ASA/PIX 8.x: تفويض RADIUS (ACS 4.x) للوصول إلى VPN باستخدام قائمة التحكم في الوصول (ACL) القابلة للتنزيل مع CLI ومثال تكوين ASDM

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان لمصادقة المستخدمين للوصول إلى الشبكة. ونظرا لأنه يمكنك تمكين تراخيص RADIUS ضمنيا، فلا يحتوي هذا القسم على معلومات حول تكوين تفويض RADIUS على جهاز الأمان. وهو يوفر معلومات حول كيفية معالجة جهاز الأمان لمعلومات قائمة الوصول التي يتم تلقيها من خوادم RADIUS.

يمكنك تكوين خادم RADIUS لتنزيل قائمة الوصول إلى جهاز الأمان أو اسم قائمة الوصول في وقت المصادقة. يسمح للمستخدم فقط بما هو مسموح به في قائمة الوصول الخاصة

بالمستخدم.

ردصم مادختسإ دنع ريوطتلل ةيلباق لئاسولا رثكأ يه ليزنتلل ةلباقلا لوصولا مئاوق ديزمل .مدختسم لكل ةبسانملا لوصولا مئاوق ريفوتل Cisco نم نمآلا يفاضإلا ىوتحملا نم تامولعملا لوح ميزات ةمئاق لوصولا ةلباقلا ليزنتلل و Cisco Secure ACS، عجرا ىلإ مئاوق التحكم [ليزنتلل ةلباقلا لوصولا يف مكحتلا مئاوق لاسرإل RADIUS مداخ نيوكت](#) في الوصول [ليزنتلل ةلباقلا IP ىلإ](#).

ارجع إلى [ASA 8.3 والإصدارات الأحدث: تفويض RADIUS (ACS 5.x) للوصول إلى VPN باستخدام ASDM و CLI مع ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا ةمئاق نيوكت](#) للتكوين المتطابق على Cisco ASA مع الإصدارات 8.3 والإصدارات الأحدث.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن ASA قيد التشغيل الكامل وتم تكوينه للسماح لـ Cisco ASDM أو CLI بإجراء تغييرات التكوين.

ملاحظة: ارجع إلى [السماح بوصول HTTPS لـ ASDM](#) أو [PIX/ASA 7.x: SSH على الواجهة الداخلية والخارجية نيوكت](#) للسماح بتكوين الجهاز عن بعد بواسطة ASDM أو Secure Shell (SSH).

المكونات المستخدمة

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

- برنامج جهاز الأمان القابل للتكيف الإصدار 7.x من Cisco والإصدارات الأحدث
- Cisco Adaptive Security Device Manager، الإصدار 5.x والإصدارات الأحدث
- Cisco VPN Client الإصدار 4.x والإصدارات الأحدث
- Cisco Secure Access Control Server 4.x

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

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جهاز الأمان Cisco PIX الإصدار 7.x والإصدارات الأحدث.

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

معلومات أساسية

يمكنك إستخدام قوائم التحكم في الوصول إلى IP القابلة للتنزيل لإنشاء مجموعات من تعريفات قائمة التحكم في الوصول (ACL) التي يمكنك تطبيقها على العديد من المستخدمين أو مجموعات المستخدمين. تسمى هذه المجموعات من تعريفات قائمة التحكم باﻟﻮﺻﻮل (ACL) محتويات قائمة التحكم باﻟﻮﺻﻮل (ACL). أيضا، عندما تقوم بدمج NAFs، فإنك تتحكم في محتويات قائمة التحكم في الوصول (ACL) التي يتم إرسالها إلى عميل AAA والذي يسعى المستخدم إلى الوصول منه. وهذا يعني أن قائمة التحكم في الوصول إلى IP القابلة للتنزيل تتضمن تعريفا واحدا أو أكثر من تعريفات محتوى قائمة التحكم في الوصول (ACL)، ويقترن كل واحد منها مع NAF أو (بشكل افتراضي) مرتبط بجميع عملاء AAA. تتحكم ميزة التحكم في الشبكة (NAF) في إمكانية تطبيق محتويات قائمة التحكم في الوصول (ACL) المحددة وفقا لعنوان IP الخاص بعميل AAA. لمزيد من المعلومات حول كيفية تنظم قوائم التحكم في الوصول إلى IP القابلة للتنزيل، راجع حول عوامل تصفية الوصول إلى الشبكة.

تعمل قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل بهذه الطريقة:

1. عندما يمنح ACS للمستخدم حق الوصول إلى الشبكة، يحدد ACS ما إذا كانت قائمة التحكم في الوصول إلى IP قابلة للتنزيل يتم تعيينها لذلك المستخدم أو لمجموعة المستخدم.

