du prochain bloc sera alors identique. Donc, si des blocs de texte chiffré identiques peuvent être trouvés avec les blocs suivants correspondants, un attaquant peut déterminer l'existence du texte en clair correspondant.

De telles "attaques de l'anniversaire" ont été examinées par Bellare et. al. dans [DESANALY]. En moyenne, un bloc de texte chiffré de taille n bits sera supposé se répéter tous les 2^[n/2] blocs. Bien qu'une seule "attaque de l'anniversaire" ne fournisse pas beaucoup d'informations à un attaquant, plusieurs de ces attaques peuvent fournir des informations utiles. Pour rendre cela peu probable, il est recommandé qu'un changement de clés survienne avant que 2^[n/2] blocs aient été envoyés sur une SA. Bellare et. al. ont formalisé cela dans [DESANALY], montrant que l'insécurité du mode CBC augmente comme O(s^2/2^n), où n est la taille de bloc en bits, et s est le nombre total de blocs chiffrés. Ces conclusions ne s'appliquent pas au mode compteur.

Mise en œuvre	Taille de code (octets)	Machine
Pluto (FreeSWAN)	258KB	Linux FreeSWAN x86
Racoon (KAME)	400KB	NetBSD 1.5 x86
Isakmpd (Erickson)	283KB	NetBSD 1.5 x86
WindRiver	142KB	PowerPC
Cisco VPN1700	222KB	PowerPC
Cisco VPN3000	350K	PowerPC
Cisco VPN7200	228KB	MIPS

Tableau 5.3-1 – Taille de code pour mises en œuvre IKE

La formule ci-dessous établit une limite aux octets qui peuvent être envoyés sur une SA CBC avant qu'un changement de clés soit exigé : B = (n/8) * 2^[n/2]
Où :
B = maximum d'octets envoyés sur la SA
n = taille de bloc en bits

Cela signifie que la taille de bloc de chiffrement ainsi que la longueur de clé doivent être prises en considération dans la décision de changement de clé. 3DES utilise une taille de bloc de n = 64 bits (2^3 octets) ; cela implique que la SA doit avoir ses clés changées avant que B = (64/8) * (2^32) = 2^35 octets soient envoyés. À 1 Gbit/s, cela implique qu'un changement de clés sera exigé toutes les 274,9 secondes (4,6 minutes) ; à 10 Gbit/s, un changement de clés est requis toutes les 27,5 secondes.

En termes d'espace de numéro de séquence, pour un message chiffré en 3DES de 512 = 2^9 octets (2^6 blocs) cela implique que la clé est devenue non sûre après environ 2^26 messages.

5.5 Problèmes de transformations

Comme les mises en œuvre de mémorisation de bloc IP peuvent opérer à des vitesses de 1 Gbit/s ou plus, la capacité à offrir les services de sécurité IPsec à de grandes vitesses est un problème aigu. Comme la prise en charge de plusieurs algorithmes multiplie la complexité et le coût de conception des matériels, un des buts de l'effort de choix de la transformation est de trouver un ensemble minimal d'algorithmes de confidentialité et d'authentification qu'on puisse mettre en œuvre dans les matériels à des vitesses allant jusqu'à 10 Gbit/s, et qui soient aussi efficaces pour une mise en œuvre dans le logiciel à des vitesses de 100 Mbit/s ou plus lent.

Dans la présente spécification, on se préoccupe principalement des transformations IPsec qui ont déjà été spécifiées, et dont des parties sont disponibles qui puissent fonctionner à un débit de ligne de 1 Gbit/s. Lorsque les algorithmes existants ne s'adaptent pas bien à 10 Gbit/s, on examine des algorithmes pour lesquels les spécifications de transformations ne sont pas encore achevées, mais pour lesquels il est prévu que des parties soient disponibles pour les inclure dans des produits qui seront prêts dans les 12 prochains mois. Avec les avancées de l'état de l'art, la gamme des algorithmes acceptables va s'élargir et des algorithmes de mise en œuvre obligatoire peuvent être pris en considération.

La Section 5 de la [RFC2406] déclare :

"Une mise en œuvre conforme à ESP DOIT prendre en charge les algorithmes de mise en œuvre obligatoire suivants :
- DES en mode CBC
- HMAC avec MD5
- HMAC avec SHA-1
- algorithme d'authentification NUL
- algorithme de chiffrement NUL".

L' algorithme DES est spécifié dans [FIPS46-3] ; on trouve les lignes directrices de mise en œuvre dans [FIPS74], et les questions de sécurité sont discutées dans [DESDIFF], [DESINT], [DESCRACK]. La transformation DES IPsec est définie dans la [RFC2405] et la transformation 3DES en mode CBC IPsec est spécifiée dans la [RFC2451].

L'algorithme MD5 est spécifié dans la [RFC1321] ; HMAC est défini dans la [RFC2104] et les questions de sécurité avec MD5 sont exposées dans [MD5Attack]. La transformation IPsec HMAC-MD5 est spécifiée dans la [RFC2403]. La transformation IPsec HMAC-SHA1 est spécifiée dans la [RFC2404].

En plus de ces algorithmes existants, le NIST est en train d'évaluer les modes suivants [NSPUE2] de AES, défini dans [FIPS197] :

AES en livre de code électronique (ECB) mode confidentialité
AES en chaînage de bloc de chiffrement (CBC) mode confidentialité
AES en retour de chiffrement (CFB, Cipher Feedback) mode confidentialité
AES en retour de résultat (OFB, Output Feedback) mode confidentialité
AES en mode compteur (CTR) mode confidentialité
AES CBC-MAC mode authentification

Lorsque on utilise les modes AES, il peut être nécessaire d'utiliser de plus grandes clés publiques; les compromis sont décrits dans la [RFC3766]. Des groupes MODP Diffie-Hellman supplémentaires à utiliser avec IKE sont décrits dans la [RFC3526].

Le projet Modes [NSPUE2] examine aussi un certain nombre d'algorithmes supplémentaires, incluant PMAC.

Pour assurer l'authentification, la protection de l'intégrité et contre la répétition, les mises en œuvre de sécurité de mémorisation de bloc IP DOIVENT prendre en charge HMAC-SHA1 [RFC2404] pour l'authentification, et AES en mode MAC CBC avec les extensions XCBC DEVRAIT être accepté [RFC3566].

