Groupe de travail RéseauRequest for Comments : 3989
Catégorie : Informational

M. Stiemerling, J. Quittek
NEC
T. Taylor
Nortel
février 2005

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

Statut du présent Mémo

Le présent mémo définit un protocole expérimental pour la communauté Internet. Il ne spécifie en aucune façon une norme Internet. Il réclame une discussion et des suggestions pour son amélioration. La distribution de ce mémo n'est pas limitée.

Notice de copyright

Résumé

Le présent mémo spécifie la sémantique pour 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-feux et les traducteurs d'adresse réseau (NAT, *Network Address Translators*). La discussion sémantique n'inclut aucune spécification d'une syntaxe concrète ou d'un protocole de transport. Cependant, on s'attend à ce qu'un protocole concret mette en œuvre la sémantique spécifiée, ou plus vraisemblablement un sur ensemble de cette sémantique. La sémantique du protocole MIDCOM est déduite des exigences MIDCOM, de la trame MIDCOM, et des décisions du groupe de travail.

Table des matières

1 Introduction

Le groupe de travail MIDCOM a défini un cadre de travail [MDC-FRM] et une liste d'exigences [MDC-REQ] pour les communications par boîtier de médiation. La prochaine étape sur le chemin d'un protocole MIDCOM est la spécification de la sémantique de protocole qui est contrainte, mais pas entièrement impliquée, par les documents mentionnés ci-dessus.

Le présent mémo suggère une sémantique pour le protocole MIDCOM. Elle est pleinement conforme aux exigences énumérées dans [MDC-REQ] et il y a consensus du groupe de travail sur les questions de sémantique.

Conformément à la charte du groupe de travail, la description de la sémantique est ciblée sur les filtres de paquets et les traducteurs d'adresse réseau (NAT), et elle prend en charge des applications qui exigent une configuration dynamique de ces middleboxes.

La sémantique est définie en termes de transactions. Deux types de base de transactions sont utilisés : transactions de demande-réponse et transactions asynchrones. Pour chaque transaction, la sémantique est spécifiée en dérivant (1) les paramètres de la transaction, (2) le traitement des messages de demande au boîtier de médiation, et (3) les transitions d'état au boîtier de médiation causées par les transactions de demande ou indiquées par les transactions asynchrones, respectivement, et (4) les messages de réponse et de notification envoyés du boîtier de médiation à l'agent afin de l'informer du changement d'état.

La sémantique peut être mise en oeuvre par tout protocole qui prend en charge ces deux types de transaction et qui est suffisamment flexible pour ce qui concerne les paramètres de transaction. Différentes mises en oeuvre pour différents protocoles peuvent nécessiter l'extension de la sémantique décrite ci-dessous par l'ajout de transactions ultérieures et/ou par l'ajout d'autres paramètres aux transactions et/ou en divisant une seule transactions en un ensemble de transactions. Indépendamment de telles extensions, la sémantique ci-dessous donne le sous-ensemble minimum nécessaire de ce qui doit être mis en oeuvre.

Le reste du présent document est structuré comme suit. La Section 2 décrit la sémantique du protocole. Elle est structurée en quatre paragraphes :

- Questions générales 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 oeuvre de protocole MIDCOM par rapport à la sémantique définie à la section 2. La Section 4 donne deux exemples d'utilisation élaborés. Enfin, la Section 5 explique comment la sémantique satisfait aux exigences de MIDCOM.

1.1 Terminologie

La terminologie du présent mémo suit les définitions données dans les documents cadre [MDC-FRM] et exigences [MDC-REQ].

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, au traitement du message au boîtier de médiation, au transfert du message de réponse du boîtier de médiation à l'agent, et au transfert facultatif des 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 qui contient 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 qui contient une demande d' informations d'état de la part du 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 de la part du boîtier de médiation aux agents qui participent à une session ouverte. Un message de notification est envoyé à chaque agent qui doit recevoir notification des événements asynchrones. Le message indique la transition d'état au boîtier de médiation.

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

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

règle de politique : en général, une règle de politique est "un bloc de base de construction d'un système fondé sur une politique. C'est la liaison d'un ensemble d'actions avec un ensemble de conditions – dans laquelle les conditions sont évaluées pour déterminer si les actions sont effectuées." [RFC3198]. Dans le contexte de MIDCOM la condition est une spécification d'un ensemble de paquets auquel les règles sont appliquées. L'ensemble des actions ne contient toujours qu'un seul élément par règle, soit l'action "reserve" *(réserver)* soit l'action "enable" *(activer).*

règle de réserve de politique : c'est une règle de politique qui contient une action de réserve. La condition de politique de cette règle est toujours vraie. L'action est la réservation de seulement une adresse IP ou d'une combinaison d'une adresse IP et d'une gamme de numéros de port sur, aucun côté, un côté, ou les deux côtés du boîtier de médiation, selon la configuration du boîtier de médiation.

règle d'activation de politique : c'est une règle de politique qui contient une action d'activation. La condition de politique consiste en un descripteur d'un ou plusieurs flux de paquets unidirectionnels ou bidirectionnels, et l'action de politique permet aux paquets qui appartiennent à ce flux de 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 de port.

Liaison de NAT : le terme de liaison de NAT tel qu'il est utilisé dans le présent document ne se réfère pas nécessairement à un lien de NAT comme défini dans [NAT-TERM]. Une liaison de NAT dans la sémantique MIDCOM se réfère à une abstraction qui permet la communication entre deux points de terminaison à travers le boîtier de médiation de type NAT. Une action d'activation peut avoir pour résultat un lien de NAT ou une session de NAT, selon la demande et ses paramètres.

1.2 Gabarit de définition de transaction

Dans les paragraphes suivants, la sémantique du protocole MIDCOM est spécifiée par transaction. Une spécification de transaction contient les entrées suivantes. Les entrées de paramètre cause d'échec et type de message de notification ne sont spécifiés que s'ils sont applicables.

Nom de transaction : nom descriptif de ce type de transaction.

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

Conformité de transaction : cette entrée contient soit 'obligatoire' soit 'facultatif'. Voir les détails 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 (succès) : cette entrée fait la liste de tous les paramètres renvoyés du boîtier de médiation à l'agent comme réponse positive à la demande antérieure. 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 à laquelle est envoyée la réponse et un paramètre indiquant la cause de l'échec. Comme ces paramètres sont obligatoires, ils ne figurent pas dans la liste du gabarit. Mais le gabarit contient une liste des causes d'échec potentielles qui peut être indiquée par le second paramètre. La liste n'est pas exhaustive. Une spécification concrète de protocole peut étendre la liste.

Type de message de notification : c'est le type du 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 au boîtier de médiation, et les transitions d'état au boîtier de médiation causées par la transaction, ou respectivement, causant la transaction.

2 Spécification de la sémantique

2.1 Conception générale du protocole

La spécification de la sémantique vise à un équilibre entre la prise en charge appropriée des applications qui requièrent 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 dans les transactions. L'état des boîtiers de médiation est décrit par les machines d'état. Les machines d'état sont définies par des états et des transitions d'état. Une seule transaction peut causer, ou être causée par des transitions d'état, dans plus d'une machine d'état, mais pour chaque machine d'état, il n'y a pas plus d'une transition par transaction.

2.1.1 Transactions du protocole

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

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

Une analyse des exigences a montré que quatre sortes de transactions sont nécessaires :
- Les transactions de configuration permettant à l'agent de demander des transitions d'état au boîtier de médiation.
- Les transaction asynchrones permettant au boîtier de médiation de changer d'état sans demande d'un agent.
- Les transactions de surveillance permettant à l'agent de demander des informations d'état au boîtier de médiation.
- Les transactions de confort qui combinent un ensemble de transactions de configuration.

Les transactions de configuration et les transactions asynchrones fournissent la fonctionnalité de protocole MIDCOM de base. Elles se rapportent aux transitions d'état du boîtier de médiation, et concernent l'établissement et la terminaison des sessions MIDCOM et des règles de politique.

Les transactions de surveillance ne se rapportent pas aux transitions d'état du 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.

Les transactions de confort simplifient les sessions MIDCOM en combinant un ensemble de transactions de configuration en une seule. Elles ne sont pas nécessaires pour le fonctionnement du protocole MIDCOM.

Comme spécifié en détail à la section 3, les transactions de configuration et les transactions asynchrones sont obligatoires. Elles doivent être mises en oeuvre par un boîtier de médiation conforme. Toutes les transactions de confort sont facultatives, et certaines des transactions de surveillance sont facultatives.

2.1.2 Types de message

Le protocole MIDCOM prend en charge trois sortes de messages : les messages de demande, les messages de réponse, et les 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 est laissé à 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, tant que les informations contenues dans les paramètres définis dans la sémantique sont toujours présents.
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.

Au cas d'échec de la 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 qui identifie la demande à laquelle la réponse est envoyée et un paramètre indiquant la cause de l'échec.

Il y a trois types de message de notification: la notification de fin 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 spécifique du boîtier de médiation.

STN : Le message de notification de fin de session contient en plus un seul paramètre qui indique la raison de la terminaison de session par le boîtier de médiation.

REN : Le message de notification 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 être regroupées en transactions concernant les sessions, en transactions concernant les règles de politique, et en transactions concernant les groupes de règles de politique. Les groupes de règles de politique peuvent être utilisés pour indiquer les relations entre les 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 état plein. Leurs états sont indépendants les uns des autres, et leurs machines d'état (une par session et une par règle de politique) peuvent être séparées. Les groupes de règles de politique sont aussi à état plein, mais le boîtier de médiation n'a pas besoin de maintenir l'état pour les groupes de règles de politique, parce que la sémantique a été choisie de telle sorte que l'état du 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 aussi bien que d'une mise en œuvre d'un protocole. Donc, la spécification de la sémantique est structurée en conséquence et on utilise deux machines d'état séparées pour illustrer la

sémantique. Prière de noter que les machines d'état conçues pour les protocoles et les mises en oeuvre concrets seront probablement plus complexes que les machines d'état présentées ici. Cependant, les machines d'état de protocole sont supposées dans le présent document être un sur ensemble des machines d'état de la sémantique.

2.1.4 Granularité

Toutes les transactions de demande sont insécables l'une par rapport à l'autre. Cela signifie que le traitement d'une demande au boîtier de médiation n'est jamais interrompu par une autre demande qui arrive ou qui est déjà dans la file d'attente. Ceci s'applique en particulier lorsque le boîtier de médiation reçoit concurremment des demandes originaires de différentes sessions. Cependant, des transactions asynchrones peuvent interrompre et/ou terminer le traitement d'une demande à tout moment.

Toutes les transactions de demande sont insécables du point de vue de l'agent. Le traitement d'une demande ne commence pas avant que la demande complète ne soit arrivée 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 le présent document est assez faible. Par souci de simplicité, nous l'avons réduit à un ensemble minimal qui satisfasse aux exigences. Une mise en œuvre réelle du protocole pourrait requérir de séparer certaines des transactions spécifiées ci-dessous en deux transactions ou plus de leurs protocoles respectifs. Les raisons pour ce faire pourraient être des contraintes du protocole particulier ou le désir d'une plus grande souplesse. En général cela ne devrait pas poser de problème. Cependant, il faudra examiner si cela pourrait changer la granularité des transactions concernées.

2.1.5 Contrôle d'accès

La propriété détermine l'accès aux règles de politique et groupes de règles de politique. Lorsque est créée une règle de politique, un identifiant unique par boîtier de médiation est généré pour l'identifier dans les transactions ultérieures. Au-delà de cet identifiant, chaque règle de politique a un propriétaire. Le propriétaire est l'agent authentifié qui a établi la règle de politique. Le boîtier de médiation utilise l'attribut de propriétaire 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 propriétaire 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 propriétaire.

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

Le boîtier de médiation peut être configuré pour permettre à des agents authentifiés spécifiques d'accéder et modifier les règles de politique de certains propriétaires spécifiques. Certainement, une configuration par défaut raisonnable laisserait chaque agent accéder à ses propres règles de politique. Aussi, il pourrait être bon de configurer une identité d'agent pour qu'elle agisse comme administrateur, permettant la modification de toutes les règles de politique possédées par tout agent. Cependant, la configuration des autorisations au boîtier de médiation est en-dehors du domaine d'application de la sémantique et du protocole MIDCOM.

2.1.6 Capacités du boîtier de médiation

Pour diverses raisons, il est utile qu'à l'établissement de session, l'agent prenne connaissance des capacités particulières du boîtier de médiation. Et donc, la procédure d'établissement de session décrite au paragraphe 2.2.1 comporte un transfert d'informations sur la capacité du boîtier de médiation à l'agent. La liste des capacités de middlebox couvertes comprend les suivantes :

- Prise en charge de la fonction pare-feu
    - Liste des fonctions de NAT prises en charge, qui pourraient inclure :
        - la traduction d'adresse
        - la traduction de port
        - la traduction de protocole
        - le double NAT
- Prise en charge de caractères génériques d'adresse IP interne
- Prise en charge de caractères génériques d'adresse IP externe
- Prise en charge de caractères génériques de port
- Prise en charge d'une ou plusieurs versions IP pour un réseau interne :
    - IPv4, IPv6, ou les deux
- Prise en charge d'une ou plusieurs versions IP pour un réseau externe :
    - IPv4, IPv6, ou les deux
- Liste des transactions facultatives de protocole MIDCOM prises en charge
- Prise en charge de règle de politique facultative spécifique de l'interface : non prise en charge ou prise en charge
- Persistance de règle de politique: persistant ou non persistant (une règle est persistante lorsque le boîtier de médiation peut sauvegarder la règle sur une mémoire non volatile, par exemple, un disque dur ou une mémoire flash)
- Durée de vie restante maximum 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 le délai de cette temporisation d'inactivité sont supprimées automatiquement du boîtier de médiation ; pour la suppression des règles de politique par les boîtiers de médiation, voir au paragraphe 2.3.13 sur l'événement de règle de politique asynchrone).
- 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 pour l'agent.