2. إذا قام ACS بتحديد موقع قائمة تحكم في الوصول إلى IP قابلة للتنزيل تم تعيينها للمستخدم أو مجموعة المستخدم، فإنه يحدد ما إذا كان إدخال محتوى ACL مقترنا بعميل AAA الذي أرسل طلب مصادقة RADIUS.

3. يرسل ACS، كجزء من جلسة عمل المستخدم، حزمة RADIUS لقبول الوصول، سمة تحدد قائمة التحكم في الوصول (ACL) المسماة، وإصدار قائمة التحكم في الوصول (ACL) المسماة.

4. إذا رد عميل AAA بأنه ال يحتوي على الإصدار الحالي من قائمة التحكم في الوصول (ACL) في ذاكرة التخزين المؤقت الخاصة به، أي أن قائمة التحكم في الوصول (ACL) جديدة أو تم تغييرها، فإن ACS يرسل قائمة التحكم في الوصول (ACL) (جديدة أو محدثة) إلى الجهاز.

قوائم التحكم في الوصول إلى IP القابلة للتنزيل هي بديل لتكوين قوائم التحكم في الوصول (ACL) في سمة RADIUS Cisco-AV-pair [26/9/1] لكل مستخدم أو مجموعة مستخدم. يمكنك إنشاء قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل مرة واحدة، ثم منحها أسماء، ثم تعيين قائمة التحكم في الوصول إلى IP القابلة للتنزيل لكل مستخدم أو مجموعة مستخدمين قابلين للتطبيق إذا قمت بإرجاع أسمائها. تكون هذه الطريقة أكثر فعالية من إذا قمت بتكوين سمة زوج RADIUS من Cisco-av لكل مستخدم أو مجموعة مستخدمين.

علاوة على ذلك، عند إستخدام قوائم التحكم في الوصول (NAF)، يمكنك تطبيق محتويات مختلفة لقائمة التحكم في الوصول (ACL) على نفس المستخدم أو مجموعة المستخدمين فيما يتعلق بعميل AAA الذي يستخدمونه. ال يلزم تكوين إضافي لعميل AAA بعد تكوين عميل AAA لاستخدام قوائم التحكم في الوصول إلى IP القابلة للتنزيل من ACS. تتم حماية قوائم التحكم في الوصول (ACL) القابلة للتنزيل بواسطة نظام النسخ

الاحتياطي أو النسخ المتماثل الذي تقم بإنشائه.

عندما تدخل تعريفات قائمة التحكم في الوصول (ACL) في واجهة ويب ACS، لا تستخدم إدخالات الكلمة الأساسية أو الاسم؛ في جميع الجوانب الأخرى، استخدم صيغة أمر قائمة التحكم في الوصول (ACL) القياسية والأسماء على عميل AAA الذي تنوي تطبيق قائمة التحكم في الوصول إلى IP القابلة للتنزيل عليه. تتضمن تعريفات قائمة التحكم في الوصول (ACL) التي تدخلها في ACS أمر واحد أو أكثر من أوامر قائمة التحكم في الوصول (ACL). يجب أن يكون كل أمر قائمة تحكم في الوصول (ACL) على سطر منفصل.

يمكنك إضافة واحد أو أكثر من محتويات قائمة التحكم في الوصول (ACL) المسماة إلى قائمة التحكم في الوصول (ACL) إلى IP القابلة للتنزيل. بشكل افتراضي، ينطبق كل محتوى قائمة تحكم في الوصول (ACL) على جميع عملاء AAA، ولكن، إذا قمت بتعريف قوائم التحكم في الوصول (NAF)، فيمكنك تقييد إمكانية تطبيق كل محتوى قائمة التحكم في الوصول (ACL) على عملاء AAA المدرجة في NAF التي تقوم بربطها. وهذا يعني، عند استخدام قوائم التحكم في الوصول (NAF)، يمكنك تطبيق كل محتوى من قوائم التحكم في الوصول (ACL) إلى IP، داخل قائمة تحكم في الوصول (ACL) واحدة قابلة للتنزيل، على العديد من أجهزة الشبكة المختلفة أو مجموعات أجهزة الشبكة وفقا لاستراتيجية أمان الشبكة لديك.

