Groupe de travail Réseau
Request for Comments: 3303
Catégorie : Information
août 2002
Traduction Claude Brière de L'Isle

P. Srisuresh, Kuokoa Networks
J. Kuthan, Fraunhofer Institute FOKUS
J. Rosenberg, dynamicsoft
A. Molitor, Aravox Technologies
A. Rayhan, Ryerson University

Architecture et cadre de communication par boîtier de médiation

Résumé
Le principal objectif de ce document est de décrire le cadre sous-jacent des communications par boîtier de médiation (MIDCOM, *middlebox communications*) pour permettre des applications complexes sans raccord à travers les boîtiers de médiation, en utilisant un tiers de confiance. Ce document et le document qui l'accompagne sur les exigences pour MIDCOM ([REQMTS]) ont été créés en préalable à la révision du mandat du groupe de travail MIDCOM.

Il y a dans l'Internet d'aujourd'hui une grande variété d'appareils intermédiaires qui exigent de l'intelligence d'application pour leur fonctionnement. Les datagrammes qui relèvent des applications de flux en temps réel, telles que SIP et H.323, et les applications d'homologue à homologue, telles que Napster et NetMeeting, ne peuvent pas être identifiées simplement en examinant les en-têtes de paquet. Pour leur fonctionnement, les boîtiers de médiation qui mettent en œuvre des services de pare-feu et de traducteur d'adresse réseau incorporent normalement l'intelligence d'application au sein de l'appareil. Le présent document spécifie une architecture et un cadre dans lesquels des tiers de confiance peuvent être délégués pour aider les boîtiers de médiation à effectuer leur travail, sans avoir recours à l'incorporation d'intelligence d'application. Cela va permettre aux boîtiers de médiation de continuer à fournir les services, tout en laissant l'application de boîtier de médiation "agnostique".

1. Introduction

Les appareils intermédiaires qui exigent de l'intelligence d'application sont le sujet de ce document. Ces appareils sont désignés comme des boîtiers de médiation tout au long de ce document. Beaucoup de ces appareils mettent en application des fonctions spécifiques fondées sur une politique, comme le filtrage des paquets, le tunnelage de réseau virtuel privé (VPN, *Virtual Private Network*), la détection d'intrusion, la sécurité et ainsi de suite. D'un autre côté, le service de traducteur d'adresse réseau (NAT, *Network Address Translator*) procure la transparence de l'acheminement à travers les domaines d'adresse (au sein de réseau d'acheminement IPv4 ou à travers des domaines d'acheminement V4 et V6) indépendamment des applications. Les passerelles de niveau d'application (ALG, *Application Level Gateway*) sont utilisées en conjonction avec les NAT pour examiner et facultativement modifier la charge utile d'application de sorte que le comportement de bout en bout de l'application reste inchangé pour la plupart des applications qui traversent les boîtiers de médiation NAT. Il peut y avoir d'autres types de services qui exigent pour leur fonctionnement d'incorporer de l'intelligence d'application dans les boîtiers de médiation. Le domaine d'application de l'exposé de ce document est cependant limité aux services de pare-feu et de NAT. Néanmoins, le cadre MIDCOM est conçu comme extensible à la prise en charge du déploiement de nouveaux services.

Un étroit couplage de l'intelligence d'application avec les boîtiers de médiation rend la maintenance de ceux-ci difficile avec l'arrivée de nouvelles applications. L'intelligence incorporée dans les applications exige normalement des mises à jour des systèmes d'exploitation avec les nouvelles applications ou les plus récentes versions des applications existantes. Les opérateurs qui exigent la prise en charge d'applications plus récentes ne seront pas capables d'utiliser les logiciels/matériels tiers spécifiques des applications et seront à la merci de leurs fabricants de boîtiers de médiation pour faire les mises à niveau nécessaires. De plus l'intelligence incorporée pour un grand nombre de protocoles d'application au sein du même boîtier de médiation augmente sa complexité et favorisera vraisemblablement les erreurs et la dégradation des performances.

Le présent document décrit un cadre dans lequel l'intelligence d'application peut être déplacée des boîtiers de médiation à des agents MIDCOM externes. L'idée de base du cadre proposé est d'imaginer un protocole MIDCOM indépendant de l'application, de sorte que les boîtiers de médiation puissent rester focalisés sur des services comme le pare-feu et le NAT. Le document cadre comporte des exigences explicites et implicites pour le protocole MIDCOM. Cependant, il faut noter que ces exigences sont seulement un sous-ensemble. Un document d'exigences distinct fait la liste détaillée des exigences.

Les agents MIDCOM qui ont de l'intelligence d'application peuvent aider les boîtiers de médiation à travers le protocole MIDCOM en permettant des applications telles que FTP, SIP et H.323. La communication entre un agent MIDCOM et un boîtier de médiation ne sera pas remarquée de l'hôte d'extrémité qui prend part à l'application, à moins qu'un des hôtes d'extrémité joue le rôle d'un agent MIDCOM. La découverte des boîtiers de médiation ou des agents MIDCOM dans le chemin d'une instance d'application sort du domaine d'application du présent document. De plus, toute communication entre les boîtiers de médiation est aussi en dehors du domaine d'application de ce document.

Le présent document décrit le cadre dans lequel prennent place les communications de boîtiers de médiation et les divers éléments qui constituent le cadre. La Section 2 décrit les termes utilisés dans le document. La Section 3 définit le cadre architectural d'un boîtier de médiation pour la communication avec les agents MIDCOM. Les sections restantes couvrent les composants du cadre, illustrant l'utilisation d'exemples de flux, et les considérations de fonctionnement avec l'architecture MIDCOM. La Section 4 décrit la nature du protocole MIDCOM. La Section 5 identifie les entités qui pourraient éventuellement héberger la fonction d'agent MIDCOM. La Section 6 examine le rôle d'un serveur de politique et sa fonction à l'égard des politiques d'autorisation de communication des agents MIDCOM. La Section 7 est une illustration des flux SIP qui utilisent le cadre MIDCOM dans lequel l'agent MIDCOM est co-résident sur un serveur mandataire SIP. La Section 8 traite des considérations de fonctionnement pour le développement d'un protocole adhérant au cadre décrit ici. La Section 9 est une déclaration d'applicabilité visant la localisation des boîtiers de médiation. La Section 11 souligne les considérations pour la sécurité au sujet des boîtiers de médiation dans la perspective du cadre MIDCOM.

2 Terminologie

Ci-dessous figurent les définitions des termes utilisés dans le reste du document.

2.1 Fonction/service de boîtier de médiation

Une fonction ou service de boîtier de médiation est une opération ou méthode effectuée par un intermédiaire du réseau qui peut exiger une intelligence spécifique de l'application pour son fonctionnement. Le filtrage des paquets fondé sur une politique (autrement dit, un pare-feu), la traduction d'adresse réseau (NAT), la détection d'intrusion, l'équilibrage de charge, le tunnelage fondé sur une politique et la sécurité IPsec sont des exemples d'une fonction (ou service) de boîtier de médiation.

2.2 Boîtier de médiation

Un boîtier de médiation *(middlebox)* est un appareil intermédiaire du réseau qui met en œuvre un ou plusieurs des services de boîtier de médiation. Un boîtier de médiation NAT est un boîtier de médiation qui met en œuvre un service de traduction d'adresse réseau. Un boîtier de médiation pare-feu est un boîtier de médiation qui met en œuvre un service de pare-feu.

Les boîtiers de médiation traditionnels incorporent de l'intelligence d'application dans l'appareil pour prendre en charge la traversée d'applications spécifiques. Les boîtiers de médiation qui prennent en charge le protocole MIDCOM seront capables d'externaliser l'intelligence d'application dans les agents MIDCOM. En réalité, certains des boîtiers de médiation peuvent continuer d'incorporer de l'intelligence d'application pour certaines applications et dépendre du protocole MIDCOM et des agents MIDCOM pour la prise en charge des applications restantes.

2.3 Pare-feu

Un pare-feu est une fonction de boîtier de médiation qui filtre les paquets sur la base d'une politique, normalement utilisée pour restreindre l'accès de/vers des appareils et applications spécifiques. Les politiques sont souvent appelées des listes de contrôle d'accès (ACL, *Access Control List*).

2.4 NAT

La traduction d'adresse réseau est une méthode par laquelle les adresses IP sont transposées d'un domaine d'adresses à un autre, fournissant un acheminement transparent pour les hôtes d'extrémité. Ici, acheminement transparent se réfère à la modification des adresses des nœuds d'extrémité en cours de route et au maintien d'état pour ces mises à jour de telle sorte que lorsque un datagramme quitte un domaine pour entrer dans un autre, les datagrammes qui appartiennent à une session sont transmis au bon hôte d'extrémité dans l'autre domaine. Voir dans [NAT-TERM] la définition de acheminement transparent, des divers types de NAT, et des termes associés utilisés. Deux types de NAT sont les plus courants. Le NAT de base, où une seule adresse IP des paquets (et les sommes de contrôle IP, TCP/UDP, pertinentes) est modifiée, et le traducteur d'accès d'adresse réseau (NAPT, *Network Address Port Translator*) où sont modifiées à la fois l'adresse et l'identifiant de couche transport, tel qu'un accès TCP/UDP (et les sommes de contrôle IP, TCP/UDP, pertinentes).

Dans le présent document, le terme NAT est très similaire au NAT IPv4 décrit dans [NAT-TERM], mais il est étendu au-delà des réseaux IPv4 pour inclure le NAT-PT IPv4-v6 décrit dans [NAT-PT]. Alors que le NAT IPv4 [NAT-TERM] traduit une adresse IPv4 en une autre adresse IPv4 pour fournir l'acheminement entre un domaine d'adresse v4 privé et un domaine d'adresse v4 externe, le NAT-PT IPv4-v6 [NAT-PT] traduit une adresse IPv4 en une adresse IPv6, et vice versa, pour fournir l'acheminement entre un domaine d'adresse v6 et un domaine d'adresse v4 externe.

Sauf spécification contraire, dans le présent document, NAT est une fonction de boîtier de médiation qui se réfère à la fois au NAT IPv4 qu'au NAT-PT IPv4-v6.

2.5 Mandataire

Un mandataire est un agent de relais intermédiaire entre les clients et les serveurs d'une application, relayant les messages de l'application entre eux. Les mandataires utilisent des mécanismes de protocole spéciaux pour communiquer avec les clients de mandataires et relayer les données de client aux serveurs et vice versa. Un mandataire termine les sessions avec le client et avec le serveur, agissant comme serveur pour le client d'hôte d'extrémité et comme client pour le serveur d'hôte d'extrémité.

Les applications telles que FTP, SIP, et RTSP utilisent une session de contrôle pour établir les sessions de données. Ces sessions de contrôle et de données peuvent prendre des chemins divergents. Bien qu'un mandataire puisse intercepter les sessions de contrôle et de données, il peut n'intercepter que la session de contrôle. C'est souvent le cas avec les applications de flux en direct telles que SIP et RTSP.

2.6 ALG

Les passerelles de niveau application (ALG, *Application Level Gateway*) sont des entités qui possèdent l'intelligence d'application spécifique et la connaissance d'une fonction de boîtier de médiation associée. Une ALG examine le trafic d'application en transit et aide le boîtier de médiation à remplir sa fonction.

Une ALG peut co-résider avec un boîtier de médiation ou résider à l'extérieur, communiquant à travers un protocole de communication de boîtier de médiation. Elle interagit avec un boîtier de médiation pour régler l'état, accéder aux filtres de contrôle, utiliser les informations d'état du boîtier de médiation, modifier une charge utile spécifique d'application, ou effectuer tout ce qui sera nécessaire pour permettre à l'application de fonctionner à travers le boîtier de médiation.

Les ALG sont différentes des mandataires. Les ALG ne sont pas visibles des hôtes d'extrémité, à la différence des mandataires qui sont des agents de relais qui terminent les sessions avec les deux hôtes d'extrémité. Les ALG ne terminent pas les sessions avec l'un et l'autre hôte d'extrémité. Au lieu de cela les ALG examinent, et facultativement modifient, le contenu de la charge utile d'application pour faciliter le flux du trafic d'application à travers un boîtier de médiation. Les ALG sont centrées sur le boîtier de médiation, en ce qu'elles assistent les boîtiers de médiation à accomplir leur fonction, tandis que les mandataires agissent comme point focal pour les serveurs d'application en relayant le trafic entre clients et serveurs d'application.

