RADIUS و +TACACS ةنراقم

المحتويات

المقدمة

هناك بروتوكولان أمان بارزان يستخدمان للتحكم في الوصول إلى الشبكات هما Cisco TACACS+ و RADIUS. يتم وصف مواصفات RADIUS في RFC 2865 ، والذي يتجاوز RFC 2138 . تلتزم Cisco بدعم كلا البروتوكولين بأفضل عروض الفئة. لا تنوي Cisco التنافس مع RADIUS أو التأثير على المستخدمين لاستخدام TACACS+. يجب عليك إختيار الحل الذي يفي باحتياجاتك على أفضل وجه. يناقش هذا المستند الاختلافات بين TACACS+ و RADIUS، حتى يمكنك إتخاذ خيار مستنير.

دعمت Cisco بروتوكول RADIUS منذ برنامج Cisco IOS® الإصدار 11.1 في فبراير 1996. تواصل Cisco تحسين عميل RADIUS بميزات وإمكانات جديدة، مما يدعم RADIUS كميزة قياسية.

قام Cisco بتقييم RADIUS بشكل جدي كبروتوكول أمان قبل تطوير TACACS+. وقد تم تضمين العديد من الميزات في بروتوكول TACACS+ لتلبية إحتياجات سوق الأمان المتنامي. ولقد صمم هذا البروتوكول بحيث يتسع مع نمو الشبكات، ولكي يتكيف مع التكنولوجيا الأمنية الجديدة مع نضوج ونضوج السوق. تكمل البنية الأساسية لبروتوكول TACACS+ بنية المصادقة والتفويض والمحاسبة (AAA) المستقلة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

خلفية RADIUS

أما RADIUS فهو خادم وصول يستخدم بروتوكول AAA. إنه نظام للأمان الموزع يضمن الوصول عن بعد إلى الشبكات وخدمات الشبكات ضد الوصول غير المصرح به. يتكون RADIUS من ثلاثة مكونات:

- بروتوكول بتنسيق إطار يستخدم بروتوكول مخطط بيانات المستخدم (UDP)/IP.
- خادم.
- زبون.

يتم تشغيل الخادم على كمبيوتر مركزي عادة في موقع العميل، بينما يقيم العملاء في خوادم الوصول إلى الطلب الهاتفي ويمكن توزيعها عبر الشبكة. أدرجت Cisco عميل RADIUS في برنامج Cisco IOS الإصدار 11.1 والإصدارات الأحدث وبرامج الأجهزة الأخرى.

نموذج العميل/الخادم

يعمل خادم الوصول إلى الشبكة (NAS) كعميل ل RADIUS. يكون العميل مسؤولا عن تمرير معلومات المستخدم إلى خوادم RADIUS المخصصة، ثم يعمل على الاستجابة التي يتم إرجاعها. تكون خوادم RADIUS مسؤولة عن تلقي طلبات اتصال المستخدم ومصادقة المستخدم وإرجاع جميع معلومات التكوين اللازمة للعميل لتقديم الخدمة للمستخدم. يمكن أن تعمل خوادم RADIUS كعملاء وكيل لأنواع أخرى من خوادم المصادقة.

أمان الشبكة

تتم مصادقة الحركات بين العميل وخادم RADIUS من خلال إستخدام سر مشترك، والذي لا يتم إرساله مطلقا عبر الشبكة. وبالإضافة إلى ذلك، يتم إرسال كلمات مرور أي مستخدم مشفرة بين العميل وخادم RADIUS. وهذا يستبعد إمكانية أن يقوم شخص يتطفل على شبكة غير آمنة بتحديد كلمة مرور مستخدم.

آليات مصادقة مرنة

يدعم خادم RADIUS العديد من الطرق لمصادقة مستخدم ما. عندما يتم توفيره مع اسم المستخدم وكلمة المرور الأصلية التي يقدمها المستخدم، يمكن أن يدعم بروتوكول PPP أو بروتوكول مصادقة كلمة المرور (PAP) أو بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (CHAP) أو تسجيل دخول UNIX وآليات المصادقة الأخرى.

توفر رمز الخادم

يوجد عدد من عمليات توزيع رموز الخوادم متاحة تجاريا ومجانا. تتضمن خوادم Cisco مصدر المحتوى الإضافي الآمن من Cisco ل Windows و Cisco Secure ACS ل UNIX و Cisco Access Registrar.

مقارنة TACACS+ و RADIUS

تقارن هذه الأقسام العديد من ميزات TACACS+ و RADIUS.

