Groupe de travail Réseau
Request for Comments : 5189
RFC rendue obsolète : 3989
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Stiemerling, NEC
J. Quittek, NEC
T. Taylor, Nortel
mars 2008

Sémantique du protocole de communication de boîtier de médiation (MIDCOM)

Résumé
Le présent document spécifie la sémantique d'un protocole de communication de boîtier de médiation (MIDCOM, *Middlebox Communication*) à utiliser par les agents MIDCOM pour interagir avec les boîtiers de médiation tels que les pare-feu et les traducteurs d'adresse réseau (NAT, *Network Address Translator*). La discussion de la sémantique n'inclut pas de spécification concrète de syntaxe ni de protocole de transport. Cependant, un protocole concret est supposé mettre en œuvre la sémantique spécifiée ou, plus probablement, un sur-ensemble de celle-ci. La sémantique du protocole MIDCOM est dérivée des exigences pour MIDCOM, du cadre MIDCOM, et des décisions du groupe de travail. Le présent document rend obsolète la RFC 3989.

Table des Matières

1. Introduction....2
1.1 Terminologie....2
1.2 Gabarit de définition de transaction....3
2. Spécification de sémantique....4
2.1 Conception générale du protocole....4
2.2 Transactions de contrôle de session....7
2.3 Transactions de règle de politique....9
2.4 Transactions de groupe de règles de politique....22
3. Déclarations de conformité....25
3.1 Conformité de mise en œuvre générale....26
3.2 Conformité de boîtier de médiation....26
3.3 Conformité d'agent....26
4. Exemples d'usage de transactions....26
4.1 Exploration des règles de politique et des groupes de règles de politique....27
4.2 Activation d'un appel signalé SIP....29
5. Conformité aux exigences de MIDCOM....32
5.1 Exigences de la machinerie du protocole....32
5.1.8 Authentification mutuelle....33
5.2 Exigence de la sémantique de protocole....34
5.3 Exigences pour la sécurité....35
6. Considérations sur la sécurité....36
7. Considérations de l'IAB sur UNSAF....36
8. Remerciements....37
9. Références....37
9.1 Références normatives....37
9.2 Références pour information....37
Appendice A. Changements par rapport à la RFC 3989....38
Adresse des auteurs....38
Déclaration complète de droits de reproduction....38

1. Introduction

Le groupe de travail MIDCOM a défini un cadre [RFC3303] et une liste d'exigences [RFC3304] pour la communication à travers un boîtier de médiation. La prochaine étape vers un protocole MIDCOM est la spécification de la sémantique du protocole qui est contrainte, mais pas complètement impliquée, par les documents mentionnés ci-dessus.

Le présent mémoire suggère une sémantique pour le protocole MIDCOM. Elle est pleinement conforme aux exigences mentionnées dans la [RFC3304] et au consensus du groupe de travail sur les question de sémantique. Le présent document rend obsolète la [RFC3989].

Conformément au mandat du groupe de travail, la description de la sémantique est ciblée sur les filtres de paquets et les traducteurs d'adresse réseau (NAT, *Network Address Translator*) et prend en charge les applications qui exigent une configuration dynamique de ces boîtiers de médiation.

La sémantique est définie en termes de transactions. Deux types de base de transactions sont utilisés : les transactions de demande et les transactions asynchrones. De plus, on distingue deux types concrets de transactions de demande : les transactions de configuration et les transactions de surveillance.

Pour chaque transaction, la sémantique est spécifiée en décrivant (1) les paramètres de la transaction, (2) le traitement des messages de demande au boîtier de médiation, (3) les transitions d'état au boîtier de médiation causées, respectivement, par les transactions de demande ou indiquées par les transactions asynchrones ; et (4) les messages de réponse et de notification envoyés du boîtier de médiation à l'agent afin d'informer l'agent du changement d'état.

La sémantique peut être mise en œuvre par tout protocole qui prend en charge ces deux types de transactions et qui est suffisamment souple à l'égard des paramètres de transaction. Des mises en œuvre différentes pour des protocoles différents peuvent devoir étendre la sémantique décrite ci-dessous par l'ajout d'autres transactions et/ou d'autres paramètres aux transactions et/ou de partager une seule transaction en un ensemble de transactions. Sans considération de ces extensions, la sémantique donnée ci après fournit le sous ensemble minimum nécessaire de ce qui doit être mis en œuvre.

Le reste de ce document est structuré comme suit : la Section 2 décrit la sémantique du protocole. Elle est structurée en quatre paragraphes : conception générale du protocole (paragraphe 2.1) contrôle de session (paragraphe 2.2) règles de politique (paragraphe 2.3) groupes de règles de politique (paragraphe 2.4). La Section 3 contient les déclarations de conformité pour les définitions de protocole MIDCOM et les mises en œuvre de protocole MIDCOM par rapport à la sémantique définie à la section 2. La Section 4 donne deux exemples élaborés d'usage. Enfin la Section 5 explique comment la sémantique satisfait les exigences de MIDCOM.

1.1 Terminologie

La terminologie dans le présent mémoire suit les définitions données dans les documents de cadre [RFC3303] et d'exigences [RFC3304].

De plus, les termes suivants sont utilisés :

transaction de demande : une transaction de demande consiste en un transfert de message de demande de l'agent au boîtier de médiation, à traiter le message au boîtier de médiation, au transfert du message de réponse du boîtier de médiation à l'agent, et au transfert facultatif de messages de notification du boîtier de médiation aux agents autres que celui qui demande la transaction. Une transaction de demande peut causer une transition d'état au boîtier de médiation.

transaction de configuration : une transaction de configuration est une transaction de demande contenant une demande de changement d'état dans le boîtier de médiation. Si elle est acceptée, elle cause un changement d'état au boîtier de médiation.

transaction de surveillance : une transaction de surveillance est une transaction de demande contenant une demande d'informations d'état au boîtier de médiation. Elle ne cause pas de transition d'état au boîtier de médiation.

transaction asynchrone : une transaction asynchrone n'est pas déclenchée par un agent. Elle peut survenir sans qu'aucun agent ne participe à une session avec le boîtier de médiation. Potentiellement, une transaction asynchrone inclut le transfert de messages de notification du boîtier de médiation aux agents qui participent à une session ouverte. Un message de notification est envoyé à chaque agent qui a besoin d'avoir une notification de l'événement asynchrone. Le message indique la transition d'état au boîtier de médiation.

agent unique : une valeur d'agent unique est unique dans le contexte de l'agent. Ce contexte inclut toutes les sessions MIDCOM auxquelles l'agent participe. Une valeur d'agent unique est allouée par l'agent.

boîtier de médiation unique : une valeur de boîtier de médiation unique est unique dans le contexte du boîtier de médiation. Ce contexte inclut toutes les sessions MIDCOM auxquelles le boîtier de médiation participe. Une valeur de boîtier de médiation unique est allouée par le boîtier de médiation.

règle de politique : en général, une règle de politique est "un bloc de construction de base d'un système fondé sur une politique. C'est le lien d'un ensemble d'actions à un ensemble de conditions -- où les conditions sont évaluées à déterminer si les actions sont effectuées" [RFC3198]. Dans le contexte de MIDCOM, la condition est une spécification d'un ensemble de paquets auxquels les règles sont appliquées. L'ensemble d'actions contient toujours juste un seul élément par règle, soit l'action "réserver", soit l'action "activer".

règle de réservation de politique : règle de politique contenant une action réserver. La condition de politique de cette règle est toujours vraie. L'action est la réservation de juste une adresse IP ou une combinaison d'une adresse IP et d'une gamme de numéros d'accès sur aucun des côtés, un côté, ou les deux côtés du boîtier de médiation, selon la configuration du boîtier de médiation.

règle d'activation de politique : règle de politique contenant une action activer. La condition de politique consiste en un descripteur d'un ou plusieurs flux de paquets unidirectionnels ou bidirectionnels, et l'action de politique active les paquets appartenant à ce flux pour traverser le boîtier de médiation. Le descripteur identifie le protocole, la direction du flux, et les adresses de source et de destination, facultativement avec une gamme de numéros d'accès.

lien de NAT : le terme lien de NAT tel qu'utilisé dans le présent document ne se réfère pas nécessairement à un lien de NAT comme défini dans la [RFC2663]. Un lien de NAT dans la sémantique MIDCOM se réfère à une abstraction qui permet la communication entre les deux points d'extrémité à travers un boîtier de médiation de type NAT. Une action activer peut résulter en un lien de NAT ou en une session de NAT, selon la demande et ses paramètres.

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

1.2 Gabarit de définition de transaction

Dans les paragraphes qui suivent, la sémantique du protocole MIDCOM est spécifiée par transaction. Une spécification de transaction contient les entrées suivantes. Les entrées de paramètre, de cause d'échec, et de type de message de notification ne sont spécifiées que si elles sont applicables.

Nom de transaction : nom de description pour ce type de transaction.

Type de transaction : le type de transaction est "configuration", "surveillanceé, ou "asynchrone". Voir au paragraphe 1.1 la description des types de transaction.

Conformité de transaction : cette entrée contient soit "obligatoire", soit 'facultatif'. Pour les détails, voir au paragraphe 2.1.8.

Paramètres de demande : cette entrée fait la liste de tous les paramètres nécessaires pour cette demande. Une description est donnée pour chaque paramètre.

Paramètres de réponse (de succès) : cette entrée fait la liste de tous les paramètres renvoyés du boîtier de médiation à l'agent comme réponse positive à la demande précédente. Une description est donnée pour chaque paramètre.

Cause d'échec : toutes les réponses négatives ont deux paramètres : un identifiant de demande qui identifie la demande sur laquelle la réponse est envoyée et un paramètre indiquant la cause d'échec. Comme ces paramètres sont obligatoires, ils ne sont pas mentionnés dans le gabarit. Mais le gabarit contient une liste des potentielles raisons de défaillance qui peuvent être indiquées par le second paramètre. La liste n'est pas exhaustive. Une spécification de protocole concrète peut étendre la liste.

Type de message de notification : cette entrée décrit le type de message de notification qui peut être utilisé par cette transaction.

Sémantique : cette entrée décrit la sémantique réelle de la transaction. En particulier, elle décrit le traitement du message de demande par le boîtier de médiation, et les transitions d'état d'un boîtier de médiation respectivement causées par ou causant la transaction.

2. Spécification de sémantique

2.1 Conception générale du protocole

La spécification de sémantique vise à un équilibre entre la prise en charge appropriée des applications qui exigent une configuration dynamique des boîtiers de médiation et la simplicité de spécification et de mise en œuvre du protocole.

Les interactions de protocole sont structurées en transactions. L'état des boîtiers de médiation est décrit par les automates à états. Les automates à états sont définis par les états et les transitions d'état. Une seule transaction peut causer ou être causée par des transitions d'état dans plus d'un automate à états, mais par automate à états il n'y a pas plus d'une transition par transaction.

2.1.1 Transactions du protocole

Les transitions d'état sont initiées soit par un message de demande provenant de l'agent au boîtier de médiation ou par um autre événement au boîtier de médiation. Dans le premier cas, le boîtier de médiation informe l'agent en envoyant un message de réponse sur la transition d'état actuelle ; dans le second, le boîtier de médiation envoie un message de notification asynchrone non sollicité à chaque agent affecté par la transaction (si il participe à une session ouverte avec le boîtier de médiation).

Les messages de demande et de réponse contiennent un identifiant de demande unique d'agent qui permet à l'agent de déterminer à quelle demande envoyée correspond une réponse reçue.

Une analyse des exigences a montré que trois sortes de transactions sont requises :
- Les transactions de configuration permettant à l'agent de demander les transitions d'état au boîtier de médiation.
- Les transactions asynchrones permettant le rapport des changements d'état qui n'ont pas été demandés par l'agent.
- Les transactions de surveillance permettant à l'agent de demander des informations d'état au boîtier de médiation.

Les transactions de configuration et les transactions asynchrones fournissent la fonction de base du protocole MIDCOM. Elles sont relatives aux transitions d'état d'un boîtier de médiation, et elles concernent l'établissement et la terminaison des sessions MIDCOM et des règles de politique.

Les transactions de surveillance ne sont pas relatées aux transitions d'état d'un boîtier de médiation. Elles sont utilisées par les agents pour explorer le nombre, l'état, et les propriétés des règles de politique établies au boîtier de médiation.

Comme spécifié en détails à la Section 3, les transactions de configuration et les transactions asynchrones sont obligatoires sauf pour le changement de durée de vie de groupe (GLC, *Group Lifetime Change*). Elles doivent être mises en œuvre par un boîtier de médiation conforme. La transaction GLC et certaines des transactions de surveillance sont facultatives.

2.1.2 Types de message

Le protocole MIDCOM prend en charge trois sortes de messages : messages de demande, messages de réponse, et messages de notification. Pour chaque sorte, différents types de message existent. Dans ce document de sémantique, les types de message sont seulement définis par la liste des paramètres. L'ordre des paramètres et leur codage relèvent d'une définition de protocole concrète. Une définition de protocole peut aussi ajouter d'autres paramètres à un type de message ou combiner plusieurs paramètres en un seul, pour autant que les informations contenues dans les paramètres définis dans la sémantique soient toujours présentes.

Pour les messages de demande et les messages de réponse positive, il existe un type de message par transaction de demande. Chaque transaction de réponse définit la liste des paramètres du message de demande et du message de réponse positive (de succès) en utilisant le gabarit de définition de transaction défini au paragraphe 1.2.

En cas d'échec d'une transaction de demande, un message de réponse négative est envoyé du boîtier de médiation à l'agent. Ce message est le même pour toutes les transactions de demande ; il contient l'identifiant de demande de la demande à laquelle est envoyée la réponse et un paramètre indiquant la cause d'échec.

Il y a trois types de message de notification : la notification de terminaison de session (STN, *Session Termination Notification*) la notification d'événement de règle de politique (REN, *Policy Rule Event Notification*) et la notification d'événement de groupe (GEN, *Group Event Notification*). Tous contiennent un identifiant de notification unique pour le boîtier de médiation.

STN : le message de notification de terminaison de session contient de plus un seul paramètre indiquant la raison de la terminaison de la session par le boîtier de médiation.

REN : le message de notification d'événement de règle de politique contient l'identifiant de notification, un identifiant de règle de politique, et la durée de vie restante de la politique.

GEN : le message de notification d'événement de groupe contient l'identifiant de notification, un identifiant de groupe de règles de politique, et la durée de vie restante du groupe de règles de politique.

2.1.3 Session, règle de politique, et groupe de règles de politique

Toutes les transactions peuvent encore être groupées en des transactions concernant les sessions, en transactions concernant les règles de politique, et transactions concernant des groupes de règles de politique. Les groupes de règles de politique peuvent être utilisés pour indiquer les relations entre règles de politique et pour simplifier les transactions sur un ensemble de règles de politique en utilisant une seule transaction par groupe au lieu d'une par règle de politique.

Les sessions et règles de politique au boîtier de médiation sont à états pleins. Leurs états sont indépendants les uns des autres, et leurs automates à états (un par session et un par règle de politique) peuvent être séparés. Les groupes de règles de politique sont aussi à états pleins, mais le boîtier de médiation n'a pas besoin de conserver l'état pour les groupes de règles de politique, parce que la sémantique a été choisie de telle sorte que l'état de groupe de règles de politique soit implicitement défini par l'état de toutes les règles de politique appartenant au groupe (voir au paragraphe 2.4).

La séparation de l'état de session et de l'état de règle de politique simplifie la spécification de la sémantique ainsi que de la mise en œuvre du protocole. Donc, la spécification de la sémantique est structurée en conséquence et on utilise deux automates à états séparés pour illustrer la sémantique. Noter que les automates à états des conceptions et mises en œuvre concrètes de protocole vont probablement être plus complexes que les automates à états présentés ici. Cependant, les automates à états du protocole sont supposés être un sur ensemble des automates à états de la sémantique de ce document.

2.1.4 Atomicité

Toutes les transactions de demande sont atomiques les unes par rapport aux autres. Cela signifie que le traitement d'une demande au boîtier de médiation n'est jamais interrompue par une autre demande arrivant ou déjà en file d'attente. Cela s'applique particulièrement quand le boîtier de médiation reçoit concurramment des demandes provenant de sessions différentes. Cependant, des transactions asynchrones peuvent interrompre et/ou terminer le traitement d'une demande à tout moment.

Toutes les transactions de demande sont atomiques du point de vue de l'agent. Le traitement d'une demande ne commence pas avant que la demande complète arrive au boîtier de médiation. Aucun état intermédiaire n'est stable au boîtier de médiation, et aucun état intermédiaire n'est rapporté à un agent.

Le nombre de transactions spécifiées dans ce document est assez petit. Là encore, dans un souci de simplicité, on l'a réduit à un ensemble minimal qui satisfait cependant les exigences. Une mise en œuvre réelle du protocole pourrait exiger de partager certaines des transactions spécifiées ci-dessous en deux transactions ou plus du protocole concerné. La raison peut en être des contraintes du protocole particulier ou le désir de plus de souplesse. En général, cela ne devrait pas être un problème. Cependant, on devrait considérer que cela pourrait changer l'atomicité des transactions affectées.

2.1.5 Contrôle d'accès

La possession détermine l'accès aux règles de politique et groupes de règles de politique. Quand une règle de politique est créée, un identifiant unique pour le boîtier de médiation est généré pour l'identifier dans les futures transactions. Au delà de l'identifiant, chaque règle de politique a un possesseur. Le possesseur est l'agent authentifié qui a établi la règle de politique. Le boîtier de médiation utilise l'attribut de possesseur d'une règle de politique pour en contrôler l'accès ; chaque fois qu'un agent authentifié demande à modifier une règle de politique existante, le boîtier de médiation détermine le possesseur de la règle de politique et vérifie si l'agent demandeur est autorisé à effectuer des transactions sur les règles de politique de l'agent possesseur.

Toutes les règles de politique appartenant au même groupe de règles de politique doivent avoir le même possesseur. Donc, les agents authentifiés ont accès soit à tous les membres d'un groupe de règles de politique, soit à aucun d'eux.

Le boîtier de médiation peut être configuré à permettre à des agents authentifiés spécifiques d'accéder et modifier les règles de politique de certains possesseurs spécifiques. Certainement, une configuration par défaut raisonnable va laisser chaque agent accéder à ses propres règles de politique. Aussi, il pourrait être bon de configurer une identité d'agent à agir comme administrateur, lui permettant de modifier toutes les règles de politique possédées par tous les agents. Cependant, la configuration de l'autorisation au boîtier de médiation sort du domaine d'application de la sémantique et du protocole MIDCOM.

