فحص CRL عبر HTTP على مركز Cisco VPN 3000

المحتويات

المقدمة

يوضح هذا المستند كيفية تمكين التحقق من قائمة إبطال الشهادات (CRL) لشهادات مرجع التصديق (CA) المثبتة في مركز VPN 3000 من Cisco باستخدام وضع HTTP.

يتوقع عادة أن تكون الشهادة صالحة طوال فترة صلاحيتها بأكملها. على أي حال، إذا أصبحت الشهادة غير صالحة بسبب أمور مثل تغيير الاسم، وتغيير الاقتران بين الموضوع و CA، وتوافق الأمان، فإن CA يبطل الشهادة. بموجب X.509، تقوم CAs بإبطال الشهادات عن طريق إصدار CRL موقع بشكل دوري، حيث يتم تعريف كل شهادة ملغاة برقمها التسلسلي. يعني تمكين فحص CRL أنه في كل مرة يستخدم فيها مركز الشبكة الخاصة الظاهرية (VPN) الشهادة للمصادقة، فإنه يتحقق أيضا من CRL لضمان عدم إبطال الشهادة التي يتم التحقق منها.

يستخدم CAs قواعد بيانات البروتوكول الخفيف للوصول للدليل (LDAP/HTTP) لتخزين قوائم التحكم في الوصول (CRLs) وتوزيعها. وقد تستخدم أيضا وسائل أخرى، ولكن مركز الشبكة الخاصة الظاهرية (VPN) يعتمد على الوصول إلى بروتوكول LDAP/HTTP.

يتم تقديم فحص HTTP CRL في مركز VPN الإصدار 3.6 أو إصدار أحدث. ومع ذلك، تم إدخال فحص قائمة التحكم في الوصول (CRL) المستندة إلى LDAP في إصدارات x.3 السابقة. يناقش هذا المستند فحص CRL فقط باستخدام HTTP.

ملاحظة: يعتمد حجم ذاكرة التخزين المؤقت ل CRL من مركزات VPN 3000 Series على النظام الأساسي ويتعذر تكوينه وفقا لرغبة المسؤول.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- لقد قمت بإنشاء نفق IPsec من عملاء أجهزة VPN 3.x باستخدام شهادات مصادقة تبادل مفتاح الإنترنت (IKE) (مع عدم تمكين فحص CRL).
- إن مركز الشبكة الخاصة الظاهرية (VPN) لديك إمكانية اتصال بخادم CA في جميع الأوقات.
- إذا كان خادم CA متصلا بالواجهة العامة، تكون قد قمت بفتح القواعد الضرورية في عامل التصفية العام (الافتراضي).

المكونات المستخدمة

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

- مركز VPN 3000 الإصدار C 4.0.1
- عميل أجهزة VPN 3.x
- خادم Microsoft CA لإنشاء الشهادة والتحقق من CRL الذي يتم تشغيله على خادم Windows 2000.

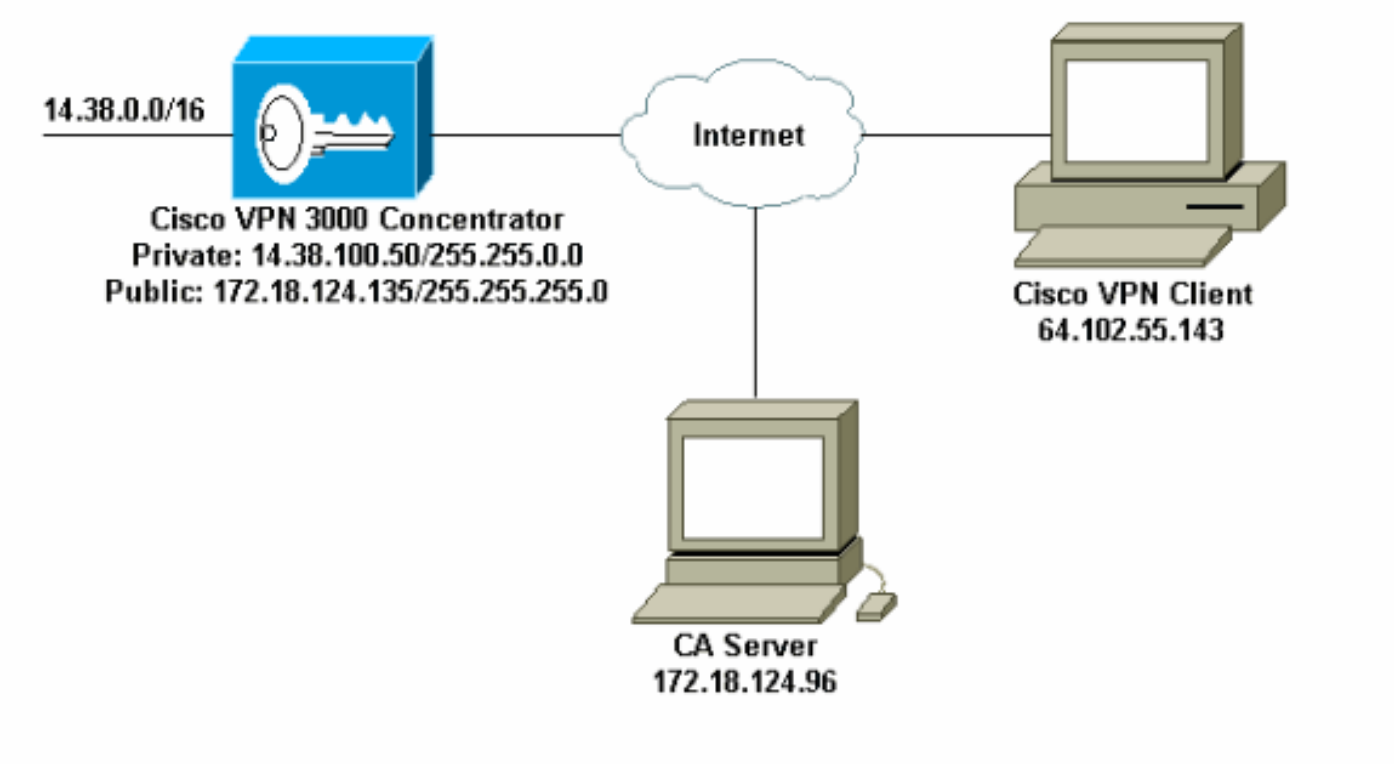
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