HMAC-SHA1 [RFC2404] est à préférer à HMAC-MD5, du fait des problèmes qui ont été soulevés au sujet de la sécurité de MD5 [MD5Attack]. Des parties de HMAC-SHA1 sont actuellement disponibles qui fonctionnent à 1 Gbit/s, l'algorithme peut être mis en œuvre dans des matériels à des vitesses allant jusqu'à 10 Gbit/s, et une spécification de transformation IPsec [RFC2404] existe. Il en résulte qu'il est très pratique d'utiliser HMAC-SHA1 comme algorithme d'authentification pour des produits prochainement commercialisés. AES en mode d'authentification CBC-MAC avec les extensions XCBC a été choisi car il évite d'ajouter une quantité substantielle de code supplémentaire si AES est déjà mis en œuvre pour le chiffrement ; un document de transformation IPsec est disponible [RFC3566].

Il existe aussi des transformations d'authentification qui sont considérablement plus efficaces à mettre en œuvre que HMAC-SHA1, ou AES en mode d'authentification CBC-MAC. UMAC [UMAC], [RFC4418] est plus efficace à mettre en œuvre dans le logiciel et PMAC [PMAC] est plus efficace à mettre en œuvre dans le matériel. PMAC est actuellement

évalué au titre du projet Modes du NIST [NSPUE2] mais une transformation IPsec n'existe pas encore ; aucune ne fait de transformation UMAC.

Pour la confidentialité, l'algorithme ESP de mise en œuvre obligatoire (DES) est inacceptable. Comme noté dans [DESCRACK], DES peut être cassé avec des ressources de calcul modestes, et est donc inapproprié pour être utilisé dans des situations exigeant de hauts niveaux de sécurité.

Pour assurer la confidentialité pour iSCSI, iFCP, et FCIP, 3DES en mode CBC [RFC2451] DOIT être pris en charge et AES en mode compteur [RFC3686] DEVRAIT être pris en charge. Pour l'utiliser dans des mises en œuvre à grande vitesse, 3DES a des inconvénients significatifs. Cependant, une transformation 3DES IPsec a été spécifiée et des parties sont disponibles qui peuvent fonctionner à 1 Gbit/s, de sorte que mettre en œuvre 3DES dans les produits est pratique à court terme.

Comme décrit dans l'Appendice B, les mises en œuvre de logiciel 3DES font des demandes excessives de calcul à des vitesses de 100 Mbit/s ou plus, écartant effectivement les mises en œuvre uniquement de logiciel. De plus, les mises en œuvre de 3DES requièrent un changement de clé avant l'épuisement de l'espace actuel de numéro de séquence IPsec de 32 bits, et ne seraient donc pas capables d'utiliser les extensions d'espace de numéros de séquence si elles étaient disponibles. Cela signifie que 3DES va exiger de très fréquents changements de clés à des vitesses de 10 Gbit/s ou plus. Donc, 3DES est d'utilisation peu pratique à très grande vitesse, ainsi que pour la mise en œuvre dans un logiciel à de plus basses vitesses (100+ Mbit/s).

5.6 Problèmes de fragmentation

Lorsque l'authentification par certificat est utilisée, la fragmentation IKE peut se rencontrer. Cela survient lorsque des chaînes de certificats sont utilisées, ou même lors de l'échange d'un seul certificat si la taille de clé ou la taille des autres champs de certificats (comme le nom distinctif et les autres OID) est assez grande. De nombreux traducteurs d'adresse réseau (NAT, *Network Address Translator*) et pare-feu ne traitent pas correctement les fragments, les éliminant en entrée et/ou en sortie.

Les routeurs sur le chemin vont aussi fréquemment éliminer les fragments après le fragment initial, car ils ne vont normalement pas contenir les en-têtes IP complets qui peuvent être comparés à une liste d'accès.

Il en résulte que lorsque la fragmentation IKE survient, les points d'extrémité vont souvent être incapables d'établir une association de sécurité IPsec. La solution à ce problème est d'installer un programme de code de NAT, pare-feu ou routeur qui puisse correctement prendre en charge les fragments. Si cela ne peut pas être fait, les solutions de remplacement suivantes peuvent être examinées :

[1] obtenir les certificats par d'autres moyens,
[2] réduire la taille de la chaîne de certificats,
[3] Réduire la taille des champs au sein des certificats. Cela inclut de réduire la taille de clé, du nom distinctif ou d'autres champs. Cela ne devrait être considéré qu'en dernier ressort.

La fragmentation peut devenir un problème lors de l'ajout d'en-têtes IPsec à une trame. Un mécanisme qui peut être utilisé pour réduire ce problème est d'utiliser la découverte de la MTU de chemin. Par exemple, lorsque TCP est utilisé comme transport pour iSCSI, iFCP ou FCIP, la découverte de la MTU du chemin, décrite dans les [RFC1191], [RFC1435], [RFC1981], peut être utilisée pour permettre aux points d'extrémité TCP de découvrir la MTU correcte, incluant les effets de l'encapsulation IPsec.

Cependant, la découverte de la MTU du chemin échoue lorsque les messages ICMP appropriés ne sont pas reçus par l'hôte. Cela arrive dans les mises en œuvre IPsec qui éliminent les paquets ICMP non authentifiés. Il peut en résulter un trou noir dans les mises en œuvre TCP simplistes, comme décrit dans la [RFC2923]. Le comportement TCP approprié est décrit au paragraphe 2.1 de la [RFC2923] :
"TCP devrait remarquer que la connexion est périmée. Après plusieurs fins de temporisations, TCP devrait tenter d'envoyer de plus petits paquets, peut-être en ôtant le fanion DF de chaque paquet. Si cela marche, il devrait continuer d'ôter le PMTUD pour la connexion pendant un délai raisonnable, après quoi il devrait la sonder à nouveau pour essayer de déterminer si le chemin a changé."

Si une PMTU ICMP est reçue par une mise en œuvre IPsec qui traite les paquets ICMP non authentifiés, cette valeur devrait être mémorisée dans la SA comme proposé dans la [RFC2401], et IPsec devrait aussi fournir une notification de cet événement à TCP afin que la nouvelle valeur de MTU puisse être correctement reflétée.

5.7 Vérifications de sécurité

Lorsque est ouverte une connexion qui exige la sécurité, les mises en œuvre de sécurité à mémorisation de bloc IP peuvent souhaiter vérifier que la connexion est protégée par IPsec. Si la sécurité est désirée et que la protection IPsec a été retirée sur une connexion, elle est réinstallée avant l'envoi de paquets non protégés par la mémorisation de bloc IP. Comme IPsec vérifie que chaque paquet arrive sur la SA correcte, tant qu'il peut s'assurer que la protection IPsec est en place, les mises en œuvre de sécurité à mémorisation de bloc IP peuvent alors être assurées que chaque paquet reçu a été envoyé par un homologue de confiance.