UDP و TCP

يستخدم RADIUS بروتوكول UDP بينما يستخدم TACACS+ بروتوكول TCP. يوفر بروتوكول TCP العديد من الميزات عبر بروتوكول UDP. يوفر بروتوكول TCP وسيلة نقل موجهة للاتصال، بينما يوفر بروتوكول UDP أفضل جهد للتسليم. يتطلب RADIUS متغيرات إضافية قابلة للبرمجة مثل محاولات إعادة الإرسال وحالات انتهاء الوقت لتعويض نقل أفضل جهد، ولكنه يفتقر إلى مستوى الدعم المضمن الذي يقدمه نقل TCP:

- يوفر إستخدام TCP إقرارا منفصلا باستلام طلب، في غضون (تقريبا) وقت جولة الشبكة (RTT)، بغض النظر عن كيفية تحميل آلية مصادقة الطرف الخلفي (إقرار TCP) وتبطئها.
- يوفر بروتوكول TCP إشارة فورية إلى تعطل الخادم أو عدم تشغيله بواسطة إعادة تعيين (RST). يمكنك تحديد متى يتعطل الخادم ويعود إلى الخدمة إذا كنت تستخدم إتصالات TCP طويلة العمر. يتعذر على UDP تحديد الفرق بين خادم معطل وخادم بطيء وخادم غير موجود.
- باستخدام رسائل keepalive لبروتوكول TCP، يمكن اكتشاف أعطال الخادم خارج النطاق الترددي باستخدام الطلبات الفعلية. يمكن الحفاظ على الاتصالات بالخوادم المتعددة في وقت واحد، ولا تحتاج إلا لإرسال رسائل إلى تلك الرسائل التي يعرف عنها أنها تعمل بكفاءة.
- يتسم بروتوكول TCP بقدر أكبر من قابلية التطوير ويتكيف مع الشبكات المتنامية والمزدحمة كذلك.

تشفير الحزمة

لا يقوم RADIUS بتشفير كلمة المرور إلا في حزمة طلب الوصول، من العميل إلى الخادم. باقي الحزمة غير مشفرة. يمكن لطرف ثالث التقاط معلومات أخرى، مثل اسم المستخدم والخدمات المعتمدة والمحاسبة.

يقوم TACACS+ بتشفير متن الحزمة بالكامل ولكنه يترك رأس TACACS+ قياسي. يوجد حقل داخل الرأس يشير إلى ما إذا كان النص الأساسي مشفرا أم لا. لأغراض تصحيح الأخطاء، من المفيد أن يكون نص الحزم غير مشفر. ومع ذلك، أثناء التشغيل العادي، يتم تشفير نص الحزمة بالكامل لمزيد من الاتصالات الآمنة.

المصادقة والتفويض

يجمع RADIUS بين المصادقة والتفويض. تحتوي الحزم القابلة للوصول التي يتم إرسالها بواسطة خادم RADIUS إلى العميل على معلومات التفويض. وهذا يجعل من الصعب فصل المصادقة والتفويض.

يستخدم TACACS+ بنية AAA، التي تفصل AAA. وهذا يسمح بحلول مصادقة منفصلة لا تزال يمكن إستخدام TACACS+ للتخويل والمحاسبة. على سبيل المثال، باستخدام TACACS+، من الممكن إستخدام مصادقة Kerberos وتفويض TACACS+ ومحاسبته. بعد مصادقة وحدة التخزين المتصلة بالشبكة (NAS) على خادم Kerberos، فإنها تطلب معلومات التفويض من خادم TACACS+ دون الاضطرار إلى إعادة المصادقة. يقوم NAS بإعلام خادم TACACS+ بأنه قام بالمصادقة بنجاح على خادم Kerberos، ومن ثم يوفر الخادم معلومات التفويض.

في أثناء جلسة العمل، إذا كانت هناك حاجة إلى فحص تخويل إضافي، يتحقق خادم الوصول من خادم TACACS+ لتحديد ما إذا كان المستخدم قد منح إذنا باستخدام أمر معين. وهذا يوفر قدرا أكبر من التحكم في الأوامر التي يمكن تنفيذها على خادم الوصول أثناء فك الارتباط بآلية المصادقة.

دعم البروتوكولات المتعددة

لا يدعم RADIUS هذه البروتوكولات:

- بروتوكول الوصول عن بعد إلى AppleTalk (ARA)
- بروتوكول التحكم في بروتوكول إطار NetBIOS
- واجهة Novell للخدمات غير المتزامنة
- اتصال X.25 PAD

يقدم TACACS+ دعم البروتوكولات المتعددة.