2.1.6 Capacités de boîtier de médiation

Pour plusieurs raisons, il est utile qu'à l'établissement de la session l'agent apprenne les capacités particulières du boîtier de médiation. Donc, la procédure d'établissement de session décrite au paragraphe 2.2.1 inclut un transfert des informations de capacités du boîtier de médiation à l'agent. La liste des capacités de boîtier de médiation couvertes inclut les suivantes :

- prise en charge de la fonction de pare-feu
- liste des fonctions de NAT prises en charge, incluant peut-être
  - la traduction d'adresse
  - la traduction d'accès
  - la traduction de protocole
  - le double NAT
- prise en charge d'adresse IP interne à caractère générique
- prise en charge d'adresse IP externe à caractère générique
- prise en charge d'accès à caractère générique
- la ou les versions IP prises en charge pour le réseau interne : IPv4, IPv6, ou les deux
- la ou les versions IP prises en charge pour le réseau externe : IPv4, IPv6, ou les deux
- liste des transactions de protocole MIDCOM facultatives prises en charge
- prise en charge de règles de politique spécifiques de l'interface
- persistance de règle de politique : persistante ou non persistante (une règle est persistante quand le boîtier de médiation peut sauvegarder la règle dans une mémoire non volatile, par exemple, un disque dur ou une mémoire flash)
- durée de vie maximum restante d'une règle de politique ou groupe de règles de politique
- temporisation d'inactivité des règles de politique dans le boîtier de médiation (les règles de politique réservées et activées non utilisées par du trafic de données pendant la durée de cette temporisation d'inactivité sont supprimées automatiquement par le boîtier de médiation ; pour la suppression des règles de politique par les boîtiers de médiation, voir au paragraphe 2.3.13, "Événement Règle de politique asynchrone (ARE)").
- nombre maximum de sessions MIDCOM simultanées.

La liste des capacités de boîtier de médiation peut être étendue par une spécification de protocole concret avec d'autres informations utiles à l'agent.

2.1.7 Identifiants d'agent et de boîtier de médiation

Pour permettre aux agents et aux boîtiers de médiation de tenir plusieurs sessions, chaque message de demande contient un paramètre qui identifie l'agent demandeur, et chaque message de réponse et chaque message de notification contient un paramètre qui identifie le boîtier de médiation. Ces paramètres ne sont pas explicitement mentionnés dans la description des transactions individuelles, parce qu'ils sont communs à toutes. Ils ne sont pas autrement référencés dans les descriptions de sémantique individuelles. Bien qu'ils ne soient pas nécessairement passés explicitement comme paramètres du protocole MIDCOM, ils pourraient être fournis par le protocole de transport sous-jacent (sûr) utilisé. Les identifiants d'agent au boîtier de médiation sont uniques pour un boîtier de médiation, et les identifiants d'un boîtier de médiation chez l'agent sont uniques pour l'agent.

2.1.8 Conformité

Les exigences pour MIDCOM dans la [RFC3304] demandent les capacités du protocole MIDCOM qui sont satisfaites par l'ensemble de transactions spécifiées ci-dessous. Cependant, il n'est pas exigé qu'une mise en œuvre réelle d'un boîtier de médiation prenne en charge toutes ces transactions. L'ensemble annoncé de transactions prises en charge peut être différent pour des agents authentifiés différents. Le boîtier de médiation informe l'agent authentifié par l'échange de capacités à l'établissement de la session sur les transactions que l'agent est autorisé à effectuer. Certaines transactions doivent être offertes à chaque agent authentifié.

Chaque définition de transaction ci-dessous a une entrée de conformité qui contient soit "obligatoire", soit "facultatif". Une transaction obligatoire doit être mise en œuvre par tout boîtier de médiation qui offre un service MIDCOM et doit être offerte à chaque agent authentifié. Une transaction facultative n'a pas nécessairement besoin d'être mise en œuvre par un boîtier de médiation ; il peut n'offrir ces transactions facultatives qu'à certains agents authentifiés. Le boîtier de médiation peut offrir une, plusieurs, toutes, ou aucune, transactions facultatives aux agents. Si il est permis à un agent d'utiliser une transaction de demande facultative est déterminé par la procédure d'autorisation du boîtier de médiation, ce qui n'est pas spécifié plus avant par le présent document.

2.2 Transactions de contrôle de session

Avant qu'aucune transaction sur les règles de politique ou groupes de règles de politique soit possible, une session MIDCOM valide doit être établie. Une session MIDCOM est une association authentifiée et autorisée entre un agent et un boîtier de médiation. Les sessions sont initiées par les agents et peuvent être terminées par l'agent ou le boîtier de médiation. Un agent et un boîtier de médiation peuvent tous deux participer à plusieurs sessions (avec des entités différentes) en même temps. Pour distinguer les différentes sessions, chaque partie utilise des identifiants de session locaux.

Toutes les transactions sont transmises dans cette session MIDCOM.

Le contrôle de session est pris en charge par trois transactions :
- établissement de session (SE, *Session Establishment*)
- terminaison de session (ST, *Session Termination*)
- terminaison de session asynchrone (AST, *Asynchronous Session Termination*)

Les deux premières sont les transactions de configuration initiées par l'agent, et la dernière est une transaction asynchrone initiée par le boîtier de médiation.

2.2.1 Établissement de session (SE)

Nom de transaction : établissement de session
Type de transaction : configuration
Conformité de transaction : obligatoire
Paramètres de demande :
- identifiant de demande : un identifiant unique pour l'agent pour confronter la demande et la réponse correspondante chez l'agent.
- version : version du protocole MIDCOM.
- défi de boîtier de médiation (mc, *middlebox challenge*) : jeton de défi d'authentification pour l'authentification du boîtier de médiation. Comme on le verra ci-dessous, ce n'est présent que dans la première itération de la demande.
- authentification d'agent (aa, *agent authentication*) : jeton d'authentification qui authentifie l'agent auprès du boîtier de médiation. Comme on le voit plus loin, ceci est mis à jour dans la seconde itération de la demande avec du matériel qui répond au défi du boîtier de médiation.

Paramètres de réponse (succès) :
- authentification de boîtier de médiation (ma, *middlebox authentication*) : jeton d'authentification qui authentifie le boîtier de médiation auprès de l'agent.
- défi d'agent (ac, *agent challenge*) : jeton de défi d'authentification pour l'authentification de l'agent.
- capacités de boîtier de médiation : liste décrivant les capacités du boîtier de médiation. Voir au paragraphe 2.1.6 la liste des capacités de boîtier de médiation.

Cause d'échec:
- échec d'authentification
- pas d'autorisation
- la version du protocole de l'agent et du boîtier de médiation ne concordent pas
- manque de ressources

Sémantique : cette transaction d'établissement de session est utilisée pour établir une session MIDCOM. Pour l'authentification mutuelle des deux parties, deux transactions d'établissement de session suivantes sont nécessaires, comme le montre la Figure 1.

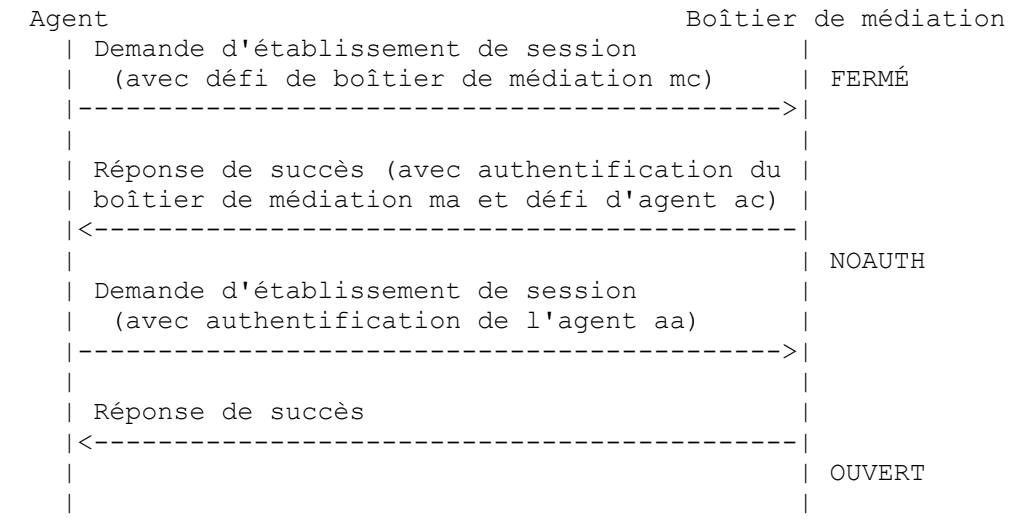


Figure 1 : Authentification mutuelle d'agent et de boîtier de médiation

L'établissement de session peut être simplifié en utilisant une seule transaction. Dans ce cas, le défi de serveur et le défi d'agent sont omis par l'envoyeur ou ignorés par le receveur, et l'authentification doit être fournie par d'autres moyens, par exemple, par la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC4346] ou IPsec [RFC4302], [RFC4303].

Le boîtier de médiation vérifie avec son point de décision de politique si l'agent demandeur est autorisé à ouvrir une session MIDCOM. Si il ne l'est pas, le boîtier de médiation génère une réponse négative avec "pas d'autorisation" comme cause d'échec. Si l'authentification et l'autorisation réussissent, la session est établie, et l'agent peut commencer à demander des transactions sur les règles de politique et les groupes de règles de politique.

Une indication des capacités du boîtier de médiation fait partie de la réponse de succès.

2.2.2 Terminaison de session (ST)

Nom de transaction : terminaison de session
Type de transaction : configuration
Conformité de transaction : obligatoire
Paramètres de demande :
- identifiant de demande : identifiant unique pour l'agent pour confronter la demande et la réponse correspondante chez l'agent.

Paramètres de réponse (seulement en cas de succès) :
- identifiant de demande : identifiant correspondant à l'identifiant de la demande.

Sémantique : cette transaction est utilisée pour clore la session MIDCOM au nom de l'agent. Après la terminaison de la session, le boîtier de médiation garde toutes les règles de politique établies jusu'à l'expiration de la durée de vie ou jusqu'à ce qu'un événement survienne qui cause leur terminaison par le boîtier de médiation.

Le boîtier de médiation génère toujours une réponse de succès. Après l'envoi de la réponse, le boîtier de médiation ne va pas envoyer d'autre message à l'agent dans la session en cours. Il ne va pas non plus traiter au sein de cette session d'autre demande qu'il aurait reçue pendant le traitement de la demande de terminaison de la session ou plus tard.

2.2.3 Terminaison de session asynchrone (AST)

Nom de transaction : terminaison de session asynchrone
Type de transaction : asynchrone
Conformité de transaction : obligatoire
Type de message de notification : notification de terminaison de session (STN, *Session Termination Notification*)
Paramètres de réponse (seulement en cas de succès) :
- raison de terminaison : raison pour laquelle la session est terminée.

Sémantique : le boîtier de médiation peut décider de terminer une session MIDCOM à tout moment. Avant de terminer la session en cours, le boîtier de médiation génère un message STN et l'envoie à l'agent. Après l'envoi de la notification, le boîtier de médiation ne va pas traiter d'autre demande de l'agent, même si elle est déjà en file d'attente au boîtier de médiation.

Après la terminaison de la session, le boîtier de médiation garde toutes les règles de politique établies jusqu'à l'expiration de leur durée de vie ou jusqu'à ce qu'un événement survienne pour lequel le boîtier de médiation les termine.

À la différence des autres transactions asynchrones, pas plus d'une notification n'est envoyée, parce que il y a seulement un agent affecté par la transaction.

2.2.4 Terminaison de session par interruption de connexion

Si une session MIDCOM est fondée sur une connexion de réseau sous-jacente, la session peut aussi être terminée par une interruption de cette connexion. Si le boîtier de médiation le détecte, il termine immédiatement la session. L'effet sur les règles de politique établies est le même que pour la terminaison de session asynchrone.

2.2.5 Automate à états de session

Un automate à états illustrant la sémantique des transactions de session est montré à la Figure 2. Les abréviations de transaction utilisées se trouvent dans les en-têtes des paragraphes de transaction.

Toutes les sessions commencent dans l'état FERMÉ. Si l'authentification mutuelle est déjà fournie par d'autres moyens, une transaction SE réussie peut causer une transition à l'état OUVERT. Autrement, elle cause une transition à l'état NOAUTH. À partir de cet état, une seconde transaction SE échouée retourne à l'état FERMÉ. Une transaction SE réussie cause une transition à l'état OUVERT. À tout moment, une transaction AST ou une défaillance de connexion peut se produire, causant une transition à l'état FERMÉ. Une transaction ST réussie à partir de NOAUTH ou OUVERT cause aussi un retour à FERMÉ. Les paramètres des transactions sont expliqués à la Figure 2 ; la valeur mc=0 représente un défi de boîtier de médiation vide.

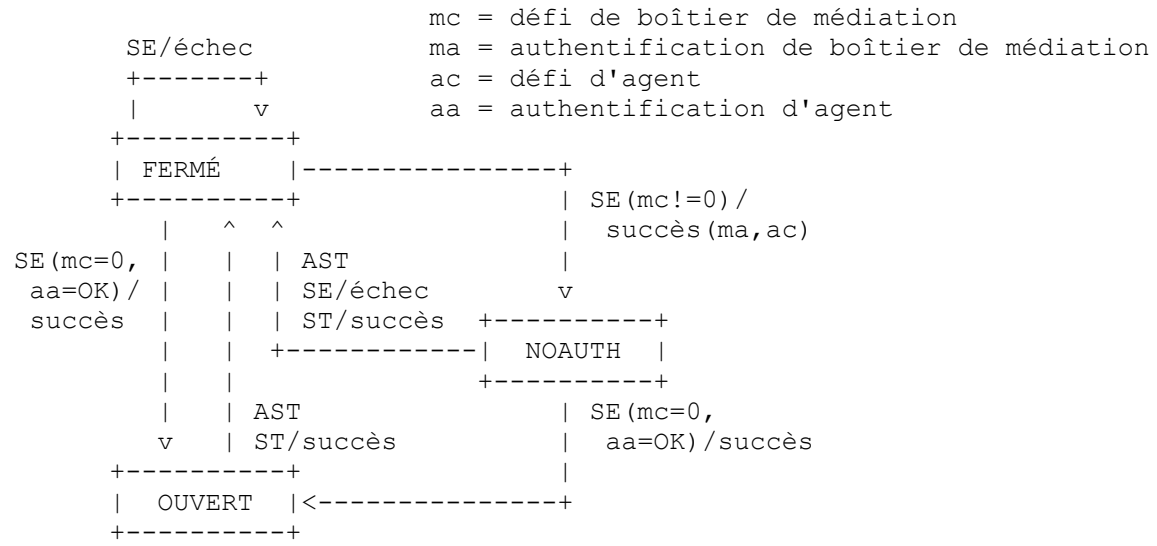


Figure 2 : Automate à états de session

2.3 Transactions de règle de politique

Ce paragaphe décrit la sémantique des transactions sur les règles de politique. Les transactions suivantes sont spécifiées :
- Règle de réservation de politique (PRR, *Policy Reserve Rule*)
- Règle d'activation de politique (PER, *Policy Enable Rule*)
- Changement de durée de vie de règle de politique (RLC, *Policy Rule Lifetime Change*)
- Liste de règles de politique (PRL, *Policy Rule List*)
- État de règle de politique (PRS, *Policy Rule Status*)
- Événement de règle de politique asynchrone (ARE, *Asynchronous Policy Rule Event*)

Les trois premières transactions (PRR, PER, RLC) sont les transactions de configuration initiées par l'agent. La quatrième et la cinquième (PRL, PRS) sont des transactions de surveillance. La dernière (ARE) est une transaction asynchrone. Les transactions PRL et PRS n'ont pas d'effet sur l'automate à états de règle de politique.

Avant qu'une transaction puisse commencer, une session MIDCOM valide doit être établie.

2.3.1 Transactions de configuration

Les transactions de règle de politique PER et RLC constituent le cœur du protocole MIDCOM. Les deux sont obligatoires, et servent à :
- configurer les liens de NAT (PER)
- configurer les passages d'entrée de pare-feu (PER)
- étendre la durée de vie des règles de politique établies (RLC)
- supprimer les règles de politique (RLC)

Certains cas exigent de connaître à l'avance quelle adresse IP (et numéro d'accès) va être choisie par le NAT dans une transaction PER. Cette information est requise avant que soient disponibles des informations suffisantes pour effectuer une transaction PER complète (voir l'exemple du paragraphe 4.2). Pour prendre en charge ces cas, les transactions de cœur sont étendues par la transaction règle de réservation politique (PRR, *Policy Reserve Rule*) qui sert à réserver des adresses et numéros d'accès aux NAT (PRR)

2.3.2 Établissement de règles de politique

PRR et PER établissent toutes deux une règle de politique. L'action au sein de la règle est "réserver" si elle est établie par PRR et "activer" si elle est établie par PER.

La transaction Règle de réservation de politique (PRR) est utilisée pour établir une réservation d'adresse sur aucun des côtés, un côté, ou les deux côtés du boîtier de médiation, selon la configuration du boîtier de médiation. La transaction retourne les adresses IP réservées et les gammes facultatives de numéros d'accès à l'agent. Aucun lien d'adresse ni configuration d'orifice d'accès *(pinhole)* n'est effectué au boîtier de médiation. Le traitement de paquets au boîtier de médiation reste inchangé.

Sur les purs pare-feu, la transaction PRR est bien traitée sans aucune réservation, mais la transition d''état du moteur du protocole MIDCOM est exactement la même que sur les NAT.

Sur un NAT traditionnel (voir la [RFC3022]) seule une adresse externe est réservée ; sur un double NAT, une adresse interne et une adresse externe sont réservées. La réservation à un NAT est pour des ressources exigées, comme des adresses IP et des numéros d'accès, pour une utilisation future. Comment la réservation est exactement faite dépend de la mise en œuvre de NAT. Dans les deux cas, la réservation concerne soit seulement une adresse IP, soit une combinaison d'une adresse IP avec une gamme de numéros d'accès.

La transaction Règle d'activation de politique (PER) est utilisée pour établir une règle de politique qui affecte le traitement de paquet au boîtier de médiation. Selon ses paramètres d'entrée, el peut utiliser la réservation établie par une transaction PRR ou créer une nouvelle règle à partir de rien.

Sur un NAT, l'action d'activation est interprétée comme une action de lien qui établit des liens entre les adresses internes et externes. À un pare-feu, l'action d'activation est interprétée comme une ou plusieurs actions de permission de configurer des orifices d'accès. Le nombre d'actions de permission dépend des paramètres de la demande et de la mise en œuvre de pare-feu.

Sur un NAT/pare-feu combiné, l'action d'activation est interprétée comme une combinaison d'actions de lien et de permission.

Les transactions PRR et PER sont décrites plus en détails aux paragraphes 2.3.8 et 2.3.9.

2.3.3 Maintien des règles de politique et des groupes de règles de politique

Chaque règle de politique a un identifiant unique pour le boîtier de médiation.

Chaque règle de politique a un possesseur. Le contrôle d'accès à la règle de politique se fonde sur la possession (voir au paragraphe 2.1.5). La possession d'une règle de politique ne change pas pendant la durée de vie de la règle de politique.