Lorsque elle est utilisée avec les protocoles de mémorisation de bloc IP, chaque connexion TCP DOIT être protégée par une SA IKE de phase 2. Le trafic provenant d'une ou plusieurs connexion TCP peut s'écouler au sein de chaque SA IPsec de phase 2. Les mises en œuvre de sécurité à mémorisation de bloc IP n'ont pas besoin de vérifier que les adresses IP et les valeurs d'accès TCP dans le paquet correspondent aux informations de la prise qui a été utilisée pour établir la connexion. Cette vérification sera effectuée par IPsec, empêchant des homologues malveillants d'envoyer des commandes sur des SA en mode rapide inappropriées.

5.8 Problèmes d'authentification

5.8.1 Certificats machine contre certificats d'utilisateur

Les accréditifs de certificat fournis par l'initiateur iSCSI durant la négociation IKE peuvent être ceux de la machine ou ceux de l'entité iSCSI. Lorsque l'authentification de la machine est utilisée, le certificat de machine est normalement mémorisé chez l'initiateur et la cible iSCSI durant un processus d'inscription. Lorsque des certificats d'utilisateur sont utilisés, le certificat d'utilisateur peut être mémorisé soit sur la machine soit sur une carte à mémoire. Pour iFCP et FCIP, les accréditifs de certificat fournis vont presque toujours être ceux de l'appareil, et seront mémorisés sur l'appareil.

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'inscription de certificat de machine soit strictement contrôlé. Par exemple, seuls les administrateurs peuvent avoir la capacité d'inscrire une machine avec un certificat de machine.

Bien que la mémorisation de certificat sur une carte à mémoire diminue la probabilité de compromission de la clé privée, les cartes à mémoire ne sont pas nécessairement désirables dans toutes les situations. Par exemple, certaines organisations qui déploient des certificats de machine les utilisent de façon à empêcher l'utilisation de matériels non approuvés. Comme l'authentification d'utilisateur peut être fournie au sein de la connexion iSCSI (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 ainsi que l'utilisateur. Comme iFCP et FCIP n'ont pas d'équivalent de la connexion iSCSI, pour ces protocoles, seule la machine est authentifiée.

Dans les circonstances dans lesquelles cette double assurance est considérée comme valable, activer 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 le certificat d'utilisateur est déployé, il est conseillé que le processus d'inscription 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'inscription peut être limitée, après quoi l'accès du mot de passe sera fermé. Une telle politique va empêcher un attaquant qui a obtenu le mot de passe d'un compte non utilisé d'obtenir un certificat d'utilisateur une fois que la période d'inscription est expirée.

5.8.2 Clés pré partagées

L'utilisation de clés pré partagées dans le mode principal d'IKE est vulnérable aux attaques par interposition lorsque il est utilisé avec des hôtes dont les adresses sont allouées de façon dynamique (comme avec des initiateurs iSCSI). En 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 prépartagée ne peut se fonder que sur les informations contenues dans l'en-tête IP. Cependant, lorsque l'allocation dynamique d'adresse IP est normale, il n'est souvent pas possible d'identifier la clé prépartagée requise sur la base de l'adresse IP.

Donc, lorsque l'authentification par clé prépartégée est utilisée avec des entités dont l'adresse est allouée de façon dynamique, la même clé prépartagée est partagée par un groupe et n'est plus capable de fonctionner comme un secret partagé efficace. Dans cette situation, ni l'initiateur ni le répondant ne s'identifient durant IKE phase 1 ; on sait seulement

que les deux parties sont membres du groupe et qu'ils connaissent la clé prépartagée. Cela permet à n'importe qui qui a accès à la clé prépartagée du groupe d'agir comme un attaquant interposé. Cette faiblesse n'est normalement pas un problème lorsque les adresses IP sont allouées de façon statique (comme avec iFCP et FCIP) car dans cette situation des clés pré partagées individuelles sont possibles au sein du mode principal IKE.

Cependant, lorsque les adresses IP sont allouées de façon dynamique et que le mode principal est utilisé avec des clés pré partagées, le répondant n'est pas authentifié sauf si l'authentification mutuelle de couche application est effectuée (par exemple, l'authentification de connexion iSCSI). Cela permet à un attaquant en possession de la clé prépartagée de groupe de se faire passer pour le répondant. En plus de permettre à l'attaquant de présenter de fausses données, l'attaquant va aussi être capable de monter une attaque de dictionnaire sur les méthodes d'authentification traditionnelles comme CHAP [RFC1994], avec le potentiel de compromettre de nombreux mots de passe en une seule fois. Cette faiblesse est largement présente dans les mises en œuvre IPsec existantes.

Les clés pré partagées de groupe ne sont pas exigées dans le mode agressif car la charge utile d'identité est envoyée plus tôt dans l'échange, et donc, la clé prépartagée peut être choisie sur la base de l'identité. Cependant, lorsque le mode agressif est utilisé, l'identité de l'usager est exposée et ceci est souvent considéré comme indésirable.

Noter qu'il faut faire attention avec le choix de la charge utile Identité de IKE phase 1 afin d'activer la transposition des identités dans les clés pré partagées même avec le mode agressif. Lorsque les charges utiles d'identité ID_IPV4_ADDR ou ID_IPV6_ADDR sont utilisées et que les adresses sont allouées de façon dynamique, la transposition des identités aux clés n'est pas possible, de sorte que les clés pré partagées de groupe sont toujours une nécessité pratique. Il en résulte que des identités autres que ID_IPV4_ADDR et ID_IPV6_ADDR (comme ID_FQDN ou ID_USER_FQDN) DEVRAIENT être employées dans les situations où le mode agressif est utilisé avec des clés pré partagées et où les adresses IP sont allouées de façon dynamique.

5.8.3 IKE et authentification de couche Application

En plus de l'authentification IKE, les mises en œuvre iSCSI utilisent leurs propres méthodes d'authentification. Des travaux sont actuellement en cours sur la sécurité du canal fibre, de sorte qu'un processus d'authentification similaire pourrait finalement s'appliquer aussi à iFCP et FCIP.