2.1.7 Identifiants d'agent et de boîtier de médiation

Pour permettre aussi bien aux agents qu'aux boîtiers de médiation d'entretenir plusieurs sessions, chaque message de demande contient un paramètre identifiant l'agent demandeur, et chaque message de réponse et chaque message de notification contient un paramètre identifiant le boîtier de médiation. Ces paramètres ne sont pas explicitement listés dans la description des transactions individuelles, parce qu'ils sont communs à tous. Ils ne sont pas autrement référencés dans les descriptions individuelles de sémantique. Bien qu'ils ne passent pas nécessairement de façon explicite pour des paramètres du protocole MIDCOM, ils peuvent être fournis par le protocole de transport sous-jacent (sécurisé) utilisé. Les identifiants d'agent au boîtier de médiation sont uniques pour le boîtier de médiation, et les identifiants de boîtier de médiation à l'agent sont respectivement uniques pour l'agent.

2.1.8 Conformité

Les exigences de MIDCOM contenues dans [MDC-REQ] demandent des capacités du protocole MIDCOM qui sont satisfaites par l'ensemble des transactions spécifiées ci dessous. Cependant, une mise en œuvre réelle d'un boîtier de médiation peut ne prendre en charge qu'un sous-ensemble de ces transactions. L'ensemble annoncé des transactions prises en charge peut être différent pour des agents authentifiés différents. Le boîtier de médiation informe à l'établissement de la session les agents authentifiés par l'échange de capacités sur les transactions que l'agent est autorisé à effectuer. Certaines transactions doivent nécessairement 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 oeuvre par tout boîtier de médiation offrant le service MIDCOM et doit être offerte à chacun des agents authentifiés. Une transaction facultative ne doit pas nécessairement être mise en oeuvre par un boîtier de médiation ; elle 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. C'est la procédure d'autorisation du boîtier de médiation qui détermine si un agent est autorisé ou non à utiliser une transaction de demande facultative, et n'est pas autrement spécifié par le présent document.

2.2 Transactions de commande de session

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

Toutes les transactions sont transmises au sein de cette session MIDCOM.

Le contrôle de session est pris en charge par trois transactions :

- Etablissement de session (SE, *Session Establishment*)
- Fin de session (ST, *Session Termination*)
- Fin de session asynchrone (AST, *Asynchronous Session Termination*)

Les deux premières sont des transactions de configuration à l'initiative de agent, et la troisième est une transaction asynchrone à l'initiative du boîtier de médiation.

2.2.1 Etablissement 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 par agent pour apparier la demande et la réponse correspondante chez l'agent.
- version : version du protocole MIDCOM.

- invite à authentification du boîtier de médiation (mc) : c'est un jeton d'invitation à authentification du boîtier de médiation. Comme on le verra ci-dessous, il n'est présent que dans la première itération de la demande.
- authentification d'agent (aa) : c'est un jeton d'authentification qui authentifie l'agent auprès du boîtier de médiation. Comme on le verra ci-dessous, il est mis à jour dans la seconde itération de la demande avec les éléments qui répondent à l'invitation du boîtier de médiation.

paramètres de réponse (succès) :
- identifiant de demande : c'est un identifiant qui correspond à la demande d'identifiant.
- authentification de middlebox (ma) : jeton d'authentification qui authentifie le boîtier de médiation à l'agent.
- jeton d'invite d'agent (ac) : jeton d'invitation à l'authentification de l'agent.
- capacités du boîtier de médiation : liste décrivant les capacités du boîtier de médiation. Voir au paragraphe 2.1.6 la liste des capacités de middlebox.

cause de l'échec :
- échec d'authentification
- pas d'autorisation
- les versions de protocole de l'agent et du boîtier de médiation ne s'apparient pas
- manque de ressources

sémantique :
Cette transaction d'établissement de session sert à établir une session MIDCOM. Pour l'authentification mutuelle des deux parties, deux transactions d'établissement de session ultérieures sont nécessaires comme indiqué à la Figure 1.

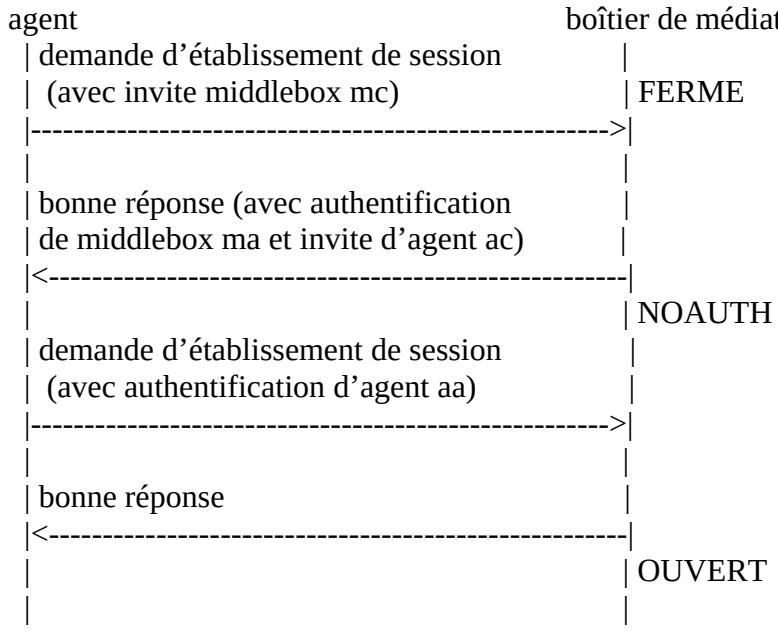

Figure 1: Authentification mutuelle de l'agent et du boîtier de médiation

L'établissement de session peut être simplifié en utilisant une seule transaction. Dans ce cas, l'invite de serveur et l'invite d'agent sont omises par l'envoyeur ou ignorées par le récepteur, et l'authentification doit être fournie par d'autres moyens, par exemple par TLS [RFC2246] ou IPsec [RFC2402][RFC2406].

Le boîtier de médiation vérifie avec son point de décision de politique si l'agent demandeur est autorisé à ouvrir une session MIDCOM. S'il ne l'est pas, le boîtier de médiation génère une réponse négative avec 'pas d'autorisation' comme cause de l'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 réussie.

2.2.2 Fin de session (ST, *session termination*)

nom de transaction : fin de session
type de transaction : configuration
conformité de transaction : obligatoire
paramètres de demande :

- identifiant de demande : identifiant unique par agent pour apparier la demande et la réponse correspondantes chez l'agent.

paramètres de réponse (seulement en cas de succès) :

- identifiant de demande : identifiant répondant à l'identifiant de la demande.

Sémantique :

Cette transaction sert à fermer la session MIDCOM au nom de l'agent. Après la fin de la session, le boîtier de médiation conserve toutes les règles de politique établies jusqu'à expiration de leur durée de vie ou jusqu'à l'intervention d'un événement qui fait que le boîtier de médiation y met un terme.

Le boîtier de médiation génère toujours une réponse de succès. Après l'envoi de la réponse, le boîtier de médiation n'enverra plus d'autre message à l'agent durant la session en cours. Elle ne traitera pas non plus dans cette session d'autres demandes reçues pendant le traitement de la demande de fin de session, ou reçues plus tard.

2.2.3 Fin de session asynchrone (AST, *Asynchronous Session Termination*)

nom de transaction : fin de session asynchrone
type de transaction : asynchrone
conformité de transaction : obligatoire
type de message de notification: notification de fin de session (STN, *Session Termination Notification*)
paramètres de réponse (seulement de réussite) :

- cause de fin : la raison de la fin de la session.

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 traitera plus aucune demande ultérieure de l'agent, même si elle était déjà en file d'attente au boîtier de médiation.

Après la fin de session, le boîtier de médiation conserve toutes les règles de politique établies jusqu'à la fin de leur durée de vie ou jusqu'à ce que survienne un événement à cause duquel le boîtier de médiation y met fin.

A la différence des autres transactions asynchrones, il n'est pas envoyé plus d'une notification parce qu'il n'y a qu'un seul agent affecté par la transaction.

2.2.4 Fin de session par interruption de connexion

Si une session MIDCOM se fonde sur une connexion de réseau sous-jacente, la session peut aussi se terminer sur 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 fin de session asynchrone.

2.2.5 Machine à états de session

La Figure 2 montre une machine à états pour illustrer la sémantique des transactions de session. Les abréviations de transaction utilisées figurent dans les en-têtes de chaque paragraphe de transaction.

Toutes les sessions commencent dans l'état FERME. Si l' authentification mutuelle a déjà été fournie par d'autres moyens, une transaction réussie SE peut causer une transition d'état à l'état OUVERT. Autrement, cela cause une transition à l'état NOAUTH. A partir de cet état, une seconde transaction SE échouée retourne à l'état FERME. Une transaction SE réussie cause une transition à l'état OUVERT. A tout moment, une transaction AST ou une défaillance de connexion peut survenir, causant une transition à l'état FERME. Une transaction ST réussie à partir de l'état NOAUTH ou OUVERT cause aussi un retour à FERME. Les paramètres des transactions sont expliqués à la Figure 2 ; la valeur mc=0 représente une invite de middlebox vide.

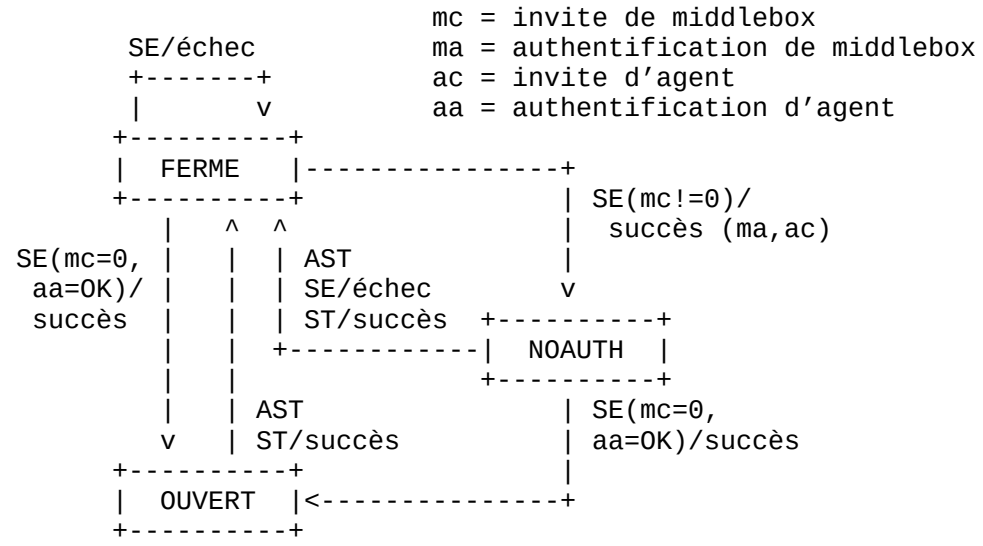

Figure 2: Machine d'état de session

2.3 Transactions de règle de politique

Ce paragraphe décrit la sémantique pour les transactions sur les règles de politique. Les transactions suivantes sont spécifiées :

- Règle de réserve de politique (PRR)
- Règle d'activation de politique (PER)

- Changement de dure de vie de règle de politique (RLC)
- Liste de règles de politique (PRL)
- Etat des règles de politique (PRS)
- Evénement de règle de politique asynchrone (ARE)

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

Avant qu'aucune 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. Toutes deux sont obligatoires, et elles servent à

- configurer les liaisons de NAT (PER)
- configurer les broches de pare-feu (PER)
- étendre la durée de vie des règles de politique établies (RLC)
- supprimer des règles de politique (RLC)

Certains cas exigent de connaître à l'avance quelle adresse IP (et numéro de port) serait choisie par le NAT dans une transaction PER. Cette information est nécessaire avant que ne soient disponibles des informations suffisantes pour effectuer une transaction PER complète (voir l'exemple au paragraphe 4.2). Pour la prise en charge de tels cas, les transactions principales sont étendues par la transaction règle de réserve de politique (PRR) afin de

- réserver les adresses et numéros de port dans les NAT (PRR)

2.3.2 Etablissement des règles de politique

PRR et PER établissent toutes deux une règle de politique. Au sein de la règle, l'action est 'réservé' si elle est établie par PRR et 'activé' si elle est établie par PER.

La transaction règle de réserve de politique (PRR) sert à 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 l'adresse IP réservée et les gammes facultatives de numéros de port à l'agent. Aucune liaison d'adresse ou configuration en micro-sas (*pinhole*) n'est effectuée au boîtier de médiation. Le traitement de paquet au boîtier de médiation reste inchangé.

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

Sur un NAT traditionnel (voir [NAT-TRAD]), seule une adresse externe est réservée ; sur un NAT double, une adresse interne et une adresse externe sont réservées. La réservation auprès d'un NAT est effectuée pour des ressources demandées, telles que des adresses IP et des numéros de port, pour utilisation future. La façon exacte dont la réservation est faite dépend de la mise en œuvre du NAT. Dans les deux cas, la réservation concerne seulement une adresse IP ou une combinaison d'une adresse IP et d'une gamme de numéros de port.

La transaction règle d'activation de politique (PER) sert à établir une règle de politique qui affecte le traitement de paquet au boîtier de médiation. Selon ses paramètres d'entrée, il peut faire usage de la réservation établie par une transaction PRR ou créer une nouvelle règle à partir de zéro.

Sur un NAT, l'action d'activation est interprétée comme une action de liaison qui établit des liens entre adresses interne et externe. A un pare-feu, l'action d'activation s'interprète comme une ou plusieurs actions admises pour des configurations en micro-sas. Le nombre d'actions admises dépend des paramètres de la demande et de la mise en œuvre du pare-feu.