Les ALG sont similaires aux mandataires, en ce que ALG et mandataires facilitent tous deux la communication spécifique d'application entre clients et serveurs.

2.7 Hôtes d'extrémité

Les hôtes d'extrémité sont des entités qui font partie d'une instance d'application sur le réseau. Les hôtes d'extrémité auxquels on se réfère dans ce document sont spécifiquement ceux qui terminent une application de flux vocal en temps réel sur IP, telles que SIP et H.323, et des applications d'homologue à homologue telles que Napster et NetMeeting.

2.8 Agents MIDCOM

Les agents MIDCOM sont des entités qui effectuent des fonctions d'ALG, logiquement externes à un boîtier de médiation. Les agents MIDCOM possèdent une combinaison de prise en compte des exigences de l'application et de connaissance de la fonction de boîtier de médiation. Cette combinaison rend les agents capables de faciliter la traversée des boîtier de médiation par les paquets de l'application. Un agent MIDCOM peut interagir avec un ou plusieurs boîtiers de médiation.

Seuls les "agents MIDCOM dans le chemin" sont pris en considération dans le présent document. Les agents MIDCOM dans le chemin sont ceux qui se trouvent sur le chemin des datagrammes que l'agent a besoin d'examiner et/ou modifier en remplissant son rôle d'agent MIDCOM. "Dans le chemin" signifie simplement ici que les paquets en question s'écoulent à travers le nœud qui héberge l'agent. Les paquets peuvent être adressés au nœud d'agent à la couche IP. Autrement, ils peuvent n'être pas adressés au nœud d'agent, mais être contraints par d'autres facteurs de s'écouler à travers lui. En fait, cela n'a aucune importance pour le protocole MIDCOM. Certains exemples d'agents MIDCOM dans le chemin sont des mandataires d'application, des passerelles, ou même des hôtes d'extrémité qui font partie de l'application.

Les agents qui ne résident pas sur les nœuds qui sont dans le chemin de leurs flux d'application pertinents sont appelés agents MIDCOM "hors du chemin" (OOP, *out-of-path*) et sortent du domaine d'application de ce document.

2.9 PDP MIDCOM

Un point de décision de politique (PDP, *Policy Decision Point*) MIDCOM est principalement un point de décision politique, tel que défini dans [POL-TERM] ; et il agit aussi comme dépositaire de politiques, détenant les profils de politiques qui se rapportent à MIDCOM afin de prendre des décisions d'autorisation. [POL-TERM] définit un PDP comme "une entité logique qui prend des décisions de politique pour elle-même ou pour d'autres éléments de réseau qui demandent de telles décisions" ; un dépositaire de politiques est "une mémoire de données spécifiques qui détient les règles de politique, leurs conditions et actions, et les données de politique qui s'y rapportent".

Un boîtier de médiation et un PDP MIDCOM peuvent communiquer plus avant si la politique du PDP MIDCOM change ou si un boîtier de médiation a besoin d'informations supplémentaires. Le PDP MIDCOM peut, à tout moment, notifier au boîtier de médiation de mettre un terme à l'autorisation d'un agent.

Le protocole qui facilite la communication entre un boîtier de médiation et un PDP MIDCOM n'a pas besoin de faire partie du protocole MIDCOM. La Section 6 de ce document traite de l'interface de PDP MIDCOM et du cadre du protocole indépendamment du cadre MIDCOM.

Les données de politique et l'interface de politique spécifiques d'une application entre un agent ou point d'extrémité d'application et un PDP MIDCOM sont en dehors des limites de ce document. Les questions de PDP MIDCOM traitées dans le présent document se focalisent sur un niveau de domaine agrégé qui convient au boîtier de médiation. Par exemple, un agent MIDCOM SIP peut choisir d'interroger un PDP MIDCOM sur le domaine administratif (ou d'entreprise) pour trouver si un certain utilisateur est autorisé à passer un appel sortant. Ce type de données de politique spécifique de l'application, qui convient à l'utilisateur final, sort des limites du PDP MIDCOM examiné dans le présent document. Il est cependant du ressort du PDP MIDCOM de spécifier les applications spécifiques de l'utilisateur final (ou leurs tuplets) qui sont autorisées à être une ALG.

2.10 Protocole de communication de boîtier de médiation (MIDCOM)

Le protocole entre un agent MIDCOM et un boîtier de médiation permet à l'agent MIDCOM d'invoquer les services du boîtier de médiation et permet au boîtier de médiation de déléguer un traitement spécifique de l'application à l'agent MIDCOM. Le protocole MIDCOM permet au boîtier de médiation d'effectuer ses opérations avec l'aide des agents MIDCOM, sans faire appel à une intelligence d'application incorporée. La principale motivation derrière l'architecture de ce protocole est de rendre possibles des applications complexes au travers de boîtiers de médiation, en utilisant un tiers de confiance , c'est-à-dire un agent MIDCOM, sans rupture dans le déroulement du processus.

Ce protocole reste encore à concevoir.

2.11 Enregistrement d'agent MIDCOM

On définit un enregistrement d'agent MIDCOM comme un processus d'approvisionnement des informations de profil de l'agent au boîtier de médiation ou au PDP MIDCOM. L'enregistrement d'agent MIDCOM est souvent une opération manuelle effectuée par un opérateur plutôt que par l'agent lui-même.

Un profil d'agent MIDCOM peut comporter la politique d'autorisation de l'agent (c'est-à-dire les tuplets de session pour lesquels l'agent est autorisé à agir comme ALG), l'entité d'hébergement de l'agent (par exemple, mandataire, passerelle, ou hôte d'extrémité) qui héberge l'agent, le profil d'accessibilité de l'agent (y compris toute information d'authentification au niveau de l'hôte) et les profils de sécurité (pour les messages échangés entre le boîtier de médiation et l'agent).

2.12 Session MIDCOM

Une session MIDCOM se définit comme une association durable entre un agent MIDCOM et un boîtier de médiation. La session MIDCOM n'est pas supposée impliquer de protocole spécifique de couche transport. Précisément, cela ne devrait pas être construit comme se référant à un protocole TCP orienté connexion.

2.13 Filtre

Un filtre est un ensemble d'informations correspondant à un paquet qui identifie un ensemble de paquets à traiter d'une certaine façon par un boîtier de médiation. Cette définition est cohérente avec [POL-TERM], qui définit un filtre comme "Un ensemble de termes et/ou critères utilisés pour séparer ou catégoriser. C'est accompli via la correspondance d'un seul ou de plusieurs champs d'en-tête de trafic et/ou de données de charge utile".

La spécification d'un quintuplet de paquets dans le cas d'un pare-feu et la spécification d'un quintuplet d'une session dans le cas d'une fonction de boîtier de médiation NAT sont des exemples de filtre.

2.14 Action de politique (ou action)

Une action de politique (ou action) est une description du traitement/service du boîtier de médiation à appliquer à un ensemble de paquets. Cette définition est cohérente avec celle de [POL-TERM], qui définit une action de politique comme la "définition de ce qui est fait pour mettre en application une règle de politique, lorsque les conditions de la règle sont satisfaites. Les actions de politique peuvent résulter en l'exécution d'une ou plusieurs opérations pour affecter et/ou configurer le trafic réseau et les ressources du réseau".

L'action de NAT Address-BIND (ou Port-BIND dans le cas de NAPT) et l'action permet/refuse de pare-feu sont des exemples d'action.

2.15 Règle de politique

C'est la combinaison d'un ou plusieurs filtres et d'une ou plusieurs actions. Les paquets qui correspondent à un filtre sont à traiter comme spécifié par la ou les actions associées. Les règles de politique peuvent aussi contenir des attributs auxiliaires tels qu'un type de règle individuelle, des valeurs de temporisation, un agent de création, etc.

Les règles de politique sont communiquées par le protocole MIDCOM.

3 Cadre architectural pour les boîtiers de médiation

Un boîtier de médiation peut mettre en œuvre une ou plusieurs des fonctions de boîtier de médiation de façon sélective sur plusieurs interfaces de l'appareil. Il peut y avoir divers agents MIDCOM qui s'interfacent avec le boîtier de médiation pour communiquer avec une ou plusieurs des fonctions du boîtier de médiation sur une interface. À ce titre, le protocole de communication du boîtier de médiation doit permettre des communications choisies entre un agent MIDCOM spécifique et une ou plusieurs fonctions de boîtier de médiation sur l'interface. Le diagramme qui suit identifie une mise en couche possible du service pris en charge par un boîtier de médiation et une liste des agents MIDCOM qui peuvent interagir avec lui.

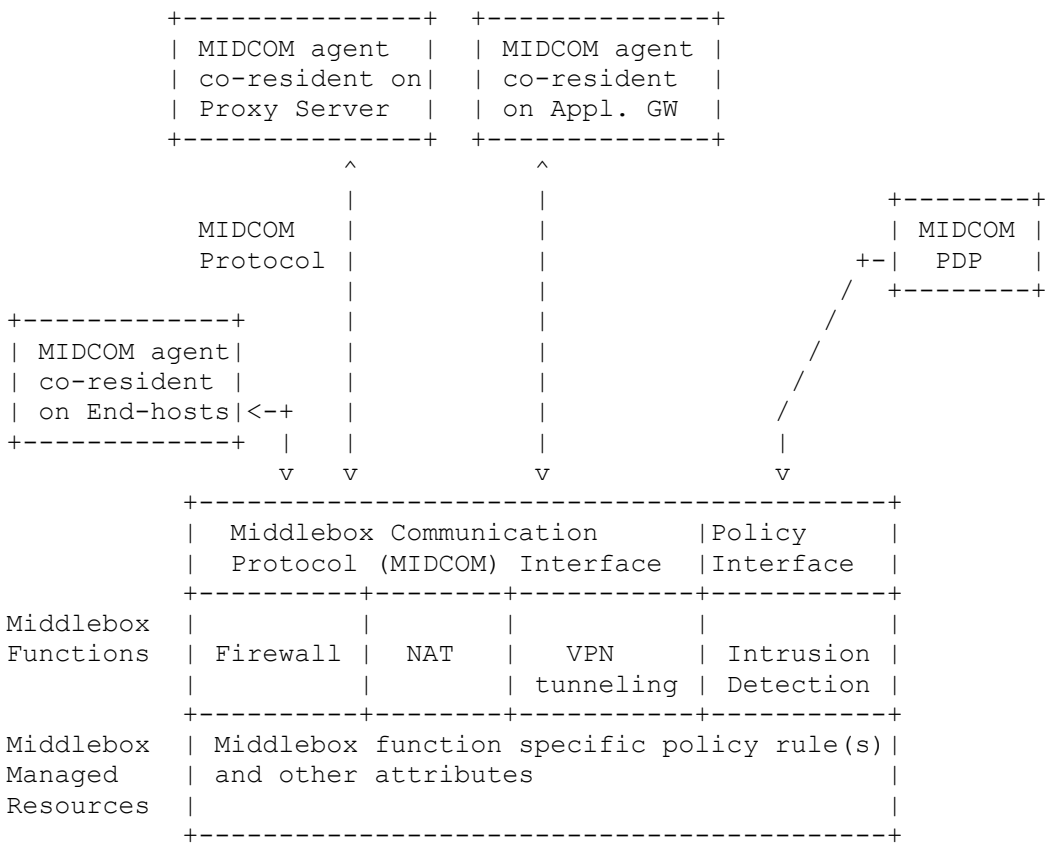


Figure 1 : agents MIDCOM en interface avec un boîtier de médiation

Les ACL de pare-feu, les NAT-BIND, les transpositions d'adresse et les états de session de NAT sont quelques unes des règles de politique spécifiques des fonctions de boîtier de médiation. Un état de session peut inclure des attributs spécifiques d'une fonction de boîtier de médiation, tels que des valeurs de temporisation, des paramètres de traduction de NAT (c'est-à-dire, des NAT-BIND), et ainsi de suite. Un état de session peut être partagé entre des fonctions de boîtier de médiation, un état de session peut être créé par une fonction, et terminé par une fonction différente. Par exemple, un état de session peut être créé par la fonction pare-feu mais terminé par la fonction NAT lorsque un temporisateur de session arrive à expiration.

Les agents MIDCOM spécifiques d'une application (co-résidents sur le boîtier de médiation ou externes au boîtier de médiation) vont examiner les datagrammes IP et aider à identifier l'application à laquelle appartient le datagramme, et assister le boîtier de médiation pour effectuer des fonctions uniques pour l'application et le service du boîtier de médiation. Par exemple, un agent MIDCOM, qui assiste un boîtier de médiation NAT, pourrait effectuer des traductions de charge utile, tandis qu'un agent MIDCOM qui assiste un boîtier de médiation pare-feu pourrait demander au pare-feu de permettre l'accès à du trafic de session, généré de façon dynamique spécifique de l'application.

