Groupe de travail Réseau
Request pour Comments: 2868
RFC mise à jour : RFC 2865
Catégorie : Information

Traduction Claude Brière de L'Isle, janvier 2008

G. Zorn, Cisco Systems, Inc.
D. Leifer, A. Rubens, Ascend Communications
J. Shriver, Intel Corporation
M. Holdrege, ipVerse
I. Goyret, Lucent Technologies
juin 2000

Attributs RADIUS pour la prise en charge du protocole de tunnelage

Statut de ce mémoire
Le présent mémoire donne des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme pour l'Internet. La distribution du présent mémo n'est soumise à aucune restriction.

Résumé
Le présent document définit un ensemble d'attributs RADIUS conçus pour la prise en charge de la fourniture du tunnelage obligatoire dans les réseaux à accès par numérotation.

1 Motivation

De nombreuses applications de protocoles de tunnelage comme L2TP impliquent un accès numéroté au réseau. Certaines, comme la fourniture d'accès aux intranets d'entreprise via l'Internet, sont caractérisées par le tunnelage volontaire : le tunnel est créé à la demande de l'usager pour un objet spécifique. D'autres applications impliquent un tunnelage obligatoire : le tunnel est créé sans aucune action de l'usager et sans permettre à l'usager de choix en la matière. Afin de fournir cette fonctionnalité, de nouveaux attributs RADIUS sont nécessaires pour porter les informations de tunnelage du serveur RADIUS aux points d'extrémité du tunnel ; le présent document définit ces attributs. On trouvera dans la RFC 2809 des recommandations spécifiques et des exemples pour l'application de ces attributs à L2TP.

2 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit en [14]. Ces mots clé signifient la même chose en majuscule ou en minuscules.

3 Attributs

Plusieurs instances de chacun des attributs définis ci-dessous peuvent être incluses dans un seul paquet RADIUS. Dans ce cas, les attributs à appliquer à tout tunnel DEVRAIENT tous contenir la même valeur dans leur champ Marqueur respectif ; autrement, le champ Marqueur NE DEVRAIT PAS être utilisé.

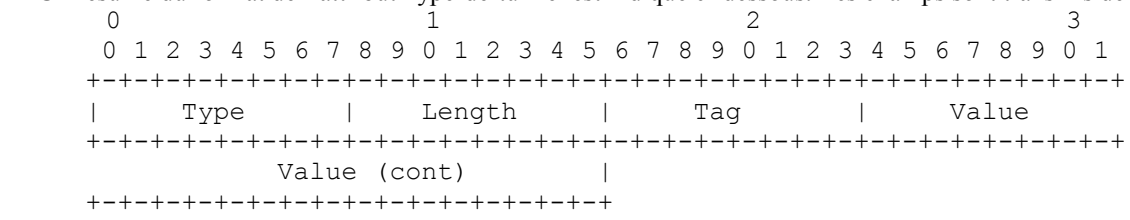
Si le serveur RADIUS retourne des attributs décrivant plusieurs tunnels, alors les tunnels DEVRAIENT être interprétés par l'initiateur de tunnel comme des solutions de remplacement et le serveur DEVRAIT inclure une instance de l'attribut Préférence-de-tunnel dans l'ensemble des attributs appartenant à chaque tunnel de remplacement. De même, si le client RADIUS inclut plusieurs ensembles d'attributs de tunnel dans un paquet de Demande-d'accès, tous les attributs appartenant à un tunnel donné DEVRAIENT contenir la même valeur dans leurs champs Marqueur respectifs et chaque ensemble DEVRAIT inclure une instance de la valeur appropriée de l'attribut Préférence-de-tunnel.

3.1 Type-de-tunnel

Description
Cet attribut indique le ou les protocoles de tunnelage à utiliser (dans le cas de l'initiateur de tunnel) ou le protocole de tunnelage utilisé (dans le cas d'une terminaison de tunnel). Il PEUT être inclus dans des paquets Demande-d'accès, Accès-Accepté et Demande-de-comptabilité. Si l'attribut Type-de-tunnel est présent dans un paquet Demande-d'accès envoyé par un initiateur de tunnel, il DEVRAIT être considéré comme une indication au serveur RADIUS des protocoles de tunnelage acceptés par le point d'extrémité de tunnel ; le serveur RADIUS PEUT cependant ignorer cette indication. Un initiateur de tunnel n'est pas obligé de mettre en œuvre un de ces types de tunnel ; si un initiateur de tunnel reçoit un paquet Accès-Accepté qui contient seulement des Type-de-tunnel inconnus ou non pris en charge, l'initiateur de tunnel DOIT se comporter comme si un Rejet-d'accès avait été reçu à la place.

