قفل المستخدمين في مجموعة مركز VPN 3000 باستخدام خادم RADIUS

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
تكوين مركز Cisco VPN 3000
تكوين خادم RADIUS
مصدر المحتوى الإضافي الآمن من Cisco لأنظمة التشغيل Windows
Cisco Secure ل UNIX
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يتلقى مركز VPN 3000 من Cisco القدرة على تأمين المستخدمين في مجموعة مركز تتخطى المجموعة التي قام المستخدم بتكوينها في عميل Cisco VPN 3000. بهذه الطريقة، يمكن تطبيق تقييدات الوصول على مجموعات مختلفة تم تكوينها على مركز VPN مع ضمان قفل المستخدمين في تلك المجموعة باستخدام خادم RADIUS.

يوضح هذا المستند كيفية إعداد هذه الميزة على Cisco Secure ACS ل Windows وCisco Secure ل UNIX ((CSUnix).

ويكون التكوين على مركز الشبكة الخاصة الظاهرية (VPN) مماثلا للتكوين القياسي. يتم تمكين إمكانية قفل المستخدمين في مجموعة معرفة على مركز VPN عن طريق تعريف سمة إرجاع في ملف تعريف مستخدم RADIUS. تحتوي هذه السمة على اسم مجموعة مركز الشبكة الخاصة الظاهرية (VPN) الذي يريد المسؤول أن يتم تأمين المستخدم فيه. هذه السمة هي سمة الفئة (سمة IETF RADIUS رقم 25)، ويجب إرجاعها إلى مركز VPN بهذا التنسيق:

```
OU=groupname;
```

حيث *groupname* هو اسم المجموعة على مركز VPN الذي يقفل المستخدم فيه. يجب *أن* تكون بحروف كبيرة، ويجب أن يكون هناك فاصلة منقوطة في النهاية.

في هذا المثال، يتم توزيع برنامج عميل شبكة VPN على جميع المستخدمين الذين لديهم ملف تعريف اتصال موجود باستخدام *اسم مجموعة* "Everyone" وكلمة المرور "Any". لكل مستخدم اسم مستخدم/كلمة مرور منفصلة (في هذا المثال، اسم المستخدم/كلمة المرور هي TEST/TEST). عند إرسال اسم المستخدم إلى خادم RADIUS، يرسل خادم RADIUS معلومات حول *المجموعة الحقيقية* التي يجب أن يكون المستخدم فيها. في المثال، هي "filtergroup".

من خلال القيام بذلك، يمكنك التحكم تماما في مهمة المجموعة على خادم RADIUS الشفاف للمستخدمين. إذا لم يعين خادم RADIUS مجموعة للمستخدم، يبقى المستخدم في مجموعة "الكل". نظرا لأن مجموعة "الكل" تحتوي على عوامل تصفية مقيدة للغاية، فلا يمكن للمستخدم تمرير أي حركة مرور. إذا قام خادم RADIUS بتعيين مجموعة للمستخدم، فإن المستخدم يرث السمات، بما في ذلك عامل التصفية الأقل تقييدا، وخاصة للمجموعة. في هذا المثال، يمكنك تطبيق عامل تصفية على المجموعة "filtergroup" على مركز VPN للسماح بجميع حركات المرور.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

ملاحظة: تم إختبار ذلك بنجاح أيضا مع ACS 3.3، ومجمع VPN 4.1.7، وزبون VPN 4.0.5.

- Cisco VPN 3000 Concentrator Series، الإصدار REL(1)4.0
- Cisco VPN Client، الإصدار REL(1)4.0
- مصدر المحتوى الإضافي الآمن من Cisco لنظام التشغيل Windows من 2.4 إلى 3.2
- Cisco Secure ل UNIX الإصدارات 2.3 و 2.5 و 2.6

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

الاصطلاحات

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

تكوين مركز Cisco VPN 3000

ملاحظة: يفترض هذا التكوين أن مركز الشبكة الخاصة الظاهرية (VPN) تم إعداده بالفعل باستخدام عناوين IP والبوابة الافتراضية ومجموعات العناوين وما إلى ذلك. يجب أن يكون المستخدم قادرا على المصادقة محليا قبل المتابعة. وإذا لم ينجح هذا، فلن تنجح هذه التغييرات.