يمكنك أيضا تغيير ترتيب محتويات قائمة التحكم في الوصول (ACL) في قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل. يقوم ACS بفحص محتويات قائمة التحكم في الوصول (ACL)، بدءا من أعلى الجدول، وتنزيلات محتوى قائمة التحكم في الوصول (ACL) الأول الذي يعثر عليه مع NAF الذي يتضمن عميل AAA الذي يتم استخدامه. عند تعيين الترتيب، يمكنك التأكد من فعالية النظام إذا قمت بوضع محتويات قائمة التحكم في الوصول (ACL) الأكثر قابلية للتطبيق على نحو أعلى في القائمة. يجب عليك أن تدرك أنه إذا كانت إجراءات العمل المحددة الخاصة بك تتضمن مجموعات من عملاء AAA الذين يتداخلون، فيجب عليك الانتقال من الإجراءات الخاصة إلى الأكثر عمومية. على سبيل المثال، يقوم ACS بتنزيل أي محتويات قائمة التحكم في الوصول (ACL) باستخدام إعداد NAF لجميع عملاء AAA والذي يأخذ في الاعتبار أي محتويات أقل في القائمة.

من أجل استخدام قائمة تحكم في الوصول (ACL) إلى IP قابلة للتنزيل على عميل AAA معين، يجب أن يتبع عميل AAA هذه الاتجاهات:

- استخدام RADIUS للمصادقة
- دعم قوائم التحكم في الوصول (ACL) إلى IP القابلة للتنزيل

هذه أمثلة على أجهزة Cisco التي تدعم قوائم التحكم في الوصول إلى IP القابلة للتنزيل:

- أجهزة ASA و PIX
- مركزات VPN 3000-Series
- أجهزة Cisco التي تشغل IOS الإصدار 12.3(8)T أو الأحدث

هذا مثال على التنسيق الذي يجب عليك استخدامه لإدخال قوائم التحكم في الوصول (ACL) إلى VPN 3000/ASA/PIX 7.x+ في مربع تعريفات قائمة التحكم في الوصول (ACL):

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
```

```
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
                                permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
                              permit TCP any host 10.160.0.1 eq 80 log
                              permit TCP any host 10.160.0.2 eq 23 log
                            permit TCP any host 10.160.0.3 range 20 30
                                  permit 6 any host HOSTNAME1
                               permit UDP any host HOSTNAME2 neq 53
                             deny 17 any host HOSTNAME3 lt 137 log
                                 deny 17 any host HOSTNAME4 gt 138
                            deny ICMP any 10.161.0.0 0.0.255.255 log
                               permit TCP any host HOSTNAME5 neq 80
```

التكوين

.في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعملاء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

:يستخدم هذا المستند إعداد الشبكة التالي

ملاحظة: ال ip ليس خاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

تكوين شبكة VPN للوصول عن بعد (IPSec)

إجراء ASDM

:أتمت هذا steps in order to شكلت الوصول عن بعد VPN

1. أخترت تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ > متقدم > IPSec > سياسات IKE> إضافة in order to خلقت ISAKMP سياسة.

2. قم بتوفير تفاصيل لسياسة ISAKMP كما هو موضح.

   طقطقة ok وطبق.

3. أخترت تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>متقدم>IPSec>IKE معلم أن يمكن ال IKE على قارن خارجي.

4. أخترت تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ > متقدم > IPSec > مجموعات تحويل IPSec > إضافة in order to خلقت ال ESP-3DES-SHA تحويل مجموعة، كما هو موضح.

   طقطقة ok وطبق.

5. أختر Configuration > Remote Access VPN (الوصول عن بعد) > Network (العميل) Access > Advanced > IPSec > Crypto Maps (خرائط التشفير) > Add لإنشاء خريطة تشفير

باستخدام السياسة الديناميكية للأولوية 1، كما هو موضح.

طقطقة ok وقبطق.

6. أخترت تشكيل>وصول عن بعد VPN>شبكة (زبون) منفذ>عنوان تعييني>عنوان بركة VPN زبون ل ال VPN زبون مستعمل. وطقطقة يضيف أن يضيف ال VPN زبون ل ال VPN زبون مستعمل.

7. أخترت تشكيل>وصول عن بعد VPN>AAA setup>AAA دان ل مجموعة ويضيف طقطقة أن يضيف ال AAA دان ل مجموعة إسم وبروتوكول .

إضافة عنوان IP لخادم AAA (ACS) والواجهة التي يتصل بها. قم أيضا بإضافة المفاتيح "سر الخادم" في منطقة معلمات RADIUS. وانقر فوق OK.

8. أخترت Configuration > Remote Access VPN (الوصول عن بعد) > Network (Client) Access ملفات تعريف اتصال IPSec > Add in order to أضفت مجموعة نفق، على سبيل المثال، TunnelGroup1 والمفاتيح المشترك مسبقا على هيئة Cisco123، كما هو موضح.

- تحت علامة التبويب أساسي، أختر مجموعة الخادم كشبكة VPN لحقل مصادقة المستخدم.
- أخترت vpnClient كالزبون عنوان بركة ل ال VPN زبون مستعمل.

وانقر فوق OK.

9. قم بتمكين الواجهة الخارجية للوصول إلى IPSec. انقر فوق تطبيق للمتابعة.

تكوين ASA/PIX باستخدام CLI

أتمت هذه steps in order to شكلت ال DHCP دان ل أن يزود عنوان إلى ال VPN زبون من الأمر خط. ارجع إلى تكوين شبكات VPN للوصول عن بعد وأ مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances للحصول على مزيد من المعلومات حول كل أمر يتم إستخدامه.

يتم تشغيل التكوين على جهاز A

!--- Specify th

timeou
timeout

!--- Create the AAA server group "vpn" and specify the protocol as RADIUS. !--- Specify the CSACS serv