Si l'attribut Type-de-tunnel est présent dans un paquet Demande-d'accès envoyé par une terminaison de tunnel, il DEVRAIT le considérer comme signifiant le protocole de tunnelage utilisé. Dans ce cas, si le serveur RADIUS détermine que l'utilisation du protocole communiqué n'est pas autorisée, il PEUT retourner un paquet Rejet-d'accès. Si une terminaison de tunnel reçoit un paquet Accès-accepté qui contient un ou plusieurs attributs Type-de-tunnel, dont aucun ne représente le protocole de tunnelage utilisé, la terminaison de tunnel DEVRAIT se comporter comme si un Rejet-d'accès avait été reçu à la place.

Un résumé du format de l'attribut Type-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 64 pour Type-de-tunnel

Longueur : Toujours 6.

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet les attributs qui se réfèrent au même tunnel. Les valeurs valides pour ce champ sont 0x01 à 0x1F, inclus. Si le champ Marqueur n'est pas utilisé, il DOIT être à zéro (0x00).

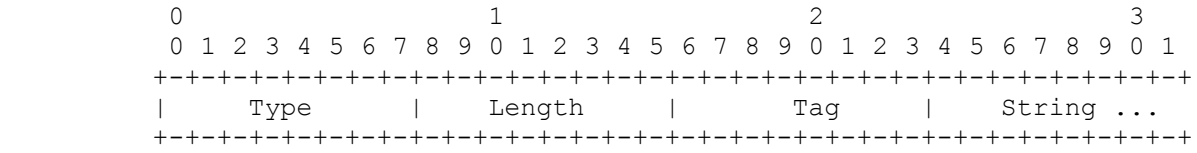
Valeur
Le champ Valeur est de trois octets et contient une des valeurs suivantes, qui indiquent le type de tunnel à lancer.

1 Protocole de tunnelage point à point (PPTP) [1]
2 Transmission de couche 2 (L2F) [2]
3 Protocole de tunnelage de couche 2 (L2TP) [3]
4 Protocole de gestion de tunnel ascendant (ATMP) [4]
5 Protocole de tunnelage virtuel (VTP)
6 En-tête d'authentification IP en mode tunnel (AH) [5]
7 Encapsulation IP dans IP (IP-IP) [6]
8 Encapsulation IP dans IP minimale (MIN-IP-IP) [7]
9 Encapsulation de charge utile de sécurité IP en mode tunnel (ESP) [8]
10 Encapsulation de route générique (GRE) [9]
11 Services virtuels à fenêtre de numérotation (DVS)
12 Tunnelage IP dans IP [10]

3.2 Type-de-support–de-tunnel

Description
L'attribut Type-de-support-de-tunnel indique quel support de transport utiliser à la création d'un tunnel pour ces protocoles (tels que L2TP) qui peuvent fonctionner sur plusieurs transports. Il PEUT être inclus aussi bien dans les paquets Demande-d'accès que Accès-accepté ; si il est présent dans un paquet Demande-d'accès, il DEVRAIT être pris comme une indication du serveur RADIUS sur les supports de tunnel acceptés par le point de terminaison de tunnel. Le serveur RADIUS PEUT cependant ignorer l'indication.

Un résumé du format de l'attribut Type-de-support-de-tunnel est donné ci-dessous. Les champs sont transmis de gauche à droite.



Type : 65 pour Type-de-support-de-tunnel

Longueur : 6

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Les valeurs valides pour ce champ sont de 0x01 à 0x1F, inclus. Si le champ Marqueur n'est pas utilisé, elle DOIT être zéro (0x00).

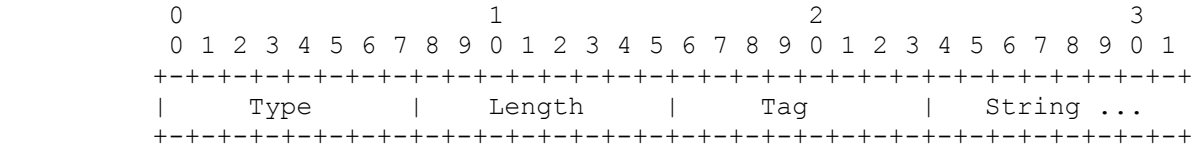
Valeur
Le champ Valeur est de trois octets et contient une des valeurs de la liste figurant sous "Numéros de famille d'adresse" dans [14]. Un extrait des valeurs pertinentes de la liste est reproduit ici pour faciliter la lecture.

1	IPv4 (IP version 4)
2	IPv6 (IP version 6)
3	NSAP
4	HDLC (8-bit multidrop)
5	BBN 1822
6	802 (inclut tous les supports 802 plus Ethernet "format canonique")
7	E.163 (POTS)
8	E.164 (SMDS, Relais de trame, ATM)
9	F.69 (Telex)
10	X.121 (X.25, Relais de trame)
11	IPX
12	Appletalk
13	Decnet IV
14	Banyan Vines
15	E.164 avec sous-adresse de format NSAP

3.3 Extrémité-client-de-tunnel

Description
Cet attribut contient l'adresse de l'extrémité initiatrice du tunnel. Il PEUT être inclus à la fois dans les paquets Demande-d'accès et Accès-accepté pour indiquer l'adresse à partir de laquelle un nouveau tunnel doit être initié. Si l'attribut Extrémité-client-de-tunnel est inclus dans un paquet Demande-d'accès, le serveur RADIUS devrait considérer la valeur comme une indication ; le serveur n'est cependant pas obligé de respecter l'indication. Cet attribut DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent des attributs Type-d'état-de-compta avec des valeurs de Début ou Fin, auquel cas il indique l'adresse à partir de laquelle le tunnel a été initié. Cet attribut, avec les attributs Extrémité-serveur-de-tunnel et Identifiant-de-connexion-de-tunnel-de-compta, peut être utilisé pour fournir un moyen universellement unique d'identifier un tunnel pour les besoins comptables et de vérification.

