CRL-Prüfung über HTTP mit einem Cisco VPN 3000-Konzentrator

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die CRL-Überprüfung (Certificate Revocation List) für Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) aktivieren, die im Cisco VPN 3000 Concentrator im HTTP-Modus installiert sind.

Ein Zertifikat ist normalerweise für seine gesamte Gültigkeitsdauer gültig. Wird ein Zertifikat jedoch ungültig, z. B. aufgrund einer Namensänderung, einer Änderung der Zuordnung zwischen dem Betreff und der CA und einer Sicherheitskompromisse, wird das Zertifikat von der Zertifizierungsstelle widerrufen. Unter X.509 widerrufen CAs Zertifikate durch regelmäßige Ausstellung eines signierten CRLs, wobei jedes widerrufene Zertifikat durch seine Seriennummer identifiziert wird. Aktivieren der CRL-Überprüfung bedeutet, dass der VPN Concentrator jedes Mal, wenn er das Zertifikat für die Authentifizierung verwendet, auch das CRL überprüft, um sicherzustellen, dass das überprüfte Zertifikat nicht widerrufen wurde.

CAs verwenden LDAP-/HTTP-Datenbanken (Lightweight Directory Access Protocol), um CRLs zu speichern und zu verteilen. Sie können auch andere Mittel verwenden, aber der VPN-Konzentrator benötigt LDAP/HTTP-Zugriff.

Die HTTP CRL-Überprüfung wird in VPN Concentrator Version 3.6 oder höher eingeführt. Die LDAP-basierte CRL-Überprüfung wurde jedoch in früheren 3.x-Versionen eingeführt. In diesem Dokument wird nur die CRL-Überprüfung mit HTTP behandelt.

Hinweis: Die CRL-Cache-Größe der VPN-Concentrators der Serie 3000 hängt von der Plattform ab und kann nicht entsprechend dem Wunsch des Administrators konfiguriert werden.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Sie haben den IPsec-Tunnel von den VPN 3.x-Hardware-Clients mithilfe von Zertifikaten für die IKE-Authentifizierung (Internet Key Exchange) erfolgreich erstellt (ohne aktivierte CRL-Überprüfung).
- Der VPN Concentrator hat jederzeit eine Verbindung zum CA-Server.
- Wenn Ihr CA-Server mit der öffentlichen Schnittstelle verbunden ist, haben Sie die erforderlichen Regeln im öffentlichen (Standard-)Filter geöffnet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VPN 3000 Concentrator Version 4.0.1 C
- VPN 3.x-Hardware-Client
- Microsoft CA-Server für die Zertifikatgenerierung und CRL-Überprüfung, die auf einem Windows 2000-Server ausgeführt wird.