1. تحت **تشكيل>نظام>خادم>مصادقة**، أضف عنوان IP الخاص بخادم RADIUS.
2. بمجرد إضافة الخادم، أستخدم الزر **إختبار** للتحقق من إمكانية مصادقة المستخدم بنجاح.إذا لم ينجح ذلك، فلن يعمل تأمين المجموعة.
3. قم بتعريف عامل تصفية يقوم بإسقاط الوصول إلى كل شيء في الشبكة الداخلية.يتم تطبيق هذا على مجموعة "Everyone" حتى يتمكن المستخدمون من المصادقة على هذه المجموعة والبقاء فيها، إلا أنهم لا يزالون غير قادرين على الوصول إلى أي شيء.
4. تحت تشكيل>**إدارة السياسة>إدارة حركة مرور البيانات>قاعدة**، **أضف قاعدة** باسم **إسقاط الكل** واترك كل شيء عند الافتراضيات.
5. تحت تشكيل>**إدارة السياسة>إدارة حركة مرور البيانات > عوامل تصفية**، قم بإنشاء مرشح يسمى إسقاط الكل، أترك كل شيء عند الافتراضيات، وقم بإضافة قاعدة إسقاط الكل إليها.
6. تحت **تشكيل>مستعمل إدارة>مجموعة** يضيف مجموعة تسمى **كل**.هذه هي المجموعة التي قام جميع المستخدمين بتكوينها مسبقا في عميل شبكة VPN. يقومون بالمصادقة داخل هذه المجموعة في البداية، ثم

يتم تأمينها في مجموعة مختلفة بعد مصادقة المستخدم. قم بتعريف المجموعة بشكل طبيعي. تأكد من إضافة عامل تصفية Drop All (الذي قمت بإنشائه) تحت علامة التبويب "عام". لاستخدام مصادقة RADIUS للمستخدمين في هذه المجموعة، قم بتعيين نوع المجموعة (أسفل علامة التبويب الهوية) ليكون **داخلي** ومصادقة (أسفل علامة التبويب IPSec) إلى **RADIUS**. تأكد من عدم تحديد ميزة "تأمين المجموعة" لهذه المجموعة.**ملاحظة:** حتى إذا لم تقم بتعريف عامل تصفية Drop All (إسقاط الكل)، فتأكد من وجود عامل تصفية واحد على الأقل معرف هنا.