Chaque règle de politique a une durée de vie individuelle. Si la durée de vie de la règle de politique arrive à expiration, la règle de politique va être terminée au boîtier de médiation. Normalement, le boîtier de médiation indique la terminaison d'une règle de politique par une transaction ARE. Une transaction Changement de durée de vie de règle de politique (RLC, *Policy Rule Lifetime Change*) peut étendre la durée de vie de la règle de politique jusqu'à la limite spécifiée par le boîtier de médiation à l'établissement de session. Aussi, une transaction RLC peut être utilisée pour abréger la durée de vie d'une règle de politique ou supprimer une règle de politique en demandant une durée de vie de zéro. (Noter que la durée de vie de cette règle de politique peut aussi être modifiée par la transaction Changement de durée de vie de groupe (GLC, *Group Lifetime Change*).)

Chaque règle de politique est un membre de exactement un groupe de règles de politique. L'appartenance au groupe ne change pas pendant la durée de vie d'une règle de politique. Le choix du groupe fait partie de la transaction qui établit la règle de politique. Cette transaction crée implicitement un nouveau groupe si l'agent n'en spécifie pas un. L'identifiant du nouveau groupe est choisi par le boîtier de médiation. Les nouveaux membres sont ajoutés à un groupe existant si la demande de l'agent en désigne un. Un groupe n'existe que tant qu'il a des règles de politique membres. Aussitôt que toutes les politiques qui appartiennent au groupe ont atteint la fin de leur durée de vie, le groupe n'existe plus.

Les agents peuvent explorer les propriétés et l'état de toutes les règles de politique auxquelles il leur est permis d'accéder en utilisant la transaction État de règle de politique (PRS, *Policy Rule Status*).

2.3.4 Événements de politique et notifications asynchrones

Si une règle de politique change son état ou si sa durée de vie restante est changée d'une autre façon que d'être diminuée, alors tous les agents qui peuvent accéder à cette règle de politique et qui participent à une session ouverte avec le boîtier de médiation en ont notification par le boîtier de médiation. Si le changement d'état ou de durée de vie a été demandé explicitement par un message de demande, alors le boîtier de médiation le notifie à l'agent demandeur en retournant la réponse correspondante. Tous les autres agents qui peuvent accéder à la politique sont notifiés par un message de notification d'événement de règle de politique (REN, *Policy Rule Event Notification*).

Noter qu'un boîtier de médiation peut servir plusieurs agents en même temps dans différentes sesssions parallèles. Entre ces agents, les ensembles de règles de politique qui peuvent être leur être accessibles peuvent se chevaucher. Par exemple, il pourrait y avoir un agent qui s'authentifie comme administrateur et peut accéder à toutes les politiques de tous les agents. Ou il pourrait y avoir un agent de sauvegarde qui fait fonctionner une session en parallèle à un agent principal et qui s'authentifie comme la même entité que l'agent principal.

Dans le cas d'une transaction PER, PRR, ou RLC, l'agent demandeur reçoit une réponse respectivement PER, PRR, ou RLC. À tous les autres agents qui peuvent accéder à la règle de politique créée, modifiée, ou terminée (et qui participent à une session ouverte avec le boîtier de médiation) le boîtier de médiation envoie un message REN portant l'identifiant de règle de politique (PID) et la durée de vie restante de la règle de politique.

En cas d'une terminaison de règle par réduction de la durée de vie ou autre événement non déclenché par un agent, le boîtier de médiation envoie un message REN à chaque agent qui peut accéder à la règle de politique particulière et qui participe à une session ouverte avec le boîtier de médiation. Cela assure qu'un agent sait toujours l'état le plus récent de toutes les règles de politique auxquelles il peut accéder.

2.3.5 Couples d'adresses

Les messages de demande et de réponse des transactions PRR, PER, et PRS contiennent des spécifications d'adresse pour les adresses IP et de transport. Ces paramètres incluent :
- la version IP
- l'adresse IP
- la longueur du préfixe d'adresse IP
- le protocole de transport
- le numéro d'accès
- la parité d'accès
- la gamme d'accès.

De plus, le message de demande de PER et le message de réponse de PRS contiennent la direction du paramètre de flux. Cette direction du paramètre de flux indique pour UDP et IP la direction des paquets qui traversent le boîtier de médiation. Pour "l'entrée", les paquets UDP traversent de l'extérieur vers l'intérieur ; pour "la sortie"', de l'intérieur vers l'extérieur. Dans les deux cas, les paquets peuvent traverser le boîtier de médiation dans une seule direction. Un flux bidirectionnel est

activé par "bidirectionnel" comme direction du paramètre de flux. Pour TCP, le flux de paquets est toujours bidirectionnel, mais la direction du paramètre de flux est définie comme :

- entrant : flux de paquets TCP bidirectionnel. Le premier paquet, avec le fanion SYN TCP établi et le fanion ACK à zéro, doit arriver au boîtier de médiation à l'interface externe.

- sortant : flux de paquets TCP bidirectionnel. Le premier paquet, avec le fanion SYN TCP établi et le fanion ACK à zéro, doit arriver au boîtier de médiation à l'interface interne.

- bidirectionnel : flux de paquets TCP bidirectionnel. Le premier paquet, avec le fanion SYN TCP établi et le fanion ACK à zéro, peut arriver à l'interface interne ou externe

On se réfère à l'ensemble de ces paramètres comme à un couple d'adresses. Un couple d'adresses spécifie soit un point d'extrémité de communication à un appareil interne ou externe, soit à des adresses allouées au boîtier de médiation. Dans ce document, on distingue quatre sortes de couples d'adresses, comme le montre la Figure 3.

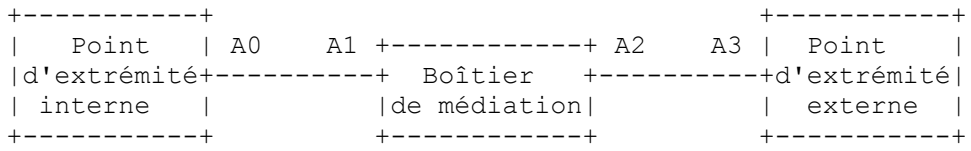


Figure 3 : Couples d'adresses A0 - A3

- A0 : point d'extrémité interne ; le couple d'adresses A0 spécifie un point d'extrémité de communication d'un appareil au sein du réseau interne, par rapport au boîtier de médiation.

- A1 : adresse interne du boîtier de médiation ; le couple d'adresses A1 spécifie un point d'extrémité virtuel de communication au boîtier de médiation au sein du réseau interne. A1 est l'adresse de destination pour les paquets qui passent du point d'extrémité interne au boîtier de médiation et est la source pour les paquets qui passent du boîtier de médiation au point d'extrémité interne.

- A2 : adresse externe du boîtier de médiation ; le couple d'adresses A2 spécifie un point d'extrémité virtuel de communication au boîtier de médiation au sein du réseau interne. A2 est l'adresse de destination pour les paquets qui passent du point d'extrémité externe au boîtier de médiation et est la source pour les paquets qui passent du boîtier de médiation au point d'extrémité externe.

- A3 : point d'extrémité externe ; le couple d'adresses A3 spécifie un point d'extrémité de communication d'un appareil au sein du réseau externe, par rapport au boîtier de médiation.

Pour un pare-feu, les points d'extrémité intérieur et extérieur sont identiques aux points d'extrémité correspondants, respectivement externe ou interne. Dans ce cas, la règle de politique installée règle la même valeur dans A2 que dans A0 (A0=A2) et règle la même valeur dans A1 que dans A3 (A1=A3).

Pour un NAT traditionnel, A2 reçoit une valeur différente de celle de A0, mais le NAT les lie. Comme pour le pare-feu, c'est aussi parce qu'il est un NAT traditionnel : A1 a la même valeur que A3.

Pour un double NAT, il y a deux liens des couples d'adresses : A1 et A2 ont toutes deux les valeurs allouées par le NAT. L'adresse externe A2 du boîtier de médiation adresse est liée au point d'extrémité interne A0, et l'adresse interne A1 du boîtier de médiation est liée au point d'extrémité externe A3.

2.3.6 Contraintes de paramètre d'adresse

Pour les paramètres de transaction qui appartiennent à un couple d'adresses, il existe des contraintes communes à tous les messages qui les utilisent. Donc, ces contraintes sont résumées ci-après et ne sont pas répétées lors de la description des paramètres dans la présentation des descriptions de transaction.

La sémantique de MIDCOM définie dans ce document spécifie le traitement de IPv4 et IPv6 comme protocole réseau, et de TCP et UDP (sur IPv4 et IPv6) comme protocole de transport. Le traitement de tout autre protocole de transport, par exemple, du protocole de transmission des commandes de flux (SCTP, *Stream Control Transmission Protocol*) n'est pas défini dans la sémantique mais peut être pris en charge par les spécifications de protocole concrètes.

Le paramètre version IP a la valeur "IPv4" ou "IPv6". Dans une règle de politique, la valeur du paramètre version IP doit être la même pour les couples d'adresses A0 et A1, et A2 et A3.

La valeur du paramètre adresse IP doit se conformer à la version IP spécifiée.

L'adresse IP d'un couple d'adresses peut être munie d'un caractère générique. Si l'utilisation de caractères génériques est permise dans l'adresse IP ou dans quelle gamme elle est permise dépend de la politique locale du boîtier de médiation ; voir aussi la Section 6, "Considérations sur la sécurité". L'utilisation de caractères génériques est spécifiée par le paramètre Longueur de préfixe d'adresse IP d'un couple d'adresses. En ligne avec l'utilisation courante d'une longueur de préfixe, ce paramètre indique le nombre de bits de poids fort de l'adresse IP qui sont fixés, tandis que le reste des bits de moindre poids de l'adresse IP est remplacé par des caractères génériques.

La valeur du paramètre Protocole de transport peut être "TCP", "UDP", ou "TOUS". Si le paramètre Protocole de transport a la valeur "TOUS", seuls les en-têtes IP sont considérés pour le traitement de paquets dans le boîtier de médiation -- c'est-à-dire, l'en-tête de transport n'est pas considéré. La valeur des paramètres Numéro d'accès, Gamme d'accès, et Parité d'accès n'est pas pertinente si le paramètre Protocole est "TOUS". Dans une règle de politique, la valeur du paramètre Protocole de transport doit être la même pour tous les couples d'adresses A0, A1, A2, et A3.

La valeur du paramètre Numéro d'accès est zéro ou un entier positif. Un entier positif spécifie un numéro d'accès concret UDP ou TCP. La valeur zéro spécifie un accès générique pour le protocole spécifié par le paramètre Protocole de transport. Si le paramètre Numéro d'accès a la valeur zéro, alors la valeur du paramètre Gamme d'accès n'est pas pertinente. Selon la valeur du paramètre Protocole de transport, ce paramètre peut vraiment se référer aux accès ou peut se référer à un concept équivalent.

Le paramètre Parité d'accès est utilisé différemment dans le contexte des règles de réservation de politique (PRR) et des règles d'activation de politique (PER). Dans le contexte d'une PRR, la valeur du paramètre peut être "impair", "pair", ou "tous". Il spécifie la parité du premier (le plus bas) numéro d'accès réservé.

Dans le contexte d'une PER, le paramètre Parité d'accès indique au boîtier de médiation si les numéros d'accès alloués au boîtier de médiation devraient avoir la même parité que les numéros d'accès respectivement internes ou externes correspondants. Dans ce contexte, le paramètre a la valeur "même" ou "tous". Si la valeur est "même", alors la parité du numéro d'accès de A0 doit être la même que la parité du numéro d'accès de A2, et la parité du numéro d'accès de A1 doit être la même que la parité du numéro d'accès de A3. Si le paramètre Parité d'accès a la valeur "tous", alors il n'y a pas de contrainte sur la parité des numéros d'accès.

Le paramètre Gamme d'accès spécifie un nombre de numéros d'accès consécutifs. Sa valeur est un entier positif. Comme le paramètre Numéro d'accès, ce paramètre définit un ensemble de numéros d'accès consécutifs commençant par le numéro d'accès spécifié par le paramètre Numéro d'accès comme le plus bas numéro d'accès et ayant autant d'éléments que spécifié par le paramètre Gamme d'accès. Une valeur de 1 spécifie un seul numéro d'accès. Le paramètre Gamme d'accès doit avoir la même valeur pour chaque couple d'adresses A0, A1, A2, et A3.

Une seule règle de politique P contenant une valeur de gamme d'accès supérieure à un est équivalente à un ensemble de règles de politique contenant un nombre n de politiques P_1, P_2, ..., P_n où n est égal à la valeur du paramètre Gamme d'accès. Chaque règle de politique P_1, P_2, ..., P_n a une valeur de paramètre Gamme d'accès de 1. La règle de politique P_1 contient un ensemble de couples d'adresses A0_1, A1_1, A2_1, et A3_1, dont chacun contient le premier numéro d'accès des couples d'adresses respectifs dans P ; la règle de politique P_2 contient un ensemble de couples d'adresses A0_2, A1_2, A2_2, et A3_2, dont chacun contient le second numéro d'accès du couple d'adresses respectif dans P ; et ainsi de suite.

2.3.7 Règles de politique spécifiques d'interface

Généralement, les agents demandent les règles de politique avec la seule connaissance de A0 et A3, c'est-à-dire, les couples d'adresses (voir au paragraphe 2.3.5). Mais dans des cas très particuliers, les agents peut avoir besoin de choisir les interfaces auxquelles est liée la règle de politique demandée. Généralement, le boîtier de médiation est attentif au choix des bonnes interfaces quand il réserve ou active une règle de politique, car il a la connaissance globale de sa configuration. Pour les agents qui veulent choisir les interfaces, des paramètres facultatifs sont inclus dans les transactions Règle de réservation de politique (PRR) et Règle d'activation de politique (PER). Ces paramètres sont appelés :

- interface interne : l'interface choisie à l'intérieur du boîtier de médiation -- c'est-à-dire, dans le domaine d'adresse privé ou protégé.
- interface externe : l'interface choisie à l'extérieur du boîtier de médiation -- c'est-à-dire, dans le domaine d'adresse public.

Les transactions État de règle de politique (PRS) incluent ces paramètres facultatifs dans leurs réponses quand ils sont pris en charge.

Les agents peuvent apprendre au démarrage de la session si des règles de politique spécifiques de l'interface sont acceptées par le boîtier de médiation, en vérifiant les capacités du boîtier de médiation (voir au paragraphe 2.1.6).

2.3.8 Règle de réserve de politique (PRR)

Nom de transaction : règle de réserve de politique
Type de transaction : configuration
Conformité de transaction : obligatoire
Paramètres de demande :
- identifiant de demande: identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de groupe : référence au groupe dont la règle de réserve de politique devrait être membre. Comme indiqué au paragraphe 2.3.3, si cette valeur n'est pas fournie, le boîtier de médiation alloue un nouveau groupe pour cette règle de réserve de politique.
- service : le service de NAT demandé du boîtier de médiation. Les valeurs admises sont "traditionnel" ou "deux fois".
- version IP interne : version IP demandée à l'intérieur du boîtier de médiation ; voir au paragraphe 2.3.5.
- adresse IP interne : adresse IP du point d'extrémité interne de communication (A0 à la Figure 3) ; voir paragraphe 2.3.5.
- numéro d'accès interne : numéro d'accès du point d'extrémité interne de communication (A0 à la Figure 3) ; voir au paragraphe 2.3.5.
- interface interne (facultatif) : interface à l'intérieur du boîtier de médiation ; voir au paragraphe 2.3.7.
- version IP externe : version IP demandée à l'extérieur du boîtier de médiation ; voir au paragraphe 2.3.5.
- interface externe (facultatif) : interface à l'extérieur du boîtier de médiation ; voir au paragraphe 2.3.7.
- protocole de transport : voir le paragraphe 2.3.5.
- gamme d'accès : nombre de numéros d'accès consécutifs à réserver ; voir au paragraphe 2.3.5.
- parité d'accès : parité demandée du premier (le plus faible) numéro d'accès à réserver ; les valeurs permises pour ce paramètre sont "impair", "pair, et "toutes". Voir aussi le paragraphe 2.3.5.
- durée de vie de règle de politique : proposition de durée de vie au boîtier de médiation pour la règle de politique demandée.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant qui correspond à l'identifiant de la demande.
- identifiant de règle de politique : identifiant de règle de politique unique au boîtier de médiation. Il est alloué par le boîtier de médiation et utilisé comme bride de règle de politique dans les transactions suivantes de règle de politique, en particulier pour se référer à la règle de réservation de politique dans une transaction PER suivante.
- identifiant de groupe : référence au groupe dont la règle de réservation de politique est membre.
- adresse IP réservée interne : adresse réservée IPv4 ou IPv6 sur le côté interne du boîtier de médiation. Pour un flux sortant, ce va être la destination à laquelle le point d'extrémité interne envoie ses paquets (A1 dans la Figure 3). Pour un flux entrant, ce va être l'adresse de source apparente des paquets tels que transmis au point d'extrémité interne (A0 dans la Figure 3). Le boîtier de médiation réserve et rapporte une adresse interne seulement dans le cas où un double NAT est utilisé. Autrement, une valeur vide pour les adresses indique qu'aucune réservation interne n'a été faite. Voir aussi le paragraphe 2.3.5.
- numéro d'accès réservé interne : voir le paragraphe 2.3.5.
- adresse IP réservée externe : adresse réservée IPv4 ou IPv6 sur le côté externe du boîtier de médiation. Pour un flux entrant, ce va être la destination à laquelle le point d'extrémité externe envoie ses paquets (A2 dans la Figure 3). Pour un flux sortant, ce va être l'adresse de source apparente des paquets tels que transmis au point d'extrémité externe (A3 dans la Figure 3). Si le boîtier de médiation est configuré comme un pur pare-feu, une valeur vide pour les adresses indique qu'aucune réservation externe n'a été faite. Voir aussi le paragraphe 2.3.5.
- numéro d'accès réservé externe : voir le paragraphe 2.3.5.
- durée de vie de règle de politique : la durée de vie de la règle de politique accordée par le boîtier de médiation, après quoi la réservation va être révoquée si elle n'a pas été déjà remplacée par une règle d'activation de politique dans une transaction PER.

Causes d'échec :
- agent non autorisé pour cette transaction,
- agent non autorisé à ajouter des membres à ce groupe,
- manque d'adresses IP,
- manque de numéros d'accès,
- manque de ressources,
- l'interface interne/externe spécifiée n'existe pas,

- l'interface interne/externe spécifiée n'est pas disponible pour le service spécifié.

Type de message de notification : notification d'événement de règle de politique (REN, *Policy Rule Event Notification*)

Sémantique : L'agent peut utiliser ce type de transaction pour réserver une adresse IP ou une combinaison d'adresse IP, type de transport, numéro d'accès, et gamme d'accès sur aucun côté, un côté, ou les deux côtés du boîtier de médiation comme nécessaire pour prendre en charge l'activation d'un flux. Normalement, la PRR va être utilisée dans des scénarios où il est nécessaire d'effectuer une telle réservation avant que des paramètres suffisants pour qu'une transaction complète d'activation de règle de politique soient disponibles. Voir un exemple au paragraphe 4.2.