Sur un NAT/pare-feu combiné, l'action d'activation s'interprète comme une combinaison d'actions liées et admises.

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

2.3.3 Maintenance des règles de politique et groupes de règles de politique

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

Chaque règle de politique a un propriétaire. Le contrôle d'accès à la règle de politique est fondé sur la propriété (voir au paragraphe 2.1.5). La propriété d'une règle de politique ne change pas durant 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 se terminera au boîtier de médiation. Normalement, le boîtier de médiation indique la fin d'une règle de politique par une transaction ARE. Une transaction de changement de durée de vie de règle de politique (RLC) peut allonger la durée de vie de la règle de politique jusqu'à la limite spécifiée par le boîtier de médiation à l'établissement de la session. Une transaction RLC peut aussi être utilisée pour raccourcir la durée de vie d'une règle de politique ou pour supprimer une règle de politique en demandant une durée de vie de zéro. (Noter que les durées de vie de règles de politique peuvent aussi être modifiées par la transaction de changement de durée de vie de groupe (GLC).)

Chaque règle de politique est un membre d'exactement un groupe de règle de politique. L'appartenance à un 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. Le nouvel identifiant de 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 appartenant au groupe ont atteint la fin de leurs durées de vie, le groupe n'existe plus.

Les agents peuvent explorer les propriétés et l'état de toutes les règles de politique auxquelles ils sont autorisés à accéder en utilisant la transaction d'état de règle de politique (PRS).

2.3.4 Evénements de politique et notifications asynchrones

Si une règle de politique change d'état ou si sa durée de vie restante est changée d'une façon autre qu'une diminution, tous les agents qui peuvent accéder à cette règle de politique et qui participent à une session ouverte avec le boîtier de médiation en reçoivent notification par le boîtier de médiation. Si le changement d'état ou de durée de vie étaient demandés explicitement par un message de

demande, le boîtier de médiation le notifie alors à l'agent demandeur en retournant la réponse correspondante. Tous les autres agents qui peuvent accéder à la politique reçoivent la notification par un message de notification d'événement de règle de politique (REN).

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

Dans le cas d'une transaction PER, PRR, ou RLC, l'agent demandeur reçoit respectivement une réponse PER, PRR, ou RLC. A 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.

Dans le cas de la fin d'une règle par le raccourcissement de sa durée de vie ou autre événement non déclanché par un agent, le boîtier de médiation envoie alors un message REN à chaque agent qui peut accéder à la règle de politique particulière et participe à une session ouverte avec le boîtier de médiation. Ceci garantit qu'un agent sait toujours l'état le plus récent de toutes les règles de politique auxquelles il peut accéder.

2.3.5 Tuplets d'adresse

Les messages de demande et réponse des transactions PRR, PER, et PRS contiennent les spécifications d'adresse pour les adresses IP et de transport. Ces paramètres comportent :

- la version IP
- l'adresse IP
- la longueur du préfixe d'adresse IP
- le protocole de transport
- le numéro de port
- la parité de port
- la gamme de port

De plus, le message de demande de PER et le message de réponse de PRS contiennent une 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 'entrant', les paquets UDP traversent de l'extérieur vers l'intérieur ; pour 'sortant', 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 avec '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 de TCP établi et le fanion ACK non établi, doit arriver au boîtier de médiation à l'interface extérieur.
- sortant : flux de paquets TCP bidirectionnel. Le premier paquet, avec le fanion SYN de TCP établi et le fanion ACK non établi, doit arriver au boîtier de médiation à l'interface intérieur.
- bidirectionnel : Le premier paquet, avec le fanion SYN de TCP établi et le fanion ACK non établi, peut arriver à l'interface intérieur ou extérieur.

On se réfère à l'ensemble de ces paramètres comme à un tuplet d'adresse. Un tuplet d'adresse spécifie un point de terminaison de communication à un appareil interne ou externe ou des adresses allouées au boîtier de médiation. Dans le présent document, on distingue quatre sortes de tuplets d'adresse, comme indiqué à la Figure 3.

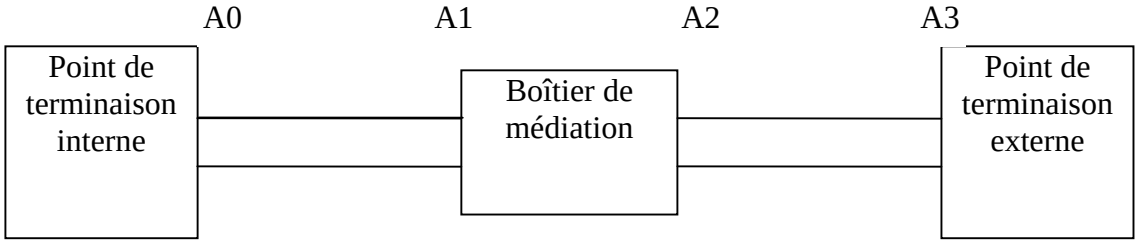

Figure 3: Tuplets d'adresse A0 - A3

- A0 -- point de terminaison interne : le tuplet d'adresse A0 spécifie un point de terminaison de communication d'un appareil au sein – par rapport au boîtier de médiation – du réseau interne.

- A1 – adresse interne du boîtier de médiation : le tuplet d'adresse A1 spécifie un point de terminaison 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 de terminaison interne au boîtier de médiation et c'est la source pour les paquets qui passent du boîtier de médiation au point de terminaison interne.

- A2 – adresse externe du boîtier de médiation : le tuplet d'adresse A2 spécifie un point de terminaison virtuel de communication au boîtier de médiation au sein du réseau externe. A2 est l'adresse de destination pour les paquets qui passent du point de terminaison externe au boîtier de médiation et c'est la source pour les paquets qui passent du boîtier de médiation au point de terminaison externe.

- A3 -- point de terminaison externe : le tuplet d'adresse A3 spécifie un point de terminaison de communication d'un appareil au sein – par rapport au boîtier de médiation – du réseau externe.

Pour un pare-feu, les points de terminaison intérieur et extérieur sont identiques aux points de terminaison externe ou interne correspondants, respectivement. Dans ce cas la règle de politique installée établit la même valeur dans A2 que dans A0 (A0=A2) et établit 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 comme dans un NAT traditionnel : A1 a la même valeur que A3.

Pour un NAT double, il y a deux liaisons de tuplets d'adresse : A1 et A2 sont deux valeurs allouées par le NAT. L'adresse externe de boîtier de médiation A2 est liée au point de terminaison interne A0, et l'adresse interne de boîtier de médiation A1 est liée au point de terminaison externe A3.

2.3.6 Contraintes de paramètres d'adresse

Pour les paramètres de transaction qui appartiennent à un tuplet d'adresse, certaines contraintes existent qui sont communes à tous les messages qui les utilisent. Ces contraintes sont donc résumées

ci-dessous et ne seront pas répétées lors de la description des paramètres dans la présentation des descriptions de transaction.

La sémantique MIDCOM définie dans le présent document spécifie le traitement de IPv4 et IPv6 comme protocoles réseau, et de TCP et UDP (sur IPv4 et IPv6) comme protocoles de transport. Le traitement de tout autre protocole de transport, par exemple, SCTP, n'est pas défini dans la sémantique mais peut être pris en charge par des spécifications de protocole concrètes.

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

La valeur du paramètre d'adresse IP doit être conforme à la version IP spécifiée.

L'adresse IP d'un tuplet d'adresse peut être remplacée par un caractère générique. La question de savoir si le remplacement de l'adresse IP par un caractère générique est admis ou dans quelle gamme il est admis dépend de la politique locale du boîtier de médiation ; voir aussi à la section 6, "Considérations de sécurité". Le remplacement par un caractère générique est spécifié par le paramètre de longueur de préfixe d'adresse IP d'un tuplet d'adresse. Conformément à l'utilisation habituelle des longueurs de préfixe, ce paramètre indique le nombre de bits de plus fort poids de l'adresse IP qui sont fixés, alors que le reste des bits de plus faible poids de l'adresse IP est remplacé par des caractères génériques.

La valeur du paramètre protocole de transport peut être 'TCP', 'UDP', ou 'TOUT'. Si le paramètre protocole de transport a la valeur 'TOUT', seuls les en-têtes IP sont pris en considération pour le traitement des paquets dans le boîtier de médiation – c'est-à-dire que l'en-tête de transport n'est pas pris en considération. Les valeurs des paramètres numéro de port, gamme de port, et parité de port sont non pertinentes si le paramètre de protocole est 'TOUT'. Dans une règle de politique, la valeur du paramètre protocole de transport doit être la même pour tous les tuplets d'adresse A0, A1, A2, et A3.

La valeur du paramètre numéro de port est soit zéro soit un entier positif. Un entier positif spécifie un numéro de port UDP ou TCP concret. La valeur zéro spécifie le remplacement du port par un caractère générique pour le protocole spécifié par le paramètre protocole de transport. Si le paramètre numéro de port a la valeur zéro, la valeur du paramètre gamme de port est alors non pertinente. Selon la valeur du paramètre protocole de transport, ce paramètre peut vraiment se référer aux ports ou bien se référer à un concept équivalent.

Le paramètre parité de port est utilisé différemment dans le contexte des règles de réserve 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 'tout'. Elle spécifie la parité du premier (inférieur) numéro de port réservé. Dans le contexte d'un PER, le paramètre parité de port indique au boîtier de médiation si les numéros de port qui lui sont alloués devraient avoir la même parité que les numéros de port, respectivement interne ou externe, correspondants. Dans ce contexte, le paramètre a la valeur 'même' ou 'tout'. Si la valeur est 'même', la parité du numéro de port de A0 doit alors être la même que la parité du numéro de port de A2, et la parité du numéro de port de A1 doit être la même que la parité du numéro de port de A3. Si le paramètre parité de port a la valeur 'tout', il n'y a alors aucune contrainte sur la parité des numéros de port.

Le paramètre gamme de port spécifie un nombre de numéros de port consécutifs. Sa valeur est un entier positif. Comme le paramètre numéro de port, ce paramètre définit un ensemble de numéros de port consécutifs commençant par le numéro de port spécifié par le paramètre numéro de port comme le plus petit numéro de port et qui a autant d'éléments que spécifié par le paramètre gamme de port. Une

valeur de 1 spécifie un seul numéro de port. Le paramètre gamme de port doit avoir la même valeur pour chaque tuplet d'adresse A0, A1, A2, et A3.

Une seule règle de politique P contenant une valeur de gamme de port 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 égale la valeur du paramètre gamme de port. Chaque règle de politique P_1, P_2, ..., P_n a une valeur de paramètre gamme de port de 1. La règle de politique P_1 contient un ensemble de tuplets d'adresse A0_1, A1_1, A2_1, et A3_1, contenant chacun le premier numéro de port des tuplets d'adresse respectifs dans P ; la règle de politique P_2 contient un ensemble de tuplets d'adresse A0_2, A1_2, A2_2, et A3_2, contenant chacun le second numéro de port des tuplets d'adresse respectifs dans P ; et ainsi de suite.

2.3.7 Règles de politique spécifiques de l'interface

Normalement, les agents demandent les règles de politique avec la connaissance seulement de A0 et A3, c'est-à-dire, les tuplets d'adresse (voir le paragraphe 2.3.5). Mais dans des cas très particuliers, les agents peuvent avoir besoin de choisir les interfaces auxquelles est liée la règle de politique demandée. Généralement, le boîtier de médiation veille à choisir les bonnes interfaces lorsqu'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 réserve de politique (PRR) et règle d'activation de politique (PER). Ces paramètres s'appellent :

- 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 lorsqu'elles sont prises en charge.

Les agents peuvent apprendre à l'établissement de session si les règles de politique spécifiques de l'interface sont prises en charge 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 : c'est un identifiant unique par agent pour apparier la demande et la réponse correspondantes chez l'agent.
- identifiant de groupe : c'est une référence au groupe duquel 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 NAT demandé du boîtier de médiation. Les valeurs admises sont 'traditionnel' ou 'double'.
- version IP interne : c'est la version IP demandée à l'intérieur du boîtier de médiation ; voir au paragraphe 2.3.5.
- Adresse IP interne : c'est l'adresse IP du point de terminaison de communication interne (A0 à la Figure 3) ; voir au paragraphe 2.3.5.

- numéro de port interne : c'est le numéro de port du point de terminaison de communication interne (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 au paragraphe 2.3.5.
- gamme de port : nombre de numéros de port consécutifs à réserver ; voir au paragraphe 2.3.5.
- parité de port : parité demandée du premier (plus petit) numéro de port à réserver ; les valeurs admises pour ce paramètre sont 'impair', 'pair', et 'tout'. Voir aussi au 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 correspondant 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 outil de règle de politique dans les transactions ultérieures de règle de politique, en particulier pour se référer à la règle de réserve de politique dans une transaction PER ultérieure.
- identifiant de groupe : référence au groupe dont la règle de réserve de politique est membre.
- adresse IP intérieure réservée : adresse IPv4 ou IPv6 réservée sur le côté interne du boîtier de médiation. Pour un flux sortant, ce sera la destination à laquelle le point de terminaison interne enverra ses paquets (A1 à la Figure 3). Pour un flux entrant, ce sera l'adresse de source apparente des paquets comme transmis au point de terminaison interne (A0 à la Figure 3). Le boîtier de médiation ne réserve et rapporte une adresse interne que dans le cas où le NAT double prend effet. Autrement, une valeur vide pour les adresses indique qu'aucune réservation interne n'a été faite. Voir aussi au paragraphe 2.3.5.
- numéro de port intérieur réservé : Voir au paragraphe 2.3.5.
- Adresse IP externe réservée : c'est l'adresse IPv4 ou IPv6 réservée sur le côté externe du boîtier de médiation. Pour un flux entrant, ce sera la destination à laquelle le point de terminaison externe envoie ses paquets (A2 à la Figure 4). Pour un flux sortant, ce sera l'adresse de source apparente des paquets comme transmis au point de terminaison externe (A3 à 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 au paragraphe 2.3.5.
- numéro de port extérieur réservé : Voir au paragraphe 2.3.5.
- durée de vie de règle de politique : la durée de vie de règle de politique allouée par le boîtier de médiation, après laquelle la réservation sera révoquée si elle n'a déjà été remplacée par une règle d'activation de politique dans une transaction PER.

cause de l'échec :

- agent non autorisé pour cette transaction
- agent non autorisé à ajouter des membres à ce groupe
- absence d'adresse IP
- absence de numéro de port
- absence de ressources
- l'interface interne/externe spécifiée n'existe pas
- l'interface interne/externe spécifiée non disponible pour le service spécifié

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

sémantique :

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

A réception de la demande, le boîtier de médiation détermine combien de réservations d'adresses (et de ports) sont nécessaires sur la base de sa configuration. Si il ne fournit que des services de filtrage de paquets, il n'effectue aucune réservation et retourne des valeurs vides pour les adresses IP et numéro de ports intérieurs et extérieurs réservés. Si il est configuré pour le NAT double, il réserve les adresses IP aussi bien intérieures qu'extérieures (et une gamme de numéros de port facultative) et les retourne. Autrement, il réserve et retourne une adresse IP extérieure (et une gamme de numéros de port facultative) et retourne des valeurs vides pour l'adresse interne et la gamme de port réservées.