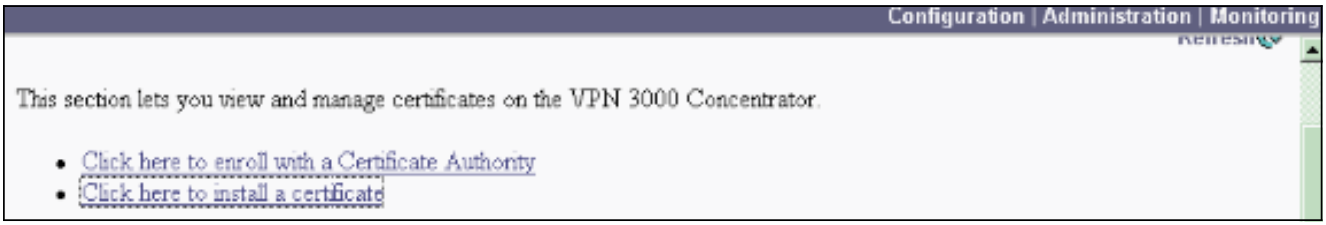


تكوين مركز VPN 3000

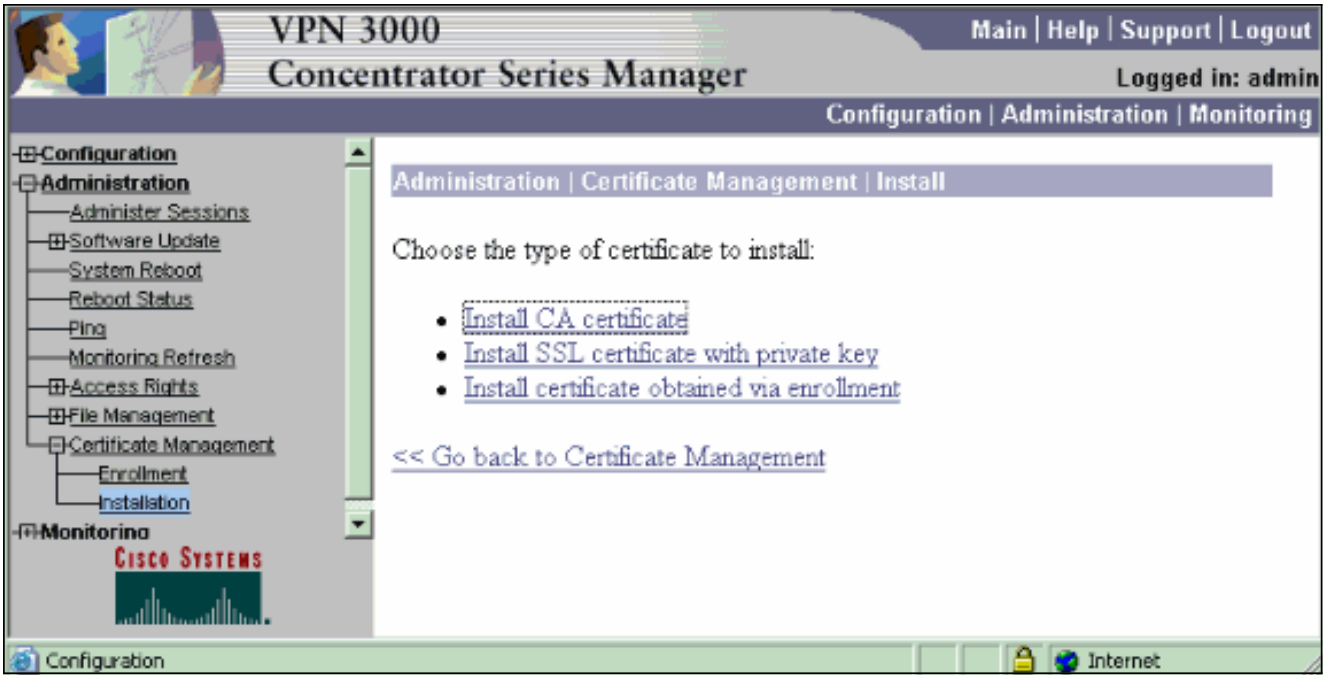
التعليمات بالتفصيل

أتمت هذا steps أن يشكل ال VPN 3000 مركز:

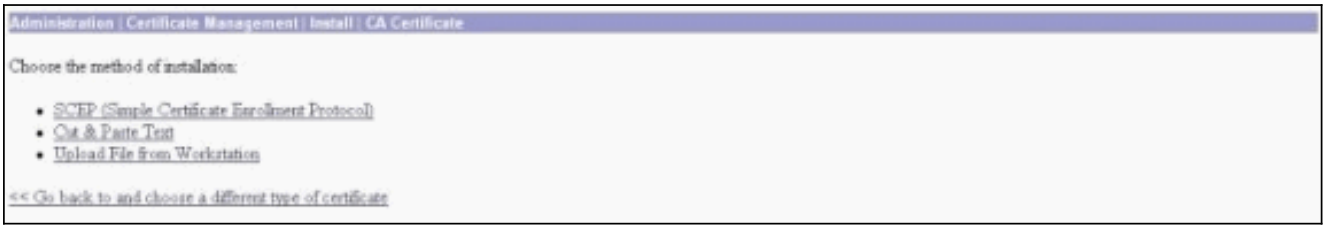
1. حدد **إدارة > إدارة الشهادات** لطلب شهادة إذا لم يكن لديك شهادة.حدد **انقر هنا لتثبيت شهادة** لتثبيت الشهادة الجذر على مركز VPN.



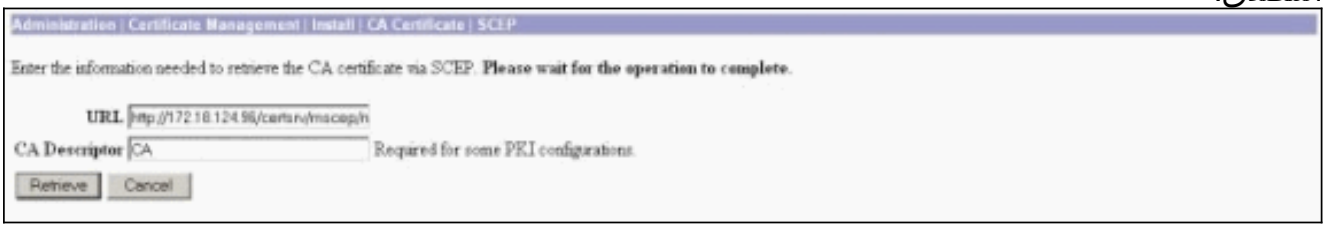
2. حدد **تثبيت شهادة المرجع المصدق**.



3. حدد **SCEP (بروتوكول تسجيل الشهادة البسيط)** لاسترداد شهادات CA.