Un résumé du format de l'attribut Extrémité-client-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 66 pour Extrémité-client-de-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet les attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieure à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (ou diverses solutions de remplacement) cet attribut appartient. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme premier octet du champ Chaîne suivant.

Chaîne
Le format de l'adresse représentée par le champ Chaîne dépend de la valeur de l'attribut Type-de-support-de-tunnel.

Si Type-de-support-de-tunnel est IPv4 (1), cette chaîne est alors le nom de domaine pleinement qualifié (FQDN) de la machine cliente du tunnel, ou c'est une adresse IP "en décimal séparé par des points". Les mises en œuvre conformes DOIVENT accepter le format en décimal séparé par des points et DEVRAIENT accepter le format FQDN pour les adresses IP.

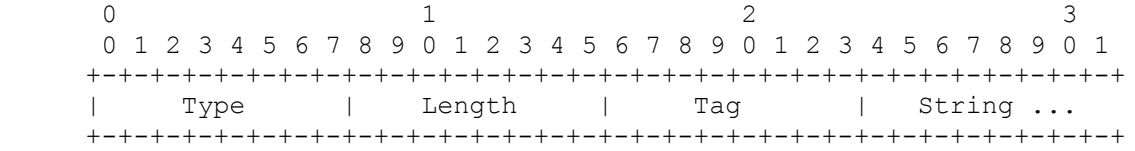
Si Type-de-support-de-tunnel est IPv6 (2), la chaîne est le FQDN de la machine cliente du tunnel, ou c'est une représentation textuelle de l'adresse dans la forme préférée ou dans une forme de remplacement [17]. Les mises en œuvre conformes DOIVENT accepter la forme préférée et DEVRAIENT accepter à la fois la forme textuelle de remplacement et le format FQDN pour les adresses IPv6.

Si Type-de-support-de-tunnel n'est ni IPv4 ni IPv6, cette chaîne est une étiquette se référant à des données de configuration locales du client RADIUS qui décrivent l'interface et l'adresse spécifique du support à utiliser.

3.4 Extrémité-serveur-de-tunnel

Description
Cet attribut indique l'adresse de l'extrémité serveur du tunnel. L'attribut Extrémité-serveur-de-tunnel PEUT être inclus (comme indication au serveur RADIUS) dans le paquet Demande-d'accès et DOIT être inclus dans le paquet Accès-accepté si l'initiation d'un tunnel est désirée. Il DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent des attributs Type-d'état-de-compta dont les valeurs sont Début ou Fin et qui appartiennent à une session tunnelée. Cet attribut, avec les attributs Extrémité-client-de-tunnel et Identifiant-de-connexion-de-tunnel-de-compta [11], peut être utilisé pour fournir un moyen universellement unique pour identifier un tunnel pour les besoins comptables et de vérification.

Un résumé du format de l'attribut Extrémité-serveur-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 67 pour Extrémité-serveur-de-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet les attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieure à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) cet attribut appartient. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme le premier octet du champ Chaîne suivant.

Chaîne
Le format de l'adresse représentée par le champ Chaîne dépend de la valeur de l'attribut Type-de-support-de-tunnel. Si Type-de-support-de-tunnel est IPv4 (1), alors cette chaîne est soit un nom de domaine pleinement qualifié (FQDN) de la machine cliente du tunnel, soit une adresse IP en "décimal séparé par des points". Les mises en œuvre conformes DOIVENT accepter le format décimal séparé par des points et DEVRAIENT accepter le format FQDN pour les adresses IP.

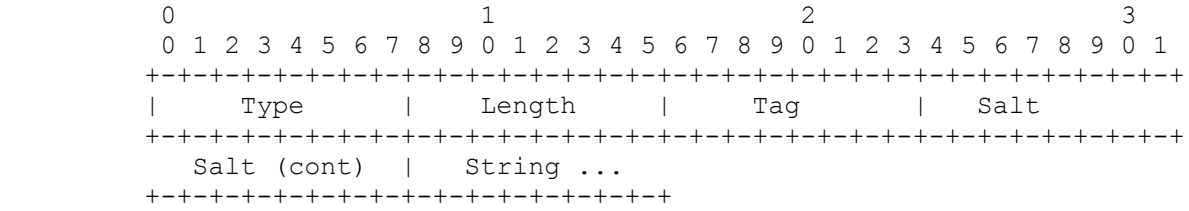
Si Type-de-support-de-tunnel est IPv6 (2), cette chaîne est alors soit le FQDN de la machine cliente du tunnel, soit une représentation textuelle de l'adresse dans la forme préférée ou de remplacement [17]. Les mises en œuvre conformes DOIVENT accepter la forme préférée et DEVRAIENT accepter les deux formes de texte de remplacement et de format FQDN pour les adresses IPv6.