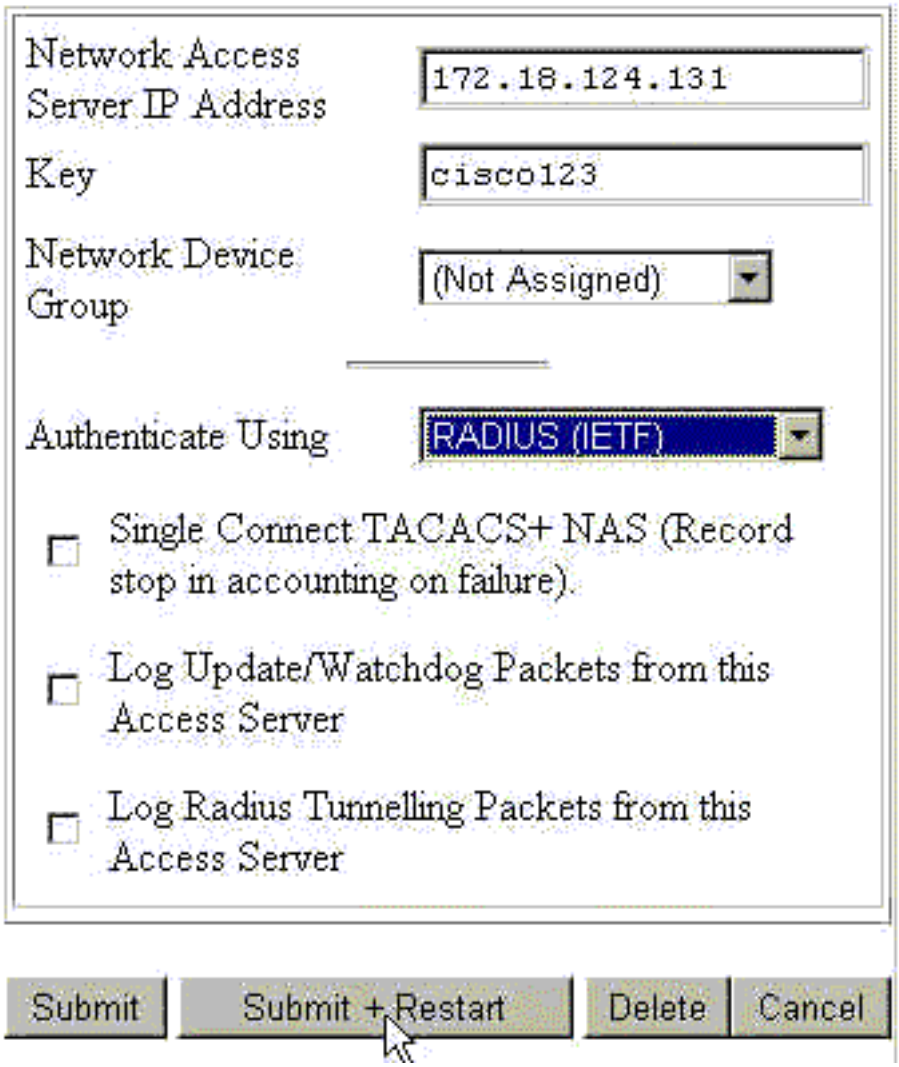
7. تحديد مجموعة الوجهة النهائية للمستخدم (المثال هو "filtergroup")، تطبيق عامل تصفية.**ملاحظة:** يجب تحديد عامل تصفية هنا. إذا كنت لا ترغب في حظر أي حركة مرور لهؤلاء المستخدمين، قم بإنشاء عامل تصفية "السماح للكل" وطبق قواعد "أي داخل" و"أي خارج" عليه. يجب تحديد عامل تصفية من نوع ما لتمرير حركة المرور. لاستخدام مصادقة RADIUS للمستخدمين في هذه المجموعة، قم بتعيين نوع المجموعة (أسفل علامة التبويب الهوية) ليكون **داخلي** ومصادقة (أسفل علامة التبويب IPSec) إلى **RADIUS**. تأكد من عدم تحديد ميزة "تأمين المجموعة" لهذه المجموعة.

تكوين خادم RADIUS

مصدر المحتوى الإضافي الآمن من Cisco لأنظمة التشغيل Windows

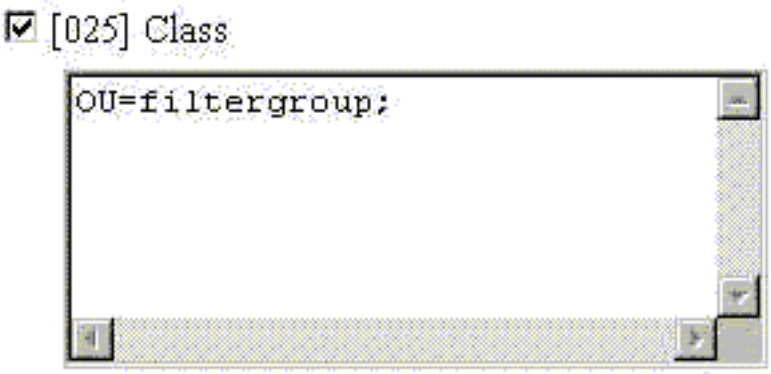
هذه الخطوات قم بإعداد مصدر المحتوى الإضافي الآمن من Cisco لخادم Windows RADIUS لقفل مستخدم ما في مجموعة معينة تم تكوينها على مركز الشبكة الخاصة الظاهرية (VPN). تذكر أن المجموعات المعرفة على خادم RADIUS لا علاقة لها بالمجموعات المعرفة على مركز VPN. يمكنك إستخدام مجموعات على خادم RADIUS لتسهيل إدارة المستخدمين. لا يجب أن تتطابق الأسماء مع ما تم تكوينه على مركز VPN.