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

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

Supposons que l'identité revendiquée dans une connexion iSCSI soir une identité d'utilisateur, tandis que l'identité revendiquée au sein de IKE soit une identité de machine. Comme seule l'identité de la machine est vérifiée sur la base du paquet, il n'y a pas de moyen pour le receveur de vérifier que seul l'utilisateur authentifié via la connexion iSCSI utilise la SA IPsec.

En fait, les mises en œuvre IPsec qui ne prennent en charge que l'authentification de machine n'auront normalement pas de moyen de distinguer entre le trafic d'utilisateur au sein du noyau. Il en résulte que lorsque l'authentification de machine est utilisée, une fois qu'une SA IPsec est ouverte, un autre utilisateur sur une machine multi utilisateurs peut être capable d'envoyer du trafic sur la SA IPsec. Ceci est vrai à la fois pour les SA de mode transport et de mode tunnel.

Pour limiter les faiblesses potentielles, les mises en œuvre de mémorisation de bloc IP DOIVENT faire de qui suit :

[1] S'assurer que la prise d'accès est contrôlée de façon appropriée. Sur un système d'exploitation multi usagers, cela implique que les prises ouvertes pour être utilisés par les protocoles de mémorisation de bloc IP DOIVENT être exclusives.

[2] Dans le cas de iSCSI, les mises en œuvre DOIVENT aussi s'assurer que les accréditifs de connexion de couche application (comme les accréditifs de connexion iSCSI) sont protégés contre l'accès non autorisé.

Si ces directives sont suivies, un processus félon ne sera pas capable d'accéder à un volume de mémorisation de bloc IP.

Bien que l'identité affirmée au sein d'IKE soit vérifiée sur la base du paquet, pour éviter les interférences entre usagers sur une certaine machine, le soutien du système d'exploitation est nécessaire. Pour tenir à part les trafic des différents usagers lorsque l'authentification d'utilisateur est prise en charge, les points d'extrémité IPsec doivent s'assurer que seul le trafic provenant de cet usager particulier est envoyé ou reçu au sein de la SA IPsec. La mise en application de cette restriction est

de la responsabilité du système d'exploitation.

Dans les pilotes iSCSI en mode noyau il n'y a normalement pas de contexte d'utilisateur pour effectuer l'authentification d'utilisateur. Dans ce cas, l'authentification est plus proche de l'authentification de machine. Dans la plupart des systèmes d'exploitation les permissions de l'appareil vont contrôler la capacité à lire/écrire de l'appareil avant le montage. Une fois l'appareil monté, les ACL établis par le système de fichiers contrôlent l'accès à l'appareil. Un administrateur peut accéder directement aux blocs sur l'appareil (par exemple, en envoyant des demandes de traversée directement au pilote d'accès comme dans Windows NT). De la même façon, un administrateur peut ouvrir une prise brute et envoyer des paquets protégés par IPsec à une cible iSCSI. La situation est analogue, et à cet égard, aucune nouvelle faiblesse n'est créée qui n'existait auparavant. Les ACL du système d'exploitation doivent être efficaces pour protéger un appareil (que ce soit un appareil SCSI ou iSCSI).

5.8.4 Autorisation de mémorisation de bloc IP

Les protocoles de mémorisation de bloc IP peuvent utiliser divers mécanismes pour l'autorisation. Lorsque ID_FQDN est utilisé comme charge utile Identité, les points d'extrémité de mémorisation de bloc IP peuvent être configurés avec une liste de FQDN autorisés. La configuration peut se faire manuellement, ou automatiquement via iSNS ou la MIB iSCSI, définie dans la [RFC4544].

En supposant la réussite de l'authentification IPsec, cette liste de FQDN peut être examinée pour déterminer les niveaux d'autorisation. Lorsque l'authentification de certificat est utilisée, il est possible de configurer les points d'extrémité de protocole de mémorisation de bloc IP avec des racines de confiance. Les racines de confiance utilisées avec les protocoles de mémorisation de bloc IP peuvent être différentes des racines de confiance utilisées à d'autres fins. Si c'est le cas, la charge de la négociation de l'utilisation des certificats appropriés incombe alors à l'initiateur IPsec.

Noter que parce que IKE ne s'accommode pas bien des chaînes de certificats, et est normalement configuré avec un ensemble limité de racines de confiance, il est très approprié pour l'usage intra-domaine.

Comme iSCSI prend en charge l'authentification de connexion, il est aussi possible d'utiliser les identités présentées au sein du Connexion iSCSI pour les besoins d'autorisation.

Dans iFCP, les propriétés de contrôle d'accès de basé découlent de l'exigence que deux passerelles iFCP en communication soient connues d'un ou plusieurs serveurs iSNS avant qu'elles puissent s'engager dans les échanges iFCP. L'utilisation facultative de la découverte de domaines dans iSNS donne des schémas de contrôle d'accès d'une plus grande complexité.

5.9 Utilisation d'AES en mode compteur

Lorsque on utilise les modes AES, il peut être nécessaire d'utiliser de plus grandes clés publiques ; les compromis sont décrits dans la [RFC3766]. Des groupes MODP Diffie-Hellman supplémentaires à utiliser avec IKE sont décrits dans la [RFC3526].

Lorsque on utilise AES en mode compteur, il est important d'éviter de réutiliser le compteur avec la même clé, même après un long temps. Le mode compteur crée du texte chiffré en OUXant le flux de clés généré avec le texte en clair. Il est très facile de récupérer le texte en clair à partir de deux messages en mode compteur chiffrés avec la même valeur de compteur, en OUXant simplement ensemble les deux paquets. Cela implique que c'est une erreur d'utiliser le chiffrement manuel d'IPsec avec le mode compteur, sauf lorsque la mise en œuvre prend des mesures héroïques pour conserver l'état à travers les sessions. Dans tous les cas, le chiffrage manuel NE DOIT PAS être utilisé car il ne fournit pas la prise en charge nécessaire de changement de clés.

Un autre problème du mode compteur est qu'il rend triviale la falsification de paquets corrects. Le mode compteur ne devrait donc jamais être utilisé sans aussi utiliser l'authentification des données.

6. Considérations relatives à l'IANA

La présente section donne des lignes directrices à l'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) en ce qui concerne l'enregistrement des valeurs du paramètre de clé SRP_GROUP au sein de iSCSI, conformément au BCP 26, [RFC2434].

Les considérations relatives à l'IANA pour le protocole iSCSI sont décrites dans la [RFC3720], Section 13 ; pour le protocole iFCP dans la [RFC4172], Section 12 ; et pour le protocole FCIP dans la [RFC3821], Appendice B.