Si Type-de-support-de-tunnel n'est ni IPv4 ni IPv6, cette chaîne est une étiquette se rapportant aux données de configuration locales du client RADIUS qui décrivent l'interface et l'adresse spécifique de support à utiliser.

3.5 Mot-de-passe-de-tunnel

Description
Cet attribut peut contenir un mot de passe à utiliser pour authentifier un serveur distant. Il ne peut être inclus que dans un paquet Accès-accepté.

Un résumé du format de l'attribut Mot-de-passe-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 69 pour Mot-de-passe-de-tunnel

Longueur : ≥ 5

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Les valeurs valides pour ce champ sont de 0x01 à 0x1F, inclus. Si la valeur du champ Marqueur est supérieure à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) appartient cet attribut ; autrement, le champ Marqueur DEVRAIT être ignoré.

Sel
Le champ Sel est long de deux octets et est utilisé pour s'assurer de l'unicité de la clé de chiffrement utilisée pour chiffrer chaque instance de l'attribut Mot-de-passe-de-tunnel survenant dans un paquet Accès-accepté donné. Le bit de plus fort poids (le plus à gauche) du champ Sel DOIT être établi (mis à 1). Le contenu de chaque champ Sel dans un paquet Accès-accepté donné DOIT être unique.

Chaîne
Le champ Chaîne en texte en clair consiste en trois sous-champs logiques : les champs Longueur-de-données et Mot-de-passe (tous deux sont exigés), et le sous-champ facultatif Bourrage. Le sous-champ Longueur-de-données est long d'un octet et contient la longueur du sous-champ Mot-de-passe non chiffré. Le sous-champ Mot-de-passe contient le mot de passe de tunnel réel. Si la longueur combinée (en octets) des sous-champs Longueur-de-données et Mot-de-passe non chiffrés n'est pas un multiple pair de 16, le sous-champ Bourrage DOIT alors être présent. Si il est présent, la longueur du sous-champ Bourrage est variable, entre 1 et 15 octets. Le champ Chaîne DOIT être chiffré comme suit, avant la transmission :

Construire une version non chiffrée du champ Chaîne en enchaînant les sous-champs Longueur-de-données et Mot-de-passe. Si nécessaire, bourrer la chaîne résultante jusqu'à ce que sa longueur (en octets) soit un multiple pair de 16. Il est recommandé d'utiliser des octets à zéro (0x00) pour le bourrage. Appelons ce texte en clair P.

Appelons S le secret partagé, R l'authentificateur pseudo-aléatoire de 128 bits de la demande (d'après le paquet de Demande-d'accès correspondant) et A le contenu du champ Sel. Découpons P en tronçons de 16 octets p(1), p(2)...p(i), où i = longueur de (P)/16. Appelons c(1), c(2)...c(i) les blocs de texte chiffré et C le texte chiffré final. Des valeurs intermédiaires b(1), b(2)...c(i) sont nécessaires. Le chiffrement est effectué de la façon suivante ('+' indique l'enchaînement) :

```
b(1) = MD5(S + R + A)     c(1) = p(1) xor b(1)     C = c(1)
b(2) = MD5(S + c(1))      c(2) = p(2) xor b(2)     C = C + c(2)
        .                         .                      .
        .                         .                      .
        .                         .                      .
b(i) = MD5(S + c(i-1))    c(i) = p(i) xor b(i)     C = C + c(i)
```

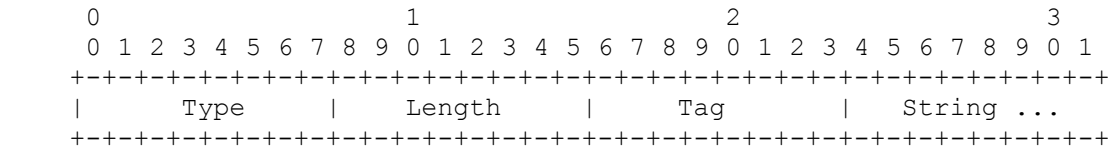
Le champ Chaîne chiffré résultant contiendra c(1)+c(2)+...+c(i).

À réception, le processus est inversé pour donner la chaîne en clair.