4 Protocole MIDCOM

Le protocole MIDCOM entre un agent MIDCOM et un boîtier de médiation permet à l'agent MIDCOM d'invoquer les services du boîtier de médiation et permet au boîtier de médiation de déléguer le processus spécifique de l'application à l'agent MIDCOM. Le protocole va permettre aux agents MIDCOM de signaler les boîtiers de médiation, de laisser des applications complexes utilisant des sessions fondées sur l'accès dynamique passer à travers elles (c'est-à-dire, des boîtiers de médiation) sans interruption de flux.

Il est important de noter qu'un agent et un boîtier de médiation peuvent être sur le même appareil physique. Dans un tel cas, ils peuvent communiquer en utilisant des formats de message du protocole MIDCOM, mais en utilisant un transport non fondé sur IP, tel que l'échange de messages IPC, ou bien; ils peuvent communiquer en utilisant une API/DLL bien définie, ou bien, l'intelligence d'application est complètement incorporée dans le service de boîtier de médiation (comme cela se fait aujourd'hui dans de nombreux appareils de pare-feu et de NAT d'inspection à états pleins).

Le protocole MIDCOM consistera en une phase d'établissement de session, une phase de fonctionnement de la session, et une phase de terminaison de la session.

L'établissement de session doit être précédé par l'enregistrement de l'agent MIDCOM auprès du boîtier de médiation ou du PDP MIDCOM. Le profil d'accès et d'autorisation de l'agent MIDCOM peut être préconfiguré sur le boîtier de médiation ou figurer sur la liste d'un PDP MIDCOM que le boîtier de médiation est configuré pour consulter. MIDCOM devra être un protocole client-serveur, initié par l'agent.

Une session MIDCOM peut être terminée par l'une des deux parties. Une terminaison de session MIDCOM peut aussi être déclanchée par (a) le boîtier de médiation ou l'agent qui quitte le service et ne sera pas disponible pour des opérations MIDCOM ultérieures, ou (b) par le PDP MIDCOM qui notifie au boîtier de médiation qu'un agent MIDCOM particulier n'est plus autorisé.

Les données du protocole MIDCOM échangées durant la période de fonctionnement sont gouvernées principalement par les services du boîtier de médiation que le protocole prend en charge. Les services de boîtier de médiation de pare-feu et de NAT sont examinés dans le présent document. Néanmoins, le cadre MIDCOM est conçu pour être extensible et aussi bien prendre en charge le développement d'autres services.

5 Agents MIDCOM

Les agents MIDCOM sont des entités logiques qui peuvent résider physiquement sur des nœuds externes à un boîtier de médiation, possédant une combinaison d'expérience de l'application et de connaissance de la fonction du boîtier de médiation. Un agent MIDCOM peut communiquer avec un ou plusieurs boîtiers de médiation. Les questions d'agent de découverte de boîtiers de médiation, ou vice versa *(sic)*, sortent du domaine d'application du présent document. Celui–ci se focalise sur le cadre dans lequel un agent MIDCOM communique avec un boîtier de médiation en utilisant un protocole MIDCOM, qui est encore à imaginer. Précisément, l'accent est mis sur les seuls agents dans le chemin.

Les agents MIDCOM dans le chemin sont des agents MIDCOM qui sont localisés naturellement au sein du chemin du message de la ou des applications auxquelles ils sont associés. Les applications de faisceaux de sessions, telles que H.323, SIP, et RTSP qui ont des sessions séparées de contrôle et de données, peuvent avoir leurs sessions qui prennent des chemins divergents. Dans ces scénarios, Les agents MIDCOM dans le chemin sont ceux qui se trouvent eux-mêmes dans le chemin de contrôle. Dans une majorité de cas, un boîtier de médiation va vraisemblablement exiger l'assistance d'un seul agent pour une application dans le seul chemin de contrôle. Cependant, il est possible qu'une fonction de boîtier de médiation, ou une application spécifique traversent le boîtier de médiation puisse exiger l'intervention de plus d'un seul agent MIDCOM pour la même application, une pour chaque sous-session de l'application.

Les mandataires et passerelles d'application sont un bon choix pour les agents MIDCOM dans le chemin, car ces entités sont par définition dans le chemin d'une application entre un client et un serveur. En plus d'héberger la fonction d'agent MIDCOM, ces entités spécifiques d'une application qui sont d'origine dans le chemin peuvent aussi mettre en application localement des choix spécifiques d'application, tels que l'abandon des messages infectés par des virus connus, ou qui n'ont pas d'authentification d'utilisateur. Ces entités peuvent s'interposer aussi bien dans des sessions de contrôle que de données. Par exemple, les sessions FTP de contrôle et de données sont interceptées par un serveur mandataire FTP.

Cependant, les mandataires peuvent aussi n'intercepter que la session de contrôle et non les sessions de données, comme c'est le cas avec les applications de flux en direct, telles que SIP et RTSP. Noter que les applications peuvent ne pas toujours traverser un mandataire et certaines applications peuvent n'avoir pas de serveur mandataire disponible.

Les mandataires SIP et les portiers H.323 peuvent être utilisés pour héberger des fonctions d'agent MIDCOM pour contrôler des boîtiers de médiation qui mettent en œuvre des fonctions de pare-feu et de NAT. L'avantage d'utiliser des entités dans le chemin, par opposition à la création d'un agent entièrement nouveau, est que l'entité dans le chemin possède l'intelligence d'application. Vous aurez seulement besoin d'activer l'utilisation du protocole MIDCOM pour être un agent MIDCOM efficace. La Figure 2 ci-dessous illustre un scénario où les agents MIDCOM dans le chemin font l'interface avec le boîtier de médiation. Disons que le PDP MIDCOM a pré configuré les mandataires dans le chemin comme agents MIDCOM de confiance sur le boîtier de médiation et que le filtre de paquet met en œuvre une politique de filtrage de paquet de "refus par défaut". Les mandataires utilisent leur connaissance de l'intelligence de l'application pour contrôler la fonction de pare-feu et permettre de façon sélective à un certain nombre de sessions de flux vocaux d'utiliser de façon dynamique le protocole MIDCOM.

Dans l'illustration ci-dessous, les mandataires et le PDP MIDCOM sont montrés à l'intérieur d'un domaine privé. L'intention est cependant de ne pas sous-entendre qu'ils sont seuls à l'intérieur des frontières privées. Les mandataires peuvent aussi résider à l'extérieur du domaine. La seule exigence est qu'il y ait une relation de confiance avec le boîtier de médiation.

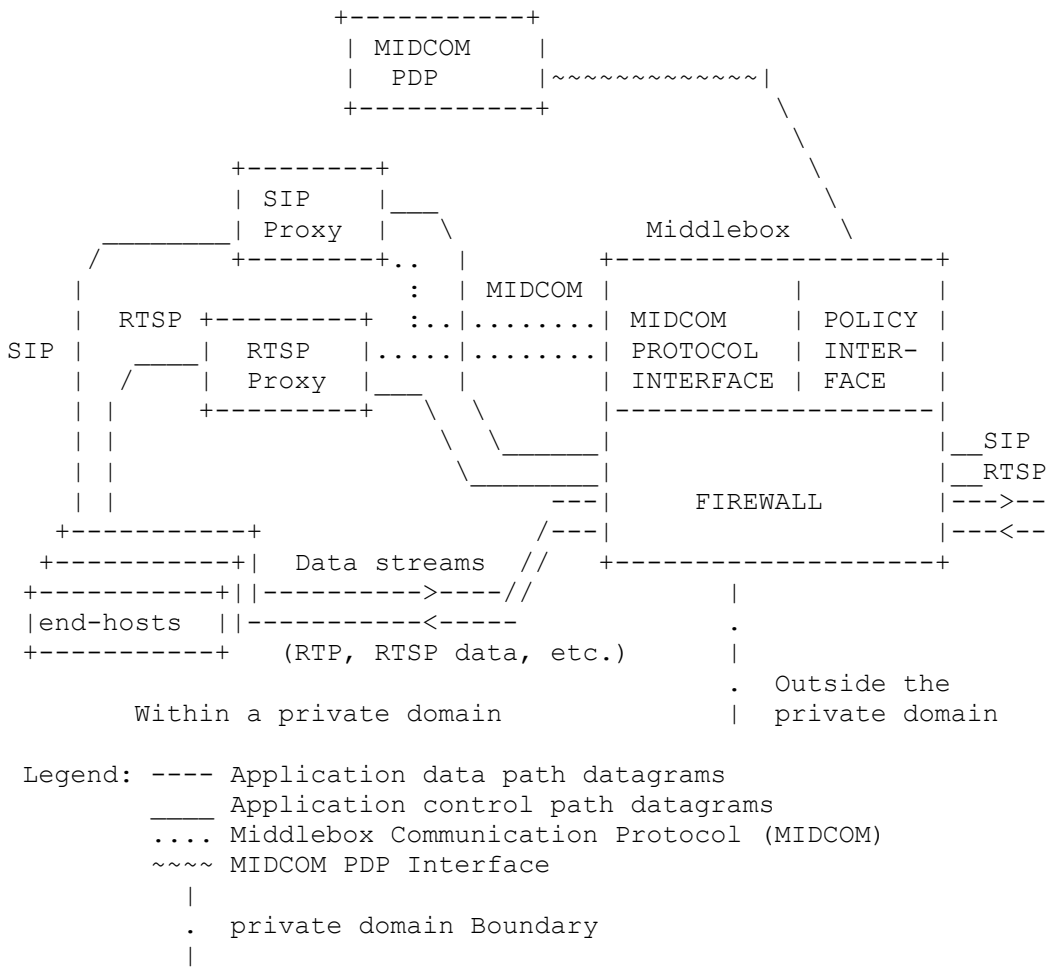


Figure 2 : Agents MIDCOM dans le chemin pour communication avec boîtier de médiation

5.1 Hôtes d'extrémité comme agents MIDCOM dans le chemin

Les hôtes d'extrémité sont une autre variante d'agents MIDCOM dans le chemin. À la différence des mandataires, les hôtes d'extrémité sont un partenaire direct de l'application et possèdent toute l'intelligence d'application de bout en bout qu'il doit y avoir. Les hôtes d'extrémité sont supposés terminer à la fois le chemin de contrôle et le chemin des données d'une application. À la différence des autres entités qui hébergent les agents MIDCOM, les hôtes d'extrémité sont capables de traiter des datagrammes sécurisés. Cependant, le problème sera celui de la possibilité de gérer – mettre à niveau tous les hôtes d'extrémité qui font fonctionner une application spécifique.

6 Fonctions de PDP MIDCOM

La décomposition fonctionnelle de l'architecture MIDCOM suppose l'existence d'une entité logique, appelée PDP MIDCOM, chargée d'effectuer les services d'autorisation et d'approvisionnement qui s'y rapportent pour le boîtier de médiation comme décrit à la figure 1. Le PDP MIDCOM est une entité logique qui peut résider physiquement sur un boîtier de médiation ou dans un nœud externe au boîtier de médiation. Le protocole employé pour la communication entre le boîtier de médiation et le PDP MIDCOM est sans relation avec le protocole MIDCOM.

Les agents sont enregistrés auprès d'un PDP MIDCOM pour l'autorisation d'invoquer les services du boîtier de médiation.

Le PDP MIDCOM conserve une liste des agents qui sont autorisés à se connecter à chacun des boîtiers de médiation que le PDP MIDCOM prend en charge. Dans le contexte du cadre MIDCOM, le PDP MIDCOM n'assiste pas un boîtier de médiation dans la mise en œuvre des services qu'il fournit.

Le PDP MIDCOM agit comme une facilité de conseil d'un boîtier de médiation, pour autoriser ou mettre un terme à l'autorisation d'un agent qui tente de se connecter au boîtier de médiation. Le principal objectif d'un PDP MIDCOM est de communiquer les informations d'autorisation des agents, de façon à s'assurer que la sécurité et l'intégrité d'un boîtier de médiation ne sont pas mises à mal. Précisément, le PDP MIDCOM devrait associer un niveau de confiance à chaque agent qui tente de se connecter à un boîtier de médiation et fournir un profil de sécurité. Le PDP MIDCOM devrait être capable de régler le cas où des hôtes d'extrémité sont des agents pour le boîtier de médiation.

