Groupe de travail Réseau
Request for Comments : 2867
Catégorie : Information
RFC mise à jour : 2866
Traduction Claude Brière de L'Isle, janvier 2008

G. Zorn, Cisco Systems, Inc.
B. Aboba, Microsoft Corporation
D. Mitton, Nortel Networks
juin 2000

Modifications de la comptabilité RADIUS pour la prise en charge de protocoles de tunnelage

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

Résumé
Le présent document définit de nouveaux attributs de comptabilité pour RADIUS et de nouvelles valeurs pour l'attribut existant Acct-Status-Type [1] conçu pour prendre en charge la fourniture du tunnelage obligatoire dans les réseaux à accès par numérotation.

Spécification des exigences
Dans le présent document, les mots clés "PEUT", "DOIT, "NE DOIT ¨PAS", "FACULTATIF", "RECOMMANDÉ", "DEVRAIT", ET "NE DEVRAIT PAS", sont à interpréter comme décrit en [2].

1 Introduction

De nombreuses applications de protocoles de tunnelage tels que PPTP [5] et L2TP [4] impliquent un accès par numérotation au réseau. Certaines, comme la fourniture d'accès sécurisé à des 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 la part de l'usager et sans lui permettre aucun choix en la matière, comme un service d'un fournisseur de service Internet (FAI). Normalement, les FAI qui fournissent un service veulent collecter des données sur ce service pour la facturation, la planification du réseau, etc. Une façon de collecter les données d'utilisation dans les réseaux à accès numéroté est l'utilisation de la comptabilité RADIUS [1]. L'utilisation de la comptabilité RADIUS permet de collecter les données d'utilisation de la numérotation en un point central, plutôt que de les mémoriser sur chaque NAS.

Pour collecter les données d'utilisation qui se rapportent au tunnelage, de nouveaux attributs RADIUS sont nécessaires ; le présent document définit ces attributs. De plus, plusieurs nouvelles valeurs sont proposées pour l'attribut Type-d'état-de-compta. Des recommandations spécifiques et des exemples pour l'application de cet attribut au protocole L2TP se trouvent dans la RFC 2809.

2 Notes de mise en œuvre

Le tunnelage obligatoire peut faire partie d'un paquetage de services fournis par une entité à une autre. Par exemple, une entreprise peut passer un contrat avec un FAI pour fournir un accès intranet à distance à ses employés via un tunnelage obligatoire. Dans ce cas, l'intégration des protocoles RADIUS et de tunnel permet au FAI et à l'entreprise de synchroniser leurs activités comptables de telle sorte que chaque partie reçoive un enregistrement de la consommation de ressources par l'utilisateur. Cela donne à l'entreprise les moyens de vérifier les factures du FAI.

Dans le domaine de la vérification, les attributs Nom-d'utilisateur, Connexion-de-tunnel-de-compta, Point-de-fin-de-tunnel-client et Point-de-fin-de-tunnel-serveur sont normalement utilisés pour identifier l'appel de façon univoque, permettant de rapprocher les Demande-de-comptabilité envoyées par le NAS des Demande-de-comptabilité correspondantes envoyées

par le serveur tunnel.

Lors de la mise en oeuvre de la comptabilité RADIUS pour le tunnelage L2TP/PPTP, le Numéro-de-série-d'appel DEVRAIT être utilisé dans l'attribut Connexion-de-tunnel-compta. En L2TP, le Numéro-de-série-d'appel est un champ de 32 bits et dans PPTP, c'est un champ de 16 bits. Dans PPTP, la combinaison de l'adresse IP et de Numéro-de-série-d'appel DEVRAIT être unique, mais ce n'est pas obligatoire. De plus, aucune méthode n'est spécifiée pour déterminer le Numéro-de-série-d'appel, ce qui laisse ouverte la possibilité d'enveloppement après un réamorçage.