Lorsque il reçoit la demande, le boîtier de médiation détermine combien de réservations d'adresse (et d'accès) sont nécessaires sur la base de sa configuration. Si il fournit seulement des services de filtrage de paquets, il n'effectue aucune réservation et retourne des valeurs vides pour les adresses IP et numéros d'accès réservés intérieurs et extérieurs. Si il est configuré pour un double NAT, il réserve des adresses IP intérieures et extérieures (et une gamme facultative de numéros d'accès) et les retourne. Autrement, il réserve et retourne une adresse IP externe (et une gamme facultative de numéros d'accès) et retourne des valeurs vides pour l'adresse interne et la gamme d'accès réservés.

Le paramètre A0 (version d'adresse IP intérieure, adresse IP intérieure, et numéro d'accès intérieur) peut être utilisé par le boîtier de médiation pour déterminer la transposition correcte de NAT et donc A2 si nécessaire. Une fois qu'une transaction PRR a réservé une adresse externe (A2) pour un point d'extrémité interne (A0) au boîtier de médiation, le boîtier de médiation doit s'assurer que cet A2 réservé est disponible dans toutes les transactions PER et PRR suivantes.

Pour les boîtiers de médiation qui prennent en charge les règles de politique spécifiques d'interface, comme défini au paragraphe 2.3.7, les paramètres facultatifs d'interface interne et externe doivent tous deux être inclus dans la demande, ou aucun d'eux ne devrait être inclus. En présence de ces paramètres, le boîtier de médiation utilise le paramètre Interface externe pour choisir l'interface à laquelle le couple d'adresse externe (adresse IP et numéro d'accès externes) est réservé, et le paramètre Interface interne pour choisir l'interface à laquelle le couple d'adresse interne (adresse IP et numéro d'accès internes) est réservé. En l'absence de ces paramètres, le boîtier de médiation choisit les interfaces particulières sur la base de sa configuration interne.

Si il y a un manque de ressources, comme d'adresses IP, de numéros d'accès, ou de mémorisation disponibles pour d'autres règles de politique, la réservation échoue alors, et une réponse d'échec appropriée est générée.

Si un groupe de règles de politique non existant a été spécifié, ou si un groupe de règles de politique existant a été spécifié qui n'est pas possédé par l'agent demandeur, aucune nouvelle règle de politique n'est alors établie, et une réponse d'échec appropriée est générée.

En cas de succès, cette transaction crée une nouvelle règle de réservation de politique. Si un groupe de règles de politique déjà existant est spécifié, alors la nouvelle règle de politique en devient membre. Si aucun groupe de politique n'est spécifié, un nouveau groupe est créé avec la nouvelle règle de politique comme seul membre. Le boîtier de médiation génère un identifiant unique de boîtier de médiation pour la nouvelle règle de politique. Le possesseur de la nouvelle règle de politique est l'agent authentifié qui a envoyé la demande. Le boîtier de médiation choisit une valeur de durée de vie qui est supérieure à zéro et inférieure ou égale au minimum de la valeur demandée et de la durée de vie maximum spécifiée par le boîtier de médiation au démarrage de la session, c'est-à-dire,

$$0 \leq \text{lt\_granted} \leq \text{MINIMUM}(\text{lt\_requested}, \text{lt\_maximum})$$

où
- lt_granted est la durée de vie actuellement accordée par le boîtier de médiation
- lt_requested est la durée de vie que l'agent a demandée
- lt_maximum est la durée de vie maximum spécifiée à l'établissement de session

Un boîtier de médiation avec capacité de NAT réserve toujours un couple d'adresse externe de boîtier de médiation (A2) en réponse à une demande PRR. Dans le cas particulier d'un boîtier de médiation combiné double NAT/NAT, l'agent peut demander seulement le service de NAT ou de double NAT en choisissant le paramètre de service "traditionnel" ou "double". Un agent qui n'a pas de préférence choisira "double". La valeur "traditionnel" ne devrait être utilisée que pour choisir le service de NAT traditionnel aux boîtiers de médiation qui offrent le NAT traditionnel et le double NAT. Dans le cas "double", le boîtier de médiation combiné double NAT/NAT réserve A2 et A1 ; le cas "traditionnel" résulte en une réservation de A2 seul. Un agent doit toujours utiliser la transaction PRR pour choisir le service NAT seul ou double NAT dans le cas particulier d'un boîtier de médiation combinant double NAT/NAT. Un boîtier de médiation pare-feu ignore ce paramètre.

Si l'identifiant de protocole est "TOUT", alors le boîtier de médiation réserve seulement la ou les adresses IP internes et/ou externes disponibles. La ou les adresses réservées sont retournées à l'agent. Dans ce cas, les paramètres de demande "gamme d'accès" et "parité d'accès" ainsi que les paramètres de réponse "numéro d'accès interne" et "numéro d'accès externe" ne sont pas pertinents.

Si l'identifiant de protocole est "UDP" ou "TCP", une combinaison d'une adresse IP et d'une séquence consécutive de numéros d'accès, commençant avec la parité spécifiée, est alors réservée, sur aucun côté, un des côtés, ou les deux côtés du boîtier de médiation, comme approprié. La ou les adresses IP et le premier (le plus bas) numéro d'accès réservé de la séquence consécutive sont retournés à l'agent. (Cela s'applique aussi aux autres protocoles qui prennent en charge les accès ou leur équivalent.)

Après l'établissement réussi d'une nouvelle règle de réservation de politique et l'envoi du message de réponse à l'agent demandeur, le boîtier de médiation vérifie si il y a d'autres agents authentifiés participant à des sessions ouvertes, qui peuvent accéder à la nouvelle règle de politique. Si le boîtier de médiation trouve un ou plusieurs de ces agents, il envoie alors un message REN faisant rapport de la nouvelle règle de politique à chacun d'eux.

Les agents MIDCOM utilisent la transaction Règle d'activation de politique (PER) pour activer les règles de réservation de politique qui ont été établies auparavant par une transaction Règle de réservation de politique (PRR). Voir aussi au paragraphe 2.3.2.

2.3.9 Règle d'activation de politique (PER)

Nom de transaction : règle d'activation de politique
Type de transaction : configuration
Conformité de transaction : obligatoire
Paramètres de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de règle de réservation de politique : référence à une règle de réservation de politique déjà existante créée par une transaction PRR. La référence peut être vide, et dans ce cas le boîtier de médiation doit allouer toutes les adresses et numéros d'accès nécessaires dans cette transaction PER. Si il n'est pas vide, alors les paramètres de demande suivants ne sont pas pertinents : identifiant de groupe, protocole de transport, gamme d'accès, parité d'accès, version IP interne, version IP externe.
- identifiant de groupe : référence au groupe dont la règle d'activation de politique devrait être membre. Comme indiqué au paragraphe 2.3.3, si cette valeur n'est pas fournie, le boîtier de médiation alloue un nouveau groupe pour cette règle d'activation de politique.
- protocole de transport : voir le paragraphe 2.3.5.
- gamme d'accès : nombre de numéros d'accès consécutifs à réserver ; voir au paragraphe 2.3.5.
- parité d'accès: parité demandée du ou des numéros d'accès à transposer. Les valeurs admises de ce paramètre sont "même" et "toutes". Voir aussi le paragraphe 2.3.5.
- direction du flux : ce paramètre spécifie la direction de la communicationactivée, soit "entrante', "sortante", soit "bidirectionnelle".
- version IP interne : version IP demandée à l'intérieur du boîtier de médiation ; voir au paragraphe 2.3.5.
- adresse IP interne : adresse IP du point d'extrémité interne de la communication (A0 dans la Figure 3) ; voir au paragraphe 2.3.5.
- numéro d'accès interne : numéro d'accès du point d'extrémité interne de la communication (A0 dans la Figure 3) ; voir au paragraphe 2.3.5.
- interface interne (facultatif) : interface à l'intérieur du boîtier de médiation ; voir au paragraphe 2.3.7.
- version IP externe : version IP demandée à l'extérieur du boîtier de médiation ; voir au paragraphe 2.3.5.
- adresse IP externe : adresse IP du point d'extrémité externe de la communication (A3 dans la Figure 3) ; voir au paragraphe 2.3.5.
- numéro d'accès externe : numéro d'accès du point d'extrémité externe de la communication (A3 dans la Figure 3) ; voir au paragraphe 2.3.5.
- interface externe (facultatif) : interface à l'extérieur du boîtier de médiation ; voir au paragraphe 2.3.7.
- durée de vie de la règle de politique : proposition du durée de vie au boîtier de médiation poir la règle de politique demandée.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant qui correspond à l'identifiant de la demande.
- identifiant de règle de politique : identifiant de règle de politique unique pour le boîtier de médiation. Il est alloué par le boîtier de médiation et utilisé comme bride de règle de politique dans les transactions ultérieures de règle de politique.

Si un identifiant de règle de réservation de politique a été fourni dans la demande, l'identifiant de règle de politique retourné a alors la même valeur.
- identifiant de groupe : référence au groupe dont la règle d'activation de politique est membre. Si un identifiant de règle de réservation de politique a été fourni dans la demande, ce paramètre identifie alors le groupe dont la règle de réservation de politique était membre.
- adresse IP interne : adresse IP fournie à l'intérieur du boîtier de médiation (A1 dans la Figure 3). En cas de double NAT, ce paramètre va être une adresse IP interne réservée à l'intérieur du boîtier de médiation. Dans tous les autres cas, ce paramètre de réponse va être identique à l'adresse IP externe passée avec la demande. Si le paramètre Identifiant de règle de réservation de politique a été fourni dans la demande et si la transaction PRR a réservé une adresse IP interne, alors l'adresse IP interne fournie dans la réponse PER va être la valeur identique à celle retournée par la réponse à la demande PRR. Voir aussi le paragraphe 2.3.5.
- numéro d'accès interne : numéro d'accès interne fourni à l'intérieur du boîtier de médiation (A1 dans la Figure 3) ; voir aussi le paragraphe 2.3.5.
- adresse IP externe : adresse IP externe fournie à l'extérieur du boîtier de médiation (A2 dans la Figure 3). En cas d'un pur pare-feu, ce paramètre va être identique à l'adresse IP interne passée avec la demande. Dans tous les autres cas, ce paramètre de réponse va être une adresse IP externe réservée à l'extérieur du boîtier de médiation. Voir aussi le paragraphe 2.3.5.
- numéro d'accès externe : numéro d'accès externe fourni à l'extérieur du NAT (A2 dans la Figure 3) ; voir au paragraphe 2.3.5..
- durée de vie de règle de politique : durée de vie de règle de politique attribuée par le boîtier de médiation.

Cause d'échec :
- agent non autorisé pour cette transaction
- agent non autorisé à ajouter des membres à ce groupe
- pas de règle de réservation de politique
- agent non autorisé à remplacer cette règle de réservation de politique
- conflit avec une règle de politique déjà existante (par exemple, les mêmes adresse-accès internes sont transposés en des paires différentes d'adresse-accès externes)
- manque d'adresses IP
- manque de numéros d'accès
- manque de ressources
- les caractères génériques IP internes ne sont pas autorisés
- les caractères génériques IP externes ne sont pas autorisés
- l'interface interne/externe spécifiée n'existe pas
- l'interface interne/externe spécifiée n'est pas disponible pour le service spécifié
- A0 réservé et A0 demandé discordants

Type de message de notification : Notification d'événement de règle de politique (REN)

Sémantique : cette transaction peut être utilisée par un agent pour activer la communication entre un point d'extrémité interne et un point d'extrémité externe indépendamment du type de boîtier de médiation (NAT, NAPT, pare-feu, NAT-PT, appareils combinés) pour du trafic unidirectionnel ou bidirectionnel.

L'agent envoie une demande d'activation qui spécifie les points d'extrémité (incluant facultativement des caractères génériques) et la direction de communication (entrante, sortante, bidirectionnelle). Les points d'extrémité de la communication sont affichés à la Figure 3. Le fonctionnement de base de la transaction PER peut être décrit par :
1. l'agent envoie A0 et A3 au boîtier de médiation,
2. le boîtier de médiation réserve A1 et A2 ou utilise A1 et A2 provenant d'une transaction PRR précédente,
3. le boîtier de médiation active le transfert de paquets entre A0 et A3 en liant A0-A2 et A1-A3 et/ou en ouvrant les orifices correspondants, tous deux en accord avec la direction spécifiée, et
4. le boîtier de médiation retourne A1 et A2 à l'agent.

Dans le cas d'un pur pare-feu de filtrage de paquets, les couples d'adresses retournés sont les mêmes que dans la demande : A2=A0 et A1=A3. Chaque partenaire utilise l'adresse réelle de l'autre. Dans le cas d'un NAT traditionnel, le point d'extrémité interne peut utiliser l'adresse réelle du point d'extrémité externe (A1=A3) mais le point d'extrémité externe utilise un couple d'adresses fourni par le NAT (A2!=A0). Dans le cas d'un appareil double NAT, les deux points d'extrémité utilisent les couples d'adresses fournis par le NAT pour s adresser à leur partenaire de communication (A3!=A1 et A2! =A0).

Si un pare-feu est combiné avec un NAT ou un double NAT, les couples d'adresses de réponse vont être les mêmes que pour le pur NAT traditionnel ou double NAT, respectivement, mais le boîtier de médiation va configurer son filtre de paquets en plus des liens de NAT effectués. Dans le cas d'un pare-feu combiné avec un NAT traditionnel, la règle de

politique peut impliquer plus d'une action d'activation pour la configuration de pare-feu, car les paquets entrants et sortants peuvent utiliser des paires différentes de source-destination.

Pour les boîtiers de médiation qui prennent en charge les règles de politique spécifiques d'interface, comme défini au paragraphe 2.3.7, les paramètres facultatifs d'interface interne et externe doivent tous deux être inclus dans la demande, ou aucun d'eux ne devrait être inclus. En présence de ces paramètres, le boîtier de médiation utilise le paramètre d'interface externe pour choisir l'interface à laquelle le couple d'adresse externe (adresse IP et numéro d'accès externes) est lié, et le paramètre interface interne pour choisir l'interface à laquelle le couple d'adresse interne (adresse IP et numéro d'accès internes) est lié. Sans la présence de ces paramètres, le boîtier de médiation choisit les interfaces sur la base de sa configuration interne.

Vérification de l'identifiant de règle de réservation de politique : si le paramètre qui spécifie la règle de réservation de politique n'est pas vide, alors le boîtier de médiation vérifie si la règle de politique référencée existe, si l'agent est autorisé à remplacer cette règle de politique, et si cette règle de politique est une règle de réservation de politique.

En cas de succès, cette transaction crée une nouvelle règle d'activation de politique. Si une règle de réservation de politique était déjà référencée, alors la règle de réservation de politique est terminée sans qu'une notification explicite soit envoyée à l'agent (autre que la réponse PER de succès).

La transaction PRR établit le point d'extrémité interne A0 durant le processus de réservation. Dans le processus de création d'une nouvelle règle d'activation de politique, le boîtier de médiation peut vérifier si le A0 demandé est égal au A0 réservé. Le boîtier de médiation peut rejeter une demande PER avec un A0 demandé non égal au A0 réservé A0 et doit alors envoyer un message d'échec approprié. Autrement, le boîtier de médiation peut changer A0 du fait de la demande PER.

Le boîtier de médiation génère un identifiant unique de boîtier de médiation pour la nouvelle règle de politique. Si une règle de réservation de politique était référencée, alors l'identifiant de la règle de réservation de politique est réutilisée.

Le possesseur de la nouvelle règle de politique est l'agent authentifié qui a envoyé la demande.

Vérification de l'identifiant de groupe de règle de politique : si aucune règle de réservation de politique n'a été spécifiée, le paramètre Groupe de règles de politique est vérifié. Si un groupe de règles de politique non existant est spécifié, ou si un groupe de règles de politique existant est spécifié qui n'est pas possédé par l'agent demandeur, alors aucune nouvelle règle de politique n'est établie, et une réponse d'échec appropriée est générée.

Si un groupe de règles de politique déjà existant est spécifié, alors la nouvelle règle de politique en devient membre. Si aucun groupe de politique n'est spécifié, alors un nouveau groupe est créé avec la nouvelle règle de politique comme seul membre.

Si la valeur du paramètre de protocole de transport est "TOUS", alors le boîtier de médiation active la communication entre l'adresse IP externe spécifiée et l'adresse IP interne spécifiée. Les adresses à utiliser par les partenaires à la communication pour s'adresser l'un à l'autre sont retournées à l'agent comme adresse IP interne et adresse IP externe. Si l'identifiant de réservation n'est pas vide et si la réservation a utilisé le même type de protocole de transport, alors les adresses IP réservées sont utilisées.

Pour les valeurs de paramètre de protocole de transport "UDP" et "TCP", le boîtier de médiation agit de façon analogue à "TOUS" mais transpose aussi les gammes de numéros d'accès, en gardant la parité d'accès, si c'est demandé.

La configuration du boîtier de médiation peut échouer à cause d'un manque de ressources, comme des adresses IP, des numéros d'accès, ou de la mémorisation disponibles pour d'autres règles de politique. Elle peut aussi échouer à cause d'un conflit avec une règle de politique établie. En cas de conflit, le mécanisme de premier arrivé, premier servi est appliqué. Les règles de politique existantes restent inchangées et les nouvelles qui arrivent sont rejetées. Cependant, en cas de chevauchement de règles de politique non en conflit (incluant des règles de politique identiques) toutes les règles de politique sont acceptées.

Le boîtier de médiation choisit une valeur de durée de vie supérieure à zéro et inférieure ou égale au minimum de la valeur demandée et de la durée de vie maximum spécifiée par le boîtier de médiation au démarrage de la session, c'est-à-dire,

$$0 \leq \text{lt\_granted} \leq \text{MINIMUM}(\text{lt\_requested}, \text{lt\_maximum})$$

où
- lt_granted est la durée de vie actuellement accordée par le boîtier de médiation
- lt_requested est la durée de vie que l'agent a demandée

- lt_maximum est la durée de vie maximum spécifiée à l'établissement de session

Dans chaque cas d'échec, une réponse d'échec appropriée est générée. La règle de réservation de politique qui est référencée dans la transaction PER n'est pas affectée en cas d'un échec dans la transaction PER -- c'est-à-dire, la règle de réservation de politique reste.

Après qu'une nouvelle règle d'activation de politique est établie avec succès et que le message de réponse a été envoyé à l'agent demandeur, le boîtier de médiation vérifie si il y a d'autres agents authentifiés qui participent à des sessions ouvertes qui peuvent accéder à la nouvelle règle de politique. Si le boîtier de médiation trouve un ou plusieurs de ces agents, il envoie alors un message REN rapportant la nouvelle règle de politique à chacun d'eux.