6.1 Authentification, intégrité et confidentialité

L'authenticité de l'hôte et la sécurité du message individuel sont deux types distincts de considérations de sécurité. L'authentification de l'hôte se réfère aux accréditifs exigés d'un agent MIDCOM pour s'authentifier auprès du boîtier de médiation et vice versa. Lorsque l'authentification échoue, le boîtier de médiation ne doit pas traiter les demandes de signalisation reçues de l'agent qui a échoué à l'authentification. L'authentification bidirectionnelle devrait être acceptée. Dans la plupart des cas, l'authentification bidirectionnelle peut être étroitement liée à l'établissement de clés pour protéger le trafic ultérieur. L'authentification est souvent exigée pour empêcher diverses attaques actives contre le protocole MIDCOM et pour l'établissement sûr du matériel de clés.

Les services de sécurité tels que l'authentification, l'intégrité des données, la confidentialité et la protection contre la répétition peuvent être adaptés pour sécuriser les messages MIDCOM dans un domaine qui n'est pas de confiance. L'authentification du message est la même que l'authentification d'origine des données et est une affirmation que l'envoyeur du message est bien celui qu'il prétend être. L'intégrité des données se réfère à la capacité de s'assurer qu'un message n'a pas été accidentellement, par malveillance ou autrement, altéré ou détruit. La confidentialité est le chiffrement d'un message avec une clé, de sorte que seuls ceux qui sont en possession de la clé puissent déchiffrer le contenu du message. Enfin, la protection contre la répétition est une forme d'intégrité de séquence, de sorte que lorsque un intrus répète une séquence de messages précédemment enregistrée, le receveur des messages répétés va simplement abandonner les messages répétés. Certaines applications du protocole MIDCOM peuvent exiger la prise en charge de la non répudiation comme option du service d'intégrité des données. Normalement, la prise en charge de la non répudiation est requise pour la facturation, les accords de niveau de service, les ordres de payement, et les reçus de livraison de service.

L'AH IPsec ([IPSEC-AH]) offre l'authentification d'origine des données, l'intégrité des données et la protection contre la répétition de message. L'ESP IPsec ([IPSEC-ESP]) fournit l'authentification d'origine des données à un moindre degré (le même que l'AH IPsec si le protocole de transport MIDCOM se trouve être TCP ou UDP), la confidentialité du message, l'intégrité des données et la protection contre la répétition. À côté des protocoles fondés sur IPsec, il y a aussi d'autres options de sécurité. La sécurité de la couche transport fondée sur TLS est une option. De nombreux mécanismes de sécurité de couche application sont disponibles. La sécurité fondée sur la simple adresse de source est une forme minimale de sécurité et on ne devrait s'appuyer sur elle que dans les environnements de la plus grande confiance, où les hôtes ne sont pas des usurpateurs.

La sécurité du message MIDCOM devra utiliser les normes existantes, chaque fois que les normes existantes satisfont aux exigences. La sécurité devra être spécifiée de façon à minimiser l'impact sur les sessions qui n'utilisent pas l'option de sécurité. La sécurité devrait être conçue pour éviter d'introduire des attaques de déni de service et en minimiser l'impact. Certains mécanismes et algorithmes de sécurité requièrent un traitement ou des capacités mémoire substantiels, auquel cas les protocoles de sécurité devraient se protéger eux-mêmes ainsi que contre de possibles attaques par inondation qui submergent le point d'extrémité (c'est-à-dire, le boîtier de médiation ou l'agent) avec de tels traitements. Pou les protocoles orientés connexion (comme TCP) qui utilisent des services de sécurité, le protocole de sécurité devrait détecter les fermetures prématurées ou les attaques qui tronquent les messages.

6.2 Enregistrement et désenregistrement des agents MIDCOM

Avant de permettre aux agents MIDCOM d'invoquer les services du boîtier de médiation, un processus d'enregistrement doit avoir lieu. L'enregistrement est un processus différent de celui de l'établissement d'une session MIDCOM. Le premier exige d'apporter des informations sur le profil de l'agent au boîtier de médiation ou au PDP MIDCOM. L'enregistrement d'agent est souvent une opération manuelle effectuée par un opérateur plutôt que par l'agent lui-même. L'établissement

d'une session MIDCOM se réfère à l'établissement d'une session de transport MIDCOM et à l'échange d'accréditifs de sécurité entre un agent et un boîtier de médiation. La session de transport utilise les informations enregistrées pour l'établissement de session.

Le profil d'un agent MIDCOM inclut la politique d'autorisation de l'agent (c'est-à-dire, des tuplets de session pour lesquels l'agent est autorisé à agir comme ALG), l'entité d'hébergement de l'agent (par exemple, mandataire, passerelle ou hôte d'extrémité qui héberge l'agent), profil d'accessibilité de l'agent (incluant toute information d'authentification au niveau de l'hôte) et profil de sécurité (c'est-à-dire, exigences de sécurité pour les messages échangés entre le boîtier de médiation et l'agent).

Un profil d'agent MIDCOM peut être préconfiguré sur un boîtier de médiation. Ensuite de cela, l'agent peut choisir d'initier une session MIDCOM avant tout trafic de données. Par exemple, la politique d'autorisation d'agent MIDCOM pour un service de boîtier de médiation peut être préconfigurée pour spécifier l'agent en conjonction avec un filtre. Dans le cas d'un pare-feu, par exemple, le tuplet ACL peut être modifié pour refléter la présence facultative de l'agent. L'ACL révisé peut parfois ressembler à ce qui suit .

(<Direction-de-session>, <Adresse-de-source>, <Adresse-de-destination>, <Protocole-IP>, <Accès-de-source>, <Accès-de-destination>, <Agent>)

Le lecteur devrait noter que ceci est un exemple qui illustre et non nécessairement la définition réelle d'un tuplet d'ACL. La description formelle de l'ACL reste encore à écrire. Les informations d'accessibilité de l'agent devraient aussi être provisionnées. Pour un agent MIDCOM, les informations d'accessibilité comportent l'adresse IP, le niveau de confiance, les paramètres d'authentification de l'hôte et les paramètres d'authentification du message. Une fois qu'une session est établie entre un boîtier de médiation et un agent MIDCOM, cette session devrait être utilisable avec plusieurs instances de la ou des applications, selon ce qui est approprié. Noter que tout ceci pourrait être regroupé dans un profil d'agent pour faciliter la gestion.

La technique décrite ci-dessus est nécessaire pour le pré enregistrement des agents MIDCOM auprès du boîtier de médiation. L'approvisionnement su boîtier de médiation peut rester inchangé, si le boîtier de médiation acquiert les agents enregistrés par un PDP MIDCOM. Dans l'un ou l'autre cas, l'agent MIDCOM devrait initier la session avant de commencer l'application. Si la session d'agent est retardé jusque après le début de l'application, l'agent pourrait être incapable de traiter le flux de contrôle pour permettre les sessions de données. Lorsque un boîtier de médiation remarque une session MIDCOM entrante, et que le boîtier de médiation n'a pas de profil antérieur de l'agent MIDCOM, le boîtier de médiation va consulter son PDP MIDCOM sur l'authenticité, l'autorisation,et les lignes directrices de confiance pour la session.

7. Illustration du cadre MIDCOM en utilisant un agent dans le chemin

Dans la figure 3 ci-dessous, on considère des applications SIP (voir [SIP]) pour illustrer le fonctionnement du protocole MIDCOM. Précisément, l'application suppose qu'un appelant, externe à un domaine privé, initie l'appel. Le boîtier de médiation est supposé être localisé à la bordure du domaine privé. Un téléphone SIP (Client/serveur d'agent d'utilisateur SIP) à l'intérieur du domaine privé est capable de recevoir des appels de téléphones SIP externes. L'appelant utilise un mandataire SIP, nœud localisé à l'extérieur du domaine privé, comme son mandataire de sortie. Aucun mandataire intérieur n'est supposé pour le demandé. Enfin, le nœud de mandataire SIP externe est désigné pour héberger la fonction d'agent MIDCOM.

Les flèches 1 et 8 de la figure ci-dessous se réfèrent à un échange d'établissement d'appel SIP entre le téléphone SIP externe et le mandataire SIP. Les flèches 4 et 5 se réfèrent à un échange d'établissement d'appel SIP entre le mandataire SIP et le téléphone SIP intérieur, et ils sont supposés traverser le boîtier de médiation. Les flèches 2, 3, 6 et 7 ci-dessous, entre le mandataire SIP et le boîtier de médiation, se réfèrent à la communication MIDCOM. Na et Nb représentent le trafic sur le chemin de support RTP/RTCP (voir [RTP]) dans le réseau externe. Nc et Nd représentent le trafic de support à l'intérieur du domaine privé.

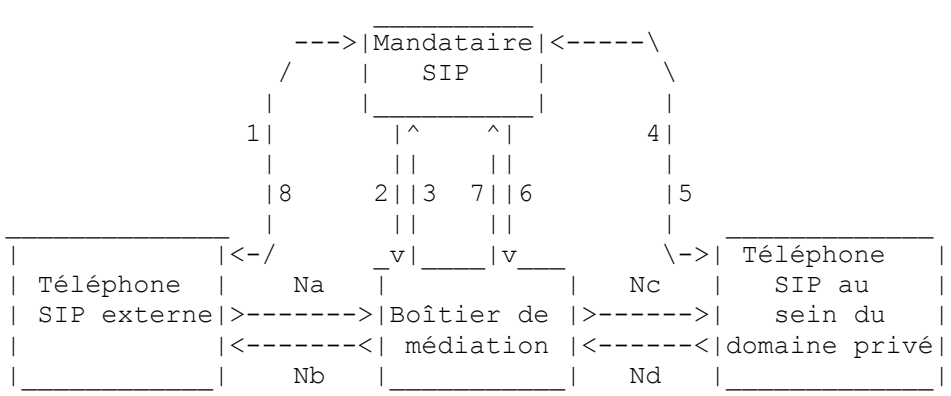


Figure 3 : Illustration du cadre MIDCOM avec mandataire SIP dans le chemin

Comme pour l'application SIP, on fait l'hypothèse que le boîtier de médiation est préconfiguré pour accepter les appels SIP dans le téléphone SIP privé. Précisément, cela impliquerait que le boîtier de médiation met en œuvre un service de pare-feu préconfiguré pour permettre les appels SIP (le numéro d'accès TCP ou UDP de destination est réglé à 5060) dans le téléphone privé. De même, le boîtier de médiation qui met en œuvre le service NAPT aurait été préconfiguré pour fournir un lien d'accès pour permette que les appels SIP entrants soient redirigés sur le téléphone SIP privé spécifique. C'est-à-dire que le INVITE provenant de l'appelant externe n'est pas fait à l'adresse IP privée mais à l'adresse externe NAPT.