6.1 Définition des termes

Les termes suivants sont utilisés ici avec la signification définie dans le BCP 26 : "espace de noms", "valeur allouée", "enregistrement".

Les politiques suivantes sont utilisées ici avec la signification définie dans le BCP 26 : "utilisation privée", "premier entré, premier servi", "révision par expert", "spécification exigée", "consensus de l'IETF", "action de normalisation".

6.2 Politiques d'enregistrement recommandées

Pour les demandes d'enregistrement où un expert désigné devrait être consulté, le directeur responsable de la zone IESG devrait mandater l'expert désigné.

Pour les demandes d'enregistrement exigeant une révision d'experts, la liste de diffusion IPS devrait être consultée, ou si le groupe de travail IPS est dissous, à une liste de diffusion désignée par le directeur de zone de l'IESG.

Le présent document définit les clés SRP_GROUP suivantes :

SRP-768, SRP-1024, SRP-1280, SRP-1536, SRP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192

Les nouvelles clés SRP_GROUP DOIVENT se conformer au format d'étiquette d'élément d'extension iSCSI décrit au paragraphe 13.5.4 de la [RFC3720].

L'enregistrement de nouvelles clés SRP_GROUP est par expert désigné avec spécification exigée. La demande est envoyée à la liste de diffusion du groupe de travail IPS ou à son successeur pour les commentaires et la révision de sécurité, et DOIT inclure une preuve non probabiliste de la primarité du groupe SRP proposé. Après une période d'un mois, l'expert désigné approuvera ou rejettera la demande d'enregistrement.

7. Références normatives

[RFC0793] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", (STD 7), septembre 1981.

[RFC1191] J. Mogul et S. Deering, "Découverte de la MTU de chemin", novembre 1990.

[RFC1435] S. Knowles, "Avis de l'IESG d'une expérience avec découverte de la MTU de chemin", mars 1993. *(Info)*

[RFC1981] J. McCann, S. Deering, J. Mogul, "Découverte de la MTU de chemin pour IP version 6", août 1996. *(D.S.)*

[RFC2104] H. Krawczyk, M. Bellare et R. Canetti, "HMAC : Hachage de clés pour l'authentification de message", février 1997.

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

[RFC2131] R. Droms, "Protocole de configuration dynamique d'hôte", mars 1997. *(Mise à jour par les RFC 3396 et 4361)*

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

[RFC2404] C. Madson, R. Glenn, "Utilisation de HMAC-SHA-1-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[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* 4306)

[RFC2408] D. Maughan, M. Schertler, M. Schneider et J. Turner, "Association de sécurité Internet et protocole de gestion

de clés (ISAKMP)", novembre 1998. *(Obsolète, voir la* RFC4306)

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

[RFC2412] H. Orman, "Protocole OAKLEY de détermination de clés", novembre 1998.

[RFC2434] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction d'une section Considérations relatives à l'IANA dans les RFC", BCP 26, octobre, 1998. *(Rendue obsolète par la* RFC 5226*)*

[RFC2451] R. Pereira, R. Adams, "Algorithmes de chiffrement ESP en mode CBC", novembre 1998. *(P.S.)*

[RFC2608] E. Guttman et autres, "Protocole de localisation de service, version 2", juin 1999. (*MàJ par* RFC3224) *(P.S.)*

[RFC2923] K. Lahey, "Problèmes de TCP avec la découverte de MTU de chemin", septembre 2000. *(Information)*

[RFC2945] T. Wu, "Système SRP d'authentification et d'échange de clés", septembre 2000. *(P.S.)*

[RFC3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins et M. Carney, "Protocole de configuration dynamique d'hôte pour IPv6 (DHCPv6)", juillet 2003.

[RFC3456] B. Patel et autres, "Protocole de configuration dynamique des hôtes (DHCPv4) Configuration du mode tunnel IPsec", janvier 2003. *(P.S.)*

[RFC3526] T. Kivinen et M. Kojo, "Groupes supplémentaires d'exponentiation modulaire (MODP) Diffie-Hellman pour l'échange de clés Internet (IKE)", mai 2003.

[RFC3566] S. Frankel, H. Herbert, "L'algorithme AES-XCBC-MAC-96 et son utilisation avec IPsec", septembre 2003. *(P.S.)*

[RFC3643] R. Weber et autres, "Encapsulation de trame sur canal fibre (FC)", décembre 2003. *(P.S.)*

[RFC3686] R. Housley, "Utilisation du mode Compteur de la norme de chiffrement évolué (AES) avec l'encapsulation de la charge utile de sécurité (ESP) dans IPsec", janvier 2004. *(P.S.)*

[RFC3720] J. Satran et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI)", avril 2004. (*MàJ par* RFC3980, RFC4850, RFC5048) *(P.S.)*

[3DESANSI] American National Standard for Financial Services X9.52-1998, "Triple Data Encryption Algorithm Modes of Operation", American Bankers Association, Washington, D.C., 29 juillet 1998

[SRPNDSS] Wu, T., "The Secure Remote Password Protocol", dans Proceedings of the 1998 Internet Society Symposium on Network and Distributed Systems Security, San Diego, CA, pp. 97-111

8. Références pour information

[AESPERF] Schneier, B., J. Kelsey, D. Whiting, D. Wagner, C. Hall, et N. Ferguson, "Performance Comparison of the AES Submissions", http://www.counterpane.com/aes-performance.html

[CRCTCP] Stone J., Partridge, C., "When the CRC and TCP checksum disagree", ACM Sigcomm, septembre 2000.

[DESANALY] Bellare, Desai, Jokippi, Rogaway, "A Concrete Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation", 1997, http://www-cse.ucsd.edu/users/mihir/papers/sym-enc.html

[DESCRACK] "Cracking DES", O'Reilly & Associates, Sebastapol, CA 2000.

[DESDIFF Biham, E., Shamir, A., "Differential Cryptanalysis of DES-like cryptosystems", Journal of Cryptology Vol 4, janvier 1991.

[DESINT] Bellovin, S., "An Issue With DES-CBC When Used Without Strong Integrity", Proceedings of the 32nd IETF, Danvers, MA, avril 1995

[FIPS46-3] U.S. DoC/NIST, "Data encryption standard (DES)", FIPS 46-3, 25 octobre 1999.