1. إضافة مركز VPN كخادم وصول شبكة (NAS) على خادم RADIUS ضمن قسم تكوين الشبكة.قم بإضافة عنوان IP الخاص بموجه الشبكة الخاصة الظاهرية (VPN) في مربع عنوان IP لنظام التخزين المتصلة بالشبكة (NAS).قم بإضافة المفتاح نفسه الذي قمت بتعريفه سابقا على مركز VPN في مربع "المفتاح".من القائمة المنسدلة مصادقة باستخدام، حدد **RADIUS (IETF)**.انقر فوق **إرسال + إعادة**



تشغيل.

2. ضمن "تكوين الواجهة"، حدد **RADIUS (IETF)** وتأكد من تحديد السمة **25 (الفئة)**.وهذا يتيح لك تغييره في تكوين المجموعة/المستخدم.
3. إضافة المستخدم.في هذا المثال، يسمى المستخدم "TEST." يمكن أن يكون هذا المستخدم في أي مصدر المحتوى الإضافي الآمن من Cisco لمجموعة Windows. بخلاف نقل السمة 25 لإخبار مركز الشبكة الخاصة الظاهرية (VPN) عن المجموعة التي سيتم إستخدامها للمستخدم، لا يوجد إرتباط بين مصدر المحتوى الإضافي الآمن من Cisco لمجموعات Windows ومجموعات مركز الشبكة الخاصة الظاهرية (VPN). يتم وضع هذا المستخدم في "group_1."
4. تحت إعداد المجموعة، قم بتحرير الإعدادات على المجموعة (في المثال، هذا هو "Group_1").
5. انقر زر **IETF RADIUS** الأخضر لتوصلك إلى السمات المناسبة.
6. قم بالتمرير لأسفل وتعديل السمة 25.
7. أضف السمة كما هو موضح هنا. إستبدال اسم المجموعة الذي تريد تأمين المستخدمين به لمجموعة عوامل التصفية.تأكد من وجود أحرف كبيرة ومن وجود فاصلة منقوطة بعد اسم



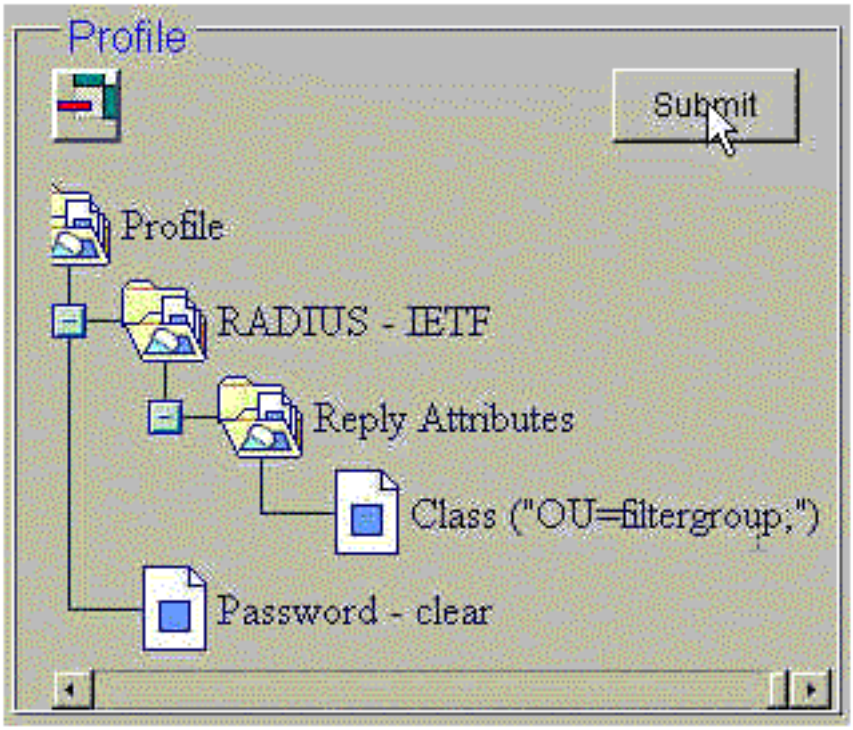
المجموعة.

8. انقر فوق **إرسال + إعادة تشغيل**.