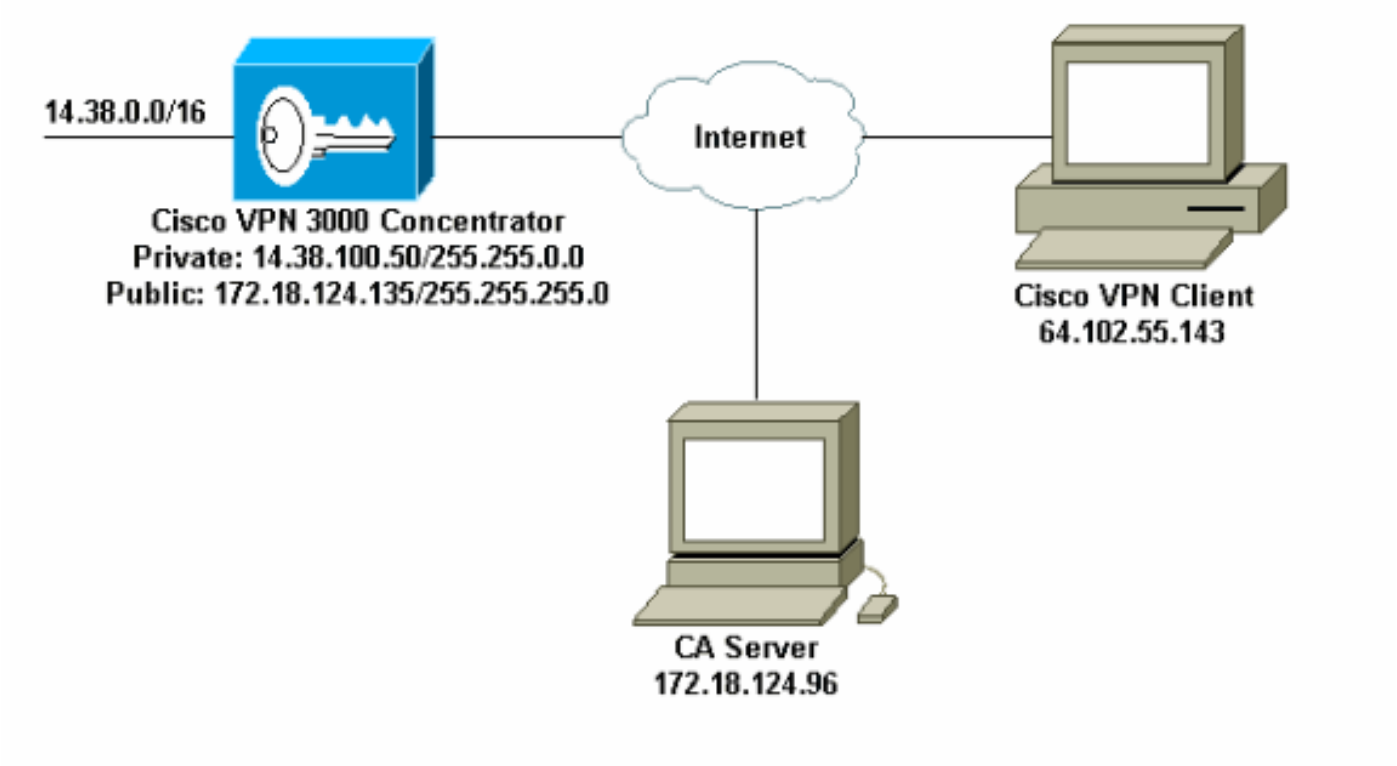
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