[FIPS74] U.S. DoC/NIST, "Guidelines for implementing and using the nbs data encryption standard", FIPS 74, avril 1981

[FIPS197] U.S. DoC/NIST, "Advanced Encryption Standard (AES)", FIPS 197, novembre 2001, http://csrc.nist.gov/CryptoToolkit/aes

[MD5Attack] Dobbertin, H., "The Status of MD5 After a Recent Attack", CryptoBytes Vol.2 No.2, Summer 1996

[NSPUE2] "Recommendation for Block Cipher Modes of Operation", National Institute of Standards et Technology (NIST) Special Publication 800-38A, CODEN: NSPUE2, U.S. Government Printing Office, Washington, DC, juillet 2001.

[PENTPERF] A. Bosselaers, "Performance of Pentium implementations", http://www.esat.kuleuven.ac.be/~bosselae/

[PMAC] Rogaway, P., Black, J., "PMAC: Proposal to NIST for a parallelizable message authentification code", http://csrc.nist.gov/encryption/modes/proposedmodes/pmac/pmac-spec.pdf

[RFC1321] R. Rivest, "Algorithme de résumé de message MD5", avril 1992. *(Information)*

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

[RFC2230] R. Atkinson, "Enregistrement de délégation d'échange de clé pour le DNS", novembre 1997. *(Information)*

[RFC2373] R. Hinden, S. Deering, "Architecture d'adressage IP version 6", juillet 1998. (*Obsolète, voir* RFC3513) *(P.S.)*

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

[RFC2403] C. Madson, R. Glenn, "Utilisation de HMAC-MD5-96 au sein d'ESP et d'AH", novembre 1998. *(P.S.)*

[RFC2405] C. Madson et N. Doraswamy, "Algorithme de chiffrement ESP DES-CBC avec IV explicite", novembre 1998.

[RFC2535] D. Eastlake 3rd, "Extensions de sécurité du système des noms de domaines", mars 1999. (*Obsolète, voir* RFC4033, RFC4034, RFC4035) *(P.S.)*

[RFC2782] A. Gulbrandsen, P. Vixie et L. Esibov, "RR DNS pour la spécification de la localisation des services (DNS SRV)", février 2000.

[RFC2845] P. Vixie et autres, "Authentification de transaction de clé secrète pour DNS (TSIG)", mai 20000 (*MàJ par* RFC3645) *(P.S.)*

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080) *(D.S.)*

[RFC2931] D. Eastlake 3rd, "Signatures de demandes et de transactions du DNS (SIG(0))", septembre 2000. *(P.S.)*

[RFC2983] D. Black, "Services différenciés et tunnels", octobre 2000. *(Information)*

[RFC3007] B. Wellington, "Mise à jour dynamique sécurisée du système des noms de domaine (DNS)", novembre 2000.

[RFC3347] M. Krueger, R. Haagens, "Protocole d'interface de systèmes de petits ordinateurs sur l'Internet (iSCSI) – exigences et considérations sur leur conception", juillet 2002. *(P.S.)*

[RFC3715] B. Aboba, W. Dixon, "Exigences de compatibilité entre IPsec et la traduction d'adresse réseau (NAT)", mars 2004. *(Info.)*

[RFC3721] M. Bakke et autres, "Interface Internet des systèmes de petits ordinateurs (iSCSI) : dénomination et découverte", avril 2004. *(Information)*

[RFC3766] H. Orman, P. Hoffman, "Détermination de la force des clés publiques utilisées pour l'échange de clés symétriques", avril 2004. (BCP0086)

[RFC3821] M. Rajagopal, E. Rodriguez, R. Weber, "Canal fibre sur TCP/IP (FCIP)", juillet 2004. *(P.S.)*

[RFC3822] D. Peterson, "Découverte de canal fibre sur des entités TCP/IP (FCIP) en utilisant le protocole de localisation de service version 2 (SLPv2)", juillet 2004. *(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.)*

[RFC4018] M. Bakke et autres, "Découverte de cibles et des serveurs de noms des interfaces systèmes de petits ordinateurs (iSCSI) en utilisant le protocole de localisation de service version 2 (SLPv2)", avril 2005. *(P.S.)*

[RFC4172] C. Monia et autres, "iFCP – un protocole pour le réseautage des mises en mémoire des canaux en fibre sur Internet", septembre 2005. *(P.S.)*

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

[RFC4418] T. Krovetz, J. Black, S. Halevi, A. Hevia, H. Krawczyk, P. Rogaway, "UMAC : un code d'authentification de message utilisant le hachage universel", mars 2006. *(Information)*

[RFC4544] M. Bakke et autres, "Définitions des objets gérés pour les interfaces système de petits ordinateurs sur Internet (iSCSI)", mai 2006. *(P.S.)*

[RFC4939] K. Gibbons et autres, "Définitions des objets gérés pour le service de noms de mémorisation sur Internet (iSNS)", juillet 2007. *(P.S.)*

[SRPDIST] Wu, T., "SRP Distribution", http://www-cs-students.stanford.edu/~tjw/srp/download.html

[UMAC] Black, J., Halevi, S., Krawczyk, H., Krovetz, T., Rogaway, P., "UMAC: Fast and provably secure message authentification", Advances in Cryptology - CRYPTO '99, LNCS vol. 1666, pp. 216-233. Version complète disponible à http://www.cs.ucdavis.edu/~rogaway/umac

[UMACPERF] Rogaway, P., "UMAC Performance", http://www.cs.ucdavis.edu/~rogaway/umac/perf00.html

9. Remerciements

Merci à Steve Bellovin de AT&T Research, William Dixon de V6 Security, David Black de EMC, Joseph Tardo et Uri Elzur de Broadcom, Julo Satran, Ted Ts'o, Ofer Biran, et Charles Kunzinger de IBM, Allison Mankin de ISI, Mark Bakke et Steve Senum de Cisco, Erik Guttman de Sun Microsystems et Howard Herbert de Intel pour leurs apports utiles aux discussions sur les problèmes de ce domaine.

Appendice A - Groupes bien connus à utiliser avec SRP

Les valeurs de module (N) et de générateur (g) pour diverses longueurs de modules sont données ci-dessous. Les valeurs ci-dessous sont tirées d'un logiciel développé par Tom Wu et Eugene Jhong pour le Stanford SRP distribution [SRPDIST], et dont il a été ensuite rigoureusement vérifié qu'ils sont premiers. Les mises en œuvre qui prennent en charge l'authentification SRP DOIVENT accepter des groupes jusqu'à 1536 bits, 1536 bits étant la longueur par défaut.

