Comparaison entre TACACS+ et RADIUS

Contenu

Introduction

Deux protocoles de sécurité importants utilisés pour contrôler l'accès aux réseaux sont Cisco TACACS+ et RADIUS. Le cahier des charges RADIUS est décrit dans RFC 2865, qui vient remplacer RFC 2138. Cisco s'engage à prendre en charge les deux protocoles avec les meilleurs offres de classe. Le but de Cisco n'est en aucun cas de faire concurrence à RADIUS ou d'inciter des utilisateurs à utiliser TACACS+. C'est à vous de choisir la solution qui répond le mieux à vos besoins. Ce document traite des différences entre TACACS+ et RADIUS, de manière à ce que vous puissiez faire un choix optimal.

Cisco prend en charge le protocole RADIUS depuis la version 11.1 du logiciel Cisco IOS® de février 1996. Cisco continue à améliorer le Client RADIUS, en y apportant de nouvelles fonctionnalités et possibilités, avec notamment la prise en charge de la norme RADIUS.

Cisco a toujours considéré RADIUS comme un protocole de sécurité avant même de développer TACACS+. De nombreuses fonctionnalités ont été introduites dans le protocole TACACS+ pour répondre aux besoins d'un marché en expansion, celui de la sécurité. Ce protocole a été conçu pour mesurer la croissance des réseaux et s'adapter aux nouvelles technologies de sécurité au fur et à mesure que le marché s'agrandit. L'architecture sous-jacente du protocole TACACS+ est un

complément à l'architecture indépendante de l'authentification, l'autorisation et la gestion des comptes (AAA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Environnement RADIUS

RADIUS est un serveur d'accès qui utilise le protocole AAA. Il s'agit d'un système de sécurité distribuée qui sécurise l'accès à distance aux réseaux et aux services réseau contre l'accès non autorisé. RADIUS comporte trois composants :

- Un protocole avec un format de trame qui utilise le protocole User Datagram Protocol (UDP)/IP.
- Un serveur.
- Un client.

Le serveur est lancé sur un ordinateur central, en général sur le site d'un client, alors que les clients sont configurés dans les serveurs d'accès commutés et peuvent être distribués dans tout un réseau. Cisco a incorporé le client RADIUS au Logiciel Cisco IOS Version 11.1 et plus tard et à d'autres logiciels de périphérique.

Modèle Client/Serveur

Un serveur d'accès au réseau (NAS) fonctionne comme un client de RADIUS. Le client est responsable de la transmission des informations utilisateur aux serveurs RADIUS choisis, puis de l'action effectuée suite à la réponse renvoyée. Les serveurs RADIUS sont responsables de la réception des demandes de connexion utilisateur, de l'authentification des utilisateurs et du renvoi des informations de configuration nécessaires afin de permettre au client de fournir un service à l'utilisateur. Les serveurs RADIUS peuvent agir en tant que clients proxy pour d'autres types de serveurs d'authentification.

Sécurité du réseau

Les transactions entre le client et le serveur RADIUS sont authentifiées à l'aide d'un secret partagé, qui n'est jamais envoyé au sein du réseau. En outre, tous les mots de passe utilisateur sont envoyés chiffrés entre le client et le serveur RADIUS. Ainsi, il est impossible pour un espion

de déchiffrer un mot de passe utilisateur sur un réseau non sécurisé.

Mécanismes d'authentification flexibles

Le serveur RADIUS prend en charge un grand choix de méthodes pour authentifier un utilisateur. Quand le nom d'utilisateur et le mot de passe original fournis par l'utilisateur sont connus, il prend en charge PPP, le Password Authentication Protocol (PAP), ou le Challenge Handshake Authentication Protocol (CHAP), UNIX login, et d'autres mécanismes d'authentification.

Disponibilité de code de serveur

Il existe un certain nombre de distributions de code de serveur disponible à l'achat ou gratuites. Les serveurs Cisco incluent Cisco Secure ACS pour Windows, Cisco Secure ACS pour UNIX et Cisco Access Registrar.