2.3.10 Changement de durée de vie de règle de politique (RLC)

Nom de transaction : changement de durée de vie de règle de politique
Type de transaction : configuration
Conformité de transaction : obligatoire
Paramètres de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de règle de politique : identifiant de la règle de politique pour laquelle il est demandé que la durée de vie soit changée. Cela peut identifier une règle de réserve de politique ou une règle d'activation de politique.
- durée de vie de règle de politique : nouvelle proposition de durée de vie pour la règle de politique.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant qui correspond à l'identifiant de la demande.
- durée de vie de règle de politique : durée de vie restante de la règle de politique accordée par le boîtier de médiation.

Cause d'échec :
- agent non autorisé pour cette transaction
- agent non autorisé à changer la durée de vie de cette règle de politique
- pas de telle règle de politique
- la durée de vie ne peut pas être étendue

Type de message de notification : Notification d'événement de règle de politique (REN)

Sémantique : l'agent peut utiliser ce type de transaction pour demander l'extension de la durée de vie d'une règle de politique établie, le raccourcissement de la durée de vie, ou la terminaison d'une règle de politique. La terminaison de règle de politique est demandée en suggérant une nouvelle durée de vie de règle de politique de zéro.

Le boîtier de médiation vérifie d'abord si la règle de politique spécifiée existe et si l'agent est autorisé à accéder à cette règle de politique. Si une des vérifications échoue, une réponse d'échec appropriée est générée. Si la durée de vie demandée est plus longue que l'actuelle, le boîtier de médiation vérifie aussi si la durée de vie de la règle de politique peut être étendue et génère un message d'échec approprié si il ne le peut pas.

Une réponse d'échec implique que la nouvelle durée de vie n'a pas été acceptée, et la règle de politique reste inchangée. Une réponse de succès est générée par le boîtier de médiation si la durée de vie de la règle de politique a été changée d'une façon quelconque.

La réponse de succès contient la nouvelle durée de vie de la règle de politique. Le boîtier de médiation choisit une valeur de durée de vie supérieure à zéro et inférieure ou égale au minimum de la valeur demandée et de la durée de vie maximum spécifiée par le boîtier de médiation au démarrage de la session , c'est-à-dire,

$$0 \leq \text{lt\_granted} \leq \text{MINIMUM}(\text{lt\_requested}, \text{lt\_maximum})$$

où
- lt_granted est la durée de vie actuellement accordée par le boîtier de médiation
- lt_requested est la durée de vie que l'agent a demandée
- lt_maximum est la durée de vie maximum spécifiée à l'établissement de session

Après l'envoi d'une réponse de succès avec une durée de vie de zéro, le boîtier de médiation va considérer que la règle de politique n'existe plus. Toute autre transaction sur cette règle de politique résulte en une réponse négative, indiquant que cette règle de politique n'existe plus.

Noter que la durée de vie d'une règle de politique peut aussi être changée par la transaction Changement de durée de vie de groupe (GLC, *Group Lifetime Change*) si elle est appliquée au groupe dont la règle de politique est membre.

Après que la durée de vie restante de règle de politique a réussi à être changée et que le message de réponse a été envoyé à l'agent demandeur, le boîtier de médiation vérifie si il y a d'autres agents authentifiés qui participent à des sessions ouvertes et peuvent accéder à la règle de politique. Si le boîtier de médiation trouve un ou plusieurs de ces agents, il envoie alors un message REN rapportant la nouvelle durée de vie restante de la règle de politique à chacun d'eux.

2.3.11 Liste de règles de politique (PRL)

Nom de transaction : Liste de règles de politique
Type de transaction : surveillance
Conformité de transaction : obligatoire

Paramètre de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant correspondant à l'identifiant de la demande.
- liste de politiques : liste des identifiants de règle de politique de toutes les règles de politique auxquelles l'agent peut accéder.

Cause d'échec :
- transaction non prise en charge
- agent non autorisé pour cette transaction

Sémantique : l'agent peut utiliser ce type de transaction pour faire la liste de toutes les politiques auxquelles il peut accéder. Généralement, l'agent a déjà cette information, mais dans des cas particiliers (par exemple, après une reprise sur défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent administratif qui peut accéder à toutes les politiques) cette transaction peut être utile.

Le boîtier de médiation vérifie d'abord si l'agent est autorisé à demander cette transaction. Si la vérification échoue, une réponse d'échec appropriée est générée. Autrement, une liste de toutes les politiques auxquelles l'agent peut accéder est retournée en indiquant l'identifiant et le possesseur de chaque politique.

Cette transaction n'a aucun effet sur l'état de la règle de politique.

2.3.12 État de règle de politique (PRS)

Nom de transaction : État de règle de politique
Type de transaction : surveillance
Conformité de transaction : obligatoire

Paramètres de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de règle de politique : identifiant unique pour le boîtier de médiation de règle de politique.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant correspondant à l'identifiant de la demande.
- possesseur de règle de politique : identifiant de l'agent qui possède cette règle de politique.
- identifiant de groupe : référence au groupe duquel la règle de politique est membre.
- action de règle de politique : ce paramètre a la valeur "réservé" ou la valeur "activé".
- protocole de transport : identifie le protocole pour lequel une réservation est demandée ; voir au paragraphe 2.3.5.
- gamme d'accès : nombre de numéros d'accès consécutifs ; voir au paragraphe 2.3.5.
- direction : direction de la communication activée par le boîtier de médiation. Applicable seulement aux règles d'activation de politique.
- version d'adresse IP interne : version de l'adresse IP interne (version IP de A0 dans la Figure 3).
- version d'adresse IP externe : version de l'adresse IP externe (version IP de A3 dans la Figure 3).
- adresse IP interne : adresse IP du point d'extrémité interne de la communication (A0 dans la Figure 3) ; voir au paragraphe 2.3.5.

- numéro d'accès interne : numéro d'accès du point d'extrémité interne de la communication (A0 dans la Figure 3) ; voir au paragraphe 2.3.5.
- adresse IP externe : adresse IP du point d'extrémité externe de la communication (A3 dans la Figure 3) ; voir au paragraphe 2.3.5.
- numéro d'accès externe : numéro d'accès du point d'extrémité externe de la communication (A3 dans la Figure 3) ; voir au paragraphe 2.3.5.
- interface interne (facultatif) : interface interne au boîtier de médiation ; voir au paragraphe 2.3.7.
- adresse IP interne : adresse IP interne fournie à l'intérieur du NAT (A1 dans la Figure 3) ; voir au paragraphe 2.3.5.
- numéro d'accès interne : numéro d'accès interne fourni à l'intérieur du NAT (A1 dans la Figure 3) ; voir au paragraphe 2.3.5.
- interface externe (facultatif) : interface externe au boîtier de médiation ; voir au paragraphe 2.3.7.
- adresse IP externe : adresse IP externe fournie à l'extérieur du NAT (A2 dans la Figure 3) ; voir au paragraphe 2.3.5.
- numéro d'accès externe : numéro d'accès externe fourni à l'extérieur du NAT (A2 dans la Figure 3) ; voir au paragraphe 2.3.5.
- parité d'accès : parité des accès alloués.
- service : service choisi dans le cas d'un boîtier de médiation qui mèle un NAT traditionnel et un double NAT (voir au paragraphe 2.3.8).
- durée de vie de règle de politique : durée de vie restante de la règle de politique.

Cause d'échec :
- transaction non prise en charge
- agent non autorisé pour cette transaction
- pas de telle règle de politique
- agent non autorisé à accéder à cette règle de politique.

Sémantique : l'agent peut utiliser ce type de transaction pour faire la liste de toutes les propriétés d'une règle de politique. Généralement, l'agent a déjà ces informations, mais dans des cas particuliers (par exemple, après la reprise sur défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent administratif qui peut accéder à toutes les règles de politique) cette transaction peut être utile.

Le boîtier de médiation vérifie d'abord si la règle de politique spécifiée existe et si l'agent est autorisé à accéder à ce groupe. Si une des vérifications échoue, une réponse d'échec appropriée est générée. Autrement, toutes les propriétés de la règle de politique sont retournées à l'agent. Certains des paramètres retournés peuvent être non pertinents, selon l'action de la règle de politique ("réservé" ou "activé") et selon les autres paramètres -- par exemple, l'identifiant de protocole.

Cette transaction n'a pas d'effet sur l'état de la règle de politique.

2.3.13 Événement Règle de politique asynchrone (ARE)

Nom de transaction : Événement de règle de politique asynchrone
Type de transaction : asynchrone
Conformité de transaction : obligatoire
Type de message de notification : notification d'événement de règle de politique (REN)

Sémantique : Le boîtier de médiation peut décider à tout moment de terminer une règle de politique. Cette transaction est déclenchée le plus fréquemment par l'expiration de la durée de vie de la règle de politique. Parmi les événements qui peuvent causer cette transaction, il y a des changements du point de décision de la règle de politique.

Le boîtier de médiation envoie un message REN à tous les agents qui participent à une session ouverte avec le boîtier de médiation et qui sont autorisés à accéder à la règle de politique. La notification est envoyée aux agents avant que le boîtier de médiation change la durée de vie de la règle de politique. Le changement de durée de vie peut être déclenché par tout autre agent autorisé et résulte en l'abrègement (lt_nouveau < lt_existant) l'extension (lt_nouveau > lt_existant) ou la terminaison de la règle de politique (lt_nouveau = 0).

La transaction ARE correspond au traitement du message REN décrit au paragraphe 2.3.4 pour plusieurs agents.

2.3.14 Automate à états de règle de politique

L'automate à états pour les transactions de règle de politique est montré à la Figure 4 avec toutes les transitions d'état possibles. Les abréviations de transaction utilisées se trouvent dans les en-têtes des paragraphes de transaction particuliers.

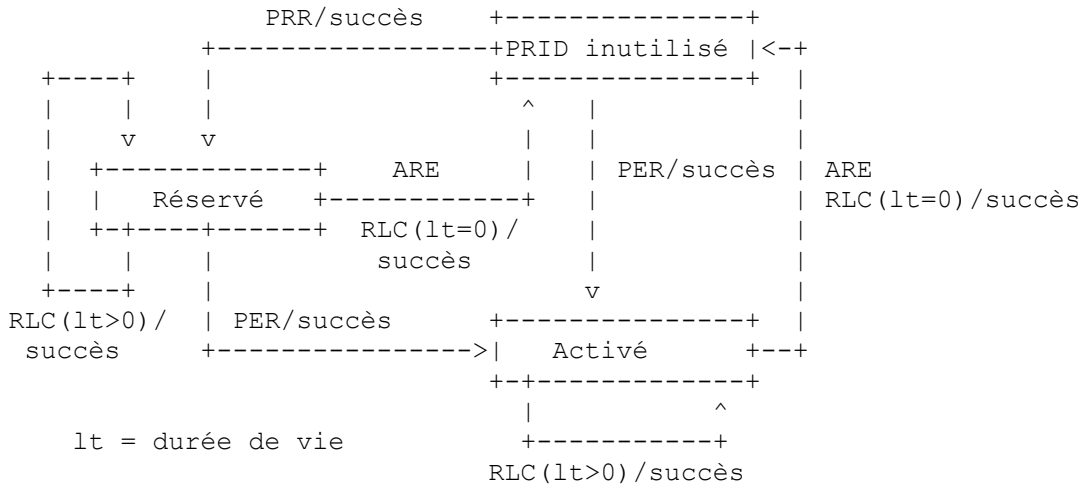


Figure 4 : Automate à états de règle de politique

Cet automate à états existe par identifiant de règle de politique (PRID). Initialement, toutes les règles de politique sont dans l'état PRID Inutilisé qui signifie que la règle de politique n'existe pas ou est inactive. Après le retour à l'état PRID Inutilisé, l'identifiant de règle de politique n'est plus lié à une règle de politique existante et peut être réutilisé par le boîtier de médiation.

Une transaction PRR réussie cause une transition de l'état initial PRID Inutilisé existant à l'état Réservé, où une réservation d'adresse est établie. À partir de là, l'état Activé peut être acquis par une transaction PER. Cette transaction peut aussi être utilisée pour entrer dans l'état Activé directement à partir de l'état PRID Inutilisé sans réservation. Dans l'état Activé, la communication demandée entre le point d'extrémité interne et le point d'extrémité externe est activée.

Les états Réservé et Activé peuvent être maintenus par des transactions RLC réussies avec une durée de vie demandée supérieure à 0. Les transitions à partir de ces deux états pour revenir à l'état PRID Inutilisé peuvent être causées par une transaction ARE ou par une transaction RLC réussie avec un paramètre de durée de vie de 0.

Un échec de transaction de demande ne change pas l'état au boîtier de médiation.

Noter que les transitions initiées par des transactions RLC peuvent aussi être initiées par des transactions GLC.

2.4 Transactions de groupe de règles de politique

Ce paragraphe décrit la sémantique des transactions sur les groupes de règles de politique. Ces transactions sont spécifiées comme suit :
- Changement de durée de vie de groupe (GLC, *Group Lifetime Change*)
- Liste de groupes (GL, *Group List*)
- État de groupe (GS, *Group Status*)

Toutes sont des transactions de demande initiées par l'agent. GLC est une transaction de configuration. GL et GS sont des transactions de surveillance qui n'ont pas d'effet sur l'automate à états de groupe.

2.4.1 Vue d'ensemble

Un groupe de règles de politique a seulement un attribut : la liste de ses membres. Toutes les politiques membres d'un seul groupe doivent être possédées par le même agent authentifié. Donc, une propriété implicite d'un groupe est son possesseur, qui est le possesseur des règles de politique membres.

Un groupe est implicitement créée quand est établie sa première règle de politique membre. Un groupe est implicitement terminé quand la dernière règle de politique membre restante est terminée. Par conséquent, la durée de vie d'un groupe est le maximum des durées de vie de toutes les règles de politique membres.

Un groupe a un identifiant unique pour le boîtier de médiation.

Les transactions de groupe de règles de politique sont déclarées comme "facultatives" par leur entrée de conformité respective à la Section 3. Cependant, elles fournissent certaines fonctions, comme la faculté qu'a l'agent d'envoyer seulement une demande au lieu de plusieurs, qui n'est pas disponible si seules des transactions obligatoire sont disponibles.

La transaction Changement de durée de vie de groupe (GLC) est équivalente à des transactions Changement de durée de vie de règle de politique (RLC effectuées simultanément sur tous les membres du groupe. Le résultat d'une transaction GLC réussie est que toutes les règles de politique membres ont la même durée de vie. Comme avec la transaction RLC, la transaction GLC peut être utilisée pour supprimer toutes les règles de politique membres en demandant une durée de vie de zéro.

Les transactions de surveillance Liste de groupe (GL) et État de groupe (GS) peuvent être utilisées par l'agent pour explorer l'état du boîtier de médiation et pour explorer ses droits d'accès. La transaction GL fait la liste de tous les groupes auxquels l'agent peut accéder, incluant des groupes possédés par d'autres agents. La transaction GS fait rapport de l'état sur un groupe individuel et fait la liste de toutes les règles de politique de ce groupe par leurs identifiants de règle de politique. L'agent peut explorer l'état des règles de politique individuelles en utilisant les identifiants de règle de politique dans une transaction État de règle de politique (PRS) (voir au paragraphe 2.3.12).

Les transactions GL et GS sont particulièrement utiles en cas de reprise sur défaillance d'un agent. L'agent qui assume le rôle du défaillant peut utiliser ces transactions pour restituer toutes les politiques qui avaient été établies par l'agent défaillant.

Les notifications sur les événements de groupe sont générées de façon analogue à celle des événements de règle de politique. Pour notifier aux agents les événements de groupe, le type de message Notification d'événement de groupe de règles de politique (GEN, *Rule Group Event Notification* (GEN) est utilisé. Les messages GEN contiennent un identifiant de notification unique pour l'agent, l'identifiant de groupe de règles de politique, et la durée de vie restante du groupe.

2.4.2 Changement de durée de vie de groupe (GLC)

Nom de transaction : Changement de durée de vie de groupe
Type de transaction : configuration
Conformité de transaction : facultatif

Paramètres de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de groupe : référence au groupe pour lequel est demandé le changement de la durée de vie.
- durée de vie de groupe : proposition de nouvelle durée de vie pour le groupe.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant correspondant à l'identifiant de la demande.
- durée de vie de groupe : durée de vie de groupe accordée par le boîtier de médiation.

Cause d'échec:
- transaction non prise en charge
- agent non autorisé pour cette transaction
- agent non autorisé à changer la durée de vie pour ce groupe
- pas de tel groupe
- la durée de vie ne peut pas être étendue

Type de message de notification : Notification d'événement de règle de politique (GEN)

Sémantique : l'agent peut utiliser ce type de transaction pour demander une extension de la durée de vie de tous les membres d'un groupe de règles de politique, pour demander un raccourcissement de la durée de vie de tous les membres, ou pour demander la terminaison de toutes les politiques membres (ce qui implique la terminaison du groupe). La terminaison est demandée en suggérant une nouvelle durée de vie de groupe de zéro.

Le boîtier de médiation vérifie d'abord si le groupe spécifié existe et si l'agent est autorisé à accéder à ce groupe. Si une des vérifications échoue, une réponse d'échec appropriée est générée. Si la durée de vie demandée est plus longue que l'actuelle, le boîtier de médiation vérifie aussi si la durée de vie du groupe peut être étendue et si elle ne le peut pas, génère un message d'échec approprié.

Une réponse d'échec implique que la durée de vie du groupe reste inchangée. Une réponse de succès est générée par le boîtier de médiation si la durée de vie du groupe a changé d'une manière ou d'une autre.

La réponse de succès contient la nouvelle durée de vie commune à toutes les règles de politique membres de ce groupe. Le boîtier de médiation choisit la nouvelle durée de vie inférieure ou égale au minimum de la durée de vie demandée et de la durée de vie maximum que le boîtier de médiation a spécifié à l'établissement de session avec ses autres capacités, c'est-à-dire,

$$0 \leq \text{lt\_granted} \leq \text{MINIMUM}(\text{lt\_requested}, \text{lt\_maximum})$$

où
- lt_granted est la durée de vie actuellement accordée par le boîtier de médiation
- lt_requested est la durée de vie que l'agent a demandée
- lt_maximum est la durée de vie maximum spécifiée à l'établissement de session

Après l'envoi d'une réponse de succès avec une durée de vie de zéro, le boîtier de médiation va terminer les règles de politique membres sans autre notification à l'agent, et va considérer le groupe et tous ses membres comme non existants. Toute autre transaction sur ce groupe de règles de politique ou sur un de ses membres résultera en une réponse négative, indiquant que ce groupe ou règle de politique, respectivement, n'existe plus.

Après le changement réussi de la durée de vie restante de groupe de règles de politique et l'envoi du message de réponse à l'agent demandeur, le boîtier de médiation vérifie si il y a d'autres agents authentifiés participant à des sessions ouvertes qui peuvent accéder au groupe de règles de politique. Si le boîtier de médiation trouve un ou plusieurs de ces agents, il envoie un message GEN rapportant la nouvelle durée de vie restante du groupe de règles de politique à chacun d'eux.