Le paramètre A0 (version d'adresse IP intérieure, adresse IP intérieure, et numéro de port intérieur) peut être utilisé par le boîtier de médiation pour déterminer la transposition de NAT correcte et donc A2 si nécessaire. Une fois qu'une transaction PRR a réservé une adresse extérieure (A2) pour un point de terminaison interne (A0) au boîtier de médiation, celui-ci doit s'assurer que ce A2 réservé est disponible dans toute transaction PER et PRR suivante.

Pour les boîtiers de médiation qui prennent en charge des règles de politique spécifiques de l'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'entre eux ne doit être inclus. En présence de ces paramètres, le boîtier de médiation utilise le paramètre d'interface externe pour choisir l'interface à laquelle le tuplet d'adresse extérieure (adresse IP et numéro de port extérieurs) est réservé, et le paramètre d'interface interne pour choisir l'interface à laquelle le tuplet d'adresse intérieur (adresse IP et numéro de port intérieurs) 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 absence de ressources, telles que des adresses IP disponibles, des numéros de port, ou de stockage pour des règles de politique ultérieures, 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 existant de règles de politique a été spécifié et qu'il n'est pas la propriété de l'agent demandeur, aucune nouvelle règle de politique n'est établie, et une réponse d'échec appropriée est générée.

En cas de succès, cette transaction crée une nouvelle règle de réserve de politique. Si un groupe de règles de politique déjà existant est spécifié, la nouvelle règle de politique devient alors un membre de ce groupe. 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 middlebox pour la nouvelle règle de politique. Le propriétaire de la nouvelle règle de politique est l'agent authentifié qui envoie la demande. 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 au maximum de la durée de vie spécifiée par le boîtier de médiation au démarrage de la session, c'est-à-dire,

0 <= lt_granted <= MINIMUM(lt_requested, lt_maximum)

où
- lt_granted est la durée de vie réellement allouée par le boîtier de médiation
- lt_requested est la durée de vie demandée par l'agent
- lt_maximum est la durée de vie maximum spécifiée au démarrage de la session

Un boîtier de médiation avec une capacité de NAT réserve toujours un tuplet d'adresse externe (A2) de middlebox en réponse à une demande PRR. Dans le cas particulier d'un boîtier de médiation NAT/double NAT combiné, l'agent peut demander seulement le service NAT ou le service double NAT en choisissant respectivement le paramètre de service 'traditionnel' ou 'double'. Un agent qui n'a aucune préférence choisit 'double'. La valeur 'traditionnel' ne devrait être utilisée qu'afin de choisir le service NAT traditionnel sur les boîtiers de médiation qui offrent à la fois le NAT traditionnel et le double NAT. Dans le cas 'double', le boîtier de médiation NAT/double NAT combiné réserve A2 et A1. Le cas 'traditionnel' a pour effet de réserver seulement A2. Un agent doit toujours utiliser la transaction PRR pour choisir le service NAT seul ou le service NAT double dans le cas particulier d'un boîtier de médiation NAT/double NAT combiné. Un boîtier de médiation pare-feu ignore ce paramètre.

Si l'identifiant de protocole est 'TOUT', le boîtier de médiation réserve alors seulement la ou les adresses IP intérieure et/ou extérieure disponibles. La ou les adresses réservées sont retournées à l'agent. Dans ce cas, les paramètres de demande " gamme de port" et " parité de port" ainsi que les paramètres de réponse " numéro de port intérieur" et " numéro de port extérieur", sont non pertinents.

Si l'identifiant de protocole est 'UDP' ou 'TCP', une combinaison d'une adresse IP et d'une séquence consécutive de numéros de port, commençant par la parité spécifiée, est réservée sur, aucun côté, un côté, ou sur les deux côtés du boîtier de médiation, selon ce qui convient. La ou les adresses IP et le premier (plus faible) numéro de port réservés de la séquence suivante sont retournés à l'agent. (Cela s'applique aussi aux autres protocoles prenant en charge des ports ou équivalents.)

Après l'établissement réussi d'une nouvelle règle de réserve de politique et l'envoi du message de réponse à l'agent demandeur, le boîtier de médiation vérifie s'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.

Les agents MIDCOM utilisent la transaction de règle d'activation de politique (PER) pour activer les règles de réserve de politique qui ont été établies auparavant par une transaction de règle de réserve 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 apparier la demande et la réponse correspondante chez l'agent.
- identifiant de règle de réserve de politique: référence à une règle de réserve de politique déjà existante créée par une transaction PRR. La référence peut être vide, auquel cas le boîtier de médiation doit allouer toutes les adresses et numéros de port nécessaires au sein de cette transaction PER. Si elle n'est pas vide, les paramètres de demande suivants sont alors non

pertinents: identifiant de groupe, protocole de transport, gamme de port, parité de port, version IP interne, version IP externe.
- identifiant de groupe : référence au groupe duquel 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 de réserve de politique.
- protocole de transport : Voir au paragraphe 2.3.5.
- gamme de port : nombre de numéros de port consécutifs à réserver ; voir au paragraphe 2.3.5.
- parité de port : parité demandée du ou des numéros de port à transposer. Les valeurs admises de ce paramètre sont 'même' et 'tout'. Voir aussi au paragraphe 2.3.5.
- direction de flux : ce paramètre spécifie la direction de communication activée, 'entrant', 'sortant', ou 'bidirectionnel'.
- 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 de terminaison de communication interne (A0 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port interne : numéro de port du point de terminaison de communication interne (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.
- adresse IP externe : adresse IP du point de terminaison de communication externe(A3 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port externe : numéro de port du point de terminaison de communication externe (A3 à la Figure 4), 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 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 correspondant 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 sert d'outil de règle de politique dans les transactions ultérieures de règle de politique. Si un identifiant de règle de réserve de politique a été fourni dans la demande, l'identifiant de règle de politique retourné doit avoir la même valeur.
- identifiant de groupe : référence au groupe duquel la règle d'activation de politique est membre. Si un identifiant de règle de réserve de politique a été fourni dans la demande, ce paramètre identifie alors le groupe duquel la règle de réserve de politique est membre.
- adresse IP intérieure : adresse IP fournie à l'intérieur du boîtier de médiation (A1 à la Figure 3). Dans le cas d'un NAT double, ce paramètre sera une adresse IP interne réservée à l'intérieur du boîtier de médiation. Dans tous les autres cas, ce paramètre de réponse sera identique à l'adresse IP interne fournie avec la demande. Si le paramètre identifiant de règle de réserve de politique a été fourni dans la demande et si la transaction PRR qui s'y rapporte réservait une adresse IP intérieure, l'adresse IP intérieure fournie dans la réponse PER sera d'une valeur identique à celle retournée par la réponse à la demande PRR. Voir aussi au paragraphe 2.3.5.
- numéro de port intérieur : numéro de port interne fourni à l'intérieur du boîtier de médiation (A1 à la Figure 3) ; voir aussi au paragraphe 2.3.5.
- adresse IP extérieure : adresse IP externe fournie à l'extérieur du boîtier de médiation (A2 à la Figure 4). Dans le cas d'un pare-feu, ce paramètre sera identique à l'adresse IP interne fournie

avec la demande. Dans tous les autres cas, ce paramètre de réponse sera une adresse IP externe réservée à l'extérieur du boîtier de médiation. Voir aussi au paragraphe 2.3.5.
- numéro de port extérieur : numéro de port externe fourni à l'extérieur du NAT (A2 à la Figure 3) ; voir au paragraphe 2.3.5.
- durée de vie de règle de politique : durée de vie de règle de politique allouée par le boîtier de médiation.

cause de l'échec:
- agent non autorisé pour cette transaction
- agent non autorisé à ajouter des membres à ce groupe
- pas de telle règle de réserve de politique
- agent non autorisé à remplacer cette règle de réserve de politique
- conflit avec une règle de politique déjà existante (par exemple, la même adresse-port interne est transposée à différentes paires adresse-port extérieures)
- absence d'adresse IP
- absence de numéro de port
- absence de ressources
- les caractères IP génériques internes ne sont pas admis
- les caractères IP génériques externes ne sont pas admis
- l'interface interne/externe spécifiée n'existe pas
- l'interface interne/externe spécifiée est non disponible pour le service spécifié
- discordance entre A0 réservé et A0 demandé

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 de terminaison interne et un point de terminaison 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 de terminaison (qui peut facultativement inclure des caractères génériques) et la direction de communication (entrant, sortant, bidirectionnel). Les points de terminaison de communication sont présentés à la Figure 3. L'opération de base de la transaction PER est décrit comme suit :

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 d'une transaction PRR précédente,
3. le boîtier de médiation active le transfert de paquet entre A0 et A3 en liant A0-A2 et A1-A3 et/ou en ouvrant les micro-sas correspondants, tous deux conformément à la direction spécifiée, et
4. le boîtier de médiation retourne A1 et A2 à l'agent.

Dans le cas d'un pare-feu pur filtre de paquets, les tuplets d'adresse retournés sont les mêmes que ceux de 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 de terminaison interne peut utiliser l'adresse réelle du point de terminaison externe (A1 = A3), mais le point de terminaison externe utilise un tuplet d'adresse fourni par le NAT (A2! = A0). Dans le cas d'un appareil NAT double, les deux points de terminaison utilisent les tuplets d'adresse 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 NAT double, les tuplets d'adresse en réponse seront les mêmes que pour, respectivement, un pur NAT traditionnel ou un NAT double, mais le boîtier de médiation configurera son filtre de paquets en plus des liaisons de NAT effectuées. Dans le cas d'un pare-feu combiné à 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 source-destination différentes.

Pour les boîtiers de médiation prenant en charge des règles de politique spécifiques de l'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 des deux. En présence de ces paramètres, le boîtier de médiation utilise les paramètres d'interface externe pour choisir l'interface à laquelle est lié le tuplet d'adresse extérieure (adresse IP et numéro de port extérieurs), et le paramètres d'interface interne pour choisir l'interface à laquelle est lié le tuplet d'adresse intérieure (adresse IP et numéro de port intérieurs). Sans la présence de ces paramètres, le boîtier de médiation choisit les différentes interfaces sur la base de sa configuration interne.

Vérification de l'identifiant de règle de réservation de politique

Si le paramètre qui spécifie l'identifiant de règle de réservation de politique n'est pas vide, le boîtier de médiation vérifie alors 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 réserve de politique.

En cas de réussite, cette transaction crée une nouvelle règle d'activation de politique. S'il était fait référence à une règle de réserve de politique, il est mis fin à la règle de réserve de politique sans qu'une notification explicite ne soit envoyée à l'agent (autre que la réponse PER de succès).

La transaction PRR établit le point de terminaison 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 ayant un A0 demandé non égal au A0 réservé, et doit alors envoyer un message d'échec approprié. Autrement, le boîtier de médiation peut changer A0 suite à la demande PER.

Le boîtier de médiation génère un identifiant unique de boîtier de médiation pour la nouvelle règle de politique. S'il était fait référence à une règle de réserve de politique, l'identifiant de la règle de réserve de politique est alors réutilisé.

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

Vérification de l'identifiant de groupe de règles de politique

Si aucune règle de réserve de politique n'était 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 la propriété de l'agent demandeur, aucune nouvelle règle de politique n'est alors établie, et une réponse d'échec appropriée est générée.

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

Si la valeur du paramètre protocole de transport est 'TOUT', le boîtier de médiation active alors la communication entre l'adresse IP externe spécifiée et l'adresse IP interne spécifiée. Les adresses à utiliser par les partenaires de 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 utilise le même type de protocole de transport, 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 celle de 'TOUT' mais transpose aussi les gammes de numéros de port, en gardant la parité de port, si cela est demandé.

La configuration du boîtier de médiation peut échouer à cause de l'absence de ressources, telles que des adresses IP disponibles, des numéros de port, ou de stockage pour des règles de politique ultérieures. Elle peut aussi échouer à cause d'un conflit avec une règle de politique établie. En cas de conflit, le mécanisme du premier entré premier servi s'applique. Les règles de politique existantes restent inchangées et les nouvelles arrivantes sont rejetées. Cependant, en cas de chevauchement non conflictuel de règles de politique (y compris de règles de politique identiques), toutes les règles de politique sont acceptées.