L'objectif de l'agent MIDCOM dans l'illustration suivante est simplement de permettre au flux de supports RTP/RTCP (voir [RTP]) de s'écouler à travers le boîtier de médiation, lorsque on utilise l'architecture du protocole MIDCOM mise en avant dans ce document. Une session SIP établit normalement deux flux de supports RTP/RTCP – un du demandé à l'appelant et un autre de l'appelant au demandé. Ces sessions de supports sont fondées sur UDP et vont utiliser des accès dynamiques. Les accès dynamiques utilisés pour les flux de supports spécifiés dans la section SDP (voir [SDP]) du message de charge utile SIP. L'agent MIDCOM va analyser la section SDP et utiliser le protocole MIDCOM pour (a) ouvrir des perforations (c'est-à-dire, permettre des tuplets de session RTP/RTCP) dans un boîtier de médiation qui met en œuvre un service de pare-feu, ou (b) créer des liens d'accès et modifier de façon appropriée le contenu de SDP pour permettre aux flux RTP/RTCP de s'écouler à travers un boîtier de médiation qui met en œuvre un service de NAT. Le protocole MIDCOM devrait être suffisamment riche et expressif pour prendre en charge les opérations décrites dans le temps imparti. Les exemples ne montrent pas les temporisateurs entretenus par l'agent pour empêcher la ou les règles de politique du boîtier de médiation d'arriver en fin de durée de vie

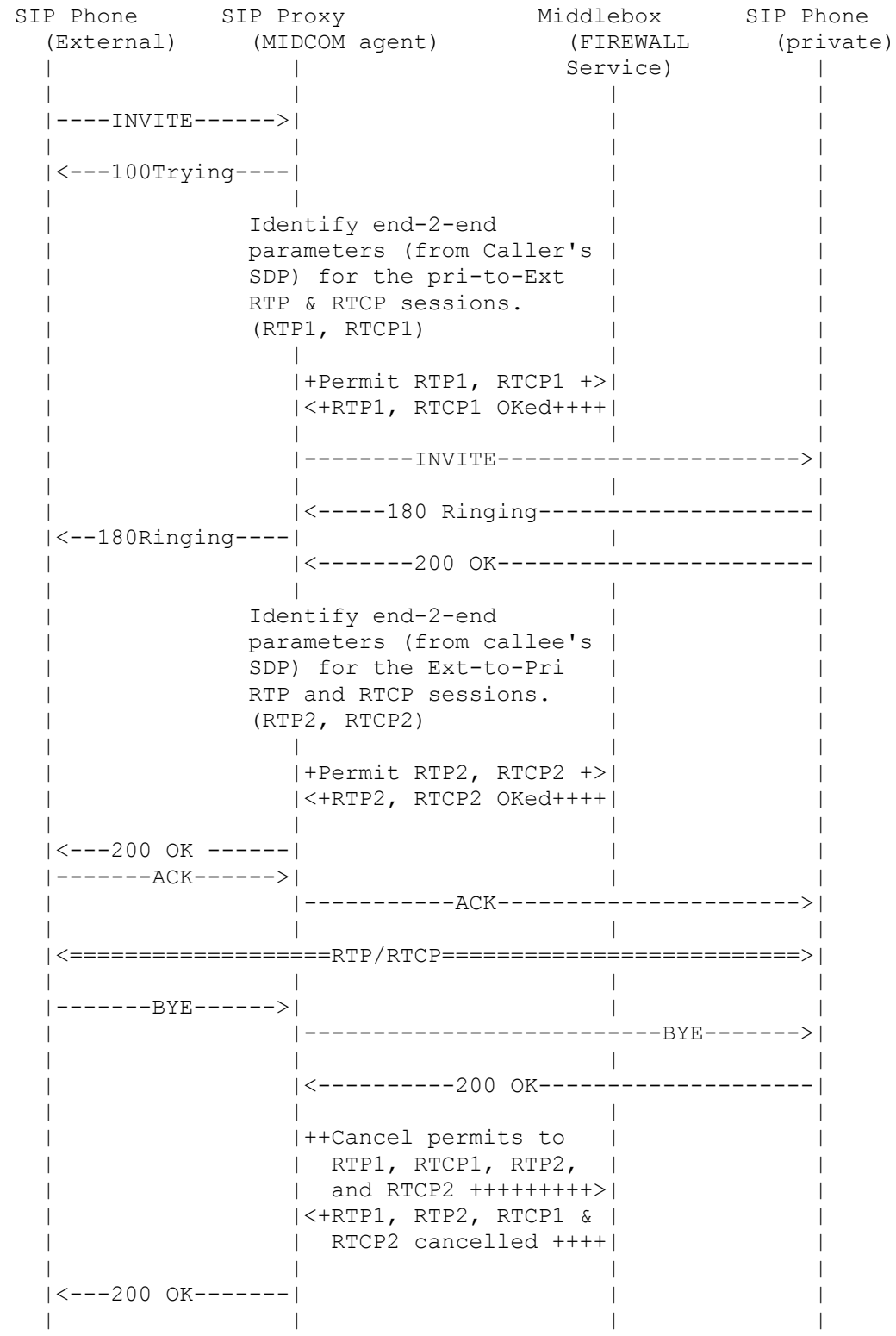
L'enregistrement de l'agent MIDCOM et la connexité entre l'agent MIDCOM et le boîtier de médiation ne sont pas montrés afin de restreindre le champ des transactions MIDCOM à permettre au boîtier de médiation de laisser passer le flux de supports. Pour la même raison, le PDP MIDCOM n'est pas montré non plus dans le diagramme ni l'écoulement du temps.

Le paragraphe suivant illustre une séquence temporelle typique des opérations avec les divers éléments impliqués dans un chemin d'application de téléphonie SIP. Chaque paragraphe est consacré à une instanciation spécifique d'un service de boîtier de médiation - NAPT (voir [NAT-TERM], [NAT-TRAD]), pare-feu et combinaison de NAPT et de pare-feu sont examinés.

7.1. Flux temporel – Boîtier de médiation mettant en œuvre un service de pare-feu

Dans l'exemple suivant, on suppose qu'un boîtier de médiation met en œuvre un service de pare-feu. Que de plus le boîtier de médiation est préconfiguré pour permettre les appels SIP (le numéro d'accès TCP ou UDP de destination est réglé à 5060) dans le téléphone privé. La ligne de temps qui suit illustre le déroulement des opérations effectuées par l'agent MIDCOM, pour permettre au flux de support RTP/RTCP de passer à travers le boîtier de médiation.

Le INVITE de l'appelant (externe) est supposé inclure la charge utile SDP. On notera que l'agent MIDCOM demande au boîtier de médiation de permettre les flux RTP/RTCP de privé à externe avant que le INVITE ne soit relayé au demandé. Cela parce que, dans SIP, l'appelant doit être prêt à recevoir le support lorsque il envoie l'INVITE avec une description de session. Si le demandé (téléphone privé) suppose cela et envoie un "support précoce" avant d'envoyer la réponse 200 OK, le pare-feu aura bloqué ces paquets sans cette signalisation initiale MIDCOM provenant de l'agent.



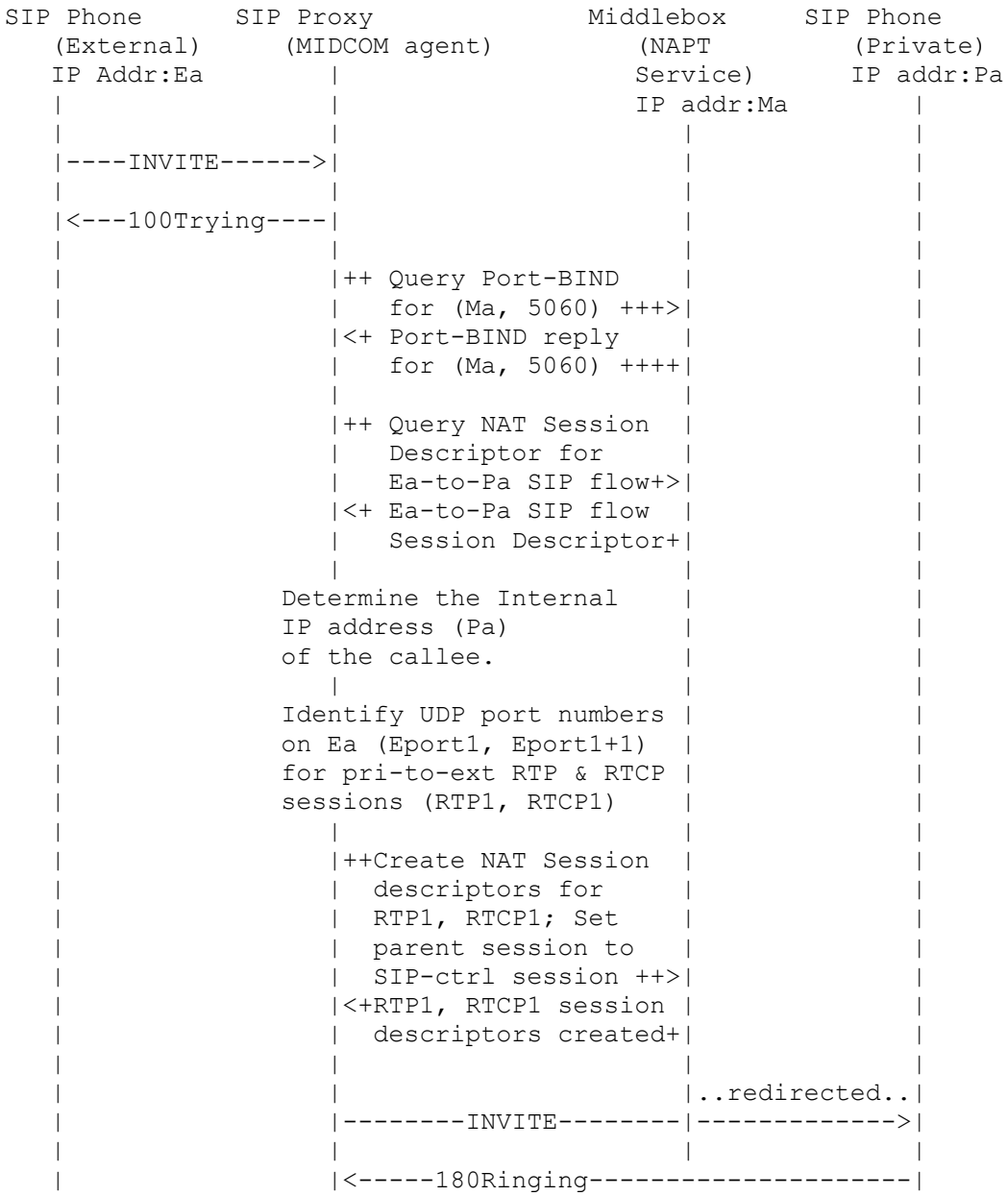
Légende : ..... Trafic de contrôle MIDCOM
------- Trafic de contrôle SIP
==== Trafic de support RTP/RTCP

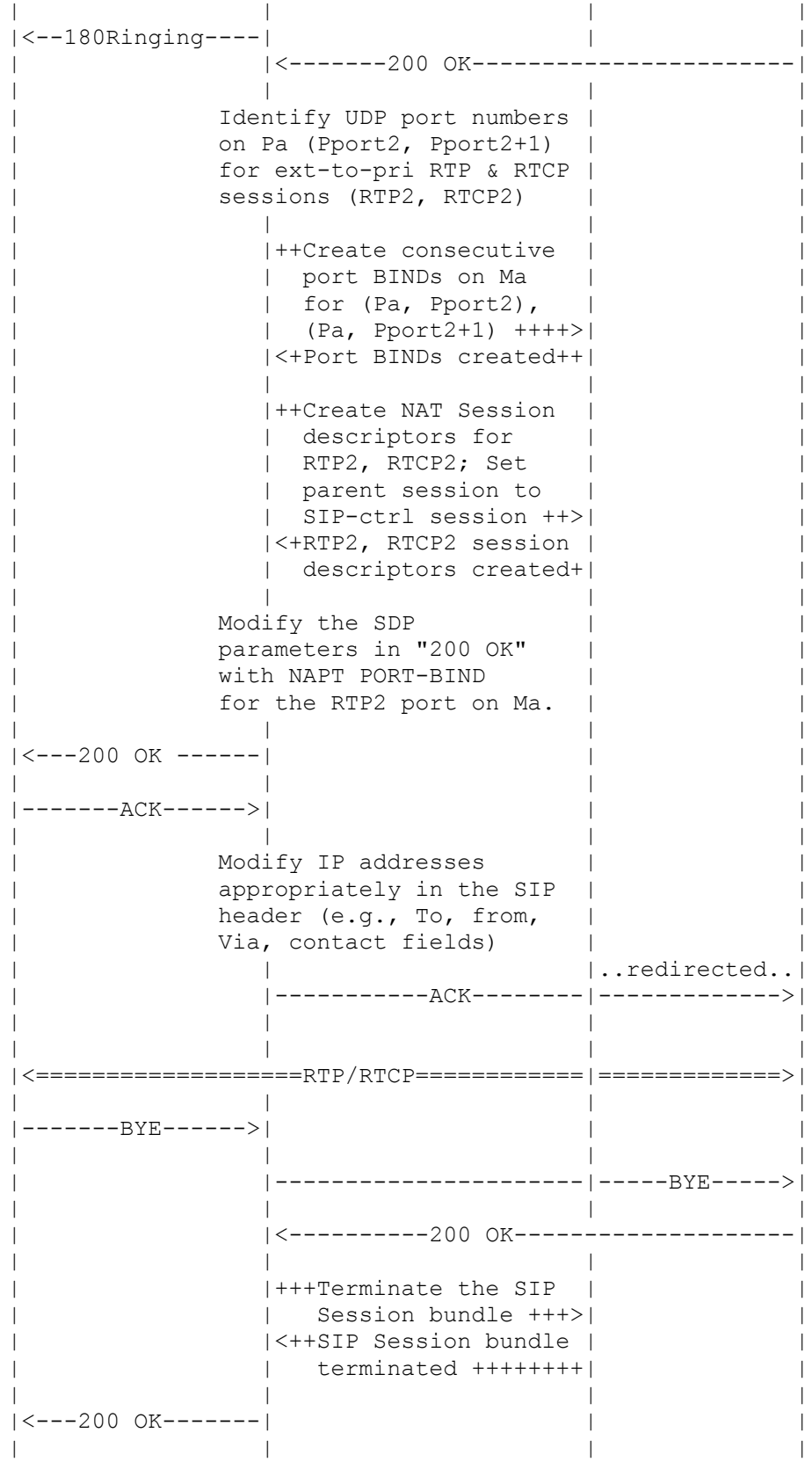
7.2 Flux temporel – Boîtier de médiation mettant en œuvre un service de NAPT

Dans l'exemple suivant, on suppose qu'un boîtier de médiation met en œuvre un service de NAPT. On suppose aussi que le boîtier de médiation est préconfiguré pour rediriger les appels SIP sur une application de téléphone privé SIP spécifique.