إدارة الموجه

لا يسمح RADIUS للمستخدمين بالتحكم في الأوامر التي يمكن تنفيذها على الموجه وتلك التي لا يمكن تنفيذها. وبالتالي، لا يكون RADIUS مفيدا لإدارة الموجه أو مرنا للخدمات الطرفية.

يوفر TACACS+ طريقتين للتحكم في تفويض أوامر الموجه لكل مستخدم أو لكل مجموعة. الطريقة الأولى هي تعيين مستويات الامتيازات للأوامر وجعل الموجه يتحقق باستخدام خادم TACACS+ ما إذا كان المستخدم مخولا أو لا يكون على مستوى الامتياز المحدد. الطريقة الثانية هي تحديد الأوامر المسموح بها بشكل صريح في خادم TACACS+، لكل مستخدم أو لكل مجموعة.

قابلية التشغيل البيني

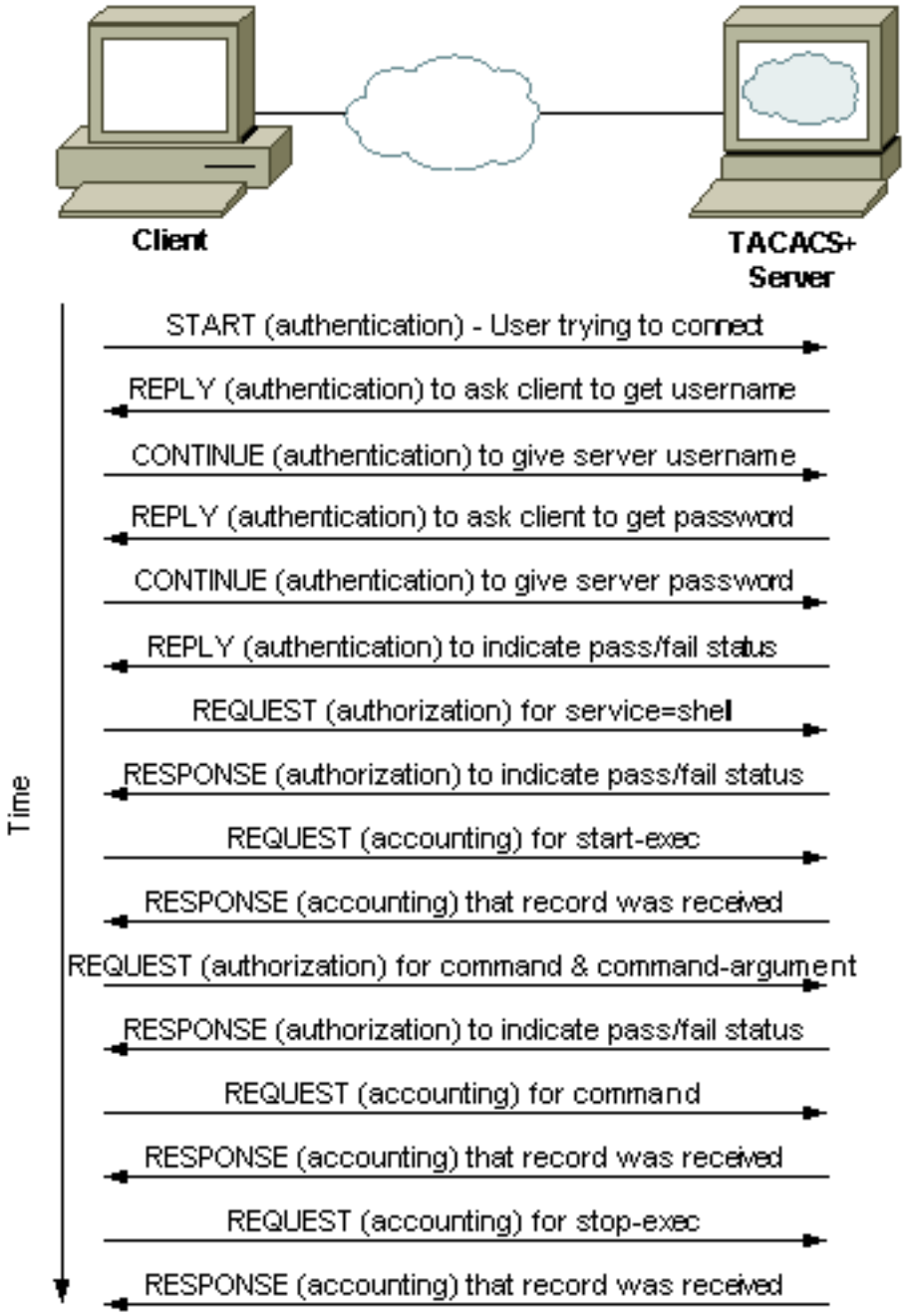
نظرا لتفسيرات مختلفة لطلب RADIUS للتعليقات (RFCs)، لا يضمن التوافق مع RADIUS RFCs قابلية التشغيل البيني. على الرغم من أن العديد من البائعين ينفذون عملاء RADIUS، إلا أن هذا لا يعني أنهم قابلون للتشغيل البيني. تقوم Cisco بتنفيذ معظم سمات RADIUS وإضافة المزيد بشكل ثابت. إذا كان العملاء يستخدمون سمات RADIUS القياسية فقط في خوادمهم، فيمكنهم التفاعل بين عدة موردين طالما أن هؤلاء الموردين ينفذون نفس السمات. ومع ذلك، يقوم العديد من الموردين بتنفيذ الملحقات التي تعد سمات خاصة. إذا كان العميل يستخدم إحدى هذه السمات الموسعة الخاصة بالمورد، فإن قابلية التشغيل البيني غير ممكنة.