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

0 <= lt_granted <= MINIMUM(lt_requested, lt_maximum)

où
- lt_granted est la durée de vie réellement allouée par le boîtier de médiation
- lt_requested est la durée de vie demandée par l'agent
- lt_maximum est la durée de vie maximum spécifiée au démarrage de la session

Dans chaque cas d'échec, une réponse d'échec appropriée est générée. La règle de réserve de politique qui est référencée dans la transaction PER n'est pas affectée dans le cas d'un échec au sein de la transaction PER – c'est-à-dire que la règle de réserve de politique demeure.

Après l'établissement réussi d'une règle d'activation 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 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 d'agent unique pour apparier la demande et la réponse correspondante chez l'agent.

- identifiant de règle de politique: identifie la règle de politique pour laquelle le changement de la durée de vie est demandé. Cela peut identifier un 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 correspondant à l'identifiant de la demande.

- durée de vie de règle de politique: durée de vie restante de la règle de politique allouée par le boîtier de médiation.

cause de l'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 allongée

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 fin de la règle de politique. La fin d'une 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 celle en cours, le boîtier de médiation vérifie aussi si la durée de vie de la règle de politique peut être allongée et génère un message d'échec approprié si elle 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. Un réponse de succès est générée par le boîtier de médiation si la durée de vie de la règle de politique a été changée de quelque façon que ce soit.

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 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 <= lt_granted <= MINIMUM(lt_requested, lt_maximum)

où
- lt_granted est la durée de vie réellement allouée par le boîtier de médiation
- lt_requested est la durée de vie demandée par l'agent
- lt_maximum est la durée de vie maximum spécifiée au démarrage de la 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 est non existante. Toute transaction ultérieure sur cette règle de politique amènera 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 s'applique au groupe dont la règle de politique est membre.

Après la réussite du changement de la durée de vie restante de la règle 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 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 règle de politique (PRL)

nom de transaction : liste de règle de politique
type de transaction : surveillance
conformité de transaction : obligatoire
paramètres de demande :

- identifiant de demande : identifiant unique d'agent pour apparier 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 politique : liste des identifiants de règle de politique de toutes les règles de politique auxquelles l'agent peut accéder.

cause de l'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. Normalement, l'agent a déjà l'information, mais dans des cas particuliers (par exemple, après la défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent d'administration 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 propriétaire de chaque politique.

Cette transaction n'a aucun effet sur l'état des règles de politique.

2.3.12 Etat 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 apparier la demande et la réponse correspondante chez l'agent.
- identifiant de règle de politique : identifiant de règle de politique unique pour le boîtier de médiation.

paramètres de réponse (succès) :

- identifiant de demande : identifiant correspondant à l'identifiant de la demande.
- propriétaire de règle de politique: identifiant de l'agent propriétaire de cette règle de politique.
- identifiant de groupe : référence au groupe dont 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 est demandée une réservation; voir au paragraphe 2.3.5.
- gamme de port : nombre de numéros de port 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 à la Figure 3).
- version d'adresse IP externe : version de l'adresse IP externe (version IP de A0 à la Figure 3
- adresse IP interne : adresse IP du point de terminaison de communication interne (A0 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port interne : numéro de port du point de terminaison de communication interne (A0 à la Figure 3) ; voir au paragraphe 2.3.5.
- adresse IP externe : adresse IP du point de terminaison de communication externe (A3 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port externe : numéro de port du point de terminaison de communication externe (A3 à 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 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port interne : numéro de port interne fourni à l'intérieur du NAT (A1 à 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 extérieure : adresse IP externe fournie à l'extérieur du NAT (A2 à la Figure 3) ; voir au paragraphe 2.3.5.
- numéro de port extérieur : numéro de port externe fourni à l'extérieur du NAT (A2 à la Figure 3) ; voir au paragraphe 2.3.5.
- parité de port : parité des ports alloués.
- service : service choisi dans le cas d'une middlebox mêlant traditionnel et NAT double (voir au paragraphe 2.3.8).
- durée de vie de règle de politique : durée de vie restante de la règle de politique.

cause de l'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. Normalement, l'agent a déjà ces informations, mais dans des cas particuliers (par exemple, après la défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent d'administration 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 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 règle de politique.

2.3.13 Evénement de règle de politique asynchrone (ARE)

nom de transaction : événement de règle de politique asynchrone
type de transaction : notification
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 mettre fin à 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 autres événements qui peuvent causer cette transaction figurent les changements de point de décision de 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 ne 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 il aboutit au raccourcissement (lt_new < lt_existing), à l'extension (lt_new > lt_existing), ou à la fin de la règle de politique (lt_new = 0).

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

2.3.14 Machine d'état de règle de politique

La Figure 4 montre la machine d'état pour les transactions de règle de politique avec toutes les transitions d'état possibles. Les abréviations de transaction figurent dans les en-têtes des paragraphes des transactions spécifiques.

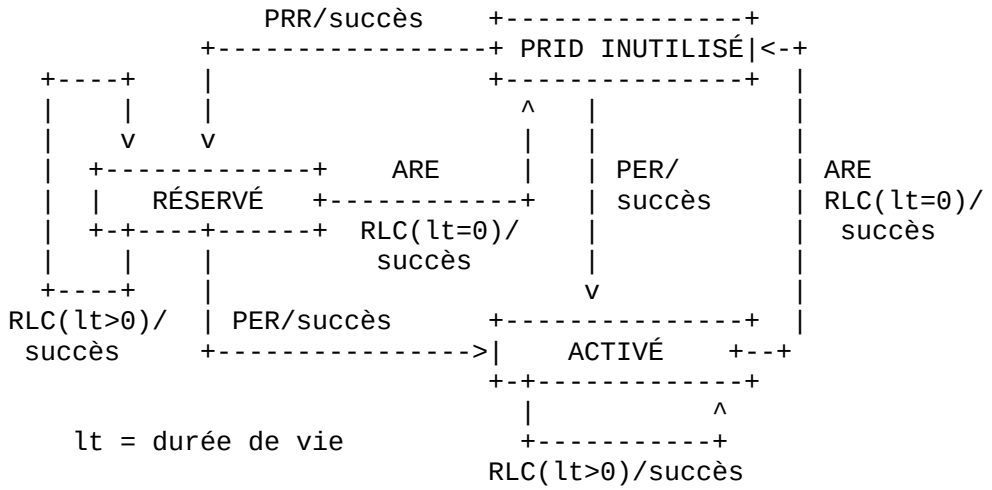

Figure 4: Machine d'état de règle de politique

Cette machine d'état existe pour chaque identifiant de règle de politique (PRID). Au départ, toutes les règles de politique sont dans l'état PRID INUTILISÉ, ce qui signifie que la règle de politique n'existe

pas ou n'est pas active. Après 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 à l'état RÉSERVÉ, dans lequel une réservation d'adresse est établie. A partir de là, une transaction PER peut entrer dans l'état ACTIVÉ. Cette transaction peut aussi être utilisée pour entrer dans l'état ACTIVE directement à partir de l'état PRID INUTILISÉ sans réservation. Dans l'état ACTIVÉ, la communication demandée entre les points de terminaison interne et 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 retourner 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 des transactions de demande ne change pas l'état au boîtier de médiation.

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

2.4 Transactions de groupe de règles de politique

La présente section décrit la sémantique pour les 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*)
- Etat de groupe (GS, *Group Status*)

Toutes sont des transactions de demande initialisées par l'agent. GLC est une transaction de confort. GL et GS sont des transactions de surveillance qui n'ont aucun effet sur la machine d'état de groupe.

2.4.1 Généralités

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 la propriété d'un même agent authentifié. Donc, une propriété implicite d'un groupe est son propriétaire, qui est le propriétaire des règles de politique membres.

Un groupe est implicitement créé lorsque sa première règle de politique membre est établie. Un groupe est implicitement terminé lorsque la dernière règle de politique membre restante est close. 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 sont déclarées 'facultatives' par leur entrée de conformité respective à la section 3. Cependant, elles fournissent certaines fonctions, comme une commodité pour l'agent, en envoyant une seule demande au lieu de plusieurs, ce qui n'est pas disponible si seules les transactions obligatoires sont disponibles.

La transaction de changement de durée de vie de groupe (GLC, *Group Lifetime Change*) est équivalente à des transactions de 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 Etat de groupe (GS) peuvent être utilisées par l'agent pour explorer l'état du boîtier de médiation et explorer ses droits d'accès. La transaction GL fait la liste de tous les groupes auxquels l'agent peut accéder, y compris les groupes possédés par d'autres agents. La transaction GS fait rapport de l'état d'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 dans le cas de défaillance d'un agent. L'agent qui reprend le rôle de celui qui est défaillant peut utiliser ces restaurations de transactions quelles que soient 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) 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 : commodité
conformité de transaction : facultatif
paramètres de demande :

- identifiant de demande : identifiant unique pour l'agent pour apparier la demande et la réponse correspondante chez l'agent.
- identifiant de groupe : référence au groupe pour lequel il est demandé de changer 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 allouée par le boîtier de médiation.

cause de l'échec :

- transaction non prise en charge
- agent non autorisé pour cette transaction
- agent non autorisé à changer la durée de vie de ce groupe
- pas de tel groupe
- la durée de vie ne peut être allongée

type de message de notification : Notification d'événement de groupe de règles 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 le raccourcissement de la durée de vie de tous les membres, ou pour demander la fin de toutes les politiques membres (ce qui implique la fin du groupe). La fin 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 celle en cours, le boîtier de médiation vérifie aussi si la durée de vie du groupe peut être allongée et génère un message d’échec approprié si elle ne le peut pas.

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 été changée d’une façon ou d’une autre.

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

0 <= lt_granted <= MINIMUM(lt_requested, lt_maximum)

où
- lt_granted est la durée de vie réellement allouée par le boîtier de médiation
- lt_requested est la durée de vie demandée par l’agent
- lt_maximum est la durée de vie maximum spécifiée à l’établissement de la session

Après avoir envoyé une réponse de succès avec une durée de vie de zéro, le boîtier de médiation mettra fin aux règles de politique membres sans autre notification à l’agent, et considèrera le groupe et tous ses membres comme non existants. Toute transaction ultérieure sur ce groupe de règles de politique ou un de ses membres aura pour résultat 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 du groupe de règles de politique et l’envoi du message de réponse à l’agent demandeur, le boîtier de médiation vérifie s’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 groupe (GL)

nom de transaction : liste de groupe
type de transaction : surveillance
conformité de transaction : facultatif
paramètres de demande :

- identifiant de demande : identifiant unique pour l’agent pour apparier 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 groupe : liste de tous les groupes auxquels l’agent peut accéder. Pour chaque groupe sur la liste, l’identifiant et le propriétaire sont indiqués.

cause de l'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. Habituellement, l'agent a déjà ces informations, mais dans des cas particuliers (par exemple, après défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent d'administration 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, il retourne une liste de tous les groupes auxquels l'agent peut accéder, qui indique l'identifiant et le propriétaire de chaque groupe.

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

2.4.4 Etat 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 pour l'agent pour apparier 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 correspondant à l'identifiant de la demande.
- propriétaire du groupe : identifiant de l'agent qui possède ce groupe de règles de politique.
- durée de vie de groupe : durée de vie restante du groupe. C'est le maximum de durée de vie restante des règles de politique de tous les membres.
- liste de 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 pour le boîtier de médiation.

cause de l'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 d'un groupe. Habituellement, l'agent a déjà ces informations, mais dans des cas particuliers (par exemple, après défaillance d'un agent) ou pour des agents particuliers (par exemple, un agent d'administration 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 demander cette transaction. Si l'une des vérifications échoue, une réponse d'échec appropriée est générée. Autrement, il retourne une liste de tous les membres du groupe qui indique l'identifiant de chaque groupe.

Cette transaction n'a aucun 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 toutes les transactions spécifiées avec leurs paramètres obligatoires. Cependant, les mises en oeuvre concrètes du protocole peuvent ne prendre en charge que certaines des transactions facultatives, et pas toutes. Les transactions qui sont exigées pour la conformité sont différentes pour l'agent et pour le boîtier de médiation.

La présente section contient des déclarations de conformité pour les mises en oeuvre du protocole MIDCOM qui se rapportent à la sémantique. La conformité est spécifiée différemment pour les agents et pour les boîtiers de médiation. Ces déclarations de conformité seront probablement étendues par une spécification concrète de protocole. Cependant, on estime qu'une telle extension ne modifiera la validité d'aucune des déclarations ci-dessous.

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

- Transactions de contrôle de session
  - établissement de session (SE) obligatoire
  - fin de session (ST) obligatoire
  - fin de session asynchrone (AST) obligatoire

- Transactions de règle de politique
  - règle de réserve de politique (PRR) obligatoire
  - règle d'activation de politique (PER) obligatoire
  - changement de durée de vie de règle de politique (RLC) obligatoire
  - liste de règles de politique (PRL) obligatoire
  - état de règle de politique (PRS) obligatoire
  - événement de règle de politique asynchrone (ARE) obligatoire

- Transactions de groupe de règles de politique
  - changement de durée de vie de groupe (GLC) facultatif
  - liste de groupe (GL) facultatif
  - état de groupe (GS) facultatif

3.1 Conformité générale de mise en œuvre

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 des transactions ultérieures.

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 dans chaque transaction tant que les informations contenues sont conservées.

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 facultatifs d'interface interne et externe dans PRR, PER, et PRS doivent être inclus tous deux ou aucun des deux lorsque des règles de politique spécifiques de l'interface sont prises en charge.

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

Une mise en œuvre conforme peut remplacer une seule transaction par un ensemble de transactions plus fines. Dans un tel cas, on doit s'assurer que l'exigence 2.1.4 (comportement déterministe) et l'exigence 2.1.5 (état connu et stable) de [MDC-REQ] sont toujours satisfaites. Lorsqu'une seule transaction est remplacée par un ensemble de plusieurs transactions plus fines, cet ensemble doit être équivalent à une transaction unique. De plus, cet ensemble de transactions doit ensuite satisfaire à l'exigence de granularité mentionnée au paragraphe 2.1.3.