Clé iSCSI ="SRP-768" [768 bits]
Module (base 16) =
B344C7C4F8C495031BB4E04FF8F84EE95008163940B9558276744D91F7CC9F402653BE7147F00F576B93754BCDD
F71B636F2099E6FFF90E79575F3D0DE694AFF737D9BE9713CEF8D837ADA6380B1093E94B6A529A8C6C2BE33E0
867C60C3262B
Générateur = 2

Clé iSCSI ="SRP-1024" [1024 bits]
Module (base 16) =
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813
D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF188

5C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
Générateur = 2

Clé iSCSI ="SRP-1280" [1280 bits]
Module (base 16) =
D77946826E811914B39401D56A0A7843A8E7575D738C672A090AB1187D690DC43872FC06A7B6A43F3B95BEAEC
7DF04B9D242EBDC481111283216CE816E004B786C5FCE856780D41837D95AD787A50BBE90BD3A9C98AC0F5FC
0DE744B1CDE1891690894BC1F65E00DE15B4B2AA6D87100C9ECC2527E45EB849DEB14BB2049B163EA04187FD
27C1BD9C7958CD40CE7067A9C024F9B7C5A0B4F5003686161F0605B
Générateur = 2

Clé iSCSI ="SRP-1536" [1536 bits]
Module (base 16) =
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A
94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB
63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772
E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C
6F315180F93499A234DCF76E3FED135F9BB
Générateur = 2

Clé iSCSI ="SRP-2048" [2048 bits]
Module (base 16) =
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757
767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE8
2918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A2
3FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032
CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9D
BFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
Générateur = 2

En plus de ces groupes, les groupes suivants PEUVENT être acceptés, la primarité de chacun d'eux ayant aussi été rigoureusement prouvée :

[1] Clé iSCSI ="MODP-3072" : le groupe de 3072 bits de la [RFC3526], générateur : 5

[2] Clé iSCSI ="MODP-4096" : le groupe de 4096 bits de la [RFC3526], générateur : 5

[3] Clé iSCSI ="MODP-6144" : le groupe de 6144 bits de la [RFC3526], générateur : 5

[4] Clé iSCSI ="MODP-8192" : le groupe de 8192 bits de la [RFC3526], générateur : 19

Appendice B – Performances logicielles des transformées IPsec

Cet appendice fournit des données sur les performances des transformations de chiffrement et d'authentification IPsec dans le logiciel. Comme les performances des transformations IPsec sont largement dépendantes de la mise en œuvre, les données présentées ici peuvent n'être pas représentatives des performances d'une certaine situation, et ne sont présentées que pour les besoins de la comparaison. D'autres données de performances sont disponibles dans [AESPERF], [PENTPERF] et [UMACPERF].

B.1 Transformations d'authentification

Le Tableau B-1 présente les cycles/octet exigés par les algorithmes AES-PMAC, AES-CBC-MAC, AES-UMAC, HMAC-MD5, et HMAC-SHA1 à diverses tailles de paquet, mise en œuvre dans le logiciel.

Taille des données	AES-PMAC	AES-CBC-MAC	AES-UMAC	HMAC-MD5	HMAC-SHA1
64	31,22	26,02	19,51	93,66	109,27
128	33,82	28,62	11,06	57,43	65,04
192	34,69	26,02	8,67	45,09	48,56
256	33,82	27,32	7,15	41,63	41,63
320	33,3	27,06	6,24	36,42	37,46

384	33,82	26,88	5,42	34,69	34,69
448	33,45	26,76	5,39	32,71	31,96
512	33,82	26,67	4,88	31,22	30,57
576	33,53	26,59	4,77	30,64	29,48
640	33,3	26,54	4,42	29,66	28,62
768	33,82	26,88	4,23	28,18	27,32
896	33,45	27,13	3,9	27,5	25,64
1024	33,5	26,67	3,82	26,99	24,71
1152	33,53	27,17	3,69	26,3	23,99
1280	33,56	26,8	3,58	26,28	23,67
1408	33,58	26,96	3,55	25,54	23,41
1500	33,52	26,86	3,5	25,09	22,87

Tableau B-1 : Cycles/octet consommé par les algorithmes d'authentification AES-PMAC, AES-CBC-MAC, AES-UMAC, HMAC-MD5, et HMAC-SHA1 à diverses tailles de paquet.

Source : Jesse Walker, Intel

Le Tableau B-2 présente les cycles/s exigés par les algorithmes AES-PMAC, AES-CBC-MAC, AES-UMAC, HMAC-MD5, et HMAC-SHA1, mis en œuvre dans le logiciel, en supposant un paquet de 1500 octets.

Transformation	Cycles/octet (logiciel)	Cycles/s à 100 Mbit/s	Cycles/s à 1 Gbit/s	Cycles/s à 10 Gbit/s
AES-UMAC (8 octets)	3,5	43 750 000	437 500 000	4 375 B
HMAC-SHA1 (20 octets)	22,87	285 875 000	2 8588 B	28 588 B
HMAC-MD5	25,09	313 625 000	3 1363 B	31 363 B
AES-CBC-MAC	26,86	335 750 000	3 358 B	33 575 B
AES-PMAC (8 octets)	33,52	419 000 000	4 19 B	41 900 B

Tableau B-2 : Performances logicielle des algorithmes d'authentification HMAC-SHA1, HMAC-MD5, AES-CBC-MAC et AES-PMAC à des taux de ligne de 100 Mbit/s, 1 Gbit/s, et 10 Gbit/s (1500 octets par paquet).

Source : Jesse Walker, Intel

À des vitesses de 100 Mbit/s, AES-UMAC peut être mis en œuvre avec seulement un modeste processeur, et les autres algorithmes peuvent être mis en œuvre, en supposant qu'un seul processeur à grande vitesse peut être dédié à la tâche. À 1 Gbit/s, seul AES-UMAC peut être mis en œuvre sur un seul processeur à grande vitesse ; plusieurs processeurs à grande vitesse (1+ GHz) seront exigés pour les autres algorithmes. À 10 Gbit/s, seul AES-UMAC peut être mis en œuvre même avec plusieurs processeurs à grande vitesse ; les autres algorithmes vont exiger un nombre prodigieux de cycles/s. Donc à 10 Gbit/s, une accélération du matériel sera requise pour tous les algorithmes à l'exception possible de AES-UMAC.

B.2 Transformations de chiffrement et d'authentification

Le Tableau B-3 présente les cycles/octet requis par les algorithmes de chiffrement AES-CBC, AES-CTR et 3DES-CBC (sans MAC) mis en œuvre dans le logiciel, pour diverses tailles de paquet.