C'est-à-dire que le INVITE provenant de l'appelant externe n'est pas fait à l'adresse IP privée, mais à l'adresse externe du NAPT. Disons que l'adresse IP du téléphone externe est Ea, l'adresse externe du boîtier de médiation NAPT est Ma, et l'adresse privée du téléphone SIP interne est Pa. Les appels SIP au téléphone SIP privé vont arriver comme sessions TCP/UDP, avec l'adresse et l'accès de destination réglés respectivement à Ma et 5060. Le boîtier de médiation va rediriger ces datagrammes sur le téléphone SIP interne. Le flux temporel qui suit illustre les opérations qu'il est nécessaire d'effectuer chez l'agent MIDCOM pour permettre au flux de support RTP/RTCP de passer à travers le boîtier de médiation.

Comme avec l'exemple précédent (paragraphe 7.1) le INVITE provenant de l'appelant (externe) est supposé inclure la charge utile SDP. On notera que l'agent MIDCOM demande au boîtier de médiation de créer des descripteurs de session NAT pour les flux RTP/RTCP de privé à extérieur avant que le INVITE soit relayé au téléphone SIP privé (pour les mêmes raisons que celles décrites au paragraphe 7.1). Si le demandé (téléphone privé) envoie un "support précoce" avant d'envoyer la réponse 200 OK, le boîtier de médiation NAPT aura bloqué ces paquets sans la signalisation initiale MIDCOM provenant de l'agent. Noter aussi qu'après la réception du 200 OK par le mandataire en provenance du téléphone privé, l'agent demande au boîtier de médiation d'allouer des descripteurs de session NAT pour les flux RTP2 et RTCP2 d'externe à privé, de sorte que les accès alloués sur le Ma pour RTP2 et RTCP2 sont contigus. Le flux RTCP ne se fait pas sur un accès non contigu. Enfin, on notera que bien que chaque flux de support (RTP1, RTCP1, RTP2 et RTCP2) soit indépendant, ils sont tous liés à la seule session de contrôle SIP, alors que leurs descripteurs de session NAT ont été créés. Finalement lorsque l'agent produit une commande de terminaison de faisceau de sessions pour la session SIP, le boîtier de médiation est supposé supprimer automatiquement toutes les sessions de flux de support associées.



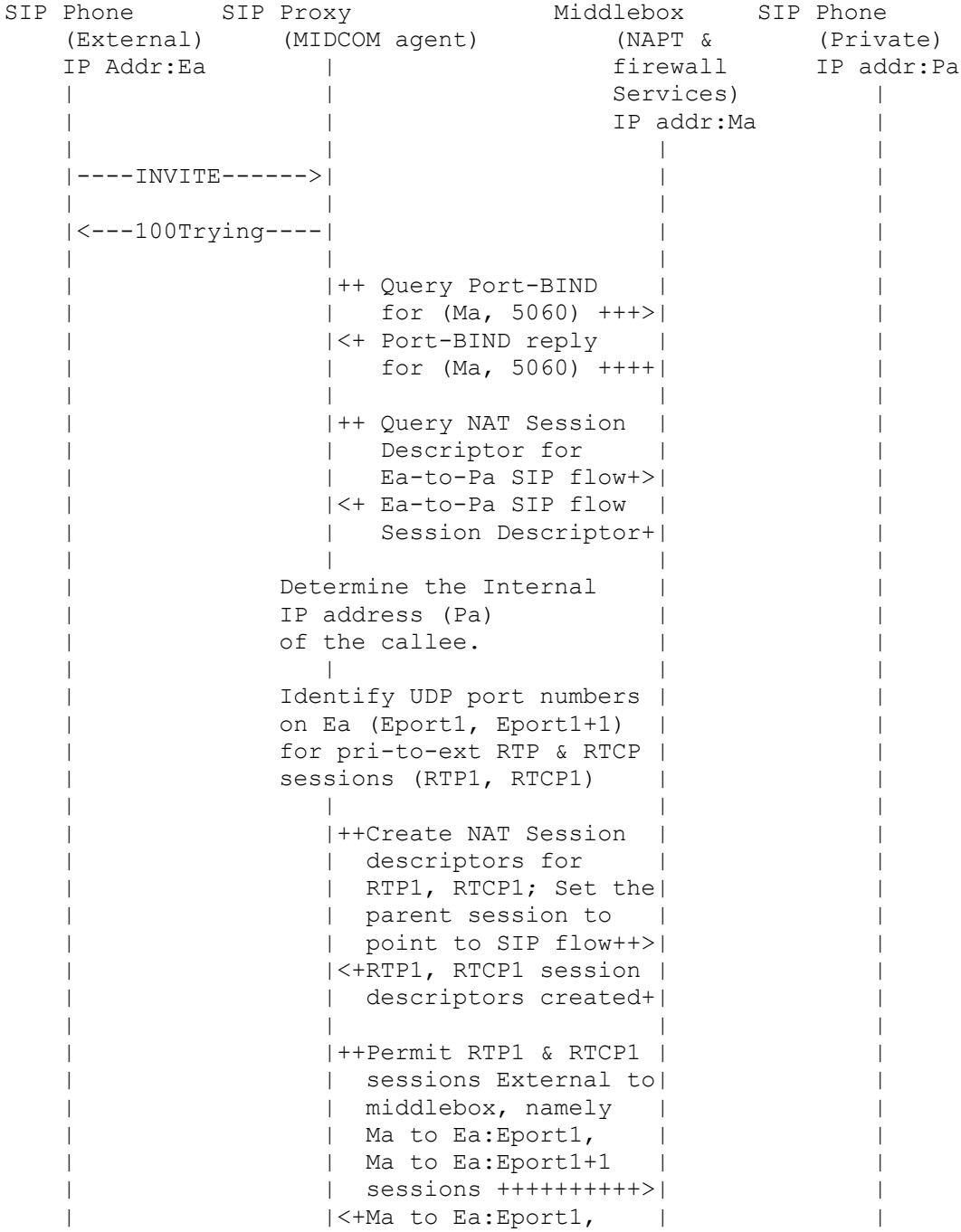


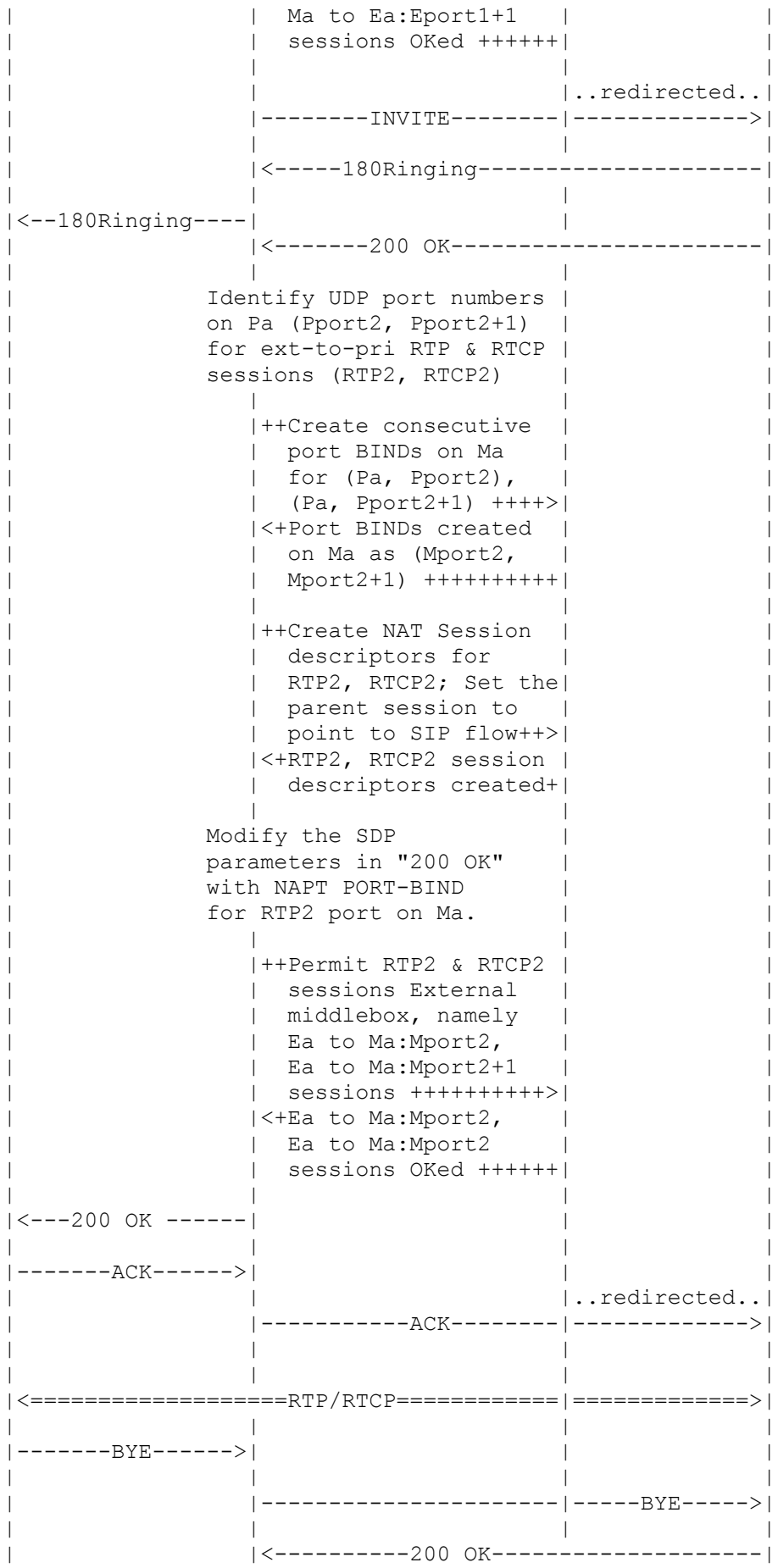
Légende : ..... Trafic de contrôle MIDCOM
------- Trafic de contrôle SIP
==== Trafic de support RTP/RTCP

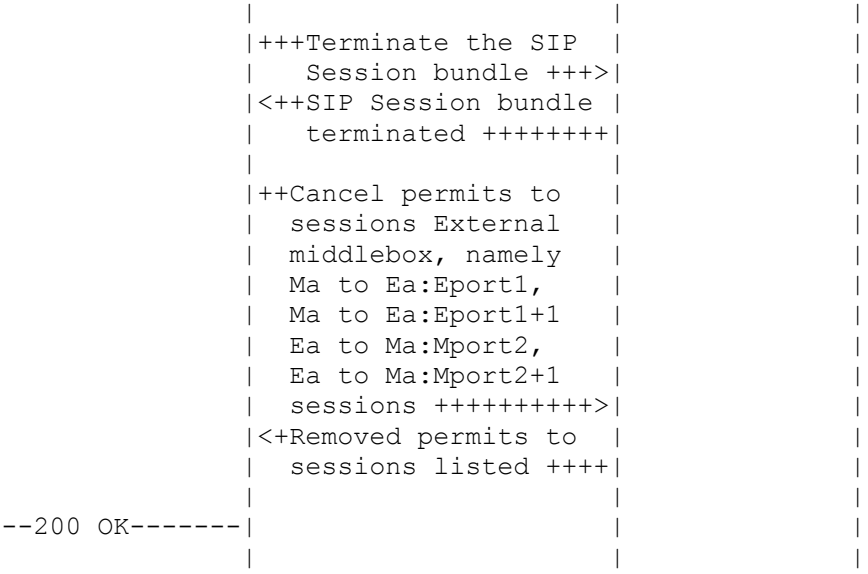
7.3 Flux temporel – Boîtier de médiation mettant en œuvre NAPT et pare-feu

Dans l'exemple suivant, on va supposer qu'un boîtier de médiation met en œuvre une combinaison de service de pare-feu et de NAPT à états pleins. On fait l'hypothèse que la fonction de NAPT est configurée pour traduire les en-têtes IP et TCP de la session SIP initiale dans le téléphone SIP privé, et que la fonction de pare-feu est configurée pour permettre la session SIP initiale.

Dans le flux temporel qui suit, on peut noter que la description du pare-feu se fonde sur les champs de paquet comme ils sont sur le réseau (par exemple, comme vus à l'interface externe du boîtier de médiation). Afin d'assurer un comportement correct des services individuels, vous remarquerez que les opérations MIDCOM spécifiques du NAT précédents les opérations spécifiques du pare-feu chez l'agent MIDCOM. Cela est remarquable dans le flux temporel ci-dessous lorsque l'agent MIDCOM traite le "200 OK" provenant du téléphone SIP privé. L'agent MIDCOM demande au départ au service de NAT qui est sur le boîtier de médiation d'établir un BIND d'accès et des descripteurs de session pour le flux de support dans les deux directions. À la suite de cela, l'agent MIDCOM détermine les paramètres de session (c'est-à-dire, les accès UDP dynamiques) pour le flux de support, tels que vus par l'interface externe et demande au service de pare-feu sur le boîtier de médiation de permettre à ces sessions de passer à travers.




Ma to Ea:Eport1+1
sessions OKed
..redirected..
INVITE
180Ringing
180Ringing
200 OK
Identify UDP port numbers
on Pa (Pport2, Pport2+1)
for ext-to-pri RTP & RTCP
sessions (RTP2, RTCP2)
++Create consecutive
port BINDs on Ma
for (Pa, Pport2),
(Pa, Pport2+1)
+Port BINDs created
on Ma as (Mport2,
Mport2+1)
++Create NAT Session
descriptors for
RTP2, RTCP2; Set the
parent session to
point to SIP flow++
+RTP2, RTCP2 session
descriptors created+
Modify the SDP
parameters in "200 OK"
with NAPT PORT-BIND
for RTP2 port on Ma.
++Permit RTP2 & RTCP2
sessions External
middlebox, namely
Ea to Ma:Mport2,
Ea to Ma:Mport2+1
sessions
+Ea to Ma:Mport2,
Ea to Ma:Mport2
sessions OKed
200 OK
ACK
..redirected..
ACK
RTP/RTCP
BYE
BYE
200 OK



Légende : ..... Trafic de contrôle MIDCOM
------- Trafic de contrôle SIP
==== Trafic de support RTP/RTCP

8 Considérations sur le fonctionnement

8.1 Sessions MIDCOM multiples entre agents et boîtier de médiation

On ne peut pas supposer qu'un boîtier de médiation n'est qu'un simple appareil qui met en œuvre juste une fonction de boîtier de médiation et rien de plus qu'un couple d'interfaces. Les boîtiers de médiation combinent souvent plusieurs fonctions intermédiaires dans le même appareil et ont la capacité d'approvisionner des interfaces individuelles du même appareil avec différents ensembles de fonctions et divers approvisionnements de la même fonction à travers les interfaces.

À ce titre, un agent MIDCOM devrait être capable d'avoir une seule session MIDCOM avec un boîtier de médiation et utiliser l'interface MIDCOM sur le boîtier de médiation pour servir d'interface avec différents services sur le même boîtier de médiation.

8.2 Notification asynchrone aux agents MIDCOM

Une notification asynchrone par un boîtier de médiation à un agent MIDCOM peut être utile pour des événements tels qu'une création de session, une terminaison de session, un échec de protocole MIDCOM, une défaillance de fonction de boîtier de médiation ou tout autre événement significatif. Indépendamment de cela, les codes d'erreur ICMP peuvent aussi être utiles pour notifier aux agents des défaillances de couche transport.

De plus, des notifications périodiques de diverses formes de données, telles que des mise à jour statistiques, seraient aussi une fonction utile qui serait bénéfique pour certains types d'agents.

8.3 Les temporisateurs sont considérés comme utiles sur les boîtiers de médiation

Lorsque il prend en charge le protocole MIDCOM, le boîtier de médiation doit allouer des ressources dynamiques, comme spécifié dans la ou les règles de politique, sur demande des agents. La libération explicite de ressources allouées de façon dynamique survient lorsque la session d'application se termine ou lorsque un agent MIDCOM demande au boîtier de médiation de libérer la ressource.

Cependant, le boîtier de médiation devrait être capable de recouvrer les ressources allouées de façon dynamique, même lorsque l'agent qui était chargé de l'allocation n'est plus en vie. Associer une durée de vie pour ces ressources dynamiques et

utiliser un temporisateur pour retracer la durée de vie peut être un bon moyen de le faire.

8.4 Les boîtiers de médiation qui prennent en charge plusieurs services

Un boîtier de médiation pourrait mettre en œuvre divers services (par exemple, de NAT et de pare-feu) dans le même boîtier. Certains de ces services peut avoir une interdépendance sur des ressources partagées et des séquences d'opérations. D'autres peuvent être indépendants les uns des autres. D'une façon générale, les séquences dans lesquelles ces opérations de fonction peuvent être effectuées sur les datagrammes sortent du domaine d'application du présent document.

Dans le cas d'un boîtier de médiation qui met en œuvre des services de NAT et de pare-feu, il est plus sûr de déclarer que le fonctionnement du NAT sur une interface va précéder un pare-feu sur la sortie et va suivre un pare-feu sur l'entrée. De plus, les listes de contrôle d'accès de pare-feu, utilisées par un pare-feu, sont supposées se fonder sur les paramètres de session, tels que vus sur l'interface qui prend en charge le service de pare-feu.

8.5 Trafic de signalisation et de données

La classe des applications auxquelles l'architecture MIDCOM s'adresse se concentre sur les applications qui ont une combinaison d'une ou plusieurs sessions de trafic de signalisation et de données. La signalisation peut être faite hors bande, utilisant une session dédiée autonome ou peut être faite dans la bande, au sein d'une session de données. Autrement, la signalisation peut aussi être faite par une combinaison des sessions à la fois autonomes et dans la bande.

SIP est un exemple d'application fondée sur des sessions distinctes de signalisation et de données. Une session SIP de signalisation est utilisée pour l'établissement d'appel entre l'appelant et un demandé. Un agent MIDCOM peut être obligé d'examiner/modifier un contenu de charge utile SIP pour régler le boîtier de médiation de telle sorte qu'il laisse passer à travers les flux de support (fondés sur RTP/RTCP). Un agent MIDCOM n'est pas obligé d'intervenir dans le trafic de données.

Les informations d'en-tête spécifique de signalisation et de contexte sont envoyées dans la bande, au sein du même flux de données pour des applications telles que celles incorporées dans HTTP, sun-RPC (incorporant une variété d'applications NFS), transactions Oracle (incorporant oracle SQL+, MS ODBC, Peoplesoft) etc.

H.323 est un exemple d'application qui envoie la signalisation à la fois dans des sessions dédiées et autonomes, aussi bien que conjointement avec des données. Le trafic de signalisation d'appel H.225.0 traverse les boîtiers de médiation selon une politique statique, aucun contrôle MIDCOM n'est nécessaire. La signalisation d'appel H.225.0 négocie aussi les accès pour un flux TCP H.245. Un agent MIDCOM est obligé d'examiner/modifier le contenu du H.245 afin que le H.245 puisse le traverser.

H.245 traverse le boîtier de médiation et porte aussi des informations de "canal logique ouvert" pour les données du support. Ainsi, l'agent MIDCOM est une fois encore obligé d'examiner/modifier le contenu de charge utile nécessaire pour laisser s'écouler le trafic de support.

L'architecture MIDCOM tient compte des applications qui la prennent en charge avec des sessions indépendantes de signalisation et de données aussi bien que des applications qui ont la signalisation et les données communiquées sur la même session.

Dans les cas où la signalisation est faite sur une seule session autonome, il est souhaitable d'avoir un agent MIDCOM qui interprète le flux de signalisation et programme le boîtier de médiation (par qui transite le flux de données) afin de laisser passer le trafic de données sans l'interrompre.

9. Déclaration d'applicabilité

Les boîtiers de médiation peuvent se situer dans un certain nombre de topologies. Cependant, le cadre de signalisation mis en avant dans le présent document peut être limité aux seuls boîtiers de médiation qui sont situés dans une zone tampon (DMZ, *De-Militarized Zone*) à la bordure d'un domaine privé, se connectant à l'Internet. Précisément, l'hypothèse est qu'on a un seul boîtier de médiation (qui opère un NAT ou pare-feu) le long du chemin de l'application. La découverte d'un boîtier de médiation le long du chemin d'une application sort du domaine d'application de ce document. On peut concevoir d'avoir

des boîtiers de médiation situés entre des départements au sein du même domaine ou à l'intérieur du domaine d'un fournisseur de service et ainsi de suite. Cependant, il faut veiller à revoir chaque scénario individuel et déterminer l'applicabilité au cas par cas.

L'applicabilité peut être illustrée comme suit. Les applications en temps réel et de flux directs, tels que la voix sur IP, et les applications d'homologue à homologue, telles que Napster et Netmeeting, exigent d'administrer des boîtiers de médiation de NAT et de pare-feu pour laisser leurs flux de support atteindre les hôtes à l'intérieur d'un domaine privé. Les exigences sont sous la forme de l'établissement de "perforations" pour permette à une session TCP/UDP (dont les paramètres d'accès sont déterminés de façon dynamique) de passer à travers un pare-feu ou de retenir une adresse/lien d'accès dans l'appareil de NAT pour permettre un accès aux sessions. Ces exigences sont satisfaites par la génération actuelle de boîtiers de médiation qui utilisent des méthodes ad hoc, telles que d'incorporer l'intelligence d'application au sein d'un boîtier de médiation pour identifier les paramètres de session dynamiques et administrer le boîtier de médiation en interne de la façon appropriée. L'objectif de l'architecture MIDCOM est de créer une façon unifiée, normalisée pour exercer cette fonctionnalité, qui existe actuellement de façon ad hoc, dans certains des boîtiers de médiation.

En adoptant l'architecture MIDCOM, les boîtiers de médiation seront capables de prendre en charge des applications plus récentes qui n'ont pas été capables de la prendre en charge jusqu'à présent. L'architecture MIDCOM ne change pas, et ne doit en aucune façon, changer les caractéristiques fondamentales des services pris en charge sur le boîtier de médiation.

Normalement, les organisations protègent une majorité de leurs ressources d'entreprise (telles que les hôtes d'extrémité) contre la visibilité au réseau externe par l'utilisation d'une zone tampon (DMZ, *De-Militarized Zone*) à la bordure du domaine. Seule une portion de ces hôtes sont admis à l'accès au monde extérieur. Le reste des hôtes et leurs noms sont uniques pour le domaine privé. Les hôtes visibles au monde extérieur et leur serveur de nom d'autorité qui transpose leurs noms en adresses réseau sont souvent configurés au sein d'une DMZ en face d'un pare-feu. Les hôtes et les boîtiers de médiation au sein d'une DMZ sont appelés des nœuds de DMZ.

La Figure 4 ci-dessous illustre la configuration d'un domaine privé avec une DMZ à sa bordure. Les configurations réelles peuvent varier. Seuls les utilisateurs de l'intérieur du domaine accèdent aux hôtes internes. Les boîtiers de médiation situés dans la DMZ peuvent être accédés par les agents intérieurs ou extérieurs au domaine.