3.6 Identifiant-de-groupe-privé-de-tunnel

Description
Cet attribut indique l'identifiant de groupe pour une session en tunnel particulière. L'attribut Identifiant-de-groupe-privé-de-tunnel PEUT être inclus dans le paquet Demande-d'accès si l'initiateur de tunnel peut pré-déterminer le groupe résultant d'une connexion particulière et DEVRAIT être inclus dans le paquet Accès-accepté si cette session en tunnel est à traiter comme appartenant à un groupe privé particulier. Les groupes privés peuvent être utilisés pour associer une session en tunnel à un groupe d'utilisateurs particuliers. Par exemple, ils peuvent être utilisés pour faciliter l'acheminement d'adresses IP non enregistrées à travers une interface particulière. Il DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent des attributs Type-d'état-de-compta avec des valeurs de Début ou Fin et qui appartiennent à une session en tunnel.

Un résumé du format de l'attribut Identifiant-de-groupe-privé-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 81 pour Identifiant-de-groupe-privé-de-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieure à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) appartient cet attribut. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme le premier octet du champ Chaîne suivant.

Chaîne
Ce champ doit être présent. Le groupe est représenté par le champ Chaîne. Il n'y a pas de restriction sur le format des identifiants de groupe.

3.7 Identifiant-d'allocation-de-tunnel

Description
Cet attribut est utilisé pour indiquer à l'initiateur du tunnel le tunnel particulier auquel une session doit être alloué. Certains protocoles de tunnelage, comme PPTP et L2TP, permettent de multiplexer des sessions entre les deux mêmes extrémités de tunnel sur le même tunnel et aussi qu'une session donnée utilise son propre tunnel dédié. Cet attribut fournit un mécanisme pour utiliser RADIUS afin d'informer l'initiateur du tunnel (par exemple, PAC, LAC) s'il faut allouer la session à un tunnel multiplexé ou à un tunnel séparé. De plus, il permet que des sessions qui partagent des tunnels multiplexés se voient allouer des tunnels multiplexés différents.

Une mise en œuvre de tunnelage particulière peut allouer des caractéristiques différentes à des tunnels particuliers. Par exemple, des tunnels différents peuvent se voir allouer des paramètres de qualité de service différents. De tels tunnels

peuvent être utilisés pour porter des sessions individuelles ou multiples. L'attribut Identifiant-d'allocation-de-tunnel permet donc au serveur RADIUS d'indiquer qu'une session particulière soit allouée à un tunnel qui fournisse un niveau de service approprié. Il est prévu que tout attribut RADIUS en rapport avec la qualité de service défini à l'avenir qui accompagne cet attribut sera associé par l'initiateur de tunnel à l'identifiant donné par cet attribut. En attendant, toute la sémantique donnée à une chaîne d'identifiant particulière est laissé à la configuration locale dans l'initiateur de tunnel.

L'attribut Identifiant-d'allocation-de-tunnel n'a de signification que pour RADIUS et l'initiateur de tunnel. l'identifiant qu'il spécifie est destiné uniquement à une utilisation locale pour RADIUS et l'initiateur de tunnel. L'identifiant alloué par l'initiateur de tunnel n'est pas convoyé à l'homologue du tunnel.

Cet attribut PEUT être inclus dans Accès-accepté. L'initiateur de tunnel qui reçoit cet attribut PEUT choisir de l'ignorer et d'allouer la session à un tunnel arbitraire multiplexé ou non multiplexé entre les extrémités désirées. Cet attribut DEVRAIT aussi être inclus dans les paquets Demande-de-comptabilité qui contiennent les Type-d'état-de-compta avec les valeurs de Début ou Fin et qui appartiennent à une session en tunnel.

Si un initiateur de tunnel prend en charge l'attribut Identifiant-d'allocation-de-tunnel, il devrait alors allouer une session à un tunnel de la façon suivante :

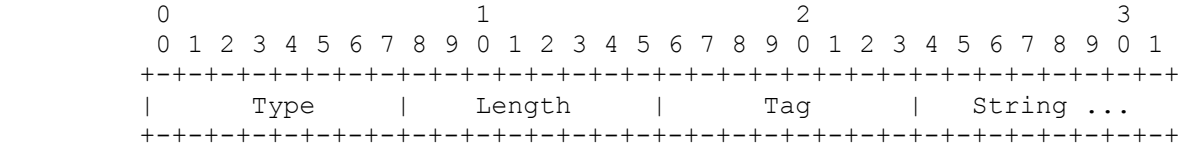
Si cet attribut est présent et qu'un tunnel existe entre les points d'extrémité spécifiés avec l'identifiant spécifié, la session devrait alors être allouée à ce tunnel.

Si cet attribut est présent et si aucun tunnel n'existe entre les points d'extrémité spécifiés avec l'identifiant spécifié, un nouveau tunnel devrait être établi pour la session et l'identifiant spécifié devrait être associé au nouveau tunnel.

Si cet attribut n'est pas présent, la session est alors allouée à un tunnel non désigné. S'il n'existe pas encore de tunnel non désigné entre les points d'extrémité spécifiés, il en est alors établi un qui est utilisé pour cette session et les sessions suivantes établies sans l'attribut Identifiant-d'allocation-de-tunnel. Un initiateur de tunnel NE DOIT PAS allouer une session pour laquelle un attribut Identifiant-d'allocation-de-tunnel n'a pas été spécifié à un tunnel non désigné (c'est-à-dire, un tunnel qui a été initié par une session spécifiant cet attribut).