Noter qu'un numéro de série d'appel de 16 bits n'est pas suffisant pour distinguer un appel donné de tous les autres appels sur une période d'une certaine durée. Par exemple, si le numéro de série d'appel est alloué de façon monotone, le NAS en question a 96 accès qui sont occupés en permanence et l'appel moyen dure 20 minutes, donc un numéro de série d'appel de 16 bits va se trouver enveloppé dans 65 536/(96 * 3 appels/heure * 24 heures/jour) = 9,48 jours.

3 Nouvelles valeurs de Type-d'état-de-compta

3.1 Début-de-tunnel

Valeur : 9

Description
Cette valeur PEUT être utilisée pour marquer l'établissement d'un tunnel avec un autre nœud. Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet Demande-de-comptabilité :

Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)
Durée-du-délai-de-compta (41)
Horodatage-d'événement (55)
Type-de-tunnel (64)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-client-de-tunnel (66)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)

3.2 Fin-de-tunnel

Valeur : 10

Description
Cette valeur PEUT être utilisée pour marquer la destruction d'un tunnel de, ou vers un autre nœud. Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet de Demande-de-comptabilité :

Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)
Durée-du-délai-de-compta (41)
Octets-d'entrée-de-compta (42)
Octets-de-sortie-de-compta (43)
Identifiant-de-session-de-compta (44)
Durée-de-session-de-compta (46)
Paquets-d'entrée-de-compta (47)
Paquets-de-sortie-de-compta (48)
Cause-de-fin-de-compta (49)
Identifiant-multi-session-de-compta (51)
Horodatage-d'événement (55)
Type-de-tunnel (64)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-client-de-tunnel (66)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)
Paquets-de-compta-en-tunnel-perdus (86)

3.3 Rejet-de-tunnel

Valeur : 11

Description
Cette valeur PEUT être utilisée pour marquer le rejet de l'établissement d'un tunnel avec un autre nœud. Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet Demande-de-comptabilité :

Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)
Durée-du-délai-de-compta (41)
Cause-de-fin-de-compta (49)
Horodatage-d'événement (55)
Type-de-tunnel (64)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-client-de-tunnel (66)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)

3.4 Début-de-liaison-tunnel

Valeur : 12

Description
Cette valeur PEUT être utilisée pour marquer la création d'une liaison tunnel. Seuls certains types de tunnel (par exemple, L2TP) acceptent plusieurs liaisons par tunnel. Cet attribut est destiné à marquer la création d'une liaison au sein d'un tunnel qui porte plusieurs liaisons. Par exemple, si un tunnel obligatoire devait porter M liaisons pendant sa durée de vie, 2(M+1) messages de comptabilité RADIUS pourraient être envoyés : un pour marquer l'initiation et la destruction du tunnel lui-même et un pour l'initiation et la destruction de chaque liaison au sein du tunnel. Si c'est seulement une seule liaison qui peut être portée dans un tunnel donné (par exemple, IPsec en mode tunnel) il n'est pas nécessaire d'inclure cet attribut dans les paquets de comptabilité, car la présence de l'attribut Début-de-tunnel impliquera l'initiation de la liaison (la seule possible).

Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet Demande-de-comptabilité :

Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)
Accès-de-NAS (5)
Durée-du-délai-de-compta (41)
Horodatage-d'événement (55)
Type-de-tunnel (64)
Point-d'extrémité-de-client-de-tunnel (66)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)

3.5 Fin-de-liaison-tunnel

Valeur : 13

Description
Cette valeur PEUT être utilisée pour marquer la destruction d'une liaison tunnel. Seuls quelques types de tunnel (par exemple, L2TP) acceptent plusieurs liaisons par tunnel. Cet attribut est destiné à marquer la destruction d'une liaison au sein d'un tunnel qui porte plusieurs liaisons. Par exemple, si un tunnel obligatoire devait porter M liaisons pendant sa durée de vie, 2(M+1) messages de comptabilité RADIUS pourraient être envoyés : un pour marquer l'initiation et la destruction du tunnel lui-même et un pour l'initiation et la destruction de chaque liaison au sein du tunnel. Si seulement une liaison peut être portée dans un tunnel donné (par exemple, IPsec en mode tunnel) il n'est pas nécessaire d'inclure cet attribut dans les paquets de comptabilité, car la présence de l'attribut Fin-de-tunnel impliquera la fin de la liaison (la seule possible).

Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet Demande-de-comptabilité :

Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)

Accès-de-NAS (5)
Durée-du-délai-de-compta (41)
Octets-d'entrée-de-compta (42)
Octets-de-sortie-de-compta (43)
Identifiant-de-session-de-compta (44)
Durée-de-session-de-compta (46)
Paquets-d'entrée-de-compta (47)
Paquets-de-sortie-de-compta (48)
Cause-de-fin-de-compta (49)
Identifiant-multi-session-de-compta (51)
Horodatage-d'événement (55)
Type-d'accès-de-NAS (61)
Type-de-tunnel (64)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-client-de-tunnel (66)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)
Paquets-de-compta-en-tunnel-perdus (86)

3.6 Rejet-de-liaison-tunnel

Valeur : 14

Description
Cette valeur PEUT être utilisée pour marquer le rejet de l'établissement d'une nouvelle liaison dans un tunnel existant. Seulement certains types de tunnel (par exemple, L2TP) acceptent plusieurs liaisons par tunnel. Si seulement une liaison peut être portée sur un tunnel donné (par exemple, IPsec en mode tunnel) cet attribut n'a pas besoin d'être inclus dans les paquets de comptabilité, car dans ce cas, l'attribut Rejet-de-tunnel a la même signification.

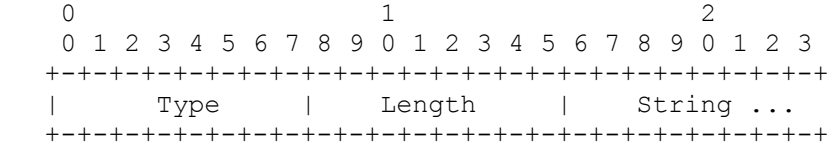
Si cette valeur est utilisée, les attributs suivants DEVRAIENT aussi être inclus dans le paquet Demande-de-comptabilité :
Nom-d'utilisateur (1)
Adresse-IP-de-NAS (4)
Durée-du-délai-de-compta (41)
Cause-de-fin-de-compta (49)
Horodatage-d'événement (55)
Type-de-tunnel (64)
Type-de-support-de-tunnel (65)
Point-d'extrémité-de-client-de-tunnel (66)
Point-d'extrémité-de-serveur-de-tunnel (67)
Connexion-de-tunnel-de-compta (68)

4 Attributs

4.1 Connexion-de-tunnel-de-compta

Description
Cet attribut indique l'identifiant alloué à la session de tunnel. Il DEVRAIT être inclus dans les paquets Demande-de-comptabilité qui contiennent l'attribut Type-d'état-de-compta qui ont la valeur Début, Fin, ou une des valeurs décrites ci-dessus. Cet attribut, conjointement avec les attributs Point-d'extrémité-de-client-de-tunnel et Point-d'extrémité-de-serveur-de-tunnel [3], peut être utilisé pour fournir le moyen d'identifier de façon univoque une session de tunnel pour les besoins de la vérification.