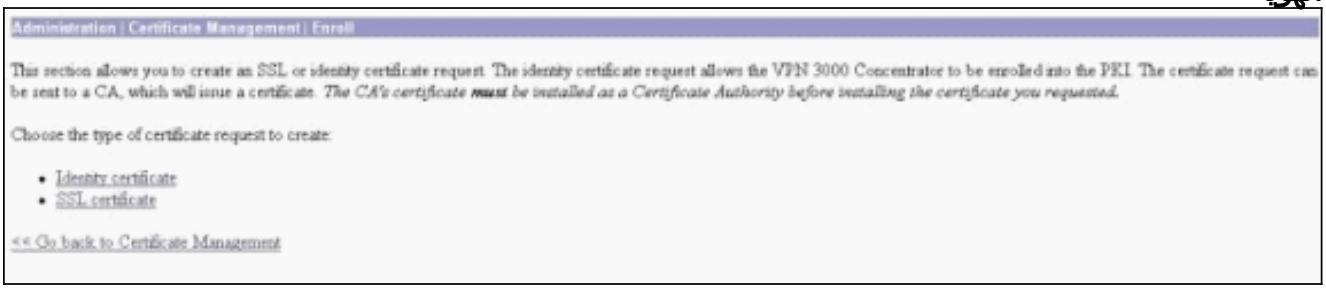


4. من نافذة SCEP، أدخل عنوان URL الكامل لخادم CA في شاشة عنوان الربط.في هذا المثال، عنوان IP لخادم CA هو 172.18.124.96. بما أن هذا المثال يستخدم خادم CA الخاص ب Microsoft، فإن عنوان URL الكامل هو http://172.18.124.96/certsrv/mscep/mscep.dll. بعد ذلك، أدخل واصف كلمة واحدة في مربع الحوار واصف CA. يستخدم هذا المثال المرجع المصدق.

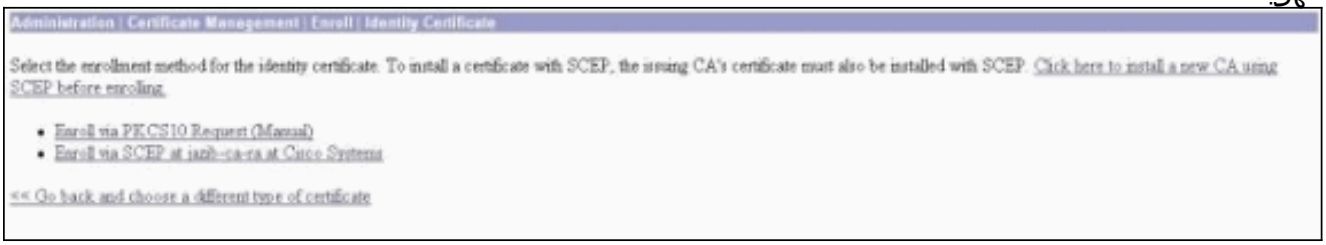


5. انقر فوق **إسترداد**.يجب أن تظهر شهادة المرجع المصدق تحت نافذة إدارة > إدارة الشهادات. إذا لم تظهر لك شهادة، ارجع إلى الخطوة 1 واتبع الإجراء مرة أخرى.

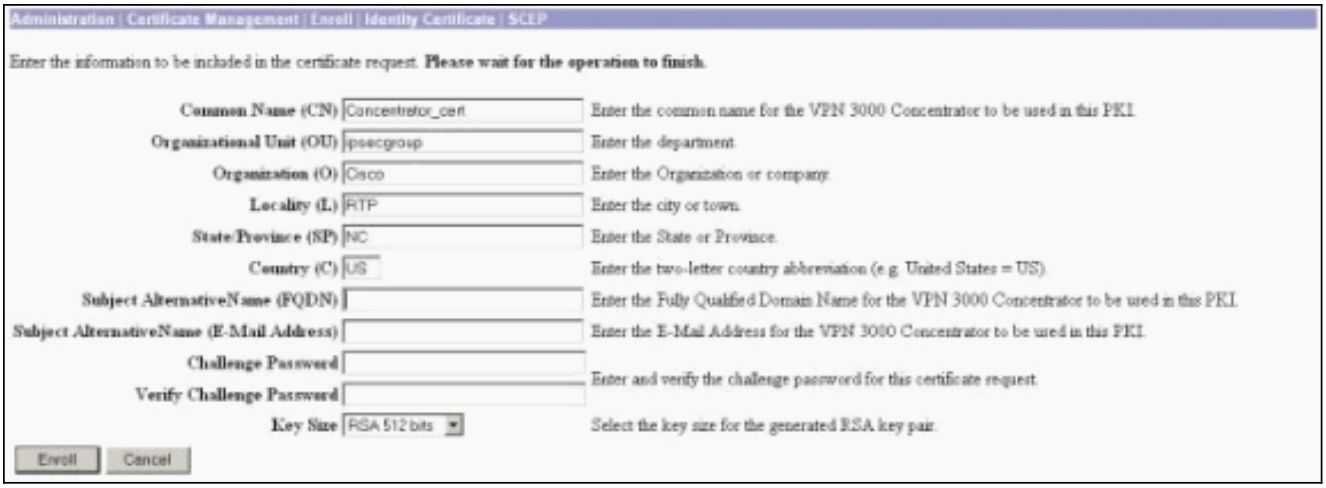
6. بمجرد حصولك على شهادة CA، حدد **الإدارة > إدارة الشهادة > التسجيل**، وانقر فوق **شهادة الهوية**.



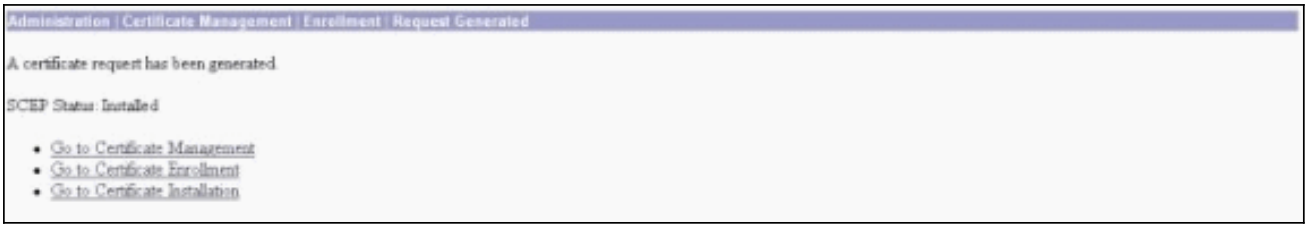
7. انقر على **التسجيل عبر SCEP في ...** لتقديم طلب لشهادة الهوية.



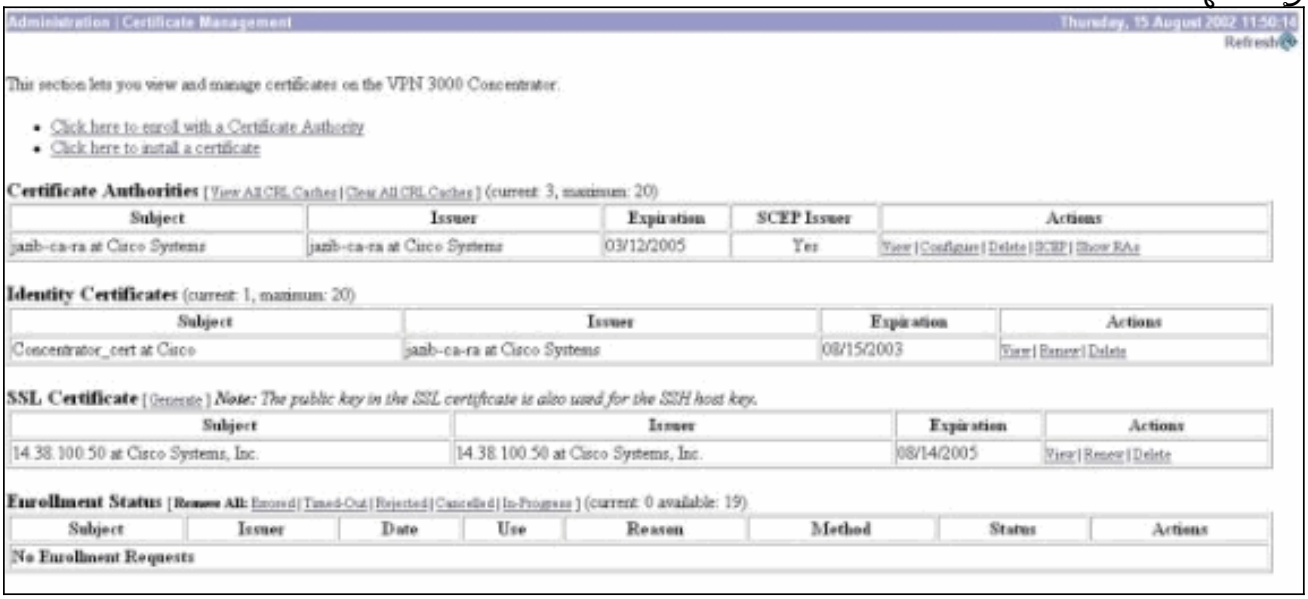
8. أكمل الخطوات التالية لملء نموذج التسجيل:أدخل الاسم الشائع لمركز تركيز الشبكة الخاصة الظاهرية (VPN) المراد إستخدامه في حقل البنية الأساسية للمفتاح العام (PKI) في الاسم الشائع (CN).أدخل القسم الخاص بك في حقل الوحدة التنظيمية (OU). يجب أن تتطابق وحدة التحكم مع اسم مجموعة IPsec الذي تم تكوينه.أدخل مؤسستك أو شركتك في حقل المؤسسة (O).أدخل مدينتك أو مدينتك في حقل "المحلية" (L).أدخل الولاية أو المقاطعة في حقل الولاية/المقاطعة (SP).أدخل دولتك في حقل الدولة (C).أدخل اسم المجال المؤهل بالكامل (FQDN) لمركز تركيز الشبكة الخاصة الظاهرية (VPN) الذي سيتم إستخدامه في PKI في حقل اسم المجال المؤهل بالكامل (FQDN).أدخل عنوان البريد الإلكتروني لمركز تركيز الشبكة الخاصة الظاهرية (VPN) المراد إستخدامه في PKI في حقل اسم الموضوع البديل (عنوان البريد الإلكتروني).أدخل كلمة مرور التحدي لطلب الشهادة في حقل "تحدي كلمة المرور".أعد إدخال كلمة مرور التحدي في حقل التحقق من تحدي كلمة المرور.حدد حجم المفتاح لزوج مفاتيح RSA الذي تم إنشاؤه من القائمة المنسدلة حجم المفتاح.