حركة المرور

نظرا للإختلافات التي تم الاستشهاد بها سابقا بين TACACS+ و RADIUS، يختلف مقدار حركة مرور البيانات التي تم إنشاؤها بين العميل والخادم. توضح هذه الأمثلة حركة مرور البيانات بين العميل والخادم ل TACACS+ و RADIUS عند إستخدامها لإدارة الموجه باستخدام المصادقة وتفويض EXEC وترخيص الأوامر (الذي لا يمكن RADIUS القيام به) ومحاسبة EXEC ومحاسبة الأوامر (الذي لا يمكن RADIUS القيام به).

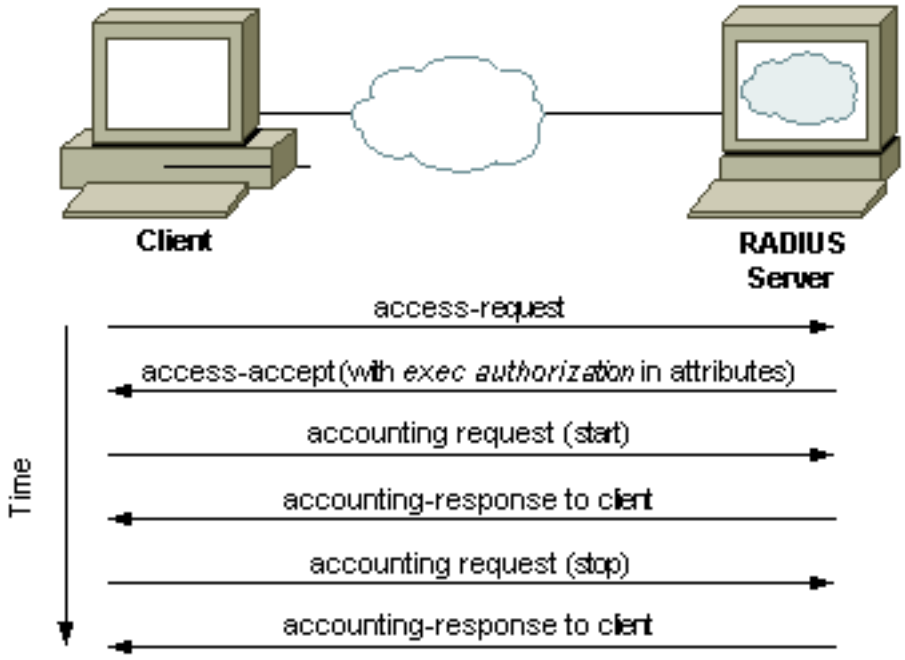
مثال حركة مرور TACACS+

يفترض هذا المثال مصادقة تسجيل الدخول، وتفويض EXEC، وتفويض الأوامر، ومحاسبة Start-stop EXEC، ومحاسبة الأوامر التي يتم تنفيذها باستخدام TACACS+ عندما يقوم مستخدم Telnet بالموجه، ويقوم بتنفيذ أمر، ويخرج الموجه:



[مثال حركة مرور RADIUS]

يفترض هذا المثال تنفيذ مصادقة تسجيل الدخول وتفويض EXEC ومحاسبة EXEC لعملية بدء التشغيل مع RADIUS عندما يقوم مستخدم Telnet بالموجه بتنفيذ أمر والخروج من الموجه (خدمات الإدارة الأخرى غير متوفرة):



دعم الأجهزة

يسرد هذا الجدول دعم TACACS+ و RADIUS AAA حسب نوع الجهاز للمنصات المحددة. وهذا يتضمن إصدار البرنامج الذي تمت إضافة الدعم فيه. تحقق من ملاحظات إصدار المنتج للحصول على مزيد من المعلومات، إذا كان المنتج غير موجود في هذه القائمة.