Comparez TACACS+ et RADIUS

Ces sections comparent plusieurs caractéristiques de TACACS+ et RADIUS.

UDP et TCP

RADIUS utilise l'UDP tandis que TACACS+ utilise l'TCP. Le TCP offre plusieurs avantages par rapport à l'UDP. Le TCP fournit un transport orienté connexion et l'UDP fournit les meilleures performances. RADIUS exige des variables programmables supplémentaires, comme les tentatives de retransmission et les délais d'attente de compensation pour de meilleures performances. Cependant, il ne possède pas tous les avantages de prise en charge intégrée que peut apporter un transport TCP.

- L'utilisation de TCP fournit un accusé de réception pour chaque demande reçue, dans (approximativement) le temps d'un aller-retour réseau (RTT), indépendamment du mode de chargement et de la lenteur du mécanisme d'authentification en arrière-plan (accusé de réception TCP).
- Le TCP indique immédiatement les éventuelles pannes ou extinctions de serveur suite à un redémarrage (RST). Vous pouvez déterminer quand un serveur tombe en panne et marche de nouveau si vous utilisez les connexions TCP longue durée. L'UDP ne peut pas faire la différence entre un serveur qui est en panne, un serveur lent, et un serveur inexistant.
- Grâce aux keepalives de TCP, les pannes de serveur peuvent être détectées hors bande avec des demandes réelles. Des connexions à plusieurs serveurs peuvent être maintenues simultanément, et vous pouvez uniquement envoyer des messages à ceux qui sont opérationnels.
- Le TCP est plus évolutif et s'adapte aux réseaux aussi bien saturés qu'en croissance.

Chiffrement des paquets

RADIUS chiffre uniquement le mot de passe dans le paquet de demande d'accès, du client au serveur. Le reste du paquet n'est pas chiffré. Les autres informations, telles que le nom d'utilisateur, les services autorisés et la traçabilité, peuvent être saisies par un tiers.

TACACS+ chiffre le corps entier du paquet mais laisse un en-tête de norme TACACS+. Dans l'en-

tête se trouve un champ qui indique si le corps est chiffré ou non. A des fins de débogage, il est utile que le corps des paquets ne soit pas chiffré. Cependant, pendant les opérations normales, le corps du paquet est entièrement chiffré pour assurer des communications plus sécurisées.

Authentification et autorisation

RADIUS combine l'authentification et l'autorisation. Les paquets d'acceptation d'accès envoyés par le serveur RADIUS au client contiennent des informations d'autorisation. Ainsi, il est difficile de dissocier l'authentification et l'autorisation.

TACACS+ utilise l'architecture AAA, qui sépare AAA. Ainsi, des solutions d'authentification distinctes existent et peuvent toujours utiliser TACACS+ pour l'autorisation et la gestion des comptes. Par exemple, avec TACACS+, il est possible d'utiliser l'authentification Kerberos et l'autorisation et la gestion des comptes TACACS+. Après que le NAS soit authentifié sur des serveurs Kerberos, il demande des informations d'autorisation depuis un serveur TACACS+ sans qu'une nouvelle authentification soit nécessaire. Le NAS informe le serveur TACACS+ qu'il s'est authentifié avec succès sur un serveur Kerberos, puis fournit les informations d'autorisation.

Lors d'une session, si un contrôle d'autorisation supplémentaire est nécessaire, le serveur d'accès effectue le contrôle à l'aide d'un serveur TACACS+ pour déterminer si un utilisateur donné est autorisé ou non à utiliser une commande en particulier. Cela permet un plus grand contrôle des commandes pouvant être exécutées sur le serveur d'accès tout en étant découplées du mécanisme d'authentification.

Prise en charge multiprotocole

RADIUS ne prend pas en charge ces protocoles :

- Protocole Appletalk Remote Access (ARA)
- Protocole NetBIOS Frame Protocol Control
- Novell Asynchronous Services Interface (NASI)
- Connexion X.25 PAD

TACACS+ propose la prise en charge multiprotocole.

Gestion du routeur

RADIUS ne permet pas à des utilisateurs de contrôler les commandes pouvant être exécutées ou non sur un routeur. Par conséquent, RADIUS n'est pas si utile pour la gestion de routeur ou flexible pour les services de terminaux.