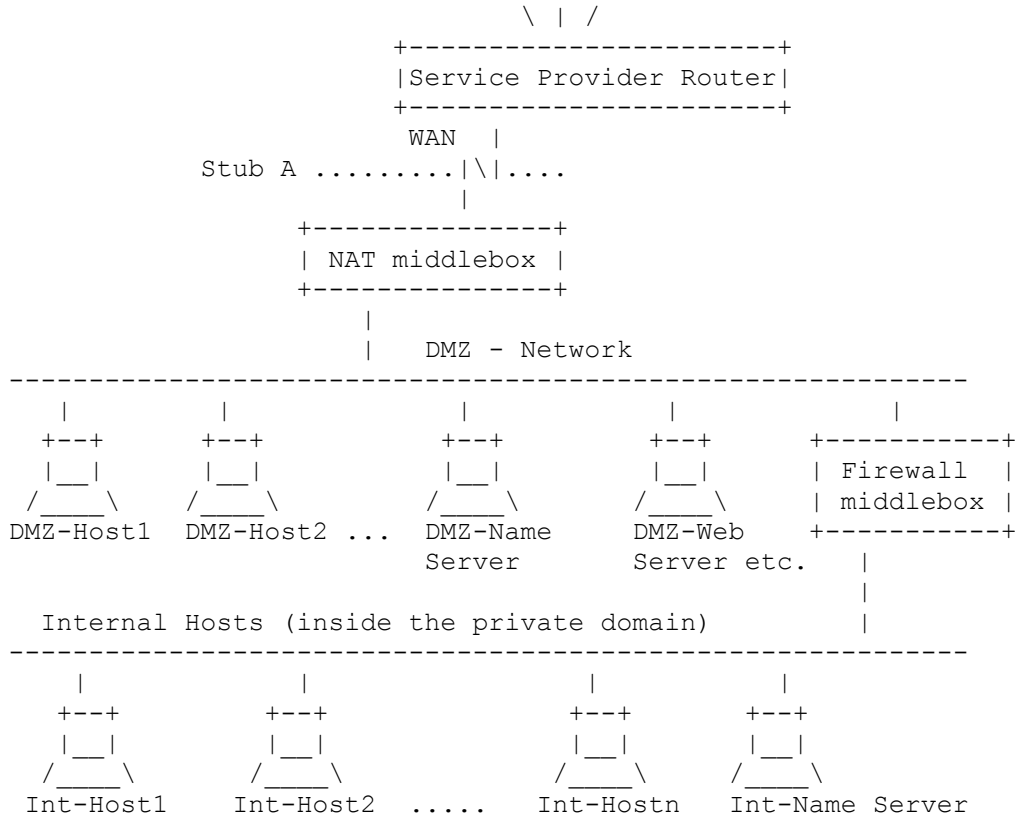


Figure 4 : configuration réseau/DMZ d'un domaine privé

10. Remerciements

Les auteurs tiennent à remercier Christian Huitema, Joon Maeng, Jon Peterson, Mike Fisk, Matt Holdrege, Melinda Shore, Paul Sijben, Philip Mart, Scott Brim et Richard Swale pour leur précieuses critiques, avis et apports sur une première version brute de ce document. Les auteurs doivent des remerciements particuliers à Eliot Lear pour le lancement de la discussion par messagerie sur les scénarios de cas d'utilisation avec un diagramme de flux d'application SIP à travers un boîtier de médiation. Un grand merci à Bob Penfield, Cedric Aoun, Christopher Martin, Eric Fleischman, George Michaelson, Wanqun Bao, et les autres du groupe de travail MIDCOM pour leurs retours très détaillés sur divers sujets et l'ajout de la clarté à l'exposé. Enfin, mais pas le moindre, les auteurs doivent beaucoup à Mark Duffy, Scott Brim, Melinda Shore et d'autres pour leur aide sur les définitions de terminologie et la discussion des exigences incorporées au sein du document cadre.

11. Considérations pour la sécurité

Ci-dessous sont exposées les considérations pour la sécurité en accédant à un boîtier de médiation. Sans la prise en charge du protocole MIDCOM, les prémisses du fonctionnement d'un boîtier de médiation exigent fondamentalement que les données soient en clair, car le boîtier de médiation a besoin d'être capable d'inspecter et/ou modifier l'en-tête et la charge utile du paquet. Cela compromet l'exigence de confidentialité dans certains environnements. De plus, la mise à jour des en-têtes de transport et la réécriture des données de charge utile d'application par le NAT empêche dans certains cas l'utilisation de la protection d'intégrité sur certains flux de données qui traversent les boîtiers de médiation NAT. Cela peut clairement poser un problème de sécurité significatif à l'application dans un domaine de transport qui n'est pas de confiance.

Le cadre du protocole MIDCOM supprime le besoin qu'un boîtier de médiation inspecte ou manipule la charge utile de transport. Cela permet aux applications de mieux se protéger de bout en bout grâce à l'aide d'un agent MIDCOM de confiance. C'est particulièrement le cas lorsque l'agent est un résident sur l'hôte d'extrémité. Lorsque un agent a la même capacité de bout en bout que l'hôte d'extrémité d'interpréter les données chiffrées et protégées en intégrité, le transit par un boîtier de médiation peut être chiffré et protégé en intégrité. L'agent MIDCOM va toujours être capable d'interpréter les données et va simplement notifier au boîtier de médiation les perforations ouvertes, installer les entrées du tableau de NAT, etc. Noter cependant que le cadre MIDCOM n'aide pas à résoudre le problème du cassage d'IPsec par le NAT car dans ce cas le boîtier de médiation modifie encore les en-têtes IP et de transport.

La sécurité entre un agent MIDCOM et un boîtier de médiation a un certain nombre de composantes. L'autorisation, l'authentification, l'intégrité et la confidentialité. Autorisation se réfère à qui un agent particulier est autorisé à signaler un boîtier de médiation avec des demandes pour une ou plusieurs applications, adhérant à un certain profil de politique. Échouer au processus d'autorisation peut indiquer une tentative de vol de ressources ou un échec dû à des déficiences administratives et/ou d'accréditifs. Dans l'un et l'autre cas, le boîtier de médiation devrait prendre les mesures appropriées pour analyser/enregistrer de telles tentatives et consulter son PDP MIDCOM désigné pour prendre les mesures nécessaires si le boîtier de médiation est configuré de cette façon. Autrement, le boîtier de médiation peut avoir recours à une politique de déni de service par défaut lorsque un agent MIDCOM échoue à produire les accréditifs requis. La Section 6 expose les interactions de boîtier de médiation à PDP MIDCOM en vue de la prise de décisions de politique.

L'authentification se réfère à la confirmation de l'identité à l'origine de tous les datagrammes reçus de celui qui les génère. L'absence d'accréditifs forts pour l'authentification des messages MIDCOM entre un agent et un boîtier de médiation peut sérieusement diminuer le service fondamental rendu par le boîtier de médiation. Une conséquence de la non authentification d'un agent serait qu'un attaquant pourrait usurper l'identité d'un agent "légitime" et ouvrir des perforations dans le pare-feu. Une autre serait qu'il pourrait autrement manipuler l'état sur un boîtier de médiation, créant une attaque de déni de service en fermant des perforations nécessaires ou en remplissant un tableau de NAT. Une conséquence de la non authentification du boîtier de médiation auprès d'un agent est qu'un attaquant pourrait se faire passer pour un boîtier de médiation et répondre aux demandes du NAT d'une manière qui pourrait détourner des données vers l'attaquant. Manquer à soumettre les accréditifs requis/valides, une fois qu'ils sont réclamés, indique une attaque en répétition, auquel cas une action appropriée est nécessaire de la part du boîtier de médiation, comme une inspection, un enregistrement de problème ou la consultation du PDP MIDCOM désigné pour refléter une telle défaillance. Une conséquence de la non protection du boîtier de médiation contre les attaques en répétition serait qu'une perforation spécifique peut être réouverte ou refermée à volonté par un attaquant, bombardant ainsi les hôtes d'extrémité de données non garanties ou causant un déni de service.

L'intégrité est nécessaire pour assurer qu'un message MIDCOM n'a pas été altéré ou détruit accidentellement ou par malveillance. Le résultat d'une absence de mise en application de l'intégrité des données dans un environnement qui n'est

pas de confiance pourrait être qu'un imposteur va altérer les messages envoyés par un agent et amener le boîtier de médiation à s'arrêter ou causer un déni de service pour l'application que l'agent tente d'activer.

La confidentialité des messages MIDCOM assure que les données de signalisation sont accessibles aux seules entités autorisés. Lorsque un agent de boîtier de médiation est déployé dans un environnement qui n'est pas de confiance, l'absence de confidentialité va permettre à un intrus d'effectuer une analyse des flux de trafic et d'espionner le boîtier de médiation. L'intrus pourrait cannibaliser une session MIDCOM moins sécurisée et détruire ou compromettre les ressources du boîtier de médiation qu'il a découvertes sur d'autres sessions. Inutile de dire que la session MIDCOM la moins sécurisée va devenir le tendon d'Achille et rendre le boîtier de médiation vulnérable aux attaques contre la sécurité.

Enfin, il peut y avoir une faiblesse de la sécurité pour les applications qui traversent un boîtier de médiation lorsque une ressource sur un boîtier de médiation est contrôlée par plusieurs agents externes. Un service de boîtier de médiation peut être interrompu du fait de directives contradictoires provenant de plusieurs agents associés à différentes fonctions de boîtier de médiation mais appliquées à la même session d'application. Il faut prendre soin de s'assurer lors de la conception des protocoles de ce que les agents pour une fonction ne sautent pas abruptement une ressources impactant une fonction différente. Autrement, la sévérité de telles manifestations pourrait être atténuée lorsque un seul agent MIDCOM est charge de la prise en charge de tous les services de boîtier de médiation pour une application, du fait de la complexité réduite et de l'effort de synchronisation pour gérer les ressources du boîtier de médiation.

Références

(Les liens sur les numéros de RFC pointent sur le texte anglais, ceux dans le corps du titre sur la traduction française)

[SIP] J. Rosenberg et autres, "SIP : Protocole d'initialisation de session", RFC3261, juin 2002. (*Mise à jour par* RFC3265, RFC3853, RFC4320, RFC4916, RFC5393)

[SDP] M. Handley et V. Jacobson, "SDP : Protocole de description de session", RFC2327, avril 1998. *(Obsolète, voir* RFC4566, *MàJ par* RFC3266)

[H.323] Recommandation UIT-T H.323. "Systèmes de communications multimédia fondés sur le paquet", 1998.

[RTP] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : protocole de transport pour applications en temps réel", RFC1889, janvier 1996. *(Obsolète, voir* RFC3550 *STD64)*

[RTSP] H. Schulzrinne, A. Rao et R. Lanphier, "Protocole de flux directs en temps réel (RTSP)", RFC2326, avril 1998.

[FTP] J. Postel et J. Reynolds, "Protocole de transfert de fichiers (FTP)", RFC0959, STD 9, octobre 1985.

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

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

[NAT-PT] G. Tsirtsis, P. Srisuresh, "Traduction d'adresse réseau – traduction de protocole (NAT-PT)", RFC2766, février 2000. (*Obsolète, voir* RFC4966) (*MàJ par* RFC3152) *(Historique)*

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

[IPsec-ESP] S. Kent et R. Atkinson, "Encapsulation de charge utile de sécurité IP (ESP)", RFC2406, novembre 1998. *(Obsolète, voir RFC 4303)*

[TLS] T. Dierks et C. Allen, "Protocole TLS version 1.0", RFC2246, janvier 1999. *(Obsolète, voir* RFC4346, *MàJ par* RFC3546, RFC5746

[POL-TERM] A. Westerinen, J. Schnizlein, J. Strassner, M. Scherling, B. Quinn, S. Herzog, A. Huynh, M. Carlson, J. Perry et S. Waldbusser, "Terminologie pour la gestion fondée sur la politique", RFC3198, novembre 2001. *(Information)*

[REQMTS] Swale, R. P., Mart, P. A., Sijben, P., Brim, S. and M. Shore, "Exigences du protocole de communications par boîtier de médiation (midcom)", RFC3304, août 2002. *(Information)*

Adresse des auteurs

Pyda Srisuresh
Kuokoa Networks, Inc.
475 Potrero Ave.
Sunnyvale, CA 94085
mél : srisuresh@yahoo.com

Jiri Kuthan
Fraunhofer Institute FOKUS
Kaiserin-Augusta-Allee 31
D-10589 Berlin, Germany
mél : kuthan@fokus.fhg.de

Jonathan Rosenberg
dynamicsoft
72 Eagle Rock Avenue
First Floor
East Hanover, NJ 07936
U.S.A.
mél : jdrosen@dynamicsoft.com

Andrew Molitor
Aravox technologies
4201 Lexington Avenue North, Suite 1105
Arden Hills, MN 55126
U.S.A.
voice: (651) 256-2700
mél : amolitor@visi.com

Abdallah Rayhan
WINCORE Lab
Electrical and Computer Engineering
Ryerson University
350 Victoria Street
Toronto, ON M5B 2K3
mél : rayhan@ee.ryerson.ca,
ar_rayhan@yahoo.ca

Déclaration complète de droits de reproduction

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