Noter que le même identifiant peut être utilisé pour désigner des tunnels différents si de tels tunnels sont entre des points d'extrémité différents.

Un résumé du format de l'attribut Identifiant-d'allocation-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 82 pour Identifiant-d'allocation-de-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir le moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieure à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) appartient cet attribut. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme le premier octet du champ Chaîne suivant.

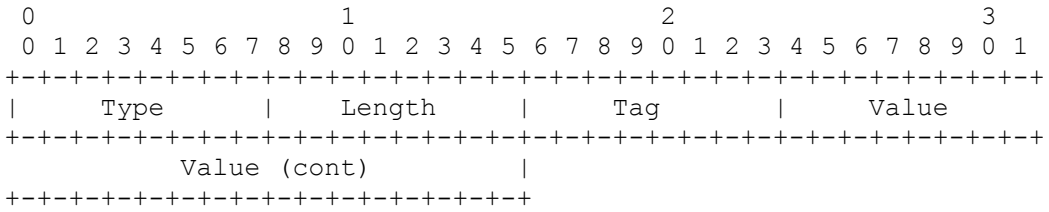
Chaîne
Ce champ doit être présent. L'identifiant de tunnel est représenté par le champ Chaîne. Il n'y a pas de restriction sur le format de l'identifiant.

3.8 Préférence-de-tunnel

Description
Si plus d'un ensemble d'attributs de tunnelage sont retournés par le serveur RADIUS à l'initiateur de tunnel, cet attribut

DEVRAIT être inclus dans chaque ensemble pour indiquer la préférence relative allouée à chaque tunnel. Par exemple, supposons que les attributs qui décrivent deux tunnels soient retournés par le serveur, un avec le Type-de-tunnel PPTP et l'autre avec un Type-de-tunnel L2TP. Si l'initiateur de tunnel ne prend en charge que l'un des Type-de-tunnel retournés, il va initier un tunnel de ce type. Si cependant, il accepte les deux protocoles de tunnel, il DEVRAIT utiliser la valeur de l'attribut Préférence-de-tunnel pour décider quel tunnel devrait être lancé. Le tunnel ayant la valeur numérique la plus faible dans le champ Valeur de cet attribut DEVRAIT recevoir la préférence la plus élevée. Les valeurs allouées à deux, ou plus, instances de l'attribut Préférence-de-tunnel au sein d'un paquet Accès-accepté donné PEUVENT être identiques. Dans ce cas, l'initiateur de tunnel DEVRAIT utiliser la métrique configurée localement pour décider quel ensemble d'attributs utiliser. Cet attribut PEUT être inclus (comme indication au serveur) dans les paquets Demande-d'accès, mais le serveur RADIUS n'est pas obligé de respecter cette indication.

Un résumé du format de l'attribut Préférence-de-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 83 pour Préférence-de-tunnel.

Longueur : Toujours 6.

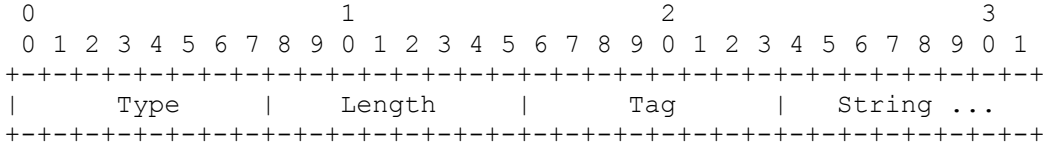
Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir un moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Les valeurs valides pour ce champ sont de 0x01 à 0x1F, inclus. Si le champ Marqueur n'est pas utilisé, il DOIT être à zéro (0x00).

Valeur
Le champ Valeur est long de trois octets et indique la préférence à donner au tunnel auquel il se réfère ; la plus forte préférence est donnée aux valeurs les moins fortes, 0x000000 étant la préférée et 0xFFFFFF la moins préférée.

3.9 Identifiant–d'authentification-de-client-tunnel

Description
Cet attribut spécifie le nom utilisé par l'initiateur de tunnel durant la phase d'authentification de l'établissement du tunnel. L'attribut Identifiant–d'authentification-de-client-tunnel PEUT être inclus (comme indication au serveur RADIUS) dans le paquet Demande-d'accès, et DOIT être inclus dans le paquet Accès-accepté si un nom d'authentification autre que par défaut est désiré. Cet attribut DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent des attributs Type-d'état-decompta avec des valeurs de Début ou de Fin et qui appartiennent à une session en tunnel.

Un résumé du format de l'attribut Identifiant–d'authentification-de-client-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 90 pour Identifiant–d'authentification-de-client-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir un moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieur à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) cet attribut

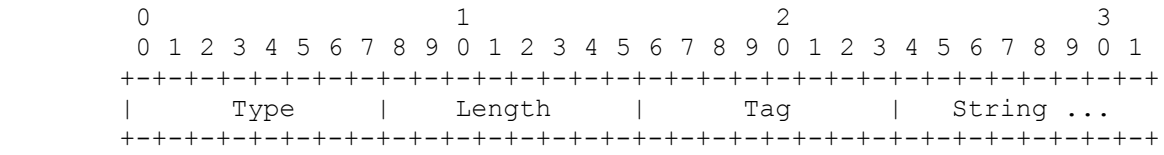
appartient. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme le premier octet du champ Chaîne suivant.

Chaîne
Ce champ doit être présent. Le champ Chaîne contient le nom d'authentification de l'initiateur de tunnel. Le nom d'authentification DEVRAIT être représenté dans le jeu de caractères UTF-8.

3.10 Identifiant–d'authentification-de-serveur-tunnel

Description
Cet attribut spécifie le nom utilisé par la terminaison de tunnel durant la phase d'authentification de l'établissement du tunnel. L'attribut Identifiant–d'authentification-de-serveur-tunnel PEUT être inclus (comme indication au serveur RADIUS) dans le paquet Demande-d'accès, et DOIT être inclus dans le paquet Accès-accepté si un nom d'authentification autre que par défaut est désiré. Cet attribut DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent des attributs Type-d'état-de-compta avec des valeurs Début ou Fin et qui appartiennent à une session en tunnel.

Un résumé du format de l'attribut Identifiant–d'authentification-de-serveur-tunnel est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 91 pour Identifiant–d'authentification-de-serveur-tunnel.

Longueur : ≥ 3

Marqueur
Le champ Marqueur est long d'un octet et est destiné à fournir un moyen de grouper dans le même paquet des attributs qui se réfèrent au même tunnel. Si la valeur du champ Marqueur est supérieur à 0x00 et inférieure ou égale à 0x1F, elle DEVRAIT être interprétée comme indiquant à quel tunnel (entre plusieurs solutions de remplacement) cet attribut appartient. Si le champ Marqueur est supérieur à 0x1F, il DEVRAIT être interprété comme le premier octet du champ Chaîne suivant.

Chaîne
Ce champ doit être présent. Le champ Chaîne contient le nom d'authentification de la terminaison de tunnel. Le nom d'authentification DEVRAIT être représenté dans le jeu de caractères UTF-8.

4 Tableau des attributs

Le tableau ci-après indique lesquels des attributs ci-dessus peuvent se trouver dans les différentes sortes de paquets, et en quelle quantité.

Demande	Accepté	Rejet	Défi	Demande-Compta	n°	Attribut
0+	0+	0	0	0-1	64	Type-de-tunnel
0+	0+	0	0	0-1	65	Type-de-support-de-tunnel
0+	0+	0	0	0-1	66	Extrémité-client-de-tunnel
0+	0+	0	0	0-1	67	Extrémité-serveur-de-tunnel
0	0+	0	0	0	69	Mot-de-passe-de-tunnel
0+	0+	0	0	0-1	81	Identifiant–de-groupe-privé-de-tunnel
0	0+	0	0	0-1	82	Identifiant-d'allocation-de-tunnel
0+	0+	0	0	0	83	Préférence-de-tunnel
0+	0+	0	0	0-1	90	Identifiant–d'authentification-de-client-tunnel
0+	0+	0	0	0-1	91	Identifiant–d'authentification-de-serveur-tunnel

Le tableau suivant définit les entrées du tableau ci-dessus :
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

5 Considérations pour la sécurité

L'attribut Mot-de-passe-de-tunnel peut contenir des informations qui ne devraient être connues que d'une extrémité de tunnel. Cependant, la méthode utilisée pour cacher la valeur de l'attribut est telle que les mandataires RADIUS qui interviennent auront connaissance des contenus. Pour cette raison, l'attribut Mot-de-passe-de-tunnel NE DEVRAIT PAS être inclus dans les paquets Accès-accepté qui pourraient passer à travers des mandataires RADIUS qui ne seraient (relativement) pas de confiance. De plus, l'attribut Mot-de-passe-de-tunnel NE DEVRAIT PAS être retourné à un client non authentifié ; si le paquet Demande-d'accès correspondant ne contenait pas une instance vérifiée de l'attribut Signature [15], le paquet Accès-accepté NE DEVRAIT PAS contenir une instance de l'attribut Mot-de-passe-de-tunnel.

Les protocoles de tunnel offrent divers niveaux de sécurité, depuis rien (par exemple PPTP) jusqu'à fort (par exemple, IPSec). Noter cependant que dans le cas de tunnelage obligatoire, toute mesure de sécurité mise en place ne s'applique qu'au trafic entre les extrémités du tunnel. En particulier, les utilisateurs finaux NE DEVRAIENT PAS se reposer sur la sécurité du tunnel pour protéger leurs données ; le chiffrement et/ou la protection de l'intégrité du trafic tunnelé NE DOIT PAS être considéré comme un remplacement de la sécurité de bout en bout.