TACACS+ propose deux méthodes pour contrôler l'autorisation des commandes de routeur par utilisateur ou par groupe. La première méthode consiste à attribuer des niveaux de privilège aux commandes et à vérifier à l'aide du routeur avec le serveur TACACS+, que l'utilisateur est autorisé ou non à un niveau de privilèges donné. La seconde méthode consiste à spécifier de manière explicite les commandes autorisées dans le serveur TACACS+ sur une base par utilisateur ou par groupe.

Interopérabilité

En raison de diverses interprétations des Request For Comments (RFC) RADIUS, la conformité

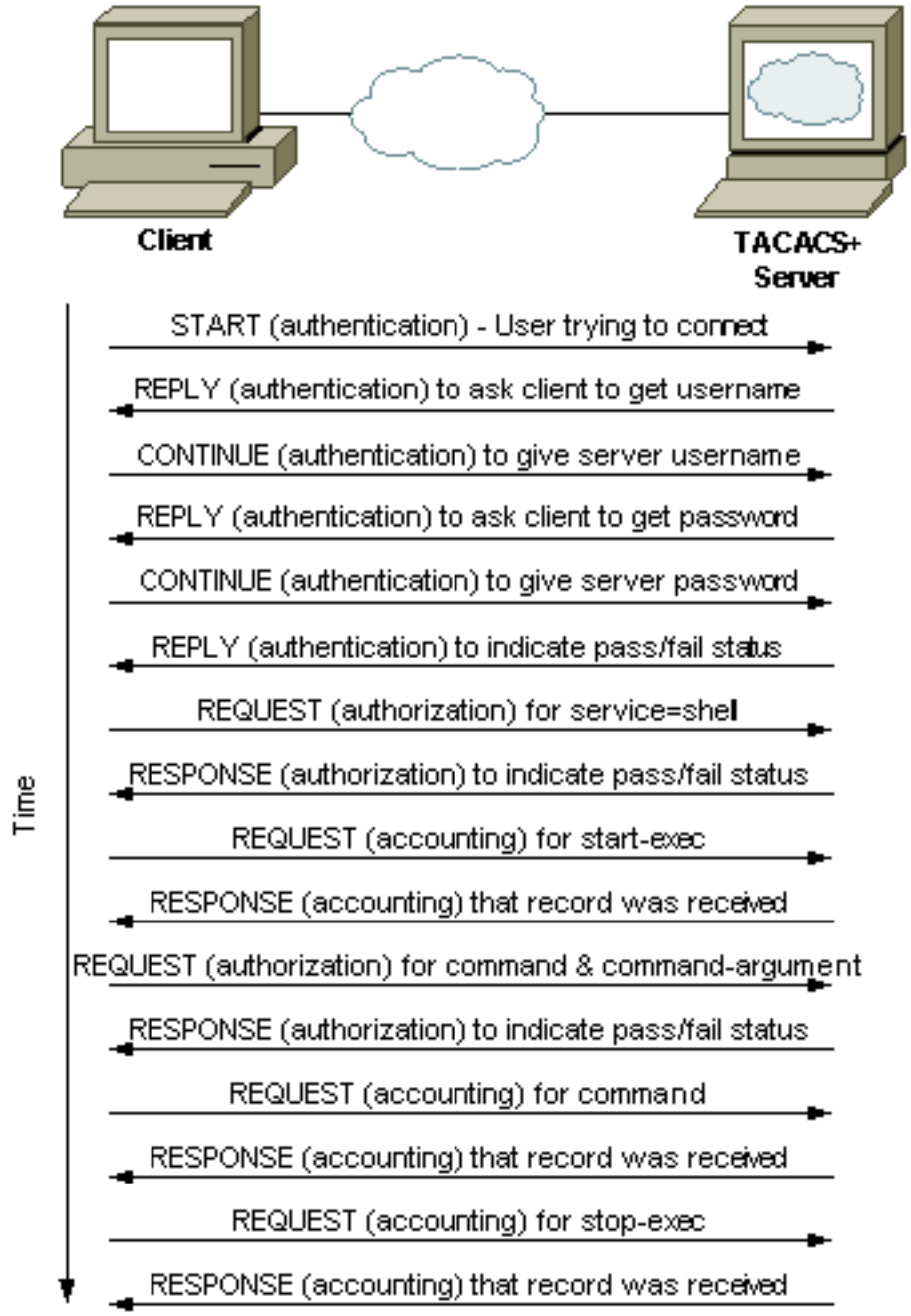
au RFC RADIUS ne garantit pas l'interopérabilité. Même si plusieurs constructeurs mettent en application des clients RADIUS, ceci ne signifie pas qu'ils sont interopérables. Cisco met en application la plupart des attributs RADIUS et en ajoute de manière consistante. Si les clients utilisent seulement les attributs RADIUS standard dans leurs serveurs, ils peuvent interopérer entre plusieurs constructeurs tant que ces constructeurs mettent en application les mêmes attributs. Cependant, beaucoup de constructeurs mettent en application les extensions qui sont des attributs de propriété industrielle. Si un client utilise un de ces attributs étendus spécifique au constructeur, l'interopérabilité n'est pas possible.