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 de 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 conforme de boîtier de médiation d'un protocole MIDCOM 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 la demande particulière.

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

Une mise en œuvre d'agent conforme d'un protocole MIDCOM ne doit utiliser aucune 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 au sein de la transaction SE.

4 Exemples d’utilisations de transactions

La présente section donne deux exemples d’utilisation des transactions spécifiées à 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 avoir accès dans 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) [RFC3261].

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

Cet exemple suppose qu’une session soit déjà établie. Il montre comment un agent peut déterminer :
- 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.

S’il y a seulement une session unique, ces actions ne sont pas nécessaires, parce que le boîtier de médiation informe les agents 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 la fin intentionnelle d’une session, l’agent peut vouloir rétablir la session et explorer quels sont les groupes et règles de politique qu’il avait établis qui sont toujours en place.

Un système d’agent peut avoir une défaillance et un autre prend sa place. Le nouveau système d’agent a alors besoin de trouver ce qui a déjà été configuré par le système défaillant et ce qui doit encore être fait.

Une troisième situation où il est utile d’explorer les règles de politique et les groupes est le cas où un agent est habilité comme 'administrateur'. Cet agent peut accéder à et modifier toute règle de politique ou groupe créé par tout autre agent.

Tous les agents vont probablement débuter leur exploration par la transaction Liste de groupes (GL), comme indiqué à la Figure 5. Sur cette demande, le boîtier de médiation retourne une liste de paires, contenant chacune un identifiant d’agent et un identifiant de groupe(GID). L’agent est informé de ce à quoi il peut accéder dans son propre groupe et dans les groupes des autres agents.

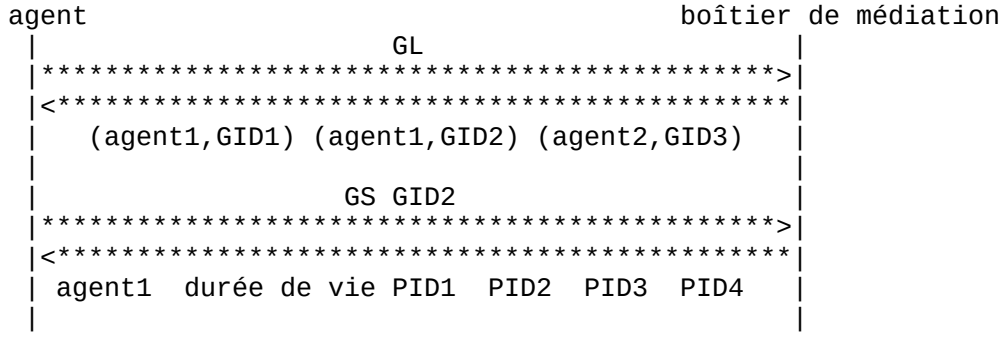

Figure 5: Utilisation de la transaction GL et GS

A la Figure 5, trois groupes sont accessibles à l’agent, et l’agent récupère les informations sur le second groupe en utilisant la transaction État de groupe (GS). Il reçoit le propriétaire 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).

Dans ce qui suit, 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 :

- propriétaire de la règle de politique
- identifiant de groupe
- action de règle de politique (réservé ou activé)
- type de protocole
- gamme de port
- direction
- adresse IP interne
- numéro de port interne
- adresse externe
- numéro de port externe
- adresse IP interne de middlebox
- numéro de port interne de middlebox
- adresse IP externe de middlebox
- numéro de port externe de middlebox
- versions d'adresse IP (non imprimées)
- service de middlebox (non imprimé)
- interface interne et externe (facultatif, non imprimé)

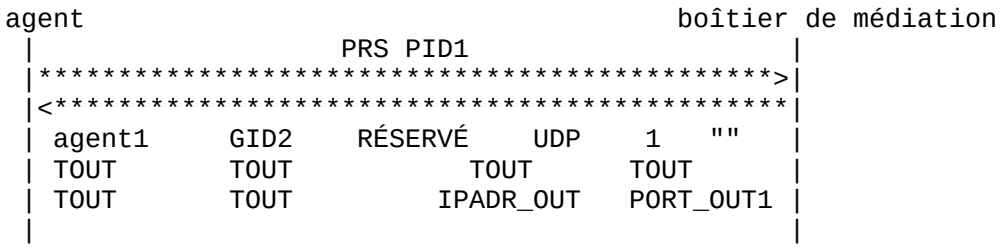

Figure 6 : Rapport d'état pour une réservation externe

Le paramètre 'TOUT' marqué à la Figure 6 sert de marque place dans les réponses d'état de règles de politique pour les règles de réserve de politique. Une règle de politique avec PID1 est une règle de réserve de politique pour le trafic UDP à l'extérieur du boîtier de médiation. Comme c'est une règle de réserve, la direction est vide. Comme il n'y a pas encore d'adresse interne ou externe impliqués, ces quatre champs sont remplacés par des caractères génériques dans la réponse. La même chose est valable pour l'adresse interne de boîtier de médiation et le numéro de port. La seule information d'adresse donnée par la réponse est l'adresse IP externe réservée du boîtier de médiation (IPADDR_OUT) et le numéro de port correspondant (PORT_OUT1). Noter que IPADR_OUT et PORT_OUT1 peuvent n'être pas remplacés par des caractères génériques, car l'action de réserve ne le prend pas en charge.

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 en ce qui concerne Adresse IP, protocole, et numéro de port, mais pour la source externe, le numéro de port est remplacé par des caractères génériques. L'adresse IP et le numéro de port externes du boîtier de médiation sont ce que l'expéditeur externe à besoin d'utiliser comme destination dans le paquet initial qu'il envoie. Au boîtier de médiation, l'adresse de destination est remplacée par l'adresse interne du récepteur final. Durant la traduction d'adresse, l'adresse IP de source et les numéros de port de source

des paquets restent inchangés. Ceci est indiqué par l'adresse interne, qui est identique à l'adresse externe.

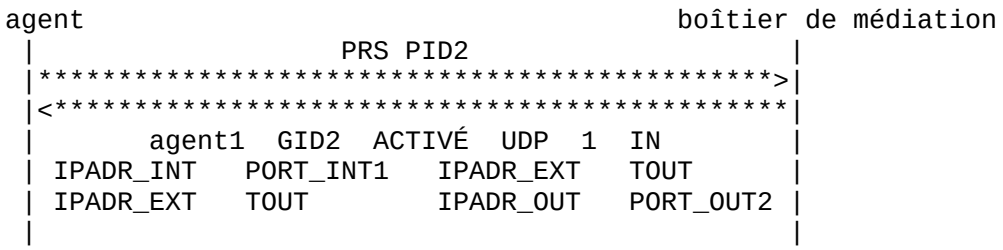

Figure 7: Rapport d'état pour paquets entrants activés

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

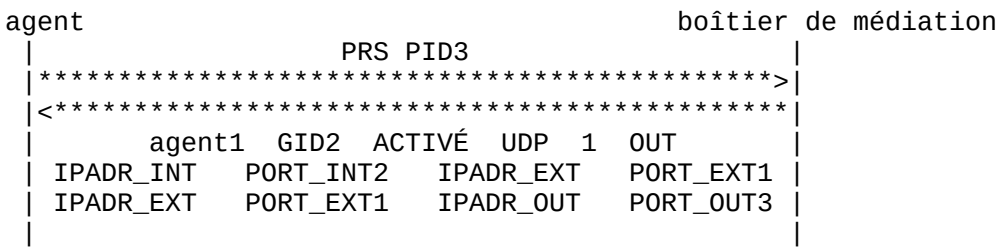

Figure 8: Rapport d'état pour paquets sortants activés

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

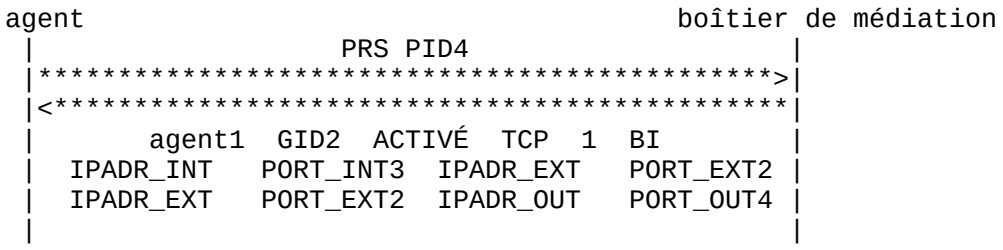

Figure 9: Rapport d'état pour le trafic TCP bidirectionnel

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

4.2 Activation d'un appel signalé SIP

Cet exemple d'utilisation de transaction élaborée montre l'interaction entre un mandataire SIP et un boîtier de médiation. Le boîtier de médiation lui-même est un traditionnel traducteur d'adresse et de port réseau (NAPT, *Network Address and Port Translator*), et deux agents d'utilisateur SIP communiquent l'un avec l'autre via le mandataire SIP et le NAPT, comme indiqué à la Figure 10. L'agent MIDCOM est co-localisé avec le mandataire SIP, et le serveur MIDCOM est au boîtier de médiation. Ainsi donc, le protocole MIDCOM joue entre le mandataire SIP et le boîtier de médiation.

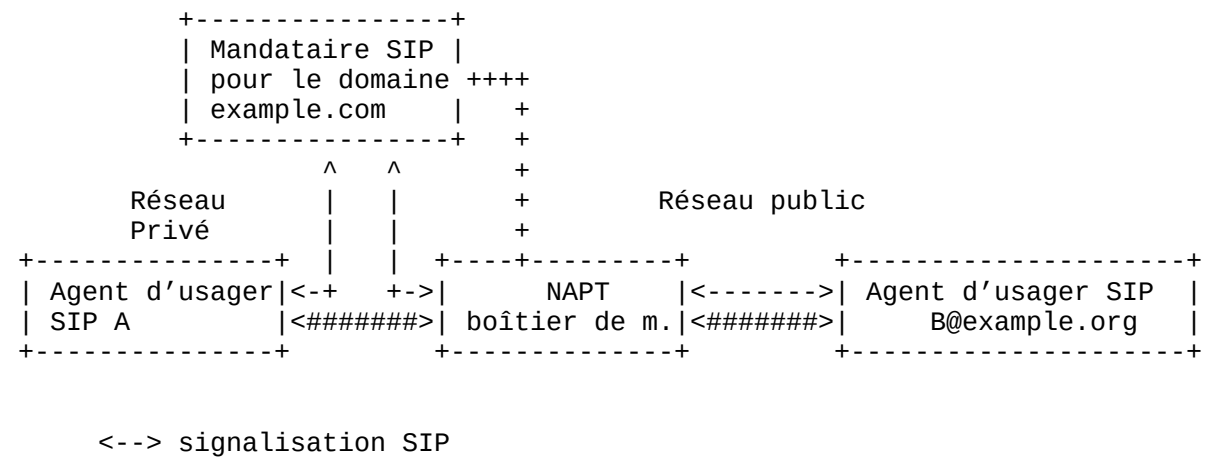

Figure 10: Exemple d'un scénario SIP

Pour les schémas de séquence ci-dessous, on fait les hypothèses suivantes :

- Le NAPT est configuré de façon statique pour transmettre la signalisation SIP depuis l'extérieur jusqu'au serveur mandataire SIP – c'est-à dire que l'adresse IP et le port 5060 externes du NAPT sont transmis au mandataire SIP interne.
- L'agent d'utilisateur SIP A, situé à l'intérieur du réseau privé, est enregistré auprès du mandataire SIP avec son adresse IP privée.
- L'usager A connaît l'URL SIP général de l'usager B. L'URL est B@example.org. Cependant, L'URL concret de l'agent d'usager SIP B, que l'usager B utilise normalement, n'est pas connu.
- Les chemins RTP sont configurés, mais pas les chemins RTCP.
- Le boîtier de médiation et le serveur SIP partagent une session MIDCOM établie.
- Certains paramètres sont omis, comme l'identifiant de demande (RID).

De plus, les abréviations suivantes sont utilisées:

- IP_AI : adresse IP interne de l'agent d'usager A
- P_AI : numéro de port interne de l' agent d'usager A pour recevoir les données RTP
- P_AE : numéro de port transposé externe de l'agent d'usager A
- IP_AE : adresse IP externe du boîtier de médiation
- IP_B : adresse IP de l'agent d'usager B
- P_B : numéro de port de l'agent d'usager B pour recevoir les données RTP
- GID : identifiant de groupe
- PID : identifiant de règle de politique

On trouvera les abréviations des transactions MIDCOM dans les en-têtes des sections concernées.

Dans notre exemple, l'usager A essaye d'appeler l'usager B. L'agent d'usager A envoie un message INVITE SIP au serveur mandataire SIP (voie à la Figure 10). La parité SDP du message SIP particulier

pertinent pour la configuration de boîtier de médiation est indiqué dans le schéma de séquence comme suit :

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

où l'étiquette m est l'étiquette de support qui contient le numéro de port UDP récepteur, et l'étiquette c contient l'adresse IP du terminal qui reçoit le flux de média.

Le message INVITE transmis à l'agent d'usager B doit contenir une adresse IP et un numéro de port publics auxquels l'agent d'utilisateur B puisse envoyer son flux de média RTP. Le mandataire SIP demande une règle d'activation de politique au boîtier de médiation avec une demande PER avec l'adresse IP et le numéro de port de l'agent d'utilisateur B remplacés par des caractères génériques. Comme ni l'adresse IP ni les numéros de port de l'agent d'usager B ne sont connus à ce moment, l'adresse de l'agent d'usager B doit être remplacé par des caractères génériques. Le remplacement par des caractères génériques de l'adresse IP et du numéro de port active la capacité 'early media' mais produit une certaine insécurité, car tout hôte extérieur peut atteindre l'agent d'usager A sur le numéro de port activé à travers le boîtier de médiation.

