Groupe de travail Réseau
Request for Comments : 4849
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Congdon, Hewlett Packard Company
M. Sanchez, Hewlett Packard Company
B. Aboba, Microsoft Corporation
avril 2007

Attribut Règle de filtre RADIUS

Résumé
Alors que la RFC 2865 définit l'attribut Filter-Id *(identifiant de filtre)* elle exige que le serveur d'accès réseau (NAS, *Network Access Server*) soit pré rempli avec les filtres désirés. Cependant, dans des situations où l'opérateur du serveur ne sait pas quels filtres ont été pré remplis, il est utile de spécifier explicitement les règles de filtre. Le présent document définit l'attribut NAS-Filter-Rule *(règle de filtre de NAS)* au sein du service d'accès commuté entrant d'utilisateur distant (RADIUS, *Remote Authentication Dial In User Service*). Cet attribut se fonde sur la paire valeur-attribut (AVP, *Attribute Value Pair*) NAS-Filter-Rule Diameter décrite dans la RFC 4005, avec la syntaxe IPFilterRule définie dans la RFC 3588.

Table des matières

1. Introduction

Le présent document définit l'attribut NAS-Filter-Rule *(règle de filtre de serveur d'accès réseau)* au sein du service d'accès commuté entrant d'utilisateur distant (RADIUS, *Remote Authentication Dial In User Service*). Cet attribut a la même fonction que l'AVP Diameter NAS-Filter-Rule (400) définie au paragraphe 6.6 de la [RFC4005] et la même syntaxe qu'une IPFilterRule définie au paragraphe 4.3 de la [RFC3588]. Cet attribut peut se révéler utile pour provisionner les règles de filtre.

Alors que le paragraphe 5.11 de la [RFC2865] définit l'attribut Identifiant de filtre (11), il exige que le serveur d'accès réseau (NAS, *Network Access Server*) soit pré rempli avec les filtres désirés. Cependant, dans des situations où l'opérateur du serveur ne sait pas quels filtres ont été pré remplis, il est utile de spécifier explicitement les règles de filtre.

1.1 Terminologie

Le présent document utilise les termes suivants :

Serveur d'accès réseau (NAS) : appareil qui fournit un service d'accès à un utilisateur d'un réseau.

Serveur RADIUS : un serveur d'authentification RADIUS est une entité qui fournit un service d'authentification à un NAS.

Mandataire RADIUS : un mandataire RADIUS agit comme un serveur d'authentification au NAS, et comme un client RADIUS au serveur RADIUS.

1.2 Langage des exigences

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

1.3 Interprétation de l'attribut

Si un NAS conforme à la présente spécification reçoit un paquet Access-Accept contenant un attribut NAS-Filter-Rule qu'il ne peut pas appliquer, il DOIT agir comme si il avait reçu un Access-Reject. La [RFC3576] exige qu'un NAS qui reçoit une demande de changement d'autorisation (CoA-Request, *Change of Authorization Request*) réponde avec un CoA-NAK si la demande contient un attribut non pris en charge. Il est RECOMMANDÉ qu'un attribut Cause d'erreur avec une valeur de "Attribut non pris en charge" (401) soit inclus dans le CoA-NAK. Comme noté dans la [RFC3576], les changements d'autorisation sont atomiques de sorte que cette situation ne résulte pas en la terminaison de la session, et que la configuration pré-existante reste inchangée. Par suite, aucun paquet de comptabilité ne devrait être généré à cause de la CoA-Request.

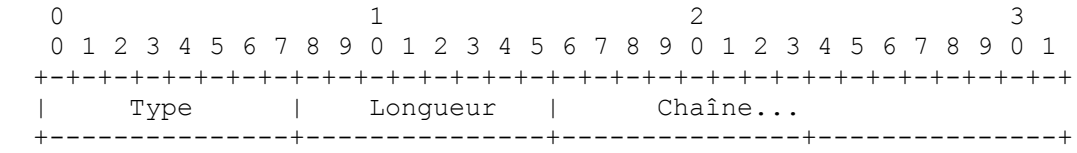
2. Attribut NAS-Filter-Rule

Description : cet attribut indique les règles de filtre à appliquer pour cer utilisateur. Zéro, un ou plusieurs attributs NAS-Filter-Rule PEUVENT être envoyés dans un paquet Access-Accept, CoA-Request, ou Accounting-Request.

