

Comparez TACACS+ et RADIUS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Environnement RADIUS](#)

[Modèle Client/Serveur](#)

[Sécurité du réseau](#)

[Mécanismes d'authentification flexibles](#)

[Disponibilité de code de serveur](#)

[Comparez TACACS+ et RADIUS](#)

[UDP et TCP](#)

[Chiffrement des paquets](#)

[Authentification et autorisation](#)

[Prise en charge multiprotocole](#)

[Gestion du routeur](#)

[Interfonctionnement](#)

[Trafic](#)

[Exemple de trafic TACACS+](#)

[Exemple de trafic RADIUS](#)

[Prise en charge de périphériques](#)

[Notes de tableau](#)

[Informations connexes](#)

Introduction

Ce document décrit et compare les deux principaux protocoles de sécurité utilisés pour contrôler l'accès aux réseaux : Cisco TACACS+ et Cisco RADIUS.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions des documents, reportez-vous à [Conseils techniques et format Cisco](#).

Informations générales

Le cahier des charges RADIUS est décrit dans RFC 2865, qui vient remplacer RFC 2138. Cisco prend en charge les deux protocoles. Le but de Cisco n'est en aucun cas de faire concurrence à RADIUS ou d'inciter des utilisateurs à utiliser TACACS+. Vous devez 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 prendre en charge RADIUS et à l'améliorer avec de nouvelles fonctionnalités.

Cisco a toujours considéré RADIUS comme un protocole de sécurité avant même de développer TACACS+. De nombreuses fonctionnalités ont été incluses dans le protocole TACACS+ pour répondre aux nouvelles exigences du marché 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).

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 s'exécute sur un ordinateur central, généralement sur le site client, tandis que les clients résident sur les serveurs d'accès à distance et peuvent être distribués sur le 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 transmet les informations utilisateur aux serveurs RADIUS désignés, puis agit sur la réponse renvoyée. Les serveurs RADIUS reçoivent les demandes de connexion utilisateur, authentifient l'utilisateur et retournent toutes les informations de configuration nécessaires au client pour fournir le 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. Cela élimine la possibilité qu'une personne surveillant un réseau non sécurisé puisse déterminer un mot de passe utilisateur.

Mécanismes d'authentification flexibles

Le serveur RADIUS prend en charge un grand choix de méthodes pour authentifier un utilisateur. Lorsqu'il est fourni avec le nom d'utilisateur et le mot de passe d'origine fournis par l'utilisateur, il peut prendre en charge PPP, le protocole d'authentification de mot de passe (PAP) ou le protocole d'authentification à échanges confirmés (CHAP), la connexion UNIX 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 du protocole TCP fournit un accusé de réception distinct de la réception d'une requête, dans un délai de transmission aller-retour (RTT) (approximativement), quel que soit le niveau de charge et de lenteur du mécanisme d'authentification principal (un accusé de

réception TCP).

- Le protocole TCP fournit une indication immédiate d'un serveur bloqué ou arrêté par une réinitialisation (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.
- Avec les keepalives TCP, les pannes de serveur peuvent être détectées hors bande avec les requêtes réelles. Les connexions à plusieurs serveurs peuvent être maintenues simultanément, et vous n'avez besoin d'envoyer des messages qu'à ceux qui sont connus pour être actifs et qui fonctionnent.
- Le protocole TCP est plus évolutif et s'adapte aux réseaux dont la taille augmente et qui sont davantage encombrés.

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+. Une fois qu'un serveur NAS s'authentifie sur un serveur Kerberos, il demande des informations d'autorisation à un serveur TACACS+ sans avoir besoin d'une nouvelle authentification. 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 de mieux contrôler les commandes pouvant être exécutées sur le serveur d'accès lorsque le mécanisme d'authentification est dissocié.

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.

Interfonctionnement

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 uniquement les attributs RADIUS standard sur leurs serveurs, ils peuvent interagir entre plusieurs fournisseurs à condition que ces derniers implémentent les mêmes attributs. Cependant, beaucoup de constructeurs mettent en application les extensions qui sont des attributs de propriété industrielle. Si un client utilise l'un de ces attributs étendus spécifiques au fournisseur, l'interopérabilité n'est pas possible.

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 version du produit pour plus d'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	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
Cisco Cache Engine	—	—	—	1.5	1.56	—
Commutateurs Cisco Catalyst	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Commutateur de services de contenu Cisco CSS 11000	5.03	5.03	5.03	5.0	5.04	—
Commutateur de services de contenu Cisco CSS 11500	5.20	5.20	5.20	5.20	5.204	—
Pare-feu Cisco PIX	4.0	4.07	4.28,5	4.0	5.27	4.28,5
Commutateurs Cisco Catalyst 1900/2820	8.x entreprise ⁹	—	—	—	—	—
Commutateurs	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 ,	12.0(5)WC5 ¹¹


Cisco catalyst 2900XL/3500XL					4	5
Concentrateur Cisco VPN 3000 ⁶	3.0	3.0	—	2.012	2.0	2.012
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 Software Advisor pour connaître la prise en charge de la plate-forme dans le logiciel Cisco IOS.
3. La comptabilisation des commandes n'est pas implémentée avant 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 la liste de contrôle d'accès pour l'autorisation RADIUS Vendor-Specific Attribute (VSA) ou TACACS+ pour le trafic VPN terminé sur PIX version 6.1 - prise en charge de l'autorisation ACL RADIUS attribute 11 pour le trafic VPN terminé sur PIX version 6.2.2 - prise en charge des ACL téléchargeables avec autorisation RADIUS pour le trafic VPN terminé sur PIX version 6.2 - prise en charge de l'autorisation pour le trafic de gestion 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 comptabilisation des paquets TCP du client VPN par le PIX.

9. Logiciel d'entreprise uniquement.
10. Mémoire flash 8 Mo nécessaire pour l'image.
11. Arrêt VPN uniquement.

 Remarque : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

Informations connexes

- [Prise en charge RADIUS](#)
- [Protocoles d'authentification/assistance TACACS/TACACS+](#)
- [Demandes de commentaires \(RFC\)](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.