2.4.3 Liste de groupes (GL)

Nom de transaction : Liste de groupes
Type de transaction : surveillance
Conformité de transaction : facultatif

Paramètres de demande :
- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant correspondant à l'identifiant de la demande.
- liste de groupes : liste de tous les groupes auxquels l'agent peut accéder. Pour chaque groupe de la liste, l'identifiant et le possesseur de la liste sont indiqués.

Cause d'échec:
- transaction non prise en charge
- agent non autorisé pour cette transaction

Sémantique : l'agent peut utiliser ce type de transaction pour faire la liste de tous les groupes auxquels il peut accéder. Généralement, l'agent a déja ces informations, mais dans des cas particuliers (par exemple, après une reprise sur défaillance de l'agent) ou pour des agents spéciaux (par exemple, un agent administratif qui peut accéder à tous les groupes) cette transaction peut être utile.

Le boîtier de médiation vérifie d'abord si l'agent est autorisé à demander cette transaction. Si la vérification échoue, une réponse d'échec appropriée est générée. Autrement, une liste de tous les groupes auxquels l'agent peut accéder est retournée, indiquant l'identifiant et le possesseur de chaque groupe.

Cette transaction n'a pas d'effet sur l'état du groupe.

2.4.4 État de groupe (GS)

Nom de transaction : État de groupe
Type de transaction : surveillance
Conformité de transaction : facultatif

Paramètres de demande :

- identifiant de demande : identifiant unique d'agent pour confronter la demande et la réponse correspondante chez l'agent.
- identifiant de groupe : référence au groupe pour lequel les informations d'état sont demandées.

Paramètres de réponse (succès) :
- identifiant de demande : identifiant qui correspond à l'identifiant de la demande.
- possesseur du groupe : identifiant de l'agent qui possède ce groupe de règles de politique.
- durée de vie du groupe : durée de vie restante du groupe. C'est le maximum de la durée de vie restante de toutes les règles de politique de tous les membres.
- liste des membres : liste de toutes les règles de politique qui sont membres du groupe. Les règles de politique sont spécifiées par leur identifiant de règle de politique unique par boîtier de médiation.

Cause d'échec:
- transaction non prise en charge
- agent non autorisé pour cette transaction
- pas de tel groupe
- agent non autorisé à faire la liste des membres de ce groupe

Sémantique : l'agent peut utiliser ce type de transaction pour faire la liste de toutes les règles de politique membres d'un groupe. Généralement, l'agent a déjà ces informations, mais dans des cas particuliers (par exemple, après une reprise sur défaillance de l'agent) ou pour des agents spéciaux (par exemple, un agent administratif qui peut accéder à tous les groupes) cette transaction peut être utile.

Le boîtier de médiation vérifie d'abord si le groupe spécifié existe et si l'agent est autorisé à accéder à ce groupe. Si une des vérifications échoue, une réponse d'échec appropriée est générée. Autrement, une liste de tous les membres du groupe est retournée, indiquant l'identifiant de chaque groupe.

Cette transaction n'a pas d'effet sur l'état du groupe.

3. Déclarations de conformité

Une définition de protocole se conforme à la sémantique définie à la Section 2 si la spécification du protocole inclut toute les transactions spécifiées avec tous leurs paramètres obligatoires. Cependant, il n'est pas exigé qu'une mise en œuvre réelle de boîtier de médiation prenne en charge toutes ces transactions. Les transactions exigées pour la conformité sont différentes pour un agent et pour un boîtier de médiation.

Cette section contient les déclarations de conformité pour les mises en œuvre de protocole MIDCOM relatives à la sémantique. La conformité est spécifiée différemment pour les agents et pour les boîtiers de médiation. Ces déclarations de conformité vont probablement être étendues par la spécification concrète de protocole. Cependant, une telle extension est supposée étendre les déclarations ci-dessous de telle façon que toutes tiennent quand même.

La liste suivante montre la propriété de conformité de transaction de toutes les transactions telles que spécifiées dans la section précédente :

Transactions de contrôle de session :
- Établissement de session (SE, *Session Establishment*) : obligatoire
- Terminaison de session (ST, *Session Termination*) : obligatoire
- Terminaison de session asynchrone (ST, *Asynchronous Session Termination*) : obligatoire

Transactions de règle de politique :
- Règle de réservation de politique (PRR, *Policy Reserve Rule* (PRR) : obligatoire
- Règle d'activation de politique (PER, *Policy Enable Rule*) : obligatoire
-Changement de durée de vie de règle de politique (RLC, *Policy Rule Lifetime Change*) : obligatoire
- Liste de règles de politique (PRL, *Policy Rule List*) : obligatoire
- État de règle de politique (PRS, *Policy Rule Status*) : obligatoire
- Événement de règle de politique asynchrone (ARE, *Asynchronous Policy Rule Event*) : obligatoire

Transactions de groupe de règles de politique :
- Changement de durée de vie de groupe (GLC, *Group Lifetime Change*) : facultatif
- Liste de groupes (GL, *Group List*) : facultatif
- État de groupe (GS, *Group Status*) : facultatif

3.1 Conformité de mise en œuvre générale

Une mise en œuvre conforme d'un protocole MIDCOM DOIT prendre en charge toutes les transactions obligatoires.

Une mise en œuvre conforme d'un protocole MIDCOM PEUT prendre en charge aucune, une, ou plusieurs des transactions suivantes : GLC, GL, GS.

Une mise en œuvre conforme PEUT étendre la sémantique du protocole par d'autres transactions.

Une mise en œuvre conforme d'un protocole MIDCOM DOIT prendre en charge tous les paramètres obligatoires de chaque transaction concernant les informations contenues. L'ensemble des paramètres peut être redéfini transaction par transaction pout autant que les informations contenues sont maintenues.

Une mise en œuvre conforme d'un protocole MIDCOM PEUT prendre en charge l'utilisation des règles de politique-spécifiques de l'interface. Les paramètres d'interface facultatifs internes et externes dans les transactions PRR, PER, et PRS DOIVENT être inclus tous ou aucun, si les règles de politique spécifiques de l'interface-sont prises en charge.

Une mise en œuvre conforme PEUT étendre la liste des paramètres des transactions.

Une mise en œuvre conforme PEUT remplacer une seule transaction par un ensemble de transactions de granularité plus fine. Dans ce cas, elle DOIT être assurée que l'exigence du paragraphe 2.1.4 (comportement déterministe) et l'exigence du paragraphe 2.1.5 (état connu et stable) de la [RFC3304] sont encore satisfaites. Quand une seule transaction est remplacée par un ensemble de plusieurs transactions de granularité fine, cet ensemble DOIT être équivalent à une seule transaction. De plus, cet ensemble de transactions DOIT encore satisfaire l'exigence d'atomicité déclarée au paragraphe 2.1.4.

3.2 Conformité de boîtier de médiation

Une mise en œuvre de boîtier de médiation d'un protocole MIDCOM prend en charge une transaction de demande si elle est capable de recevoir et traiter toutes les instances possibles de message correct de la transaction de demande particulière et si elle génère une réponse correcte pour toute demande correcte qu'elle reçoit.

Une mise en œuvre de boîtier de médiation d'un protocole MIDCOM prend en charge une transaction asynchrone si elle est capable de générer correctement le message de notification correspondant.

Une mise en œuvre de boîtier de médiation d'un protocole MIDCOM conforme doit informer l'agent de la liste des transactions prises en charge au sein de la transaction SE.

3.3 Conformité d'agent

Une mise en œuvre d'agent d'un protocole MIDCOM prend en charge une transaction de demande si elle peut générer correctement le message de demande correspondant et si elle peut recevoir et traiter toutes les réponses correctes possibles à ces demandes particulières.

Une mise en œuvre d'agent d'un protocole MIDCOM prend en charge une transaction de demande asynchrone si elle peut recevoir et traiter toutes les instances possibles de message correct de la transaction particulière.

Une mise en œuvre conforme d'agent d'un protocole MIDCOM ne doit pas utiliser de transaction facultative non prise en charge par le boîtier de médiation. Le boîtier de médiation informe l'agent de la liste des transactions prises en charge dans la transaction SE.

4. Exemples d'usage de transactions

Cette Section donne deux exemples d'utilisation des transactions spécifiées dans la Section 2. Le premier montre comment un agent peut explorer toutes les règles de politique et groupes de règles de politique auxquels il peut accéder à un boîtier de médiation. Le second exemple montre la configuration d'un boîtier de médiation en combinaison avec l'établissement d'une session de voix sur IP avec le protocole d'initialisation de session (SIP, *Session Initiation Protocol*) [RFC3261].

4.1 Exploration des règles de politique et des groupes de règles de politique

Cet exemple suppose une session déjà établie. Il montre comment un agent peut trouver
- à quels groupes il peut accéder et qui possède ces groupes,
- l'état et la liste des membres de tous les groupes accessibles, et
- l'état et les propriétés de toutes les règles de politique accessibles.

Si il y a juste une seule session, ces actions ne sont pas nécessaires, parce que le boîtier de médiation informe l'agent de chaque transition d'état de toute règle de politique ou groupe de règles de politique. Cependant, après l'interruption d'une session ou après une terminaison intentionnelle de la session, l'agent pourrait vouloir rétablir la session et explorer quels groupes et règles de politique il avait établi sont toujours en place.

Aussi, un système d'agent peut avoir une défaillance et un autre peut prendre la suite. Alors le nouveau système d'agent a besoin de découvrir ce qui a déjà été configuré par le système défaillant et ce qu'il reste à faire.

Une troisième situation où l'exploration des règles et groupes de politique est utile est le cas d'un agent avec autorisation de "administrateur". Cet agent peut accéder à, et modifier, toute règle de politique ou groupe créé par un autre agent.

Tous les agents vont probablement commencer leur exploration avec la transaction de liste de groupe (GL) comme le montre la Figure 5. À cette demande, le boîtier de médiation retourne une liste de paires, chacune contenant un identifiant d'agent et un identifiant de groupe (GID). L'agent est informé de ses propres groupes et de à quels groupes d'autres agents il peut accéder.

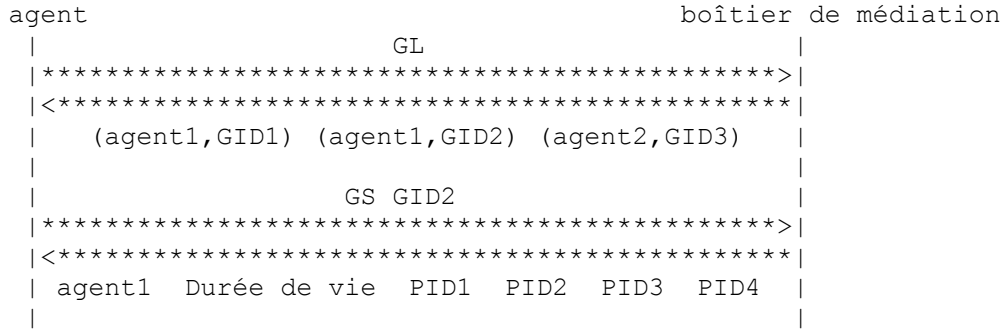


Figure 5 : Utilisation des transactions GL et GS

Dans la Figure 5, trois groupes sont accessibles à l'agent, et l'agent restitue les informations sur le second groupe en utilisant la transaction État de groupe (GS) . Il reçoit le possesseur du groupe, la durée de vie restante, et la liste des règles de politique membres, dans ce cas, contenant quatre identifiants de règle de politique (PID).

Ensuite, l'agent explore ces quatre règles de politique. L'exemple suppose que le boîtier de médiation est un NAPT traditionnel. La Figure 6 montre l'exploration de la première règle de politique. En réponse à une transaction État de règle de politique (PRS) le boîtier de médiation retourne toujours la liste de paramètres suivante :
- possesseur de règle de politique
- identifiant de groupe
- action de règle de politique (réservation ou activation)
- type de protocole
- gamme d'accès
- direction
- adresse IP interne
- numéro d'accès interne
- adresse externe
- numéro d'accès externe
- adresse IP interne de boîtier de médiation
- numéro d'accès interne de boîtier de médiation
- adresse IP externe de boîtier de médiation
- numéro d'accès externe de boîtier de médiation
- versions d'adresse IP (non imprimé)
- service de boîtier de médiation (non imprimé)
- interface intérieure et extérieure (facultatif, non imprimé)

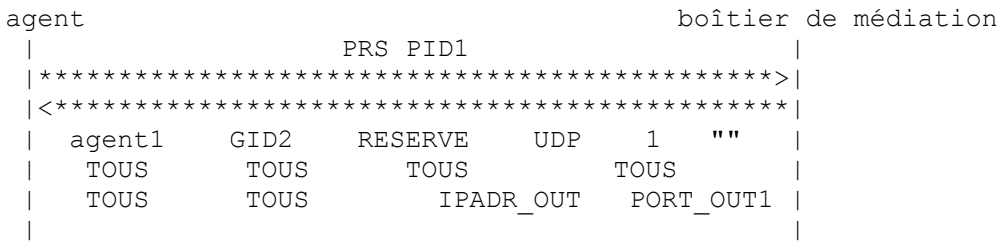


Figure 6 : Rapport d'état pour une réservation sortante

Le paramètre "TOUS" mentionné dans la Figure 6 est utilisé comme fourre-tout dans les réponses d'état de règle de politique pour les règles de réservation de politique. La règle de politique avec PID1 est une règle de réservation de politique pour le trafic UDP à l'extérieur du boîtier de médiation. Comme c'est une règle de réservation, la direction est vide. Comme il n'y a pas encore d'adresse interne ou externe impliquée, ces quatre champs sont remplacés par un caractère générique dans la réponse. Il en est de même pour l'adresse et numéro d'accès internes du boîtier de médiation. La seule information d'adresse données par la réponse est l'adresse IP réservée externe du boîtier de médiation (IPADR_OUT) et le numéro d'accès correspondant (PORT_OUT1). Noter que IPADR_OUT et PORT_OUT1 ne peuvent pas être remplacés par des caractères génériques, car l'action de réservation n'accepte pas cela.

L'application de PRS à PID2 (Figure 7) montre que la seconde règle de politique est une règle d'activation de politique pour les paquets UDP entrants. La destination interne est fixée concernant l'adresse IP, le protocole, et le numéro d'accès, mais pour la source externe, le numéro d'accès est remplacé par un caractère générique. L'adresse IP et le numéro d'accès externes du boîtier de médiation sont ce que l'envoyeur externe a besoin d'utiliser comme destination dans le paquet d'origine qu'il envoie. Au boîtier de médiation, l'adresse de destination est remplacée par l'adresse interne du receveur final. Durant la traduction d'adresse, l'adresse IP de source et les numéros d'accès de source des paquets restent inchangés. C'est indiqué par l'adresse interne, qui est identique à l'adresse externe.

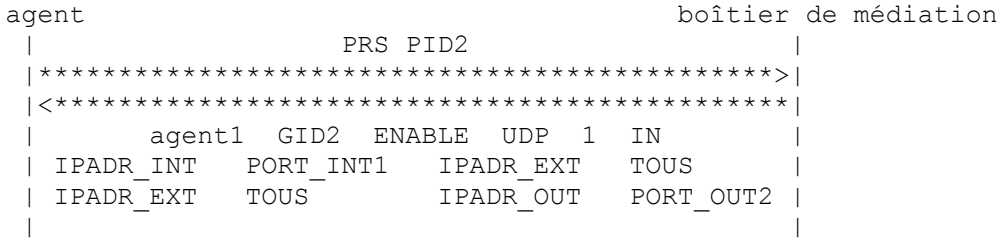


Figure 7 : Rapport d'état pour paquets entrants activé

Pour les NAT traditionnels, l'identité de l'adresse IP et numéro d'accès internes avec l'adresse IP et numéro d'accès externes tient toujours (A1=A3 dans la Figure 3). Pour un pur pare-feu, l'adresse IP et numéro d'accès externes sont toujours identiques à l'adresse IP et numéro d'accès internes (A0=A2 dans la Figure 3).

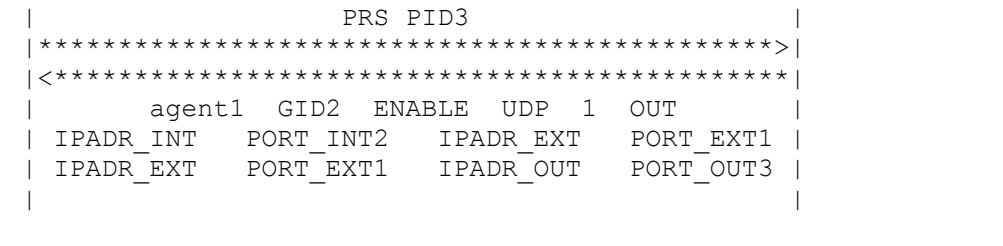


Figure 8 : Rapport d'état pour paquets sortants activé

La Figure 8 montre une communication UDP sortante activée entre les mêmes hôtes. Ici tous les numéros d'accès sont connus. Comme là encore, A1=A3, l'envoyeur interne utilise l'adresse IP et numéro d'accès externes comme destination dans les paquets d'origine. Au pare-feu, l'adresse IP et numéro d'accès internes de source sont remplacés par l'adresse IP et numéro d'accès externes montrés du boîtier de médiation.

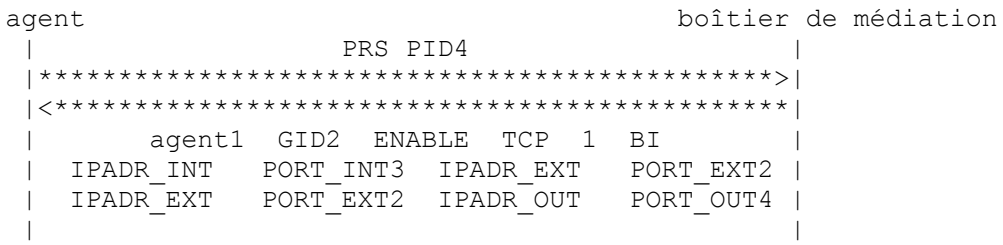
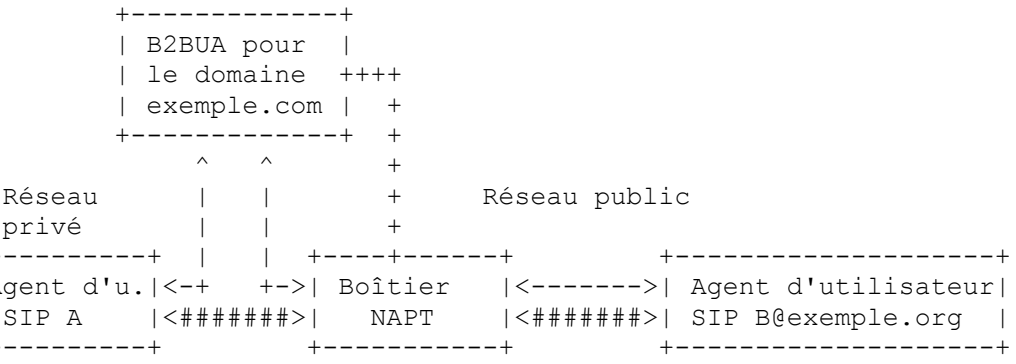


Figure 9 : Rapport d'état pour trafic TCP bidirectionnel

Finalement, la Figure 9 montre le rapport d'état pour le trafic bidirectional TCP activé. Noter que, là encore, A1=A3. Pour les paquets sortants, seuls l'adresse IP et les numéros d'accès de source sont remplacés au boîtier de médiation, et pour les paquets entrants, seuls l'adresse IP et les numéros d'accès de destination sont remplacés.