Le trafic

En raison des différences précédemment citées entre TACACS+ et RADIUS, le niveau de trafic généré entre le client et le serveur diffère. Ces exemples illustrent le trafic entre le client et le serveur pour TACACS+ et RADIUS une fois utilisés pour la gestion du routeur avec l'authentification, l'autorisation exec, l'autorisation de commande (ce que RADIUS ne peut pas faire), la gestion des comptes exec et la gestion des comptes de commandes (ce que RADIUS ne peut non plus pas faire).

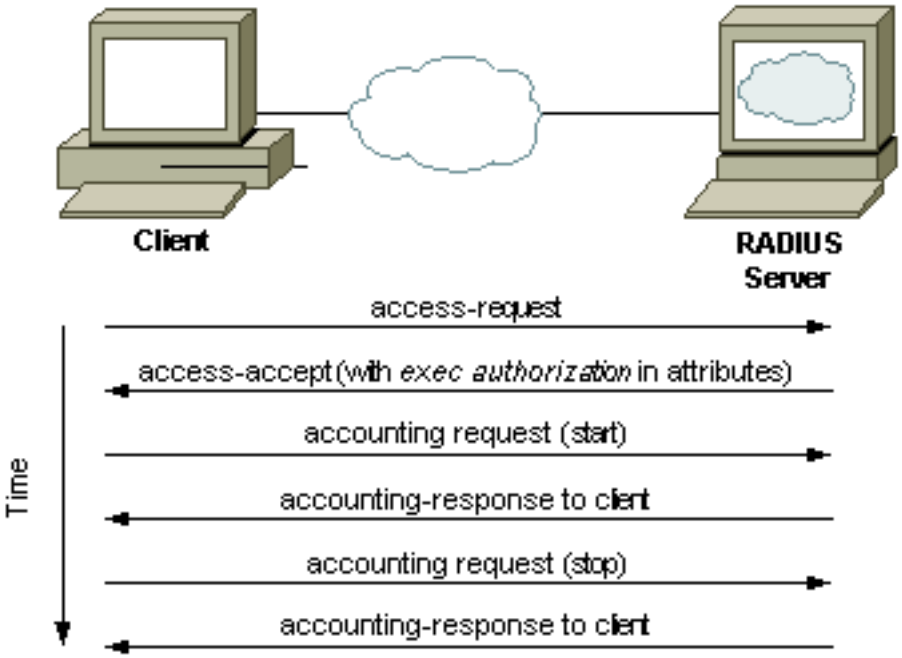
Exemple de trafic TACACS+

Cet exemple suppose que l'authentification de connexion, l'autorisation exec, l'autorisation de commande, la gestion des comptes start-stop exec et la gestion des comptes de commande sont mis en œuvre avec TACACS + quand un utilisateur effectue la commande telnet sur un routeur, exécute une commande et quitte le routeur :