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



Type : 68 pour Connexion-de-tunnel-de-compta

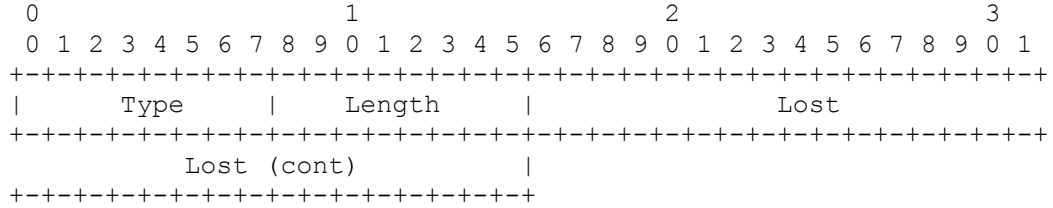
Longueur : ≥ 3

Chaîne
Le format de l'identifiant représenté par le champ Chaîne dépend de la valeur de l'attribut Type-de-tunnel [3]. Par exemple, pour identifier pleinement une connexion de tunnel L2TP, l'identifiant de tunnel L2TP et l'identifiant d'appel peuvent être codés dans ce champ. Le codage exact de ce champ dépend de la mise en œuvre.

4.2 Paquets-de-compta-en-tunnel-perdus

Description
Cet attribut indique le nombre de paquets perdus sur une liaison donnée. Il DEVRAIT être inclus dans des paquets Demande-de-comptabilité qui contiennent un attribut Type-d'état-de-compta ayant la valeur Fin-de-liaison-de-tunnel.

Un résumé du format de l'attribut Acct-Tunnel-Packets-Lost est indiqué ci-dessous. Les champs sont transmis de gauche à droite.



Type : 86 pour Paquets-de-compta-en-tunnel-perdus

Longueur : 6

Perdu : Le champ Perdu est long de 4 octets et représente le nombre de paquets perdus sur la liaison.

5 Tableau des attributs

Le tableau suivant indique les attributs qui peuvent être trouvés dans les paquets Demande-de-comptabilité. Aucun attribut de tunnel ne devrait se trouver dans les paquets Réponse-de-comptabilité.

Demande	**n°**	**Attribut**
0-1	64	Type-de-tunnel
0-1	65	Type-de-support-de-tunnel
0-1	66	Point-d'extrémité-de-client-Tunnel
0-1	67	Point-d'extrémité-de-serveur-Tunnel
0-1	68	Connextion-de-tunnel-de-compta
0	69	Mot-de-passe-de-tunnel
0-1	81	Identifiant-de-groupe-privé-de-tunnel
0-1	82	Identifiant-d'allocation-de-tunnel
0	83	Préférence-de-tunnel
0-1	86	Paquets-de-compta-en-tunnel-perdus

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

6 Considérations pour la sécurité

En "reniflant" les paquets de comptabilité RADIUS, il est possible à un espion d'effectuer une analyse passive des connexions tunnel.

7 Références

[1] C. Rigney, "Comptabilité de RADIUS", RFC 2139, avril 1997.

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

[3] G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege et I. Goyret, "Attributs RADIUS pour la prise en charge du protocole de tunnel", RFC 2868, juin 2000.

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

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

8 Remerciements

Merci à Aydin Edguer, Ly Loi, Matt Holdrege et Gurdeep Singh Pall pour leurs contributions marquantes et la relecture.

9 Adresse des auteurs

Les questions sur le présent mémo peuvent aussi être adressées à

Glen Zorn	Dave Mitton	Bernard Aboba
Cisco Systems, Inc.	Nortel Networks	Microsoft Corporation
500 108th Avenue N.E., Suite 500	880 Technology Park Drive	One Microsoft Way
Bellevue, Washington 98004	Billerica, MA 01821	Redmond, Washington 98052
USA	USA	USA
téléphone : +1 425 438 8218	téléphone : +1 978 288 4570	téléphone : +1 425 936 6605
Fax : +1 425 438 1848	Fax : +1 978 288 3030	Fax : +1 425 936 7329
mél : gwz@cisco.com	mél : dmitton@nortelnetworks.com	mél : aboba@internaut.com

10 Déclaration complète de droits de propriété

SOCIETY ET LA INTERNET ENGINEERING TASK FORCE DÉCLINENT TOUTES GARANTIES, EXPRIMÉES OU IMPLICITES, Y COMPRIS MAIS NON LIMITÉES À TOUTE GARANTIE QUE L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Remerciement

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