```
!--- PHASE 2 CONFIGURATION ---! !--- The encryption types for Phase 2 are defined here

                                                                                    !--- D

                                                                                !--- Specifies the in

!--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !--- The configuratio
```

```
!--- Associate the vpnclient pool to the tunnel group using the addres
```

تكوين عميل شبكة VPN من Cisco

حاول الاتصال ب Cisco ASA مع عميل Cisco VPN للتحقق من تكوين ASA بنجاح.

1. أختر ترتيب البداية>برامج>Cisco Systems VPN عميل>VPN عميل.

2. انقر على جديد لتشغيل الإطار "إنشاء اتصال VPN جديد".

3. الجديد.كإتصال إضافة تفاصيل ألما

فيضيف في ASA ال من خارج عنوان العلم تدخل .وصف مع "الاتصال الإدخال" اسم أدخل VPN (TunnelGroup1) مجموعة نفق اسم أدخل ثم .صندوق كلمة المرور (مفتاح مشترك) و ASA في تكوينها تم كما (Cisco123 - سابقا .حفظ فوق انقر.

4. انقر فوق الاتصال الذي تريد إستخدامه، ثم انقر فوق الاتصال من الإطار الرئيسي لعميل شبكة VPN.

5. عندما يطلب منك، أدخل اسم المستخدم:cisco وكلمة المرور : password1 كما تم تكوينها في ASA ل xauth، وانقر موافق للاتصال بالشبكة عن بعد.

6. يتم توصيل عميل شبكة VPN مع ASA في الموقع المركزي.

7. بمجرد تأسيس الاتصال بنجاح، أختر إحصائيات من قائمة الحالة للتحقق من تفاصيل النفق.

تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي

يمكنك تكوين قوائم الوصول القابلة للتنزيل على Cisco Secure ACS كمكون لملف تعريف مشترك ثم تعيين قائمة الوصول إلى مجموعة أو مستخدم فردي.

لتنفيذ قوائم الوصول الديناميكية، يجب تكوين خادم RADIUS لدعمه. عندما يقوم المستخدم بالمصادقة، يرسل خادم RADIUS قائمة وصول أو اسم قائمة وصول قابلة للتنزيل إلى الأمان. يتم السماح بالوصول إلى خدمة معينة أو رفضه بواسطة قائمة الوصول. يحذف جهاز الأمان قائمة الوصول عند انتهاء صلاحية جلسة عمل المصادقة.

في هذا المثال، تتم مصادقة مستخدم "cisco" ل IPSec VPN بنجاح، ويرسل خادم RADIUS قائمة الوصول القابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول (ACL)، راجع قسم [قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة].

أتمت هذا steps in order to شكلت RADIUS في cisco أمن acs.

1. أختر شبكة تشكيل على اليسار، وطقطقة يضيف مدخل أن يضيف مدخل ل ال ASA في ال RADIUS لدان قاعدة معطيات.

2. أدخل 172.16.1.2 في حقل عنوان IP للعميل، وأدخل "Cisco123" لحقل المفتاح السري المشترك. أختر RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) في المصادقة باستخدام المربع المنسدل. انقر على إرسال. .

3. أدخل ال username في المستعمل مجال في ال cisco أمن قاعدة معطيات، وطقطقة يضيف/يحرر.

في اذه يالثم، ال username cisco.

4.دنع 1.ةملك اضيأ ةملكلا ،لاثم اذه يف ."cisco" ل رورملا ةملك لخدأ ،يلاتلا راطإلا يف
إلاسر قوف رقنا ،ءاهتنالا.

5.اهضرعي يتلا ةمدقتملا تارايخلا يأ ددحتل ةمدقتملا تارايخلا ةحفص مدختست كنإ
اذإ ACS بيو ةهجاو نم ىرخأ قطانم يف رهظت يتلا تاحفصلا طيسبت كنكمي .ACS
رقنا مث ،ةهجاولا نيوكت قوف رقنا .اهمدختست ال يتلا ةمدقتملا تارايخلا ءافخإب تمق
قوف ةمدقتملا تارايخلا ةحفص حتفل ةمدقتملا تارايخلا.

مئاوقو مدختسملا ىوتسم ىلع ليزنتلل ةلباقلا ACL مئاووقب صاخلا عبرملا ددح
ةعومجملا ىوتسم ىلع ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا.

دنع - مدختسملا ىوتسم ىلع ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا مئاوق
ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا مئاوق مسق رايخلا اذه حيتي ،رايتخالا
مدختسملا دادعإ ةحفص يف (لوصولا يف مكحتلا مئاوق).

دنع - ةعومجملا ىوتسم ىلع ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا مئاوق
ليزنتلل ةلباقلا (ACL) لوصولا يف مكحتلا مئاوق مسق رايخلا اذه حيتي ،رايتخالا
يف ةحفص دادعإ ةعومجملا.

6.مئاوق ىلع رقناو ،كرتشملا فيرعتلا فلم تانوكم ىلع رقنا ،لقنتلا طيرش يف
ليزنتلل ةلباقلا IP ىلإ لوصولا يف مكحتلا.

ةظحالم: اذإ مل رهظت مئاوق مكحتلا يف لوصولا ىلإ IP ةلباقلا ليزنتلل يف ةحفص
(ACL) تانوكم فلم فيرعتلا كرتشملا، فيجب نيكمت مئاوق مكحتلا يف لوصولا
(ACL) ةلباقلا ليزنتلل ىلع ىوتسم مدختسملا وأ رايخ مئاوق مكحتلا يف لوصولا
ةلباقلا ليزنتلل ىلع ىوتسم ةعومجملا وأ امهالك يف ةحفص تارايخلا ةمدقتملا نم
مسق نيوكت ةهجاولا.

7.ةلباقلا IP ىلإ لوصولا يف مكحتلا مئاوق ةحفص رهظت .(Add) ةفاضإ قوف رقنا
ليزنتلل.

8.ةديدجلا IP ىلإ (ACL) لوصولا يف مكحتلا ةمئاق مسا بتكا ،مسالا عبرم يف

ةظحالم: نكمي نأ يوتحي مسا ةمئاق مكحتلا يف لوصولا ىلإ IP ىلع ام لصي ىلإ 27
افرح. بجي الأ يوتحي مسالا ىلع تافاسم وأ يأ نم هذه فرحألا: وا ةلصاف (-) وأ سوق أيسر
وأ (") صيصنت تامالع وأ (\) ةيفلخ ةلئام ةطرش وأ (/) ةلئام ةطرش وأ ([) سوق أيسر وأ ([)
ةطرش (-) وأ (<) ىنمي ةيواز سوق وأ (>) سوق أيسر.

ةديدجلا IP ىلإ (ACL) لوصولا يف مكحتلا ةمئاقل افصو بتكا ،فصولا عبرم يف.
نكمي نأ لصي فصولا ىلإ 1000 فرح.

(ACL) لوصولا يف مكحتلا ةمئاق ىلإ (ACL) لوصولا يف مكحتلا ةمئاق ىوتحم ةفاضإل
ىلإ IP ةديدجلا، رقنا قوف إضافة.

9.ديدجلا (ACL) لوصولاب مكحتلا ةمئاق ىوتحم مسا بتكا ،مسالا عبرم يف

ةظحالم: نكمي نأ يوتحي مسا ىوتحم ةمئاق مكحتلا يف لوصولا (ACL) ىلع ام لصي

إلى 27 حرف. يجب أن يحتوي الاسم على مسافات أو أي من هذه الأحرف: واصلة (-) أو قوس أيسر ([) أو شرطة سائلة خلفية (\) أو شرطة مائلة (/) أو قوس أيسر ([) أو قوس أيمن (]) أو علامات تنصيص (") أو قوس أيسر (<) أو قوس أيمن (>) أو شرطة (-).

في مربع تعريفات قائمة التحكم في الوصول (ACL)، اكتب تعريف قائمة التحكم في الوصول (ACL) الجديد.

ملاحظة: عند إدخال تعريفات قائمة التحكم في الوصول (ACL) في واجهة ويب ACS، لا تستخدم إدخالات الكلمة الأساسية أو الاسم؛ وبدلاً من ذلك، ابدأ بالكلمة الأساسية السماح أو الرفض.

لحفظ محتوى قائمة التحكم في الوصول (ACL)، انقر فوق إرسال.

10. تظهر صفحة قوائم التحكم في الوصول إلى IP القابلة للتنزيل مع محتوى قائمة التحكم في الوصول (ACL) الجديد المدرج بالاسم في عمود محتويات قائمة التحكم في الوصول (ACL). لربط NAF بمحتوى قائمة التحكم في الوصول، أختر NAF من قائمة التحكم في الوصول (ACL) تصفية الوصول إلى الشبكة إلى يمين المحتوى الجديد لقائمة التحكم في الوصول. وبشكل افتراضي، يكون NAF (جميع عملاء AAA). إذا لم تقم بتعيين NAF، فإن ACS يربط محتوى قائمة التحكم في الوصول (ACL) بجميع أجهزة الشبكة، وهو الإعداد الافتراضي.

لتعيين ترتيب محتويات قائمة التحكم في الوصول (ACL)، انقر فوق زر الاختيار الخاص بتعريف قائمة التحكم في الوصول (ACL)، ثم انقر فوق أعلى أو أسفل لإعادة وضعه في القائمة.