Exemple de trafic RADIUS

Cet exemple suppose que l'authentification de connexion, l'autorisation exec et la gestion des comptes start-stop exec sont mis en œuvre avec RADIUS quand un utilisateur effectue la commande telnet sur un routeur, exécute une commande et quitte le routeur (les autres services de gestion ne sont pas disponibles) :



Prise en charge de périphériques

Ce tableau présente la prise en charge TACACS+ et RADIUS AAA par type de périphérique pour les plates-formes sélectionnées. La version de logiciel pour laquelle la prise en charge a été ajoutée est incluse. Consultez les notes de distribution du produit pour de plus amples informations si votre produit ne figure pas dans cette liste.

Périphérique Cisco	Authentification TACACS+	Autorisation TACACS+	Gestion des comptes TACACS+	Authentification RADIUS	Autorisation RADIUS	Gestion des comptes RADIUS
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	tous les points d'accès	tous les points d'accès	tous les points d'accès
Logiciel Cisco IOS[2 de]	10.33	10.33	10.33[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco Cache Engine	--	--	--	1.5	1.5[6]	--
Commutateurs Cisco Catalyst	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[5]
Commutateur de	5.03	5.03	5.03	5.0	5.0[4]	--

services de contenu Cisco CSS 11000						
Commutateur de services de contenu Cisco CSS 11500	5.20	5.20	5.20	5.20	5.20[4]	--
Pare-feu Cisco PIX	4.0	4.0[7]	4.2[8,5]	4.0	5.2[7]	4.2[8,5]
Commutateurs Cisco Catalyst 1900/2820	8.x entreprise[9]	--	--	--	--	--
Commutateurs Cisco catalyst 2900XL/3500XL	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[11]	12.0(5)WC5[11,4]	12.0(5)WC5[11,5]
Concentrateur [6] de Cisco VPN 3000	3.0	3.0	--	2.0[12]	2.0	2.0[12]
Concentrateur Cisco VPN 5000	--	--	--	5.2X[12]	5.2X[12]	5.2X[12]

Notes de tableau

1. Arrêt des clients sans fil uniquement, pas de trafic d'administration disponible dans les versions autres que la version de Cisco IOS 12.2(4)JA ou supérieure. Dans la version de Cisco IOS 12.2.(4)JA ou supérieure, l'authentification pour l'arrêt des clients sans fil et le trafic d'administration sont disponibles.
2. Consultez le Navigateur de fonctionnalités (remplacé par une version plus récente disponible ici : Software Advisor (clients enregistrés uniquement)) pour assurer la prise en charge de plate-forme dans le logiciel Cisco IOS.

3. La gestion des comptes de commandes n'est disponible qu'à partir de la version du logiciel Cisco IOS 11.1.6.3.
4. Aucune autorisation de commande.
5. Aucune gestion des comptes de commandes.
6. Blocage d'URL uniquement, pas de trafic d'administration.
7. Autorisation pour le trafic non-VPN par PIX.**Remarque:** Version 5.2 - Prise en charge de liste d'accès pour l'autorisation d'attribut spécifique au constructeur (VSA) RADIUS Access Control List (ACL) ou TACACS+ pour arrêt de trafic VPN sur PIX version 6.1 - Prise en charge de l'autorisation d'attribut 11 ACL RADIUS pour arrêt de trafic VPN sur PIX version 6.2.2 - Prise en charge ACLs avec autorisation RADIUS pour l'arrêt de trafic VPN sur PIX version 6.2 - Prise en charge d'autorisation de trafic d'administration PIX via TACACS+.
8. Gestion des comptes pour trafic non-VPN via PIX uniquement, pas de trafic d'administration.**Remarque:** Version 5.2 - Prise en charge de la gestion de comptes pour les paquets TCP de client VPN via PIX.
9. Logiciel d'entreprise uniquement.
10. Mémoire flash 8 Mo nécessaire pour l'image.
11. Arrêt VPN uniquement.

Informations connexes

- Page d'assistance RADIUS
- TACACS+ dans la documentation d'IOS
- Page de support TACACS/TACACS+
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems