المقارنة بين TACACS + وRADIUS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
معلومات أساسية
خلفية RADIUS
نموذج العميل/الخادم
أمان الشبكة
آليات مصادقة مرنة
توفر رمز الخادم
المقارنة بين TACACS + وRADIUS
TCP و UDP
تشفير الحزمة
المصادقة والتفويض
دعم البروتوكولات المتعددة
إدارة الموجه
قابلية التشغيل البيني
حركة مرور البيانات
مثال حركة مرور TACACS+
مثال حركة مرور RADIUS
دعم الأجهزة
ملاحظات الجدول
معلومات ذات صلة

المقدمة

يصف هذا المستند ويقارن بين بروتوكولي أمان بارزين يُستخدمان للتحكم في الوصول إلى الشبكات وهما RADIUS وTACACS+ من Cisco.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

معلومات أساسية

يتم وصف مواصفات بروتوكول RADIUS في RFC 2865 ، والذي يتجاوز RFC 2138 . تدعم Cisco كلا البروتوكولين. 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 دعم RADIUS وتحسينه بمميزات وإمكانات جديدة.

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

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 يتواجد 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 لـ RADIUS. يقوم العميل بتمرير معلومات المستخدم إلى خوادم RADIUS المخصصة، ثم يعمل على الاستجابة التي يتم إرجاعها. تتلقى خوادم RADIUS طلبات اتصال المستخدم، وتصادق المستخدم، وتعيد 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 يزيل أحتمالية قيام شخص ما 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 اللتين يقدمهما المستخدم، يمكن أن يدعم بروتوكول PPP أو بروتوكول مصادقة كلمة المرور (PAP) أو بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي (CHAP) وسجل الدخول إلى 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.

المقارنة بين TACACS + وRADIUS

تقارن هذه الأقسام العديد من مميزات TACACS+ و RADIUS.

TCP و UDP

يستخدم RADIUS بروتوكول UDP بينما يستخدم TACACS+ بروتوكول TCP. يوفر بروتوكول TCP العديد من المميزات 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 النهاية الخلفية (إقرار TCP) وإبطاله.

- يوفر بروتوكول TCP إشارة فورية إلى تعطل الخادم أو إيقافه 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 إلى إرسال رسائل إلى تلك الرسائل التي يعرف أنها قيد التشغيل.

- يتسم بروتوكول TCP بقدر أكبر من قابلية التطوير ويتكيف مع الشبكات التي تزيد من الحجم بالإضافة إلى زيادة الازدحام.

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 الحاجة 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 بينما يتم إلغاء اقتران آلية 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

ال يسمح RADIUS للمستخدمين بالتحكم في الأوامر التي يمكن تنفيذها على الموجه وتلك التي ال يمكن تنفيذها. وبالتالي، ال 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 ال 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)، ال يضمن التوافق مع RADIUS RFCs قابلية التشغيل البيني. على الرغم من أن العديد من البائعين ينفذون عملاء RADIUS، إلا أن هذا ال 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 العمل بين عدة موردين طالما أن وكلاء 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 مرور البيانات

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 ال يمكن RADIUS القيام به) ومحاسبة EXEC ومحاسبة الأوامر (الذي ال يمكن RADIUS القيام به).

مثال حركة مرور TACACS+

يفترض هذا المثال تنفيذ تسجيل الدخول إلى المصادقة، وتفويض EXEC، وتفويض الأوامر، ومحاسبة Start-stop EXEC، ومحاسبة الأوامر باستخدام TACACS+ عندما يقوم مستخدم Telnet إلى موجه، وتنفيذ أمر، والخروج من الموجه:

مثال حركة مرور RADIUS

يفترض هذا المثال تنفيذ تسجيل الدخول إلى المصادقة وتفويض EXEC ومحاسبة EXEC لعملية بدء التشغيل مع RADIUS عندما يقوم مستخدم Telnet إلى موجه بتنفيذ أمر والخروج من الموجه (ال تتوفر خدمات الإدارة الأخرى).

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 Cisco IOS®[2]	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 11000 من Cisco	5.03	5.03	5.03	5.0	5.04	—
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 8.x من Enterprise[9]	—	—	—	—	—
cisco مادة حافزة 2900xl/3500xl مفتاح	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]
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 12.2(4)JA أو الإصدارات الأحدث. في برنامج Cisco IOS الإصدار 12.2(4)JA أو إصدار أحدث، يمكن المصادقة لكل من إنهاء العملاء اللاسلكيين وحركة مرور الإدارة.

2. تحقق من Software Advisor (مرشد البرامج) للحصول على دعم النظام الأساسي داخل

برنامج Cisco IOS.

3. ال يتم تنفيذ عملية محاسبة الأوامر حتى إصدار برنامج Cisco IOS Software 11.1.6.3.
4. ال يوجد تفويض للأوامر.
5. ال 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 (VSA) أو تفويض PIX - الإصدار 6.1 من بروتوكول TACACS+ لحركة مرور VPN التي يتم إنهاؤها على ACL 11 لحركة مرور VPN التي يتم إنهاؤها على سمة RADIUS دعم تفويض الإصدار 6.2.2 - دعم قوائم التحكم في الوصول القابلة للتنزيل مع إنهاء إدارة مرور حركة تفويض RADIUS لحركة مرور VPN على الإصدار 6.2 - دعم تفويض TACACS+ من خلال PIX.<

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 VPN من خلال PIX.

9. برامج المؤسسات فقط.
10. يحتاج لذاكرة Flash سعة 8 ميجا للصورة.
11. إنهاء شبكة VPN فقط.

> ملاحظة: يمكن فقط لمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco ومعلومات داخلية.

معلومات ذات صلة

- دعم RADIUS
- بروتوكولات TACACS/TACACS+ الدعم / المصادقة
- طلبات التعليقات (RFCs)
- الدعم الفني والتنزيلات من Cisco

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 دائماً إلى المستند الإنجليزي الأصلي (الرابط متوفر).