4.2 Activation d'un appel signalé SIP

Cet exemple d'usage de transaction élaboré montre l'interaction entre un agent d'utilisateur de boucle locale (B2BUA, *back-to-back user agent*) et un boîtier de médiation. Le boîtier de médiation lui-même est un traducteur traditionnel d'adresse et d'accès réseau (NAPT, *Network Address and Port Translator*) et deux agents d'utilisateur SIP communiquent ensemble via le B2BUA et un NAPT, comme le montre la Figure 10. L'agent MIDCOM est colocalisé avec le B2BUA, et le serveur MIDCOM est au boîtier de médiation. Donc, le protocole MIDCOM fonctionne entre le B2BUA et le boîtier de médiation.



<--> signalisation SIP
<##> trafic RTP
++++ protocole MIDCOM

Figure 10 : Exemple d'un scénario SIP

Pour les séquences de messages ci-dessous, on fait les hypothèses suivantes :
- Le NAPT est configuré statiquement à transmettre la signalisation SIP provenant de l'extérieur au B2BUA ; c'est-à-dire, le trafic à l'adresse IP et l'accès 5060 externes du NAPT est transmis au B2BUA interne.
- L'agent d'utilisateur SIP A, situé à l'intérieur du réseau privé, est enregistré au B2BUA avec son adresse IP privée.
- L'utilisateur A connaît l'URL général SIP pour l'utilisateur B. L'URL est B@exemple.org. Cependant, l'URL concret de l'agent d'utilisateur SIP B, qu'utilise actuellement d'utilisateur B, n'est pas connu.
- Les chemins RTP sont configurés, mais pas les chemins du protocole de commande RTP (RTCP).
- Le boîtier de médiation et le B2BUA partagent une session MIDCOM établie.
- Certains paramètres sont omis, comme l'identifiant de demande (RID).

De plus, on utilise les abréviations suivantes :
- IP_AI : adresse IP interne de l'agent d'utilisateur A
- P_AI : numéro d'accès interne de l'agent d'utilisateur A pour recevoir les données RTP
- P_AE : numéro d'accès transposé externe de l'agent d'utilisateur A
- IP_AE : adresse IP externe du boîtier de médiation
- IP_B : adresse IP de l'agent d'utilisateur B
- P_B : numéro d'accès de l'agent d'utilisateur B pour recevoir des données RTP
- GID : identifiant de groupe
- PID : identifiant de règle de politique

Les abréviations des transactions MIDCOM se trouvent dans les titres des paragraphes particuliers.

Dans notre exemple, l'utilisateur A essaye d'appeler l'utilisateur B. L'agent d'utilisateur A envoie un message SIP INVITE au B2BUA (voir la Figure 10). La partie SDP du message SIP particulier pertinente pour la configuration du boîtier de médiation est montrée dans les séquences de messages comme suit :

```
SDP: m=..P_AI..
   c=IP_AI
```

où l'étiquette m est l'étiquette de supports qui contient le numéro d'accès UDP receveur, et l'étiquette c contient l'adresse IP du terminal qui reçoit le flux de supports.

Le message INVITE transmis à l'agent d'utilisateur B doit contenir une adresse IP et un numéro d'accès publics auxquels l'agent d'utilisateur B peut envoyer son flux de supports RTP. Le B2BUA demande une règle d'activation de politique au boîtier de médiation avec une demande PER avec l'adresse IP et le numéro d'accès munis d'un caractère générique, de l'agent d'utilisateur B. Comme ni l'adresse IP ni les numéros d'accès de l'agent d'utilisateur B ne sont connus à ce moment, l'adresse de l'agent d'utilisateur B doit être remplacée par des caractères génériques. L'adresse IP et les numéros d'accès remplacés par des caractères génériques permettent la capacité "support précoce" mais résulte en une certaine insécurité, car tout hôte externe peut atteindre l'agent d'utilisateur A sur le numéro d'accès activé à travers le boîtier de médiation.

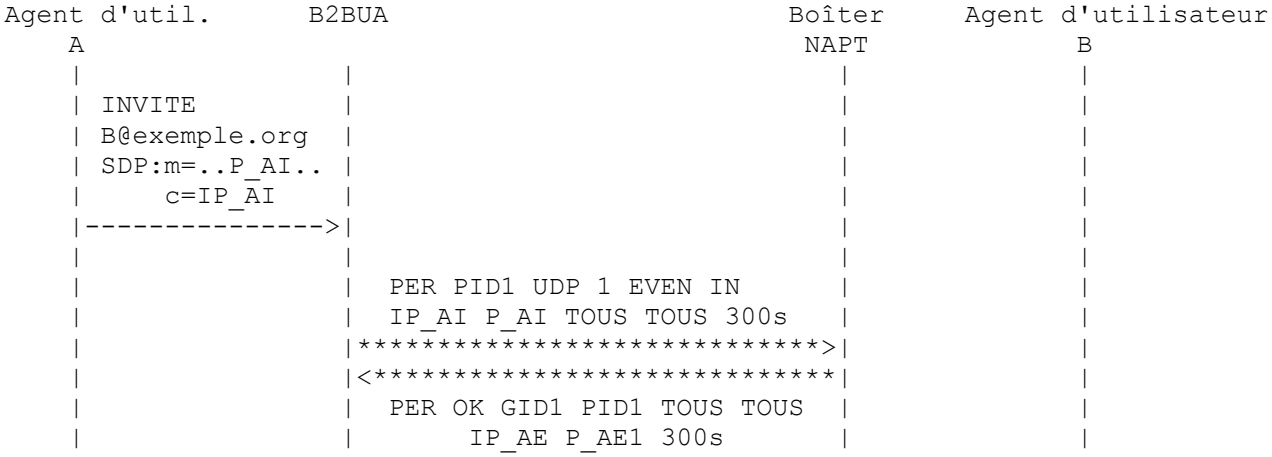


Figure 11 : PER avec adresse et numéro d'accès à caractères génériques

Une réponse PER de succès, comme montré à la Figure 11, résulte en un lien de NAT au boîtier de médiation. Ce lien permet au trafic UDP provenant de tout hôte extrérieur au réseau privé de l'agent d'utilisateur A d'atteindre l'agent d'utilisateur A. Donc l'agent d'utilisateur B pourrait commencer à envoyer du trafic immédiatement après la réception du message INVITE, comme le pourrait tout autre hôte -- même des hôtes dont la participation n'est pas prévue, comme des hôtes malveillants.

Si le boîtier de médiation ne prend pas en charge ou ne permet pas les adresses IP avec caractères génériques pour des raisons de sécurité, la demande PER va être rejetée avec une cause d'échec appropriée, comme "caractères génériques IP non pris en charge". Néanmoins, le B2BUA a besoin d'une adresse IP et numéro d'accès externes au boîtier de médiation (le NAPT) afin de transmettre le message SIP INVITE.

Si l'adresse IP de l'agent d'utilisateur B est encore inconnue (elle va être envoyée par agent d'utilisateur B dans le message de réponse SIP) et si une adresse IP avec caractères génériques n'est pas permise, le B2BUA utilise la transaction PRR.

En utilisant la demande PRR, le B2BUA demande une adresse IP et numéro d'accès externes (voir la Figure 12) sans établir déjà un lien ou orifice de NAT. La demande PRR contient le paramètre de service "tw" -- c'est-à-dire, l'agent MIDCOM choisit la valeur par défaut. Dans cette configuration, avec NAPT et sans double NAT, seule une adresse externe est réservée. Dans la charge utile SDP du message INVITE, le B2BUA remplace l'adresse IP et le numéro d'accès de l'agent d'utilisateur A par l'adresse IP et accès réservés provenant de la réponse PRR (voir la Figure 12). Le message SIP INVITE est transmis à l'agent d'utilisateur B avec un corps SIP modifié contenant l'adresse et le numéro d'accès externes, auxquels l'agent d'utilisateur B va envoyer ses flux de supports RTP.

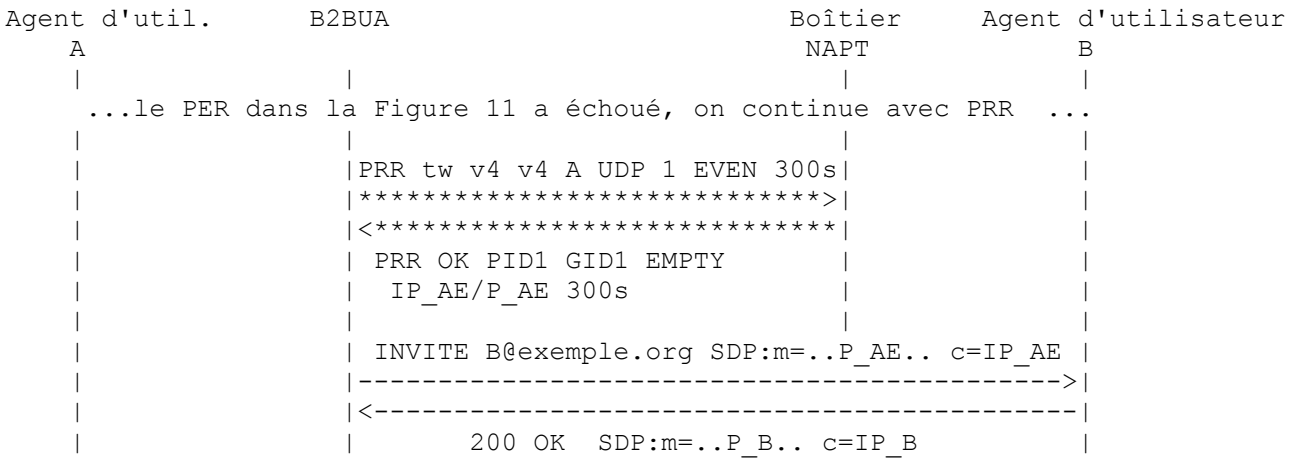


Figure 12 : Réservation d'adresse avec la transaction PRR

Cette réponse SIP "200 OK" contient l'adresse IP et le numéro d'accès auxquels l'agent d'utilisateur B va recevoir un flux de supports. L'adresse IP est supposée être égale à l'adresse IP d'où l'agent d'utilisateur B va envoyer ses flux de supports.

Maintenant, le B2BUA a des informations suffisantes pour établir le lien de NAT complet avec une transaction de règle d'activation de politique (PER) ; c'est-à-dire, les données UDP/RTP de l'appel peuvent s'écouler de l'agent d'utilisateur B à l'agent d'utilisateur A. La transaction PER fait référence à la réservation en passant le PID de la PRR (PID1).

Pour la direction opposée, les données UDP/RTP provenant de l'agent d'utilisateur A à B doivent aussi être activées. C'est fait par une seconde transaction PER avec tous les paramètres nécessaires (voir la Figure 13). Le message de demande contient l'identifiant de groupe (GID1) que le boîtier de médiation a alloué dans la première transaction PER. Donc, les deux règles de politique sont devenues membres du même groupe. Après avoir activé les deux flux UDP/RTP, le B2BUA peut transmettre le message "200 OK" SIP à l'agent d'utilisateur A pour indiquer que l'appel téléphonique peut commencer.

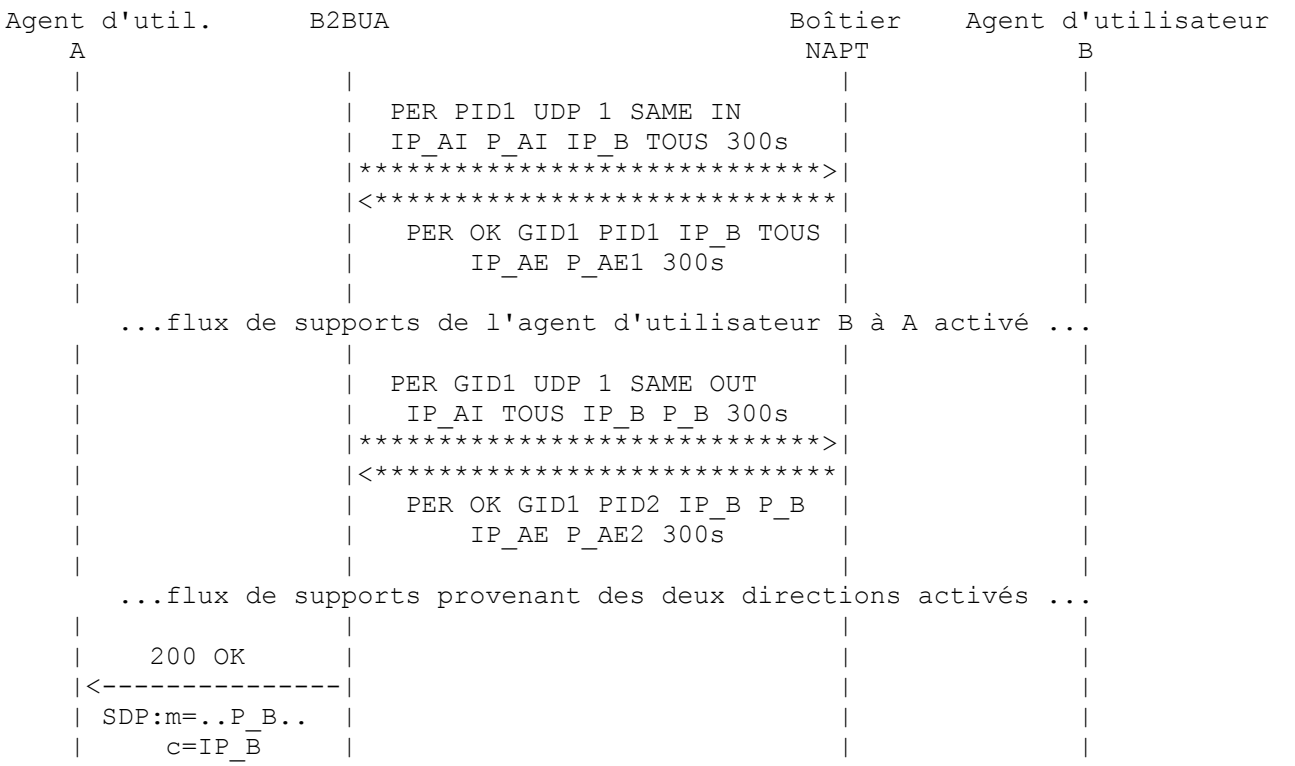
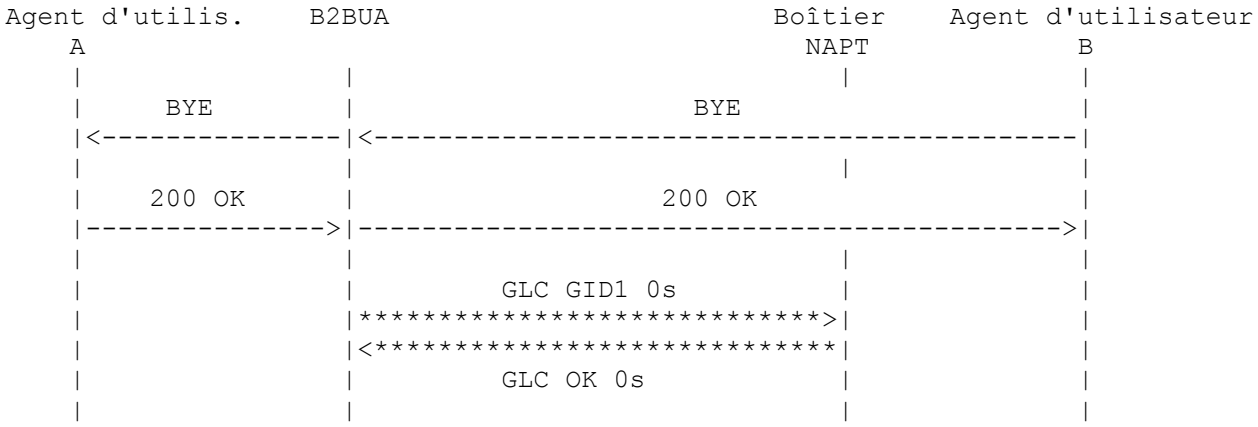


Figure 13 : Établissement de règle de politique pour les flux UDP

L'agent d'utilisateur B décide de terminer l'appel et envoie son message "BYE" SIP à l'agent d'utilisateur A. Le B2BUA transmet les messages SIP et termine ensuite le groupe, en utilisant une transaction Changement de durée de vie de groupe

(GLC) avec une durée de vie restante demandée de 0 seconde (voir la Figure 14). La terminaison du groupe inclut de terminer toutes les règles de politique membres.



...les deux liens de NAT pour les flux de supports sont supprimés...

Figure 14 : Terminaison des groupes de règles de politique

5. Conformité aux exigences de MIDCOM

Cette Section explique la conformité de la sémantique spécifiée aux exigences MIDCOM. Elle est structurée en accord avec la [RFC3304] :
- Conformité aux exigences de machinerie de protocole (paragraphe 5.1)
- Conformité aux exigences de sémantique du protocole (paragraphe 5.2)
- Conformité aux exigences de sécurité (paragraphe 5.3)

On se réfère aux exigences par le numéro du paragraphe dans lequel elles sont définies : "l'exigence x.y.z" se réfère à l'exigence spécifiée au paragraphe x.y.z de la [RFC3304].

5.1 Exigences de la machinerie du protocole

5.1.1 Association autorisée

La sémantique spécifiée permet à un agent MIDCOM d'établir une association autorisée entre lui et le boîtier de médiation. L'agent s'identifie par le mécanisme d'authentification de la transaction Établissement de session décrite au paragraphe 2.2.1. Sur la base de cette authentification, le boîtier de médiation peut déterminer si il va ou non être permis à l'agent de demander un service. Donc, l'exigence 2.1.1 est satisfaite.

5.1.2 Agent connecté à plusieurs boîtiers de médiation

Comme spécifié au paragraphe 2.2, le protocole MIDCOM permet à l'agent de communiquer avec plus d'un boîtier de médiation simultanément. Le choix d'un mécanisme pour séparer les différentes sessions est laissé à la définition concrète de protocole. Il doit fournir une transposition claire des messages de protocole en sessions ouvertes. Alors l'exigence 2.1.2 est satisfaite.

5.1.3 Plusieurs agents connectés au même boîtier de médiation

Comme spécifié au paragraphe 2.2, le protocole MIDCOM permet au boîtier de médiation de communiquer avec plus d'un agent simultanément. Le choix d'un mécanisme pour séparer les différentes sessions est laissé à la définition concrète de protocole. Il doit fournir une transposition claire des messages de protocole en sessions ouvertes. Alors l'exigence 2.1.3 est satisfaite.