UNIX J Cisco Secure

هذه الخطوات قم بإعداد خادم Cisco Secure UNIX RADIUS لقفل مستخدم ما في مجموعة معينة تم تكوينها على مركز VPN. تذكر أن المجموعات المعرفة على خادم RADIUS لا علاقة لها بالمجموعات المعرفة على مركز VPN. يمكنك إستخدام مجموعات على خادم RADIUS لتسهيل إدارة المستخدمين. لا يجب أن تتطابق الأسماء مع ما تم تكوينه على مركز VPN.

1. قم بإضافة مركز VPN في NAS على خادم RADIUS أسفل قسم المتقدم.أختر قاموسا يسمح بإرسال السمة 25 كسمة رد. على سبيل المثال، IETF أو ascend.
2. إضافة المستخدم.في هذا المثال، المستخدم هو "TEST." يمكن أن يكون هذا المستخدم في أي مجموعة Cisco Secure UNIX أو لا يوجد مجموعة. بخلاف نقل السمة 25 إلى أسفل لمعرفة المجموعة التي يجب إستخدامها للمستخدم لمركز تركيز الشبكة الخاصة الظاهرية (VPN)، لا يوجد إرتباط بين مجموعات Cisco Secure UNIX ومجموعات مركز الشبكة الخاصة الظاهرية (VPN).
3. تحت ملف تعريف المستخدم/المجموعة، قم بتعريف سمة إرجاع IETF (RADIUS).
4. قم بإضافة سمة الفئة، والسمة رقم **25**، وقم بتعيين قيمتها **OU=filtergroup**؛. استبدل المجموعة المعرفة على مركز الشبكة الخاصة الظاهرية (VPN) بمجموعة التصفية.**ملاحظة:** في Cisco Secure UNIX، قم بتعريف السمة المحاطة بعلامات الاقتباس. يتم إزالتها عندما يتم إرسال السمة إلى مركز VPN. يجب أن يبدو ملف تعريف المستخدم/المجموعة مماثلا



لهذا.

5. انقر فوق **إرسال** لحفظ كل إدخال.تظهر إدخالات Cisco Secure UNIX النهائية مماثلة لهذا الإخراج:

```
ViewProfile -p 9900 -u NAS.172.18.124.132/. #
                    User Profile Information
                  }user = NAS.172.18.124.132
                              profile_id = 68
                           profile_cycle = 1
                  "NASNAME="172.18.124.132
                      "SharedSecret="cisco
                        "RadiusVendor="IETF
                "Dictionary="DICTIONARY.IETF

                                        {

                ViewProfile -p 9900 -u TEST/. #
                    User Profile Information
                                  }user = TEST
```

```
                                                    profile_id = 70
                                    set server current-failed-logins = 0
                                                    profile_cycle = 3
                                            "********" password = clear
                                                      } radius=IETF
                                                    } =check_items
                                                          "TEST"=2
                                                                 {
                                                  } =reply_attributes
                                                  "OU=filtergroup"=25
   The semi-colon does NOT appear !--- after the group name, even though it has to be ---!
  included !--- when it defines the attribute via the GUI. } } } # ./ViewProfile -p 9900 -u
 filtergroup User Profile Information user = filtergroup{ profile_id = 80 profile_cycle = 1
radius=IETF { check_items= { 2="filtergroup" } } } # ./ViewProfile -p 9900 -u Everyone User
       Profile Information user = Everyone{ profile_id = 67 profile_cycle = 1 radius=IETF {
                                                  { { { "check_items= { 2="Anything
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- معالجة سمة المجموعة والمستخدم للعميل ل VPN 3000 من Cisco على مركز VPN 3000
- صفحة دعم تقنية RADIUS (خدمة مصادقة طلب اتصال المستخدم البعيد)
- تدعم مركزات Cisco VPN 3000 Series الصفحات
- صفحات دعم عميل VPN 3000 من Cisco
- صفحات دعم منتجات بروتوكول أمان IP (IPSec)
- طلبات التعليقات (RFCs)
- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم منتجات Windows
- الإعلامات الميدانية لمنتجات الأمان
- Cisco Secure ACS لصفحة دعم منتجات UNIX
- الدعم الفني - 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).