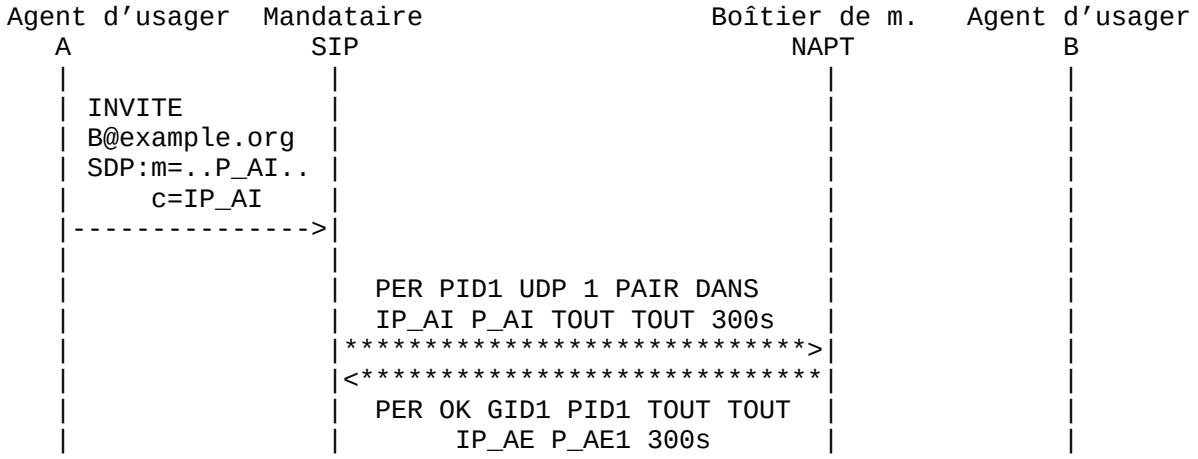

Figure 11: PER avec adresse et numéro de port remplacés par des caractères génériques

Une réponse de PER réussie, comme indiqué à la Figure 11, résulte en une liaison du NAT au boîtier de médiation. Cette liaison permet au trafic UDP provenant de tout hôte extérieur au réseau privé de l'agent d'usager A d'atteindre l'agent d'usager A. Ainsi l'agent d'usager B peut commencer à envoyer du trafic immédiatement après avoir reçu le message INVITE, comme pourrait le faire tout autre hôte – et même des hôtes dont il n'est pas prévu qu'ils participent, comme un hôte hostile.

Si le boîtier de médiation ne prend pas en charge ou ne permet pas le remplacement de l'adresse IP par des caractères génériques pour des raisons de sécurité, la demande PER sera rejetée avec une cause de l'échec appropriée, comme 'caractères génériques IP non pris en charge'. Cependant, le serveur de mandataire SIP a besoin d'une adresse IP et d'un numéro de port extérieurs au boîtier de médiation (le NAPT) afin de transmettre le message SIP INVITE.

Si l'adresse IP de l'agent d'usager B n'est toujours pas connue (elle sera envoyée par l'agent d'usager B dans le message de réponse SIP) et si le remplacement d'adresse IP par des caractères génériques n'est pas permis, le serveur mandataire SIP utilise la transaction PRR.

En utilisant la demande PRR, le serveur mandataire SIP demande une adresse IP et un numéro de port extérieurs (voir la Figure 12) sans déjà établir une liaison NAT ou micro-sas. La demande PRR doit contenir le paramètre de service 'tw' -- c'est-à-dire que l'agent MIDCOM choisit la valeur par défaut. Dans cette configuration, avec un NAPT et sans un NAT double, seule une adresse externe est réservée. Dans la charge utile SDP du message INVITE, le serveur mandataire SIP remplace l'adresse IP et le numéro de port de l'agent d'usager A par l'adresse IP et le port réservés de la réponse PRR (voir la Figure 12). Le message SIP INVITE est transmis à l'agent d'usager B avec un corps SDP modifié qui contient l'adresse et le numéro de port externes, auxquels l'agent d'usager B va envoyer son flux de média RTP.

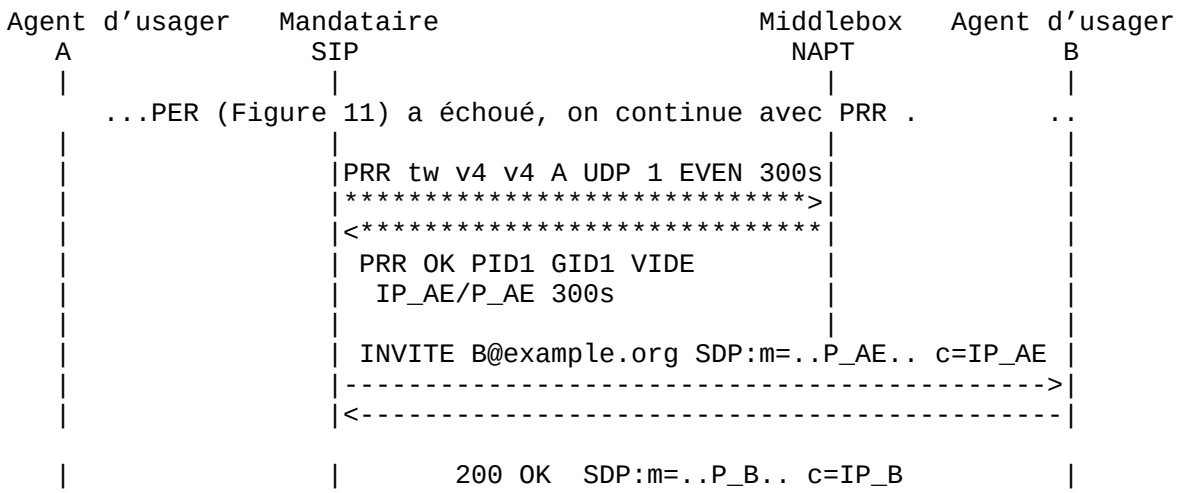

Figure 12: Réservation d'adresse avec une transaction PRR

Cette réponse SIP '200 OK' contient l'adresse IP et le numéro de port auxquels l'agent d'usager B va recevoir un flux de média. L'adresse IP est supposée être égale à l'adresse IP d'où l'agent d'usager B va envoyer son flux de média.

Le serveur mandataire SIP a maintenant des informations suffisantes pour établir la liaison complète du NAT avec une transaction de règle d'activation de politique (PER), c'est-à-dire que les données UDP/RTP de l'appel peuvent passer de l'agent d'usager B à l'agent d'usager 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 de l'agent d'usager A à B doivent aussi être activées. Cela est fait par une seconde transaction PER avec tous les paramètres nécessaires (voir à 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 mandataire SIP peut transmettre le message SIP '200 OK' à l'agent d'usager A pour indiquer que l'appel téléphonique peut commencer.

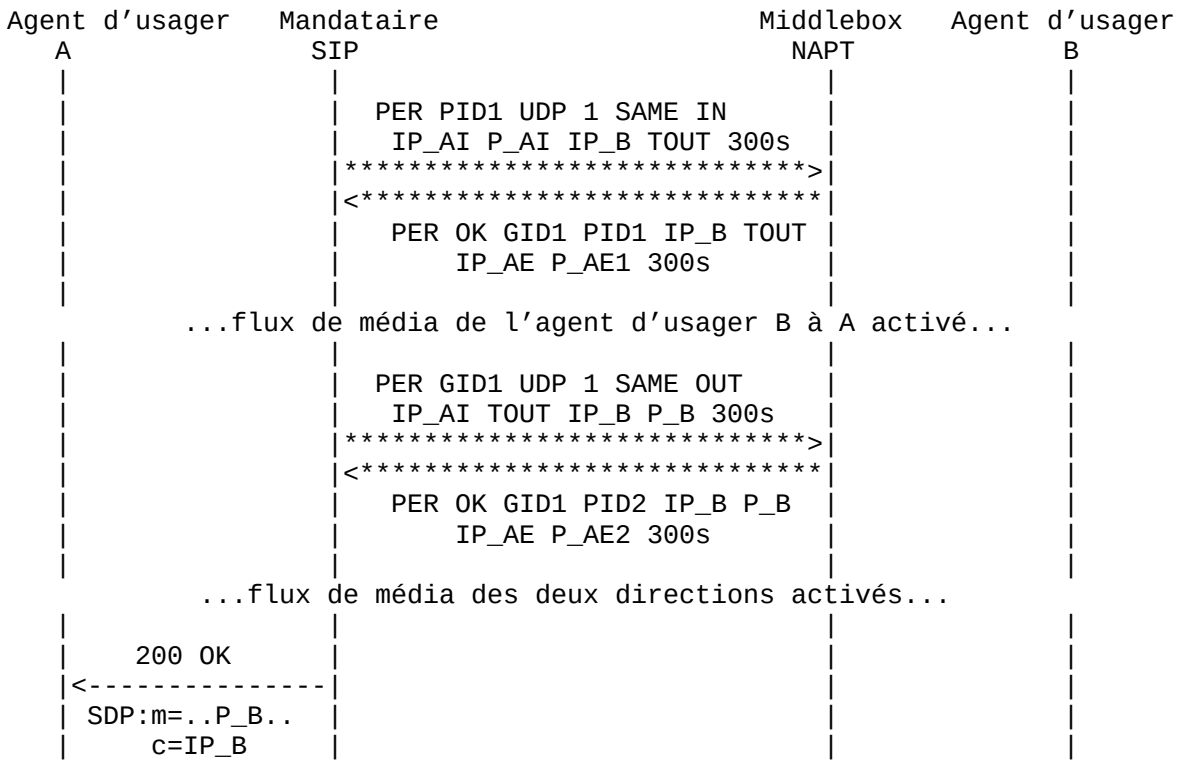

Figure 13 : Etablissement de règle de politique pour flux UDP

L'agent d'usager B décide de terminer l'appel et envoie son message SIP 'BYE' à l'agent d'usager A. Le mandataire SIP transmet tous les messages SIP et termine ensuite le groupe, en utilisant une transaction de changement de durée de vie de groupe (GLC) avec une durée de vie restante demandée de 0 seconde (voir à la Figure 14). La terminaison du groupe inclut la terminaison des règles de politique de tous les membres.

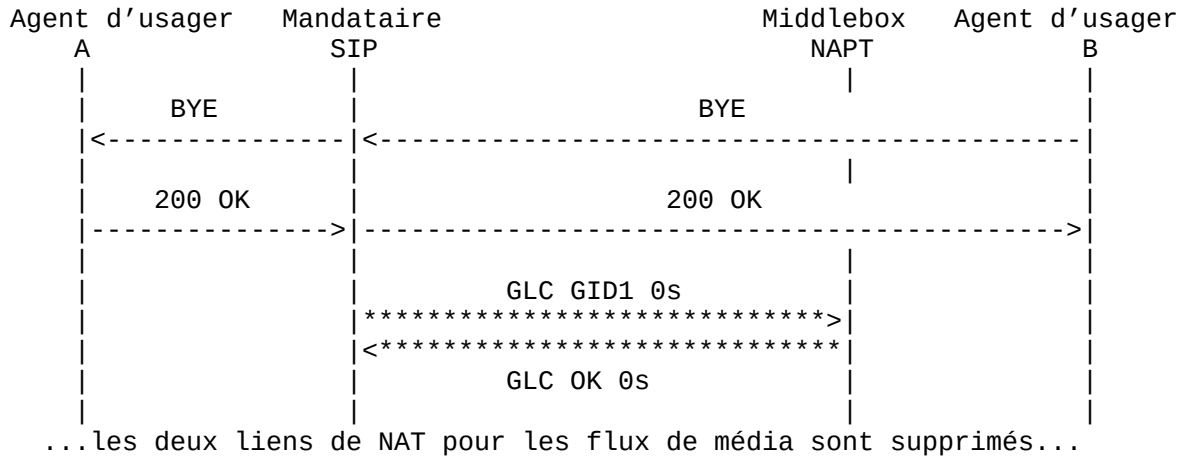

Figure 14 : Terminaison des groupes de règles de politique

5 Conformité aux exigences du MIDCOM

La présente section explique la conformité de la sémantique spécifiée aux exigences MIDCOM. Elle est structurée conformément à [MDC-REQ] :

- conformité aux exigences du mécanisme du protocole (paragraphe 5.1)
- conformité aux exigences de sémantique du protocole (paragraphe 5.2)
- conformité aux exigences de sécurité (paragraphe 5.3)

Les références des exigences sont données par le numéro du paragraphe de leur définition : "exigence x.y.z" se réfère à l'exigence spécifiée au paragraphe x.y.z de [MDC-REQ].

5.1 Exigences du mécanisme du protocole

5.1.1 Association autorisée

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

5.1.2 Un agent se connecte à plusieurs boîtiers de médiation

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

5.1.3 Plusieurs agents se connectent au même boîtier de médiation

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

5.1.4 Comportement déterministe

Il est dit au paragraphe 2.1.2 que le traitement d'une demande d'un agent ne doit pas être interrompu par quelque demande que ce soit, du même ou d'un autre agent. Cela donne la granularité des transactions de demande et évite les conditions de compétition qui résultent en un comportement imprévisible au boîtier de médiation.

Le comportement du boîtier de médiation ne peut être prévisible que 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 des agents.

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

5.1.5 Etat connu et stable

Il est dit au paragraphe 2.1 que les transactions de demande sont uniques l'une par rapport à l'autre et du point de vue d'un agent. Toutes les transactions sont clairement définies comme transitions d'état qui laissent l'état en cours stable et bien défini et entrent dans un nouvel état stable et bien défini ou qui restent dans l'état en cours stable et bien défini. Le paragraphe 2.1 demande clairement que les états intermédiaires ne soient pas stables et ne soit rapportés à aucun 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 faire correspondre de façon univoque chaque réponse à une des demandes qu'il a envoyée au boîtier de médiation, parce que les identifiants de demande uniques pour l'agent sont utilisés à cette fin. Les notifications se comprennent toutes seules d'après leur définition.