9. حدد **تسجيل** وعرض حالة SCEP في حالة الاقتراع.
10. انتقل إلى خادم المرجع المصدق للموافقة على شهادة الهوية. بمجرد الموافقة عليه على خادم CA، يجب تثبيت حالة
.SCEP

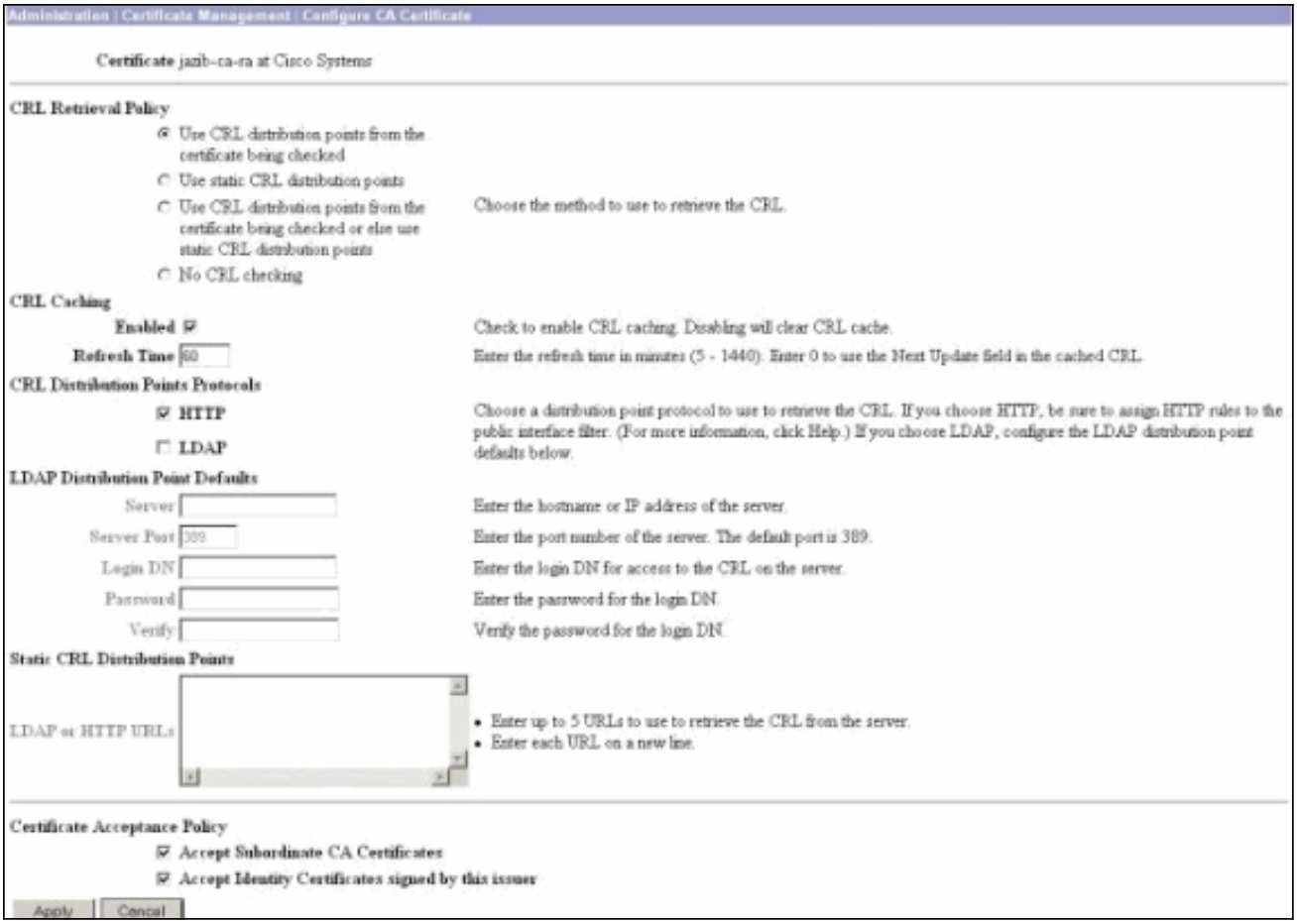


11. تحت إدارة الشهادات، يجب أن ترى شهادة هويتك.إذا لم تقم بذلك، فتحقق من السجلات الموجودة على خادم CA للحصول على مزيد من أستكشاف الأخطاء
وإصلاحها.