6 Considérations relatives à l'IANA

Le présent document définit un certain nombre de numéros "magiques" à conserver par l'IANA. La présente section explique les critères que doit utiliser l'IANA pour allouer des numéros supplémentaires dans chacune de ces listes. Les paragraphes suivants décrivent la politique d'allocation pour les espaces de nom définis ailleurs dans ce document.

6.1 Valeurs de l'attribut Type-de-tunnel

Les valeurs 1 à 12 de l'attribut Type-de-tunnel sont définies au paragraphe 5.1 ; les valeurs restantes sont disponibles pour être allouées par l'IANA avec le consensus IETF [16].

6.2 Valeurs de l'attribut Support-de-tunnel

Les valeurs 1 à 15 de l'attribut Support-de-tunnel sont définies au paragraphe 5.2 ; les valeurs restantes sont disponibles pour être allouées par l'IANA avec le consensus IETF [16].

7 Références

[1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little et G. Zorn, "Protocole de tunnelage point à point (PPTP)", RFC 2637, juillet 1999.

[2] A. Valencia, M. Littlewood et T. Kolar, "Protocole Cisco de transmission de couche 2 'L2F'", RFC 2341, mai 1998.

[3] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn et B. Palter, "Protocole de tunnelage de couche 2 (L2TP)", RFC 2661, août 1999.

[4] K. Hamzeh, "Protocole de gestion de tunnel ascendant - ATMP", RFC 2107, février 1997.

[5] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", RFC 2401, novembre 1998.

[6] C. Perkins, C., "Encapsulation IP au sein de IP", RFC 2003, octobre 1996.

[7] C. Perkins, "Encapsulation minimale au sein de IP", RFC 2004, octobre 1996.

[8] R. Atkinson, "Encapsulation de charge utile de sécurité sous IP (ESP)", RFC 1827, août 1995.

[9] S. Hanks, T. Li, D. Farinacci et P. Traina, "Encapsulation de routage générique (GRE)", RFC 1701, octobre 1994.

[10] W. Simpson, "IP dans le tunnelage IP", RFC 1853, octobre 1995.

[11] G. Zorn et D. Mitton, "Modifications de la comptabilité RADIUS pour la prise en charge du protocole de tunnel", RFC 2867, juin 2000.

[12] C. Rigney, S. Willens, A. Rubens et W. Simpson, "Service d'authentification à distance de l'usager appelant (RADIUS)", RFC 2865, juin 2000.

[13] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[14] J. Reynolds et J. Postel, "Numéros alloués", STD 2, RFC 1700, octobre 1994.

[15] C. Rigney, W. Willats et P. Calhoun, "Extensions RADIUS", RFC 2869, juin 2000.

[16] T. Narten et H. Alvestrand, "Lignes directrices pour la rédaction de la section Considérations relatives à l'IANA dans les RFC", BCP 26, RFC 2434, octobre 1998.

[17] R. Hinden et S. Deering, "Architecture d'adressage IP version 6", RFC 2373, juillet 1998.

8 Remerciements

Merci à Dave Mitton pour avoir souligné une fâcheuse dépendance en boucle dans la définition originale de l'attribut Mot-de-passe-de-tunnel et (sans ordre particulier) à Kory Hamzeh, Bertrand Buclin, Andy Valencia, Bill Westfield, Kris Michielsen, Gurdeep Singh Pall, Ran Atkinson, Aydin Edguer, et Bernard Aboba pour leurs apports utiles et leur relecture.

9 Adresse du président

Le groupe de travail RADIUS peut être contacté par l'intermédiaire de son président :

Carl Rigney
Livingston Enterprises
4464 Willow Road
Pleasanton, California 94588
téléphone : +1 925 737 2100
mél : cdr@telemancy.com

10 Adresse des auteurs

Les questions sur le présent mémoire peuvent aussi être adressées à

Glen Zorn	Dory Leifer	John Shriver
Cisco Systems, Inc.	Ascend Communications	Intel Corporation
500 108th Avenue N.E., Suite 500	1678 Broadway	28 Crosby Drive
Bellevue, Washington 98004	Ann Arbor, MI 48105	Bedford, MA 01730
USA	USA	USA
téléphone : +1 425 438 8218	téléphone : +1 734 747 6152	téléphone : +1 781 687 1329
FAX: +1 425 438 1848		
mél : gwz@cisco.com	mél : leifer@del.com	mél : John.Shriver@intel.com

Allan Rubens	Matt Holdrege	Ignacio Goyret
Ascend Communications	ipVerse	Lucent Technologies
1678 Broadway	223 Ximeno Ave.	One Ascend Plaza
Ann Arbor, MI 48105	Long Beach, CA 90803	1701 Harbor Bay Parkway
USA	USA	Alameda, CA 94502
téléphone : +1 313 761 6025		téléphone : +1 510 769 6001
mél : acr@del.com	mél : matt@ipverse.com	mél : igoyret@lucent.com

11 Déclaration complète de droits de propriété

Remerciement

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