L'attribut NAS-Filter-Rule n'est pas destiné à être utilisé en concurrence avec tout autre attribut de règle de filtre, incluant les attributs Filter-Id (11) et NAS-Traffic-Rule [Traffic]. Les attributs NAS-Filter-Rule et NAS-Traffic-Rule NE DOIVENT PAS apparaître dans le même paquet RADIUS. Si un attribut NAS-Traffic-Rule est présent, un NAS qui met en œuvre la présente spécification DOIT éliminer en silence tous les attributs NAS-Filter-Rule qui sont présents. Les attributs Filter-Id et NAS-Filter-Rule NE DEVRAIENT PAS apparaître dans le même paquet RADIUS. Étant donnée l'absence dans la [RFC4005] de règles de préséance bien définies pour combiner les attributs Filter-Id et NAS-Filter-Rule dans un seul ensmble de règles, le comportement des NAS qui reçoivent les deux attributs est indéfini, et donc une mise en œuvre de serveur RADIUS ne peut pas supposer un comportement cohérent.

Lorsque plusieurs attributs NAS-Filter-Rule sont inclus dans un paquet RADIUS, les champs Chaîne des attributs sont à enchaîner pour former un ensemble de règles de filtre. Comme noté au paragraphe 2.3 de la [RFC2865], "le serveur émetteur NE DOIT PAS changer l'ordre des attributs de même type", de sorte que les mandataires RADIUS ne vont pas réordonner les attributs NAS-Filter-Rule.

Un sommaire du format de l'attribut NAS-Filter-Rule est présenté ci-dessous. Les champs sont transmis de gauche à droite.



Type : 92

Longueur : ≥ 3

Chaîne : le champ Chaîne fait un ou plusieurs octets. Il contient les règles de filtre dans la syntaxe IPFilterRule définie au paragraphe 4.3 de la [RFC3588], avec les règles individuelles de filtre séparées par un NUL (0x00). Un attribut NAS-Filter-Rule peut contenir une règle partielle, une règle, ou plus d'une règle. Les règles de filtre peuvent être

continuées à travers les limites d'attribut, de sorte que les mises en œuvre ne peuvent pas supposer que les règles individuelles de filtre commencent ou finissent sur des limites d'attribut.

L'ensemble des attributs NAS-Filter-Rule DEVRAIT être créé en enchaînant les règles de filtre individuelles, séparées par un octet NUL (0x00). Les données résultantes devraient être partagées sur des limites de 253 octets pour obtenir un ensemble d'attributs NAS-Filter-Rule. À réception, les règles de filtre individuelles sont déterminées en enchaînant le contenu de tous les attributs NAS-Filter-Rule, et en séparant les règles de filtre individuelles avec l'octet NUL (0x00) comme délimiteur.

3. Tableau des attributs

Le tableau suivant indique quels attributs peuvent se trouver avec quelles sortes de paquets, et en quelle quantité.

Demande d'accès	Accès accepté	Accès rejeté	Défi d'accès	Demande de CoA	Demande de compta.	N°	Attribut
0	0+	0	0	0+	0+	92	NAS-Filter-Rule

La signification des entrées du tableau ci-dessus est la suivante :
0 : cet attribut NE DOIT PAS être présent dans le paquet.
0+ : zéro, une ou plusieurs instances de cet attribut PEUVENT être présentes dans le paquet.
0-1 : zéro ou une instance de cet attribut PEUT être présente dans le paquet.

4. Considérations sur Diameter

Le paragraphe 6.6 de la [RFC4005] définit l'AVP NAS-Filter-Rule (400) avec la même fonction que l'attribut RADIUS NAS-Filter-Rule. Pour assurer l'interopérabilité, les passerelles Diameter/RADIUS devront être configurées à traduire l'attribut RADIUS 92 en AVP Diameter NAS-Filter-Rule (400) et vice versa.

Lors de la traduction des AVP Diameter NAS-Filter-Rule en attributs RADIUS NAS-Filter-Rule, l'ensemble d'attributs NAS-Filter-Rule est créé en enchaînant les règles de filtre individuelles, séparées par un octet NUL. Les données résultantes DEVRAIENT alors être séparées sur les limites de 253 octets.

Lors de la traduction des attributs RADIUS NAS-Filter-Rule en AVP Diameter NAS-Filter-Rule, les règles individuelles sont détérminées en enchaînant le contenu de tous les attributs NAS-Filter-Rule, et en séparant ensuite les règles de filtre individuelles avec l'octet NUL comme délimiteur. Chaque règle est alors codée comme une seule AVP Diameter NAS-Filter-Rule.

Noter qu'un message Diameter traduit peut être plus grand que la taille maximum de paquet RADIUS (4096 octets). Lorsque une passerelle Diameter/RADIUS reçoit un message Diameter contenant une AVP NAS-Filter-Rule qui est trop grosse pour tenir dans un paquet RADIUS, la passerelle Diameter/RADIUS va répondre à l'homologue Diameter d'origine avec une AVP Code de résultat de valeur DIAMETER_RADIUS_AVP_UNTRANSLATABLE (5018), et avec une AVP Failed-AVP contenant l'AVP NAS-Filter-Rule. Comme la réparation de l'erreur va probablement exiger de reprendre les règles de filtre, l'homologue générateur devrait traiter la combinaison d'une AVP Result-Code de valeur DIAMETER_RADIUS_AVP_UNTRANSLATABLE et d'une AVP Failed-AVP contenant une AVP NAS-Filter-Rule comme une erreur terminale.