12. حدد **عرض** على شهادتك المستلمة لمعرفة ما إذا كانت شهادتك تحتوي على نقطة توزيع CDP) CRL).تسرد CDP جميع نقاط توزيع CRL من مصدر هذه الشهادة. إذا كان لديك CDP على شهادتك، وتستخدم اسم DNS لإرسال استعلام إلى خادم CA، فتأكد من أن لديك خوادم DNS معرفة في مركز VPN الخاص بك لحل اسم المضيف بعنوان IP. في هذه الحالة، يكون مثال اسم مضيف خادم CA هو jazib-pc الذي يحل إلى عنوان 172.18.124.96 IP على خادم
.DNS

13. انقر على **تكوين** في شهادة CA لتمكين تدقيق CRL على الشهادات المستلمة.إذا كان لديك CDP على شهادتك التي إستلمتها وتريد إستخدامها، حدد **إستخدام نقاط توزيع CRL من الشهادة التي يتم فحصها**.ونظرا لأنه يتعين على النظام إسترداد CRL وفحصه من نقطة توزيع على الشبكة، فإن تمكين فحص CRL قد يبطئ من أوقات إستجابة النظام. أيضا، إذا كانت الشبكة بطيئة أو مزدحمة، فقد يفشل التحقق من CRL. قم بتمكين التخزين المؤقت ل CRL للحد من هذه المشاكل المحتملة. يقوم هذا بتخزين قوائم التحكم في الوصول (CRLs) التي تم إستردادها في الذاكرة المتطايرة المحلية وبالتالي يسمح لمركز تركيز الشبكة الخاصة الظاهرية (VPN) بالتحقق من حالة إبطال الشهادات بسرعة أكبر.مع تمكين التخزين المؤقت ل CRL، يتحقق مركز الشبكة الخاصة الظاهرية (VPN) أولا من وجود CRL المطلوب في ذاكرة التخزين المؤقت ويتحقق من الرقم التسلسلي للشهادة مقابل قائمة الأرقام التسلسلية في CRL عندما تحتاج إلى التحقق من حالة إبطال الشهادة. تعتبر الشهادة ملغاة إذا تم العثور على رقمها التسلسلي. يقوم مركز الشبكة الخاصة الظاهرية (VPN) باسترداد CRL من خادم خارجي إما عندما لا يعثر على CRL المطلوب في ذاكرة التخزين المؤقت، أو عندما تنتهي فترة صلاحية CRL المخزنة مؤقتا، أو عندما يكون قد انقضى وقت التحديث الذي تم تكوينه. عندما يستقبل مركز الشبكة الخاصة الظاهرية (VPN) قائمة تحكم في الوصول (CRL) جديدة من خادم خارجي، فإنه يقوم بتحديث ذاكرة التخزين المؤقت باستخدام قائمة التحكم في الوصول (CRL) الجديدة. يمكن أن تحتوي ذاكرة التخزين المؤقت على ما يصل إلى 64 قائمة من قوائم التحكم في الوصول للوسائط (CRL).**ملاحظة:** ذاكرة التخزين المؤقت ل CRL موجودة في الذاكرة. وبالتالي، يعمل إعادة تمهيد مركز VPN على مسح ذاكرة التخزين المؤقت ل CRL. يقوم مركز الشبكة الخاصة الظاهرية (VPN) بإعادة ملء ذاكرة التخزين المؤقت ل CRL باستخدام قوائم التحكم في الوصول (CRL) المحدثة أثناء معالجة طلبات مصادقة النظير الجديدة.إذا حددت **إستخدام نقاط توزيع CRL الثابتة**، فيمكنك إستخدام حتى خمس نقاط توزيع CRL ثابتة، كما هو محدد في هذا الإطار. إذا أخترت هذا الخيار، يجب أن تقوم بإدخال عنوان URL واحد على الأقل.يمكنك أيضا تحديد **إستخدام نقاط توزيع CRL من الترخيص الذي يتم فحصه**، أو تحديد **إستخدام نقاط توزيع CRL الثابتة**. إذا لم يتمكن مركز الشبكة الخاصة الظاهرية (VPN) من العثور على خمس نقاط توزيع CRL في الشهادة، فإنه يضيف نقاط توزيع CRL ثابتة، حتى حد الخمس نقاط. إذا أخترت هذا الخيار، قم بتمكين بروتوكول واحد على الأقل لنقطة توزيع CRL. يجب أيضا إدخال نقطة توزيع CRL ثابتة واحدة على الأقل (ولا أكثر من خمسة).حدد **عدم التحقق من CRL** إذا كنت تريد تعطيل التحقق من CRL.تحت التخزين المؤقت ل CRL، حدد المربع **ممكن** للسماح لتركيز VPN بذاكرة التخزين المؤقت لقوائم التحكم في الوصول (CRL) المسترجعة. الإعداد الافتراضي ليس لتمكين التخزين المؤقت ل CRL. عند تعطيل التخزين المؤقت ل CRL (إلغاء تحديد المربع)، يتم مسح ذاكرة التخزين المؤقت ل CRL.إذا قمت بتكوين سياسة إسترداد CRL تستخدم نقاط توزيع CRL من الشهادة التي يتم فحصها، أختر بروتوكول نقطة توزيع لاستخدامه في إسترداد CRL. أخترت **HTTP** في هذه الحالة أن يسترد ال CRL. قم بتعيين قواعد HTTP إلى عامل تصفية الواجهة العامة إذا كان خادم CA الخاص بك موجها إلى الواجهة العامة.