De plus, la transaction liste de groupe (paragraphe 2.4.3), la transaction état de groupe (paragraphe 2.4.4), la transaction liste de règle de politique (paragraphe 2.3.11), et la transaction état de règle de politique (paragraphe 2.3.12) permettent à l'agent à tout moment pendant une session de restaurer les informations concernant :

- tous les groupes de règles de politique auxquels il peut accéder,
- les règles de politique membres de tous les groupes accessibles et leur état,
- toutes les règles de politique auxquelles il peut accéder, et
- l'état de toutes les règles de politique accessibles.

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

5.1.6 Rapport d'état

Comme indiqué au paragraphe précédent, le boîtier de médiation informe l'agent sans ambiguïté de chaque transition d'état se rapportant à tout service demandé par l'agent. Ainsi à tout moment l'agent peut restaurer les informations d'état sur toutes les règles de politique et groupes de règles de politique accessibles. Et donc, l'exigence 2.1.6 est satisfaite.

5.1.7 Messages non sollicités (notifications asynchrones)

La sémantique inclut des messages asynchrones de notifications du boîtier de médiation à l'agent, y compris le message Notification de fin de session, le message Notification d'événement de règle de politique (REN), et le message Nnotification d'événement de groupe(GEN) (voir au paragraphe 2.1.2). Ces notifications rapportent chaque changement d'état des règles de politique ou groupes de règles de politique qui n'étaient pas explicitement demandés par l'agent. Et donc, l'exigence 2.1.7 est satisfaite par la sémantique spécifiée ci-dessus.

5.1.8 Authentification mutuelle

Comme spécifiée au paragraphe 2.2.1, la sémantique requiert une authentification mutuelle de l'agent et du boîtier de médiation, en utilisant deux transactions d'établissement de session successives ou une authentification mutuelle fournie à une couche de protocole inférieure. Et donc, l'exigence 2.1.8 est satisfaite.

5.1.9 Terminaison de session par tout un chacun

La spécification de la sémantique établit au paragraphe 2.2.2 que l'agent peut demander la fin de la session en générant la demande de fin de session et que le boîtier de médiation ne peut pas rejeter cette demande. Ensuite, le paragraphe 2.2.3 établit que le boîtier de médiation peut envoyer la notification de fin de session asynchrone à tout moment et terminer ainsi la session. Et donc, l'exigence 2.1.9 est satisfaite.

5.1.10 Résultat de demande

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

5.1.11 Interfonctionnement de versions

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

5.1.12 Traitement déterministe des règles de chevauchement

Les seules actions de règle de politique spécifiées sont 'réservé' et 'activé'. Pour les pare-feu, les actions d'activation ou les actions de réserve en chevauchement ne créent pas de conflit, et donc un pare-feu acceptera toujours les règles de chevauchement comme spécifié au paragraphe 2.3.2 (en supposant que l'autorisation nécessaire soit donnée).

Pour les NAT, réservé et activé peuvent entrer en conflit. Si une demande conflictuelle arrive, elle est rejetée, comme établit au paragraphe 2.3.2. Si une demande en chevauchement arrive et qu'elle n'entre pas en conflit avec celles qu'elle chevauche, elle est acceptée (en supposant que l'autorisation nécessaire 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 Exigences sémantiques du protocole

5.2.1 Syntaxe et sémantique extensibles

L'exigence 2.2.1 demande explicitement l'extensibilité de la syntaxe du protocole. Ceci doit être réglé par la définition de protocole concrète. La spécification de la 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 boîtiers de médiation et que la même règle de politique peut s'appliquer à tous. Et donc, l'exigence 2.2.2 est satisfaite.

5.2.3 Groupes d'ensembles de règles

La sémantique prend explicitement en charge le regroupement des règles et transactions de politique sur les 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 terminaison de toutes les règles de politique qui sont membres du groupe particulier. Et donc, l'exigence 2.2.3 est satisfaite.

5.2.4 Extension de la durée de vie d'une 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. Et donc, l'exigence 2.2.4 est satisfaite.

5.2.5 Modes résistants à l'échec

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 entièrement, et sont soit un succès, soit un échec. Toutes les transactions de demande incluent une liste des causes de l'échec. Ces causes de l'échec incluent l'indication des paramètres invalides le cas échéant. En cas d'échec, une des raisons spécifiées est retournée du boîtier de médiation à l'agent. Et donc, l'exigence 2.2.5 est satisfaite.

5.2.6 Causes d'échec

La sémantique inclut un paramètre cause de l'échec dans chaque réponse d'échec. Et donc, l'exigence 2.2.6 est satisfaite.

5.2.7 Manipulation de la même règle de politique par plusieurs agents

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

Si le boîtier de médiation est suffisamment configurable, son administrateur peut le configurer de telle sorte qu'un agent authentifié soit autorisé à accéder et modifier les règles de politique et groupes de règles possédés par un autre agent. Puisque la sémantique spécifiée ne l'interdit pas, cela satisfait l'exigence 2.2.7.

5.2.8 Portage des règles de filtrage

La transaction de règle d'activation de politique spécifiée au paragraphe 2.3.8 peut porter cinq tuplets de règles de filtrage. Ceci satisfait à l'exigence 2.2.8.

5.2.9 Parité des numéros de port

Comme spécifié au paragraphe 2.3.6, l'agent est capable de demander la conservation de la parité de port lors de la réservation de numéros de port avec la transaction PRR (voir au paragraphe 2.3.8) et lors de l'établissement des liens d'adresse avec la transaction PER (voir au paragraphe 2.3.9). Et donc, l'exigence 2.2.9 est satisfaite.

5.2.10 Gamme consécutive de numéros de port

Comme spécifié au paragraphe 2.3.6, l'agent est à même de demander une gamme de numéros de port consécutifs lors de la réservation de numéros de port avec la transaction PRR (voir au paragraphe 2.3.8) et lors de l'établissement des liens d'adresse ou micro-sas avec la transaction PER (voir au paragraphe 2.3.9). Et donc, l'exigence 2.2.10 est satisfaite.

5.2.11 Chevauchement de règles de politique contradictoires

L'exigence 2.2.11 se fonde sur l'hypothèse que des actions contradictoires de règle de politique, telles que 'activé'/'admis' et 'désactivé'/'non admis' sont prises en charge. En conformité avec les décisions prises par le groupe de travail suite à la finalisation du document décrivant les exigences, celle-ci n'est pas satisfaite par la sémantique parce que aucune action ' désactivé'/'non admis ' n'est prise en charge.

5.3 Exigences de sécurité

5.3.1 Authentification, confidentialité, intégrité

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

5.3.2 Confidentialité facultative des messages de contrôle

L'utilisation d'IPsec ou TLS permet à l'agent et au boîtier de médiation d'utiliser une méthode de codage (y compris l'absence de codage). Et donc, l'exigence 2.3.2 est satisfaite.

5.3.3 Fonctionnement à travers des domaines qui ne sont pas de confiance

Le fonctionnement à travers des domaines qui ne sont pas de confiance est pris en charge par l'authentification mutuelle et par l'utilisation de la protection par TLS ou IPsec. Et donc, l'exigence 2.3.3 est satisfaite.

5.3.4 Atténuation des attaques de rejeu

La sémantique spécifiée atténue les attaques de rejeu et satisfait l'exigence 2.3.4 en obligeant à l'authentification mutuelle de l'agent et du boîtier de médiation, ainsi qu'à l'utilisation de la protection de TLS ou d'IPsec.

Une atténuation supplémentaire peut être fournie au titre de la définition d'un protocole MIDCOM concret -- par exemple, en exigeant des nombres consécutifs croissants pour les identifiants de demande.

6 Considérations sur la sécurité

L'interaction entre un boîtier de médiation et un agent (voir [MDC-FRM]) est un point très sensible pour la sécurité. La configuration des règles de politique à partir d'une entité extérieure à un boîtier de médiation paraît contradictoire par nature à la fonction de boîtier de médiation. Et donc des moyens efficaces doivent être utilisés pour garantir :

- l'authentification mutuelle entre agent et boîtier de médiation,
- l'autorisation,
- l'intégrité du message, et
- la confidentialité du message.

La sémantique définit un mécanisme pour garantir l'authentification mutuelle entre agent et 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 demander une action au boîtier de médiation. La sémantique repose sur des protocoles sous jacents, tels que TLS ou IPsec, pour maintenir l'intégrité du message et la confidentialité des données transférées entre les deux entités.

Pour l'utilisation de TLS et d'Ipsec, les deux côtés doivent utiliser des laissez-passer configurés en toute sécurité pour l' authentification et l'autorisation.

La configuration de règles de politique avec des adresses IP et des numéros de port remplacés par des caractères génériques provoque un certain risque, comme celui d'ouvrir largement les règles de politique possédant des caractères génériques. Une règle de politique possédant un nombre excessif de caractères génériques serait A0 et A3 avec l'adresse IP réglée à 'tout' Adresse IP, par exemple. Ce type de micro-sas rendrait le boîtier de médiation inutile, au sens de la sécurité, car tout paquet pourrait traverser le boîtier de médiation sans autre vérification. La politique locale du boîtier de médiation devrait rejeter de telle demandes d'activation de règle de politique.

Une configuration par défaut raisonnable pour le remplacement par des caractères génériques serait qu'un seul numéro de port puisse être remplacé par des caractères génériques et que toutes les adresses IP doivent être établies sans caractère générique. Cependant, il y a certains cas où la sécurité entre en concurrence avec la fonctionnalité.

L'exemple décrit au paragraphe 4.2 montre comment les appels en signalisation SIP peuvent être traités d'une façon sûre sans caractère générique dans les adresses IP. Mais certaines applications à signalisation SIP peuvent faire usage de média précoces (voir au paragraphe 5.5 of [RFC3398]). Pour recevoir un média précoce, les boîtiers de médiation doivent être configurés avant que le second participant à la session ne soit connu. Comme elle n'est pas connue, l'adresse IP du second participant doit être remplacée par des caractères génériques.

Dans de tels cas et plusieurs autres similaires, il y a une décision de politique de sécurité que doit prendre l'opérateur du boîtier de médiation. L'opérateur peut configurer le boîtier de médiation de telle sorte qu'il prenne en charge plus de fonctionnalités, par exemple, en permettant les adresses IP avec des caractères génériques, ou en faisant en sorte que le fonctionnement du réseau soit plus sûr, par exemple,en interdisant les adresses IP à caractères génériques.

7 Considérations de l'IAB sur UNSAF

La fixation d'auto adressage unilatérale (UNSAF, *UNilateral Self-Address Fixing*) est décrite dans la [RFC3424] comme un processus qui se déroule aux points de terminaison d'origine qui essayent de déterminer ou fixer l'adresse (et le port) par lequel ils sont connus d'un autre point de terminaison. Les propositions d'UNSAF, telles que STUN [RFC3489] sont considérées comme une classe générale de sujets de travail pour la traversée de NAT et comme solutions pour des scénarios sans communication par boîtier de médiation (MIDCOM).

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

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

8 Remerciements

Nous remercions tous ceux qui ont contribué à la discussion sur la sémantique pour le grand nombre de commentaires pertinents qui ont circulé sur la liste des destinataires.

9 Références

9.1 Références normatives

[MDC-FRM] Srisuresh, P., Kuthan, J., Rosenberg, J., Molitor, A., et A. Rayhan, "Middlebox communication architecture and framework"' (*Architecture et cadre de travail de communication par boîtier de médiation*), RFC 3303, août 2002.

[MDC-REQ] Swale, R., Mart, P., Sijben, P., Brim, S., et M. Shore, "Middlebox Communications (MIDCOM) Protocole Requirements" (*Exigences du protocole des communications par boîtier de médiation (MIDCOM*°), RFC 3304, août 2002.

[NAT-TERM] Srisuresh, P. et M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations" (*Terminologie et considérations sur les traducteursd'adresse de réseau IP (NAT)*), RFC 2663, août 1999.

[NAT-TRAD] Srisuresh, P. et K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)" (*Traducteur d'adresse de réseau IP traditionnel (TNAT)*), RFC 3022, janvier 2001.

9.2 Références informatives

[RFC2246] Dierks, T. et C. Allen, "The TLS Protocole Version 1.0", RFC 2246, janvier 1999.

[RFC2402] Kent, S. et R. Atkinson, "IP Authentication Header", RFC 2402, novembre 1998.

[RFC2406] Kent, S. et R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, novembre 1998.

[RFC3198] Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., et S. Waldbusser, "Terminology for Policy-Based Management", RFC 3198, novembre 2001.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., et E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, juin 2002.

[RFC3398] Camarillo, G., Roach, A., Peterson, J., et L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", RFC 3398, décembre 2002.

[RFC3424] Daigle, L. et IAB, "IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation", RFC 3424, novembre 2002.

[RFC3489] Rosenberg, J., Weinberger, J., Huitema, C., et R. Mahy, "STUN - Simple Traversal of User Datagram Protocole (UDP) Through Network Address Translators (NATs)", RFC 3489, mars 2003.

Adresse des auteurs

Martin Stiemerling
NEC Europe Ltd.
Network Laboratories
Kurfuersten-Anlage 36
69115 Heidelberg
Germany
Phone: +49 6221 90511-13
EMail: stiemerling@netlab.nec.de

Juergen Quittek
NEC Europe Ltd.
Network Laboratories
Kurfuersten-Anlage 36
69115 Heidelberg
Germany
Phone: +49 6221 90511-15
EMail: quittek@netlab.nec.de

Tom Taylor
Nortel
1852 Lorraine Avenue
Ottawa, Ontario
Canada K1H 6Z8

Phone: +1 613 763 1496
EMail: taylor@nortel.com

Déclaration de Copyright

Propriété intellectuelle

Remerciement

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