5. Considérations relatives à l'IANA

La présente spécification ne crée aucun nouveau registre.

Le présent document utilise l'espace de noms de RADIUS [RFC2865], voir <http://www.iana.org/assignments/radius-types>. Une valeur a été allouée dans la section "Types d'attributs RADIUS". L'attribut RADIUS pour lequel une valeur a été allouée est :

92 - NAS-Filter-Rule

Le présent document utilise aussi l'espace de noms Diameter [RFC3588]. Une valeur d'AVP de code de résultat Diameter pour l'erreur DIAMETER_RADIUS_AVP_UNTRANSLATABLE a été allouée. Comme c'est une défaillance permanente, l'allocation (5018) est dans la gamme 5xxx.

6. Considérations sur la sécurité

La présente spécification décrit l'utilisation de RADIUS aux fins d'authentification, d'autorisation et de comptabilité. Les menaces et les problèmes de sécurité pour cette application sont décrits dans les [RFC3579] et [RFC3580] ; les problèmes de sécurité rencontrés dans l'itinérance sont décrits dans la [RFC2607].

Le présent document spécifie un nouvel attribut qui peut être inclus dans les paquets RADIUS existants, qui sont protégés comme décrit dans les [RFC3579] et [RFC3576]. Voir dans ces documents une description plus détaillée.

Les mécanismes de sécurité pris en charge par RADIUS et Diameter se concentrent sur la prévention d'une attaque d'usurpation de paquets ou de modification des paquets en transit. Ils n'empêchent pas un serveur ou mandataire RADIUS/Diameter autorisé de modifier, insérer, ou supprimer des attributs dans une intention malveillante. Les attributs de filtre modifiés ou supprimés par un mandataire RADIUS/Diameter peuvent permettre à un utilisateur d'obtenir un accès réseau sans les filtres appropriés ; si le mandataire devait aussi modifier les paquets de comptabilité, alors la modification ne serait pas reflétée dans les journaux du serveur de comptabilité.

Comme le protocole RADIUS ne prend actuellement pas en charge la négociation de capacités, un serveur RADIUS ne peut pas découvrir automatiquement si un NAS prend en charge l'attribut NAS-Filter-Rule. Un NAS traditionnel non conforme à la présente spécification peut éliminer en silence l'attribut NAS-Filter-Rule tout en permettant à l'utilisateur d'accéder au réseau. Cela peut causer une réception inappropriée par l'utilisateur d'un accès non filtré au réseau. Par suite, l'attribut NAS-Filter-Rule NE DEVRAIT être envoyé qu'à un NAS connu pour le prendre en charge.

7. Références

7.1 Références normatives

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

[RFC2865] C. Rigney et autres, "Service d'authentification à distance de l'utilisateur appelant (RADIUS)", juin 2000. (*MàJ par* RFC2868, RFC3575, RFC5080, RFC8044) *(D.S.)*

[RFC3588] P. Calhoun et autres, "Protocole fondé sur Diameter", septembre 2003. (*Remplacée par la* RFC6733) *(P.S.)*

[RFC4005] P. Calhoun et autres, "Application de serveur d'accès au réseau Diameter", août 2005. *(P.S.) (Remplacée par* RFC7155)

7.2 Références pour information

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

[RFC3576] M. Chiba et autres, "Extensions d'autorisation dynamique au service d'authentification distante d'utilisateur appelant (RADIUS)", juillet 2003. (*Obsolète, voir* RFC5176) *(Information)*

[RFC3579] B. Aboba, P. Calhoun, "Prise en charge du protocole d'authentification extensible (EAP) par RADIUS", septembre 2003. (*MàJ par* RFC5080) *(Information)*

[RFC3580] P. Congdon et autres, "Lignes directrices pour l'utilisation du service d'authentification distante d'utilisateur appelant (RADIUS) par IEEE 802.1X", septembre 2003. *(Information)*

[Traffic] Congdon, P., Sanchez, M., Lior, A., Adrangi, F., and B. Aboba, "RADIUS Attributes for Filtering and

Redirection", Travail en cours, mars 2007.

8. Remerciements

Les auteurs tiennent à remercier Emile Bergen, Alan DeKok, Greg Weber, Glen Zorn, Pasi Eronen, David Mitton, et David Nelson de leurs contributions au présent document.

Adresse des auteurs

Paul Congdon
Hewlett Packard Company
ProCurve Networking by HP
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747
mél : paul.congdon@hp.com

Mauricio Sanchez
Hewlett Packard Company
ProCurve Networking by HP
8000 Foothills Blvd, M/S 5662
Roseville, CA 95747
mél : mauricio.sanchez@hp.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
mél : bernarda@microsoft.com

Déclaration complète de droits de reproduction

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