Taille des données	AES-CBC	AES-CTR	3DES-CBC
64	31,22	26,02	156,09
128	31,22	28,62	150,89
192	31,22	27,75	150,89
256	28,62	27,32	150,89
320	29,14	28,1	150,89
384	28,62	27,75	148,29
448	28,99	27,5	149,4
512	28,62	27,32	148,29
576	28,33	27,75	147,72
640	28,62	27,06	147,77
768	28,18	27,32	147,42
896	28,25	27,5	147,55
1024	27,97	27,32	148,29
1152	28,33	27,46	147,13
1280	28,1	27,58	146,99

1408	27,91	27,43	147,34
1500	27,97	27,53	147,85

Tableau B-3 : Cycles/octet consommés par les algorithmes de chiffrement AES-CBC, AES-CTR et 3DES-CBC à diverses tailles de paquet, mis en œuvre dans le logiciel.

Source : Jesse Walker, Intel

Le Tableau B-4 présente les cycles/seconde requis par les algorithmes de chiffrement AES-CBC, AES-CTR et 3DES-CBC (sans MAC) mis en œuvre dans le logiciel, aux taux de ligne de 100 Mbit/s, 1 Gbit/s, et 10 Gbit/s (en supposant des paquets de 1500 octets).

Transformation	Cycles/octet (logiciel)	Cycles/s à 100 Mbit/s	Cycles/s 1 Gbit/s	Cycles/s à 10 Gbit/s
AES-CBC	27,97	349 625 000	3 496 3 B	34 963 B
AES-CTR	27,53	344 125 000	3 441 3 B	34 413 B
3DES–CBC	147,85	1 848 13 B	18 481 3 B	184 813 B

Tableau B-4 : Performance logicielle des algorithmes de chiffrement AES-CBC, AES-CTR, et 3DES aux taux de ligne de 100 Mbit/s, 1 Gbit/s, et 10 Gbit/s (paquets de 1500 octets).

Source : Jesse Walker, Intel

À des vitesses de 100 Mbit/s, les modes AES-CBC et AES-CTR peuvent être mis en œuvre avec un processeur à grande vitesse, tandis que 3DES va exiger plusieurs processeurs à grande vitesse. À des vitesses de 1 Gbit/s, plusieurs processeurs à grande vitesse sont nécessaires pour les modes AES-CBC et AES-CTR. À des vitesses de 1+ Gbit/s pour 3DES, et 10 Gbit/s pour tous les algorithmes, la mise en œuvre dans le logiciel est infaisable, et une accélération du matériel est requise.

Le Tableau B-5 présente les cycles/octet requis pour les algorithmes combinés de chiffrement/authentification : AES CBC + CBCMAC, AES CTR + CBCMAC, AES CTR + UMAC, et AES-OCB à diverses tailles de paquet, mis en œuvre dans le logiciel.

Taille des données	AES CBC +CBCMAC	AES CTR + CBCMAC	AES CTR + UMAC	AES-OCB
64	119,67	52,03	52,03	57,23
128	70,24	57,23	39,02	44,23
192	58,97	55,5	36,42	41,63
256	57,23	55,93	35,12	40,32
320	57,23	55,15	33,3	38,5
384	57,23	55,5	32,95	37,29
448	58,72	55	32,71	37,17
512	58,54	55,28	32,52	36,42
576	57,81	55,5	31,8	37
640	57,75	55,15	31,74	36,42
768	57,67	55,5	31,65	35,99
896	57,61	55,75	31,22	35,68
1024	57,56	55,61	31,22	35,45
1152	57,52	55,21	31,22	35,55
1280	57.75	55.15	31.22	36.16
1408	57.47	55.34	30.75	35.24
1500	57.72	55.5	30.86	35.3

Tableau B-5 : Cycles/octet des algorithmes combinés de chiffrement/authentification : AES CBC + CBCMAC, AES CTR + CBCMAC, AES CTR + UMAC, et AES-OCB à diverses tailles de paquet, mis en œuvre dans le logiciel.

Le Tableau B-6 présente les cycles/seconde requis pour les algorithmes de chiffrement et d'authentification AES CBC + CBCMAC, AES CTR + CBCMAC, AES CTR + UMAC, et AES-OCB fonctionnant aux débits de ligne de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, en supposant des paquets de 1500 octets.

Transformations	Cycles/octet (logiciel)	Cycles/s à 100 Mbit/s	Cycles/s à 1 Gbit/s	Cycles/s à 10 Gbit/s
AES CBC + CBCMAC	57,72	721 500 000	7 215 B	72,15 B
AES CTR + CBCMAC	55,5	693 750 000	6,938 B	69,38 B
AES CTR + UMAC	30,86	385 750 000	3,858 B	38,58 B
AES-OCB	35,3	441 250 000	4,413 B	44,13 B

Tableau B-6 : Cycles/seconde requis pour les algorithmes de chiffrement et d'authentification AES CBC + CBCMAC, AES CTR + CBCMAC, AES CTR + UMAC, et AES-OCB, fonctionnant à des taux de ligne de 100 Mbit/s, 1 Gbit/s et 10 Gbit/s, en supposant des paquets de 1500 octets.

Source : Jesse Walker, Intel

À des vitesses de 100 Mbit/s, les algorithmes peuvent être mis en œuvre sur un processeur à grande vitesse. À des vitesses de 1 Gbit/s, plusieurs processeurs à grande vitesse sont nécessaires, et aucun des algorithmes ne peut être mis en œuvre dans un logiciel à un taux de ligne de 10 Gbit/s.

Adresse des auteurs

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
téléphone : +1 425 706 6605
Fax: +1 425 936 7329
mél : bernarda@microsoft.com

Venkat Rangan
Brocade Communications Systems Inc.
1745 Technology Drive,
San Jose, CA 95110
téléphone : +1 408 333 7318
Fax: +1 408 333 7099
mél : vrangan@brocade.com

Franco Travostino
Director, Content Internetworking Lab
Nortel Networks
3 Federal Street
Billerica, MA 01821
téléphone : +1 978 288 7708
mél : travos@nortelnetworks.com

Jesse Walker
Intel Corporation
2211 NE 25th Avenue
Hillboro, OR 97124
Fax: +1 503 264 4843
mél : jesse.walker@intel.com

Joshua Tseng
McDATA Corporation
3850 North First Street
San Jose, CA 95134-1702

mél : joshtseng@yahoo.com

Déclaration complète de droits de reproduction

Propriété intellectuelle

Remerciement

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