مراقبة

حدد **إدارة>إدارة الشهادات** وانقر فوق **عرض جميع ذاكرات التخزين المؤقت ل CRL** لمعرفة ما إذا كان مركز VPN لديك قد قام بتخزين أي من قوائم التحكم في الوصول الخاصة بالمنفذ (CRL) مؤقتا من خادم CA.

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

أخشاب من مركز

قم بتمكين هذه الأحداث على مركز VPN للتأكد من عمل فحص CRL.

1. حدد **تكوين>نظام>أحداث>فئات** لتعيين مستويات التسجيل.
2. تحت اسم الفئة حدد إما IKE أو **IKEDBG** أو **IPSec** أو **IPSECDBG** أو CERT.
3. انقر فوق إما **إضافة** أو **تعديل**، واختر **الخطورة إلى خيار السجل 1-13**.
4. انقر فوق **تطبيق** إذا كنت تريد التعديل، أو **إضافة** إذا كنت تريد إضافة إدخال جديد.

سجلات التركيز الناجحة

إذا نجح فحص CRL، فسيتم ملاحظة هذه الرسائل في سجلات الأحداث القابلة للتصفية.

```
SEV=7 CERT/117 RPT=1 13:11:23.520 08/15/2002 1315
.The requested CRL was found in cache
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl
```

```
SEV=8 CERT/46 RPT=1 13:11:23.520 08/15/2002 1317
(CERT_CheckCrl(62f56e8, 0, 0

SEV=7 CERT/2 RPT=1 13:11:23.520 08/15/2002 1318
Certificate has not been revoked: session = 2

SEV=8 CERT/50 RPT=1 13:11:23.530 08/15/2002 1319
(CERT_Callback(62f56e8, 0, 0

SEV=5 IKE/79 RPT=2 64.102.60.53 13:11:23.530 08/15/2002 1320
[Group [ipsecgroup
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

راجع سجلات المكثف الناجحة للمخرجات الكاملة لسجل مركز ناجح.

السجلات الفاشلة

إذا لم ينجح إيداع CRL، فسيتم ملاحظة هذه الرسائل في سجلات الأحداث القابلة للتصفية.

```
SEV=7 CERT/6 RPT=2 18:00:36.730 08/15/2002 1332
Failed to retrieve revocation list: session = 5

SEV=7 CERT/114 RPT=2 18:00:36.730 08/15/2002 1333
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
.have been configured

SEV=7 CERT/8 RPT=2 18:00:36.730 08/15/2002 1335
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
.from the server
```

ارجع إلى سجلات المكثف الملغاة للحصول على الإخراج الكامل لسجل مركز معطل.

ارجع إلى سجلات العميل الناجحة للحصول على الإخراج الكامل لسجل عميل ناجح.

ارجع إلى سجلات العملاء الملغاة للحصول على الإخراج الكامل لسجل عميل فاشل.

استكشاف الأخطاء وإصلاحها

راجع أستكشاف أخطاء الاتصال وإصلاحها على مركز VPN 3000 للحصول على مزيد من المعلومات حول أستكشاف الأخطاء وإصلاحها.

معلومات ذات صلة

- صفحة دعم مركزات Cisco VPN 3000 Series
- صفحة دعم عميل Cisco VPN 3000
- مفاوضة IPSec/بروتوكولات IKE
- 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).