لحفظ قائمة التحكم في الوصول (ACL) إلى IP، انقر فوق إرسال.

ملاحظة: ترتيب محتويات قائمة التحكم في الوصول (ACL) هام. ومن الأعلى إلى الأسفل، يقوم ACS بتنزيل تعريف قائمة التحكم في الوصول (ACL) الأول فقط الذي يحتوي على إعداد NAF قابل للتطبيق، والذي يتضمن الإعداد الافتراضي لجميع عملاء AAA، إذا تم استخدامه. بشكل نموذجي، تنتقل قائمة محتويات قائمة التحكم في الوصول (ACL) من القائمة التي تحتوي على أكثر (أضيق) NAF تحديدا إلى القائمة التي تحتوي على أكثر NAF عامة (جميع عملاء AAA).

ملاحظة: يدخل ACS قائمة التحكم في الوصول (ACL) إلى IP الجديدة، والتي تدخل حيز التنفيذ على الفور. على سبيل المثال، إذا كانت قائمة التحكم في الوصول (ACL) إلى IP مخصصة للاستخدام مع جدران حماية PIX، فإنها توفر ليتم إرسالها إلى أي جدار حماية PIX يحاول مصادقة المستخدم الذي لديه قائمة التحكم في الوصول (ACL) إلى IP القابلة للتنزيل التي تم تعيينها إلى ملف تعريف المستخدم أو المجموعة الخاص به.

11. انتقل إلى صفحة إعداد المستخدم وقم بتحرير صفحة المستخدم. تحت قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل، انقر فوق خانة الاختيار تعيين قائمة التحكم في الوصول (ACL) إلى IP. أختر قائمة تحكم في الوصول (ACL) من IP إلى التحكم في الوصول (ACL). في حالة الانتهاء من تكوين خيارات حساب المستخدم، انقر فوق إرسال لتسجيل الخيارات.

تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة

أكمل الخطوات من 1 إلى 9 من تكوين ACS لقائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم الفردي واتبع هذه الخطوات لتكوين قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمجموعة في Cisco ACS الآمن.

في هذا المثال، ينتمي مستخدم شبكة VPN لـ IPSec "cisco" إلى مجموعات VPN. يتم تطبيق سياسات مجموعة VPN على جميع المستخدمين في المجموعة.

تتم مصادقة مستخدم مجموعة VPN"cisco"بنجاح، ويرسل خادم RADIUS قائمة وصول قابلة للتنزيل إلى جهاز الأمان. يمكن للمستخدم "cisco" الوصول إلى خادم 10.1.1.2 فقط ويرفض جميع الوصول الآخر. للتحقق من قائمة التحكم في الوصول (ACL)، ارجع إلى قسم قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة.

1. في شريط التنقل، انقر فوق إعداد المجموعة. يتم فتح صفحة تحديد إعداد المجموعة.

2. عينت مجموعة 1 إلى VPN، وطقطقة يرسل.

3. من قائمة المجموعة، أختر مجموعة، ثم انقر تحرير الإعدادات.

4. تحت قسم قوائم التحكم في الوصول (ACL) القابلة للتنزيل، انقر فوق خانة الاختيار تعيين قائمة التحكم في الوصول (ACL) إلى IP. أختر قائمة تحكم في الوصول (ACL) إلى IP من القائمة.

5. انقر فوق إرسال لحفظ إعدادات المجموعة التي قمت بإجرائها للتو.

6. انتقل إلى "إعداد المستخدم" وقم بتحرير المستخدم الذي تريد إضافته إلى المجموعة. انقر فوق إرسال عند الانتهاء من VPN.

   يتم الآن تطبيق قائمة التحكم في الوصول (ACL) القابلة للتنزيل التي تم تكوينها لمجموعة VPN على هذا المستخدم.

7. لمتابعة تحديد إعدادات المجموعة الأخرى، قم بتنفيذ إجراءات أخرى في هذا الفصل، حسب ما يكون منطبقا

تكوين إعدادات IETF RADIUS لمجموعة مستخدمين

عند تنزيل اسم قائمة وصول قمت بإنشائها بالفعل على جهاز الأمان من خادم RADIUS، قم بتكوين السمة IETF RADIUS filter-id (السمة رقم 11) كما يلي:

```
<#root>

filter-id=acl_name
```

تتم مصادقة مستخدم مجموعة VPN"cisco" بنجاح، ويقوم خادم RADIUS بتنزيل اسم قائمة وصول قمت بإنشائها بالفعل على جهاز الأمان . يمكن التحكم في الوصول (جديد) لقائمة وصول قمت بإنشائها بالفعل على جهاز الأمان من خادم ASA باستثناء الأجهزة الموجودة داخل شبكة "cisco" الوصول إلى جميع المستخدم. للتحقق من قائمة التحكم في الوصول (ACL)، راجع قسم قائمة التحكم في الوصول إلى معرفة التصفية. 10.1.1.2

وفقا للمثال، تم تكوين قائمة التحكم في الوصول (ACL) المسماة جديدة للتصفية في ASA.

```
<#root>

access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

تظهر هذه المعلومات فقط عندما تكون صحيحة. لقد قمت بتهيئة:

- تكوين الشبكة RADIUS في وتوكولات RADIUS لاستخدام أحد برو عميل AAA
- تكوين قسم RADIUS (IETF) في صفحة RADIUS على مستوى المجموعة في سمات RADIUS الواجهة وواجهة الويب

يتم إرسال سمات RADIUS كملف تعريف لكل مستخدم من ACS إلى عميل AAA الطالب.

لتكوين إعدادات سمة IETF RADIUS لتطبيقها كتخويل لكل مستخدم في المجموعة الحالية، قم بتنفيذ هذه الإجراءات:

1. في شريط التنقل، انقر فوق إعداد المجموعة.

   يتم فتح صفحة تحديد إعداد المجموعة.

2. من قائمة المجموعة، أختر مجموعة، ثم انقر تحرير الإعدادات.

   يظهر اسم المجموعة في أعلى صفحة إعدادات المجموعة.

3. قم بالتمرير إلى سمات RADIUS الخاصة ب IEFT. لكل سمة IETF RADIUS، يجب عليك تخويل المجموعة الحالية. حدد خانة الاختيار الخاصة بسمة [011] Filter-Id، ثم قم بإضافة اسم قائمة التحكم في الوصول (ACL) المحدد من قبل ASA (جديد) في التخويل الخاص بالسمة في الحقل. ارجع إلى عرض ASA الذي يشغل إخراج التكوين.

4. لحفظ إعدادات المجموعة التي قمت بإجرائها وتطبيقها مباشرة، انقر فوق إرسال وتطبيق.

   ملاحظة: لحفظ إعدادات مجموعتك وتطبيقها لاحقا، انقر فوق إرسال. عندما تكون مستعدا لتنفيذ التغييرات، أختر تكوين النظام > التحكم في الخدمة. ثم أختر إعادة التشغيل.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

مترجم أداة الإخراج (للعملاء المسجلين فقط) يدعم بعض أوامر show. استخدم أداة مترجم الإخراج لعرض تحليل مُخرَج الأمر show .

إظهار أوامر التشفير

- show crypto isakmp sa— يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.

```
<#root>

ciscoasa#

sh crypto isakmp sa


                                    Active SA: 1
              Rekey SA: 0 (A tunnel will report 1 Active
                            and 1 Rekey SA during rekey)
                                Total IKE SA: 1

                              1   IKE Peer: 192.168.10.2
Type    : user                    Role    : responder
Rekey   : no                      State   : AM_ACTIVE
                                    ciscoasa#
```

- show crypto ipSec—يعرض الإعدادات المستخدمة من قبل SAs الحالية.

```
<#root>

ciscoasa#

                                  sh crypto ipsec sa

                                  interface: outside
            Crypto map tag: outside_dyn_map, seq num: 1,
                                local addr: 192.168.1.1

                     local ident (addr/mask/prot/port):
                                  (0.0.0.0/0.0.0.0/0/0)
                    remote ident (addr/mask/prot/port):
                     (192.168.5.1/255.255.255.255/0/0)
             current_peer: 192.168.10.2, username: cisco
                 dynamic allocated peer ip: 192.168.5.1

                       #pkts encaps: 65, #pkts encrypt:
                                   65, #pkts digest: 65
                       #pkts decaps: 65, #pkts decrypt:
                                   65, #pkts verify: 65
              #pkts compressed: 0, #pkts decompressed: 0
            #pkts not compressed: 4, #pkts comp failed:
                                0, #pkts decomp failed: 0
            #pre-frag successes: 0, #pre-frag failures:
                                0, #fragments created: 0
                         #PMTUs sent: 0, #PMTUs rcvd: 0,
               #decapsulated frgs needing reassembly: 0
                         #send errors: 0, #recv errors: 0

                      local crypto endpt.: 192.168.1.1,
                    remote crypto endpt.: 192.168.10.2
```

```
                                path mtu 1500, ipsec overhead 58,
                                                media mtu 1500
                                   current outbound spi: EEF0EC32

                                                inbound esp sas:
                                         spi: 0xA6F92298 (2801345176)
                                    transform: esp-3des esp-sha-hmac none
                                          in use settings ={RA, Tunnel, }
                                     slot: 0, conn_id: 86016, crypto-map:
                                                outside_dyn_map
                            sa timing: remaining key lifetime (sec):
                                                            28647
                                                IV size: 8 bytes
                                         replay detection support: Y
                                                outbound esp sas:
                                         spi: 0xEEF0EC32 (4008766514)
                                    transform: esp-3des esp-sha-hmac none
                                          in use settings ={RA, Tunnel, }
                                     slot: 0, conn_id: 86016, crypto-map:
                                                outside_dyn_map
                            sa timing: remaining key lifetime (sec): 28647
                                                IV size: 8 bytes
                                         replay detection support: Y
```

قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم/المجموعة

تحقق من قائمة التحكم في الوصول (ACL) القابلة للتنزيل للمستخدم Cisco. يتم تنزيل قوائم التحكم في الوصول (ACL) من CSACS.

```
<#root>

ciscoasa(config)#

sh access-list

                            access-list cached ACL log flows: total 0,
                                                denied 0 (deny-flow-max 4096)
                                                    alert-interval 300
                                                access-list 101; 1 elements
                        access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0
                                                192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411

                        access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic)
                        access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit
                                                ip any host 10.1.1.2 (hitcnt=2) 0x334915fe
                        access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny
                                                ip any any (hitcnt=40) 0x7c718bd1
```

قائمة التحكم في الوصول (ACL) لمعرف عامل التصفية

اقوم بتطبيق Filter-ID [011] على المجموعة - VPN، ويتم تصفية مستخدمي المجموعة وفقا لقائمة التحكم في الوصول (ACL) (الجديدة) المعرفة في ASA.

<#root>

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
denied 0 (deny-flow-max 4096)
alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
255.255.255.0 192.168.5.0 255.255.255.0
(hitcnt=0) 0x8719a411
access-list new; 2 elements

access-list new line 1 extended deny ip
any host 10.1.1.2 (hitcnt=4) 0xb247fec8
access-list new line 2 extended permit ip any any
(hitcnt=39) 0x40e5d57c
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. يتم أيضا عرض إجراء تصحيح الأخطاء للعينة.

ملاحظة: للحصول على مزيد من المعلومات حول أستكشاف أخطاء الوصول عن بعد IPSec VPN وإصلاحها، ارجع إلى حلول أستكشاف أخطاء الشبكة الخاصة الظاهرية (VPN) ل L2L والوصول عن بعد وIPSec وإصلاحها.

مسح الاقترانات الأمنية

عند أستكشاف الأخطاء وإصلاحها، تأكد من مسح اقترانات الأمان الموجودة بعد إجراء تغيير. في الوضع ذي الامتيازات ل PIX، أستخدم الأوامر التالية:

- مسح [crypto] ipSec sa—يحذف رسائل IPSec النشطة. تشفير الكلمة الأساسية إختياري.
- مسح [crypto] isakmp sa—يحذف شبكات IKE النشطة. تشفير الكلمة الأساسية إختياري.

أوامر استكشاف الأخطاء وإصلاحها

مجرم أداة مجرم الإخراج (للعملاءالمسجلين فقط) يعدم أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل جَرخُم الأمر show .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر debug.

- debug crypto ipSec 7—يعرض مفاوضات IPSec للمرحلة 2.
- debug crypto isakmp 7—يعرض مفاوضات ISAKMP للمرحلة 1.

معلومات ذات صلة

- Cisco نم ASA 5500 Series فيكتلل ةلباقلا نامألا ةزهجأ معد ةحفص
- Cisco ASA 5500 Series Adaptive Security Appliances ةلدعملا نامألا ةزهجأ رماوأ عجارم Command References
- Cisco PIX 500 Series Security Appliances نامألا ةزهجأ معد ةحفص
- Cisco نم ةلدعملا نامألا لولح ةزهجأ ريدم
- IKE تالوكوتورب/IPsec ةضوافم معد ةحفص
- Cisco نم VPN ةكبش ليمع معد ةحفص
- Windows ليغشتلا ةمظنأل Cisco نم نمآلا لوصولا يف مكحتلا مداخ
- (RFCs) تاقيلعتلا تابلط
- Cisco Systems - تادنتسملاو ينقتلا معدلا

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).