5.1.4 Comportement déterministe

Le paragraphe 2.1.2 déclare que le traitement d'une demande d'un agent ne peut pas être interrompu par une demande du même agent ou d'un autre. Cela assure l'atomicité parmi les transactions de demande et évite des conditions de conflit résultant en un comportement imprévisible du boîtier de médiation.

Le comportement du boîtier de médiation peut seulement être prévisible du point de vue de ses administrateurs. Du point de vue d'un agent, le comportement du boîtier de médiation est imprévisible, car l'administrateur peut, par exemple, modifier l'autorisation de l'agent à tout moment sans que l'agent soit capable d'observer ce changement. Par conséquent, le comportement du boîtier de médiation n'est pas nécessairement déterministe du point de vue d'un agent.

Comme la prévisibilité du comportement du boîtier de médiation est donnée à son administrateur, l'exigence 2.1.4 est satisfaite.

5.1.5 État connu et stable

Le paragraphe 2.1 déclare que les transactions de demande sont atomiques par rapport à chaque autre et du point de vue d'un agent. Toutes les transactions sont clairement définies comme des transitions d'état qui soit quittent l'état courant stable, bien défini, et entrent dans un nouvel état stable, bien défini, soit restent dans l'état courant stable, bien défini. Le paragraphe 2.1 demande clairement que les états intermédiaires ne soient pas stables et ne soient pas rapportés à un agent.

De plus, pour chaque transition d'état un message est envoyé à l'agent correspondant, soit une réponse, soit une notification. L'agent peut transposer de façon univoque chaque réponse en une des demandes qu'il a envoyées au boîtier de médiation, parce que des identifiants de demande uniques par agent sont utilisés à cette fin. Les notifications sont auto explicatives par leur définition.

De plus, les transactions Liste de groupe (paragraphe 2.4.3) État de groupe (paragraphe 2.4.4) Liste de règle de politique (paragraphe 2.3.11) et État de règle de politique (paragraphe 2.3.12) permettent à l'agent de restituer à tout moment durant une session des informations sur :
- tous les groupes de règles de politique auxquels il peut accéder,
- l'état et les règles de politique membres de tous les groupes accessibles,
- toutes les règles de politique auxquelles il peut accéder, et
- l'état de toutes les règles de politique accessibles.

Donc, l'agent est précisément informé de l'état du boîtier de médiation (pour autant que les services demandés par l'agent sont affectés) et l'exigence 2.1.5 est satisfaite.

5.1.6 Rapport d'état

Comme expliqué au paragraphe précédent, le boîtier de médiation informe sans ambiguïté l'agent de toute transition d'état relative à tout service demandé par l'agent. Aussi, à tout moment l'agent peut restituer toutes les informations d'état sur toutes les règles de politique et groupes de règles de politique accessibles. Donc, l'exigence 2.1.6 est satisfaite.

5.1.7 Messages non sollicités (notifications asynchrones)

La sémantique inclut des messages de notification asynchrone du boîtier de médiation à l'agent, incluant le message Notification de terminaison de session (STN, *Session Termination Notification*) le message Notification d'événement de règle de politique (REN, *Policy Rule Event Notification*) et le message Notification d'événement de groupe (GEN, *Group Event Notification*) (voir au paragraphe 2.1.2). Ces notifications rapportent tout changement d'état de règles de politique ou groupes de règles de politique qui n'a pas été explicitement demandé par l'agent. Donc, l'exigence 2.1.7 est satisfaite par la sémantique spécifiée ci-dessus.

5.1.8 Authentification mutuelle

Comme spécifié au paragraphe 2.2.1, la sémantique exige l'authentification mutuelle de l'agent et du boîtier de médiation, en utilisant soit deux transactions successives d'établissement de session soit l'authentification mutuelle fournie sur une couche de protocole inférieure. Donc, l'exigence 2.1.8 est satisfaite.

5.1.9 Terminaison de session par une partie

La spécification de sémantique déclare au paragraphe 2.2.2 que l'agent peut demander la terminaison de la session en générant la demande Terminaison de session et que le boîtier de médiation ne peut pas rejeter cette demande. Le paragraphe 2.2.3 déclare ensuite que le boîtier de médiation peut envoyer la notification Terminaison de session asynchrone à tout moment et terminer ensuite la session. Donc, l'exigence 2.1.9 est satisfaite.

5.1.10 Résultat de demande

Le paragraphe 2.1 déclare que chaque demande d'un agent est suivie par une réponse du boîtier de médiation qui indique le succès ou l'échec. Donc, l'exigence 2.2.10 est satisfaite.

5.1.11 Interfonctionnement de version

Le paragraphe 2.2.1 déclare que l'agent doit spécifier le numéro de version du protocole qu'il va utiliser durant la session. Le boîtier de médiation peut accepter cela et agir en accord avec cette version du protocole ou peut rejeter la session si il ne prend pas cette version en charge. Si l'établissement de session est rejeté, l'agent peut essayer à nouveau avec une autre version. Donc, l'exigence 2.2.11 est satisfaite.

5.1.12 Traitement déterministe de chevauchement de règles

Les seules actions de règle de politique spécifiées sont "réservé" et "activé". Pour les pare-feu, le chevauchement des actions d'activation ou de réservation ne crée aucun conflit, donc un pare-feu va toujours accepter les règles qui se chevauchent comme spécifié au paragraphe 2.3.2 (en supposant que l'autorisation requise soit donnée).

Pour les NAT, réservation et activation peuvent entrer en conflit. Si une demande contraire arrive, elle est rejetée, comme déclaré au paragraphe 2.3.2. Si une demande en chevauchement arrive sans être en conflit avec celles qu'elle chevauche, elle est acceptée (en supposant que l'autorisation requise soit donnée).

Donc, le comportement du boîtier de médiation en présence de règles qui se chevauchent peut être prédit de façon déterministe, et l'exigence 2.1.12 est satisfaite.

5.2 Exigence de la sémantique de protocole

5.2.1 Syntaxe et sémantique extensibles

L'exigence 2.2.1 demande explicitement l'extensibilité de la syntaxe de protocole. Cela doit être traité par la définition concrète de protocole. La spécification de sémantique est de toutes façons extensible, parce que de nouvelles transactions peuvent être ajoutées.

5.2.2 Règles de politique pour différents types de boîtiers de médiation

Le paragraphe 2.3 explique que la sémantique utilise des transactions identiques pour tous les types de boîtier de médiation et que la même règle de politique peut être appliquée à tous. Donc, l'exigence 2.2.2 est satisfaite.

5.2.3 Groupes d'ensemble de politique

La sémantique prend explicitement en charge le groupement de règles de politique et transactions en groupes de règles de politique, comme décrit au paragraphe 2.4. Les transactions de groupe peuvent être utilisées pour l'extension de la durée de vie et la termination de toutes les règles de politique qui sont membres du groupe particulier. Donc, l'exigence 2.2.3 est satisfaite.

5.2.4 Extension de durée de vie de règle de politique

La sémantique inclut une transaction pour l'extension explicite de la durée de vie des règles de politique, comme décrit au paragraphe 2.3.3. Donc, l'exigence 2.2.4 est satisfaite.

5.2.5 Modes de défaillance robustes

Les transitions d'état au boîtier de médiation sont clairement spécifiées et communiquées à l'agent. Il n'y a pas d'état intermédiaire atteint par un traitement partiel d'une demande. Toutes les demandes sont toujours traitées complètement, avec succès ou sans succès. Toutes les transactions de demande incluent une liste des raisons de défaillance. Ces raisons de défaillance couvrent l'indication des paramètres invalides lorsque applicable. En cas d'échec, une des raisons spécifiées est retournée du boîtier de médiation à l'agent. Donc, l'exigence 2.2.5 est satisfaite.

5.2.6 Causes de défaillance

La sémantique inclut un paramètre Cause d'échec dans chaque réponse d'échec. Donc, l'exigence 2.2.6 est satisfaite.

5.2.7 Plusieurs agents manipulent la même règle de politique

Comme spécifié aux paragraphes 2.3 et 2.4, chaque règle de politique et groupe de règles de politique installé a un possesseur, qui est l'agent authentifié créateur de la règle de politique ou du groupe, respectivement. L'identité authentifiée est entrée pour autoriser l'accès aux règles de politique et groupes.

Si le boîtier de médiation est suffisamment configurable, son administrateur peut le configurer à ce que un agent authentifié soit autorisé à accéder et modifier les règles de politique et groupes possédés par un autre agent. Parce que la sémantique spécifiée n'empêche pas cela, elle satisfait à l'exigence 2.2.7.

5.2.8 Portage des règles de filtrage

La transaction Règle d'activation de politique spécifiée au paragrape 2.3.8 peut porter des quintuples règles de filtrage. Cela satisfait l'exigence 2.2.8.

5.2.9 Parité des numéros d'accès

Comme spécifié au paragraphe 2.3.6, l'agent est capable de demander que soit gardée la parité d'accès quand il réserve des numéros d'accès avec la transaction PRR (voir au paragraphe 2.3.8) et quand il établt des liens d'adresses avec la transaction PER (voir au paragraphe 2.3.9). Donc, l'exigence 2.2.9 est satisfaite.

5.2.10 Gammes consécutives de numéros d'accès

Comme spécifié au paragraphe 2.3.6, l'agent est capable de demander une gamme consécutive de numéros d'accès quand il réserve des numéros d'accès avec la transaction PRR (voir au paragraphe 2.3.8) et quand il établit des liens d'adresses ou des orifices d'accès avec la transaction PER (voir au paragraphe 2.3.9). Donc, l'exigence 2.2.10 est satisfaite.

5.2.11 Règles de politiques en chevauchement contradictoires

L'exigence 2.2.11 se fonde sur l'hypothèse que les actions contradictoires de règle de politique, comme "activer"/"permettre" et "désactiver"/"interdire", sont acceptées. En conformité avec les décisions prises par le groupe de travail après la finalisation du document des exigences, cette exigence n'est pas satisfaite par la sémantique parce que aucune action "désactiver"/"interdire" n'est prise en charge.

5.3 Exigences pour la sécurité

5.3.1 Authentification, confidentialité, intégrité

La définition de sémantique prend en charge l'authentification mutuelle d'un agent et d'un boîtier de médiation dans la transaction Établissement de session (paragraphe 2.2.1). L'utilisation d'un protocole sous-jacent tel que TLS ou IPsec est obligatoire. Donc, l'exigence 2.3.1 est satisfaite.

5.3.2 Confidentialité facultative des messages de contrôle

L'utilisation de IPsec ou TLS permet à un agent et un boîtier de médiation d'utiliser une méthode de chiffrement (incluant pas de chiffrement). Donc, l'exigence 2.3.2 est satisfaite.

5.3.3 Fonctionnement sur des domaines non de confiance

Le fonctionnement sur des domaines non de confiance est pris en charge par l'authentification mutuelle et par l'utilisation de la protection par TLS ou IPsec. Donc, l'exigence 2.3.3 est satisfaite.

5.3.4 Atténuation des attaques en répétition

La sémantique spécifiée atténue les attaques en répétition et satisfait l'exigence 2.3.4 en exigeant l'authentification mutuelle d'un agent et d'un boîtier de médiation, et en rendant obligatoire l'utilisation de la protection par TLS ou IPsec.

Une atténuation plus forte peut être fournie au titre d'une définition concrète de protocole MIDCOM -- par exemple, en exigeant des numéros consécutivement croissants pour les identifiants de demande.

6. Considérations sur la sécurité

L'interaction entre un boîtier de médiation et un agent (voir la [RFC3303]) est un point très sensible à l'égard de la sécurité. La configuration des règles de politique à partir d'une entité extérieure à un boîtier de médiation paraît contraire à la nature d'un boîtier de médiation. Donc, des moyens efficaces doivent être utilisés pour assurer :
- l'authentification mutuelle entre l'agent et un boîtier de médiation,
- l'autorisation,
- l'intégrité du message , et
- la confidentialité du message.

La sémantique définit un mécanisme pour assurer l'authentification mutuelle entre un agent et un boîtier de médiation (voir au paragraphe 2.2.1). En combinaison avec l'authentification, le boîtier de médiation est capable de décider si un agent est autorisé à demandr une action au boîtier de médiation. La sémantique s'appuie sur les protocoles sous-jacents, tels que TLS ou IPsec, pour maintenir l'intégrité de message et la confidentialité des données transférées entre les deux entités.

Pour l'usage de TLS et IPsec, les deux côtés doivent utiliser des accréditifs configurés de façon sûre pour l'authentification et l'autorisation.

La configuration de règles de politique avec des adresses IP et numéros d'accès munis de caractères génériques résulte en certains risques, comme d'ouvrir exagérément les règles de politique avec caractère générique. Une règle de politique excessivement munie de caractères générique serait A0 et A3 avec l'adresse IP réglée à "toute" adresse IP, par exemple. Ce type d'orifice d'accès rendrait le boîtier de médiation, au sens de la sécurité, sans usage, car tout paquet pourrait traverser le boîtier de médiation sans autre vérification. La politique locale du boîtier de médiation devrait rejeter de telles demandes d'activation de règle de politique.

Une configuration par défaut raisonnable pour l'utilisation de caractères génériques serait qu'un seul numéro d'accès puisse être muni d'un caractère générique et que toutes les adresses IP doivent être réglées sans caractère générique. Cependant, il y a des cas où la sécurité doit être mise en balance avec la fonctionnalité.

L'exemple décrit au paragraphe 4.2 montre comment les appels signalés par SIP peuvent être servis de façon sûre sans mettre de caractères génériques dans les adresses IP. Mais certaines applications signalées par SIP utilisent des supports précoces (voir au paragraphe 5.5 de la [RFC3398]). Pour recevoir des supports précoces, les boîtiers de médiation doivent être configurés avant que le second participant à une session soit connu. Comme elle n'est pas connue, l'adresse IP du second participant a besoin d'être munie de caractères génériques.

Dans de tels cas et plusieurs autres similaires, c'est une décision de politique de sécurité à prendre par l'opérateur du boîtier de médiation. L'opérateur peut configurer le boîtier de médiation de telle façon qu'il prenne en charge plus d'une fonction, par exemple, en permettant de munir les adresses IP de caractères génériques, ou pour que le fonctionnement du réseau soit plus sûr, par exemple, en interdisant de mettre des caractères génériques dans les adresses IP.

7. Considérations de l'IAB sur UNSAF

L'auto correction d'adressage unilatérale (UNSAF, *UNilateral Self-Address Fixing*) est décrite dans la [RFC3424] comme un processus aux points d'extrémité d'origine qui tentent de déterminer ou corriger l'adresse (et l'accès) par lequel ils sont connus par un autre point d'extrémité. Les propositions d'UNSAF, comme la simple traversée de NAT par le protocole UDP (STUN, *Simple Traversal of the UDP Protocol through NAT*) [RFC3489], sont considérées comme une classe générale de substituts pour la traversée de NAT et comme des solutions pour les scénarios sans communication à travers un boîtier de médiation (MIDCOM).

Le présent document décrit la sémantique du protocole pour une telle solution de communication à travers un boîtier de médiation (MIDCOM). MIDCOM n'est pas destiné à être un substitut à court terme, mais plus comme une solution à long terme pour la communication à travers un boîtier de médiation. Dans MIDCOM, les points d'extrémité ne sont pas impliqués dans l'allocation, la maintenance, et la suppression des adresses et accès au boîtier de médiation. Le plein contrôle des adresses et accès au boîtier de médiation est situé au serveur MIDCOM.

Donc, le présent document répond aux considérations sur UNSAF de la [RFC3424] en proposant une solution de remplacement à long terme.

8. Remerciements

Nous tenons à remercier toutes les personnes qui ont contribué sur la liste de diffusion à la discussion sur la sémantique par un grand nombre de précieux commentaires.

9. Références

9.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

9.2 Références pour information

[RFC2663] P. Srisuresh, M. Holdrege, "Terminologie et considérations sur les traducteurs d'adresse réseau IP (NAT)", août 1999. *(Information)*

[RFC3022] P. Srisuresh, K. Egevang, "Traducteur d'adresse réseau IP traditionnel", janvier 2001. *(Information)*

[RFC3198] A. Westerinen et autres, "Terminologie pour la gestion fondée sur la politique", novembre 2001. *(Information)*

[RFC3261] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", juin 2002. (*Mise à jour par* 3265, 3853, 4320, 4916, 5393, 6665, 8217, 8760)

[RFC3303] P. Srisuresh et autres, "Architecture et cadre de communication par boîtier de médiation", août 2002. *(Information)*

[RFC3304] R. P. Swale et autres, "Exigences du protocole de communications par boîtier de médiation (midcom)", août 2002. *(Info.)*

[RFC3398] G. Camarillo et autres, "Transposition du SSU RNIS en SIP", décembre 2002. *(P.S.)*

[RFC3424] L. Daigle, éd., IAB, "Considérations de l'IAB sur l'auto correction d'adressage unilatérale (UNSAF) à travers la traduction d'adresse réseau", novembre 2002. *(Information)*

[RFC3489] J. Rosenberg et autres, "STUN - Simple traversée par le protocole de datagramme d'utilisateur (UDP) des traducteurs d'adresse réseau (NAT)", mars 2003. (*Obsolète, voir* RFC5389) *(P.S.)*

[RFC3989] M. Stiemerling et autres, "Sémantique du protocole de communications par boîtier de médiation (MIDCOM)", février 2005. (*Obsolète, voir* RFC5189) *(Information)*

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

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

[RFC4346] T. Dierks et E. Rescorla, "Protocole de sécurité de la couche Transport (TLS) version 1.1", avril 2006. *(Remplace* RFC2246 *; Remplacée par* RFC5246 *; MàJ par* RFC4366, 4680, 4681, 5746, 6176, 7465, 7507, 7919)

Appendice A. Changements par rapport à la RFC 3989

1. L'exemple du paragraphe 4.2 utilisait un serveur mandataire SIP qui modifiait le corps d'un message SIP. C'est une violation de la RFC 3261. Cela a été corrigé en remplaçant le serveur mandataire SIP par un agent d'utilisateur de bout en bout.

2. On a ajouté des précisions sur l'ensemble utilisé de types de transaction.

3. Au paragraphe 3.1, "Conformité générale de mise en œuvre ", on utilise maintenant les mots clés de la RFC 2119.

4. Des changements rédactionnels mineurs ont été faits et les références ont été mises à jour.

Adresse des auteurs

Martin Stiemerling
NEC Europe Ltd.
Kurfuersten-Anlage 36
69115 Heidelberg
Germany
téléphone : +49 6221 4342-113
mél : stiemerling@nw.neclab.eu

Juergen Quittek
NEC Europe Ltd.
Kurfuersten-Anlage 36
69115 Heidelberg
Germany
téléphone : +49 6221 4342-115
mél : quittek@nw.neclab.eu

Tom Taylor
Nortel
1852 Lorraine Ave.
Ottawa, Ontario
Canada K1H 6Z8
téléphone : +1 613 763 1496
mél : tom.taylor@rogers.com

Déclaration complète de droits de reproduction