جهاز Cisco	مصادقة TACACS+	تفويض TACACS+	محاسبة TACACS+	مصادقة RADIUS	تفويض RADIUS	محاسبة RADIUS
Cisco Aironet[1]	12.2(4)JA	12.2(4)JA	12.2(4)JA	جميع نقاط الوصول	جميع نقاط الوصول	جميع نقاط الوصول
برنامج IOS 2 من Cisco	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
محرك ذاكرة التخزين المؤقت من Cisco	—	—	—	1.5	1.56	—
محولات Cisco Catalyst switches	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
محول خدمات المحتوى CSS	5.03	5.03	5.03	5.0	5.04	—

11000 من Cisco						
محول خدمات المحتوى CSS 1500 من Cisco	5.20	5.20	5.20	5.20	5.204	—
جدار حماية Cisco PIX	4.0	4.07	4.28,5	4.0	5.27	4.28,5
المحولات Cisco Catalyst 1900/2820 switches	الإصدار x.8 من Enterprise[9]	—	—	—	—	—
cisco مادة حفازة 2900xl/3500xl مفتاح	8).11.2 SA6(0[1]	8).11.2 SA6(0[1]	5)12.0 WC5(1[1]	).11.2 SA6(8[10]	5)12.0 WC5(1[1]، 4	(5)12.0 WC5[11]، 5
مركز Cisco VPN 3000[6]	3.0	3.0	2.012	—	2.0	2.012
مركز Cisco VPN 5000	—	—	5.2×[12]	—	5.2×[12]	5.2×[12]

ملاحظات الجدول

1. إنهاء الأجهزة العميلة اللاسلكية فقط، وليس حركة مرور الإدارة في الإصدارات الأخرى من برنامج Cisco IOS الإصدار 12.2JA(4) أو الإصدارات الأحدث. في برنامج Cisco IOS الإصدار 12.2JA(4) أو إصدار أحدث، يمكن المصادقة لكل من إنهاء العملاء اللاسلكيين وحركة مرور الإدارة.
2. تحقق من متصفح الميزات (الذي تم تجاوزه الآن بواسطة Software Advisor (مرشد البرامج) (العملاء المسجلون فقط)) لدعم النظام الأساسي داخل برنامج Cisco IOS.
3. لا يتم تنفيذ عملية محاسبة الأوامر حتى برنامج Cisco IOS Software، الإصدار 11.1.6.3.
4. لا يوجد تفويض للأوامر.
5. لا توجد محاسبة للأوامر.
6. حظر URL فقط، وليس حركة مرور البيانات الإدارية.
7. ترخيص حركة المرور غير الخاصة بشبكة VPN من خلال PIX.**ملاحظة:** الإصدار 5.2 - دعم قائمة الوصول

لسمة مورد RADIUS (ACL) الخاصة ببائع RADIUS (VSA) أو تفويض TACACS+ لحركة مرور VPN التي تنتهي على PIX الإصدار 6.1 - دعم تفويض RADIUS لسمة ACL 11 لإنهاء حركة مرور VPN على PIX الإصدار 6.2.2 - دعم قوائم التحكم في الوصول القابلة للتنزيل مع إنهاء حركة مرور VPN على PIX الإصدار 6.2 - دعم تفويض حركة مرور PIX من خلال TACACS+.

8. محاسبة حركة المرور غير الخاصة بشبكة VPN من خلال PIX فقط، وليس حركة مرور الإدارة.**ملاحظة:** الإصدار 5.2 - دعم المحاسبة لحزم TCP لعميل شبكة VPN من خلال PIX.
9. برامج المؤسسات فقط.
10. يحتاج لذاكرة Flash سعة 8 ميجا للصورة.
11. إنهاء شبكة VPN فقط.

معلومات ذات صلة

- صفحة دعم RADIUS
- TACACS+ في وثائق IOS
- صفحة دعم TACACS/TACACS+
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).