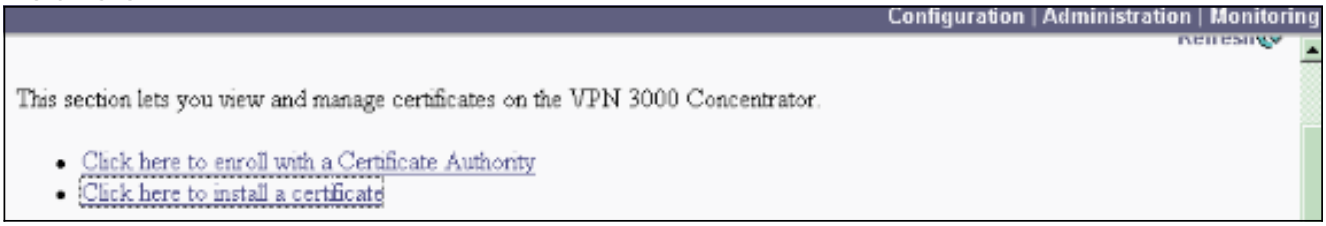


Konfigurieren des VPN 3000-Konzentrators

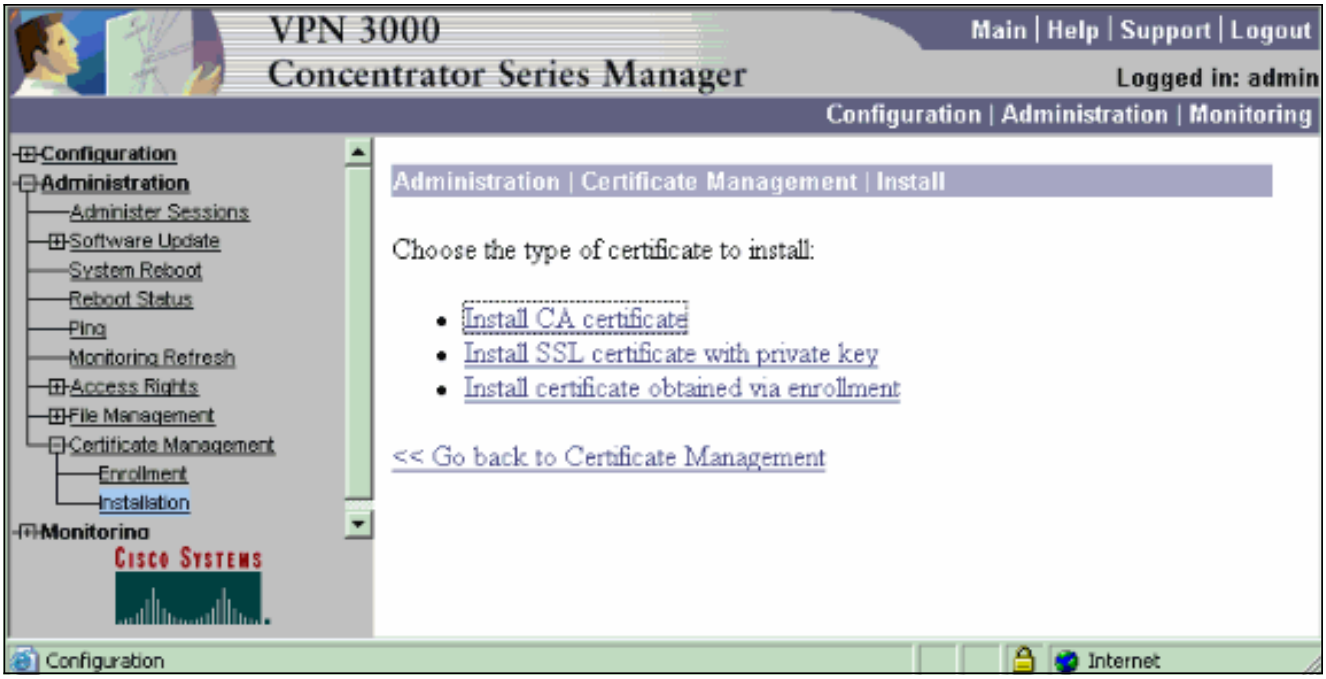
Schrittweise Anleitung

Gehen Sie wie folgt vor, um den VPN 300-Konzentrator zu konfigurieren:

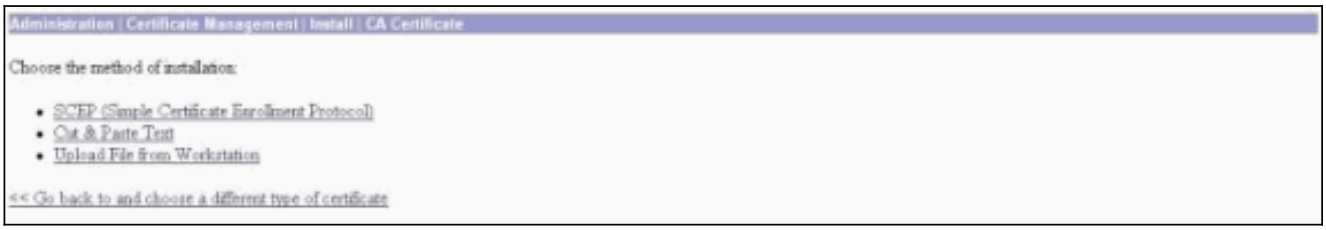
1. Wählen Sie **Administration > Certificate Management** aus, um ein Zertifikat anzufordern, wenn Sie kein Zertifikat besitzen.Wählen Sie **Klicken Sie hier, um ein Zertifikat** zur Installation des Stammzertifikats im VPN Concentrator **zu installieren**.



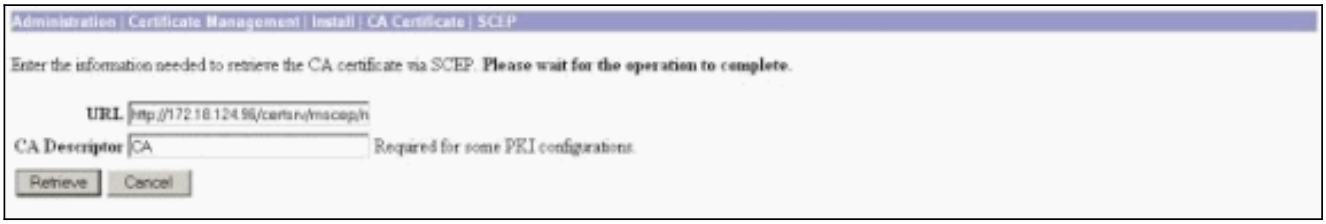
2. Wählen Sie **Zertifizierungsstellenzertifikat installieren aus**.



3. Wählen Sie **SCEP (Simple Certificate Enrollment Protocol)**, um die CA-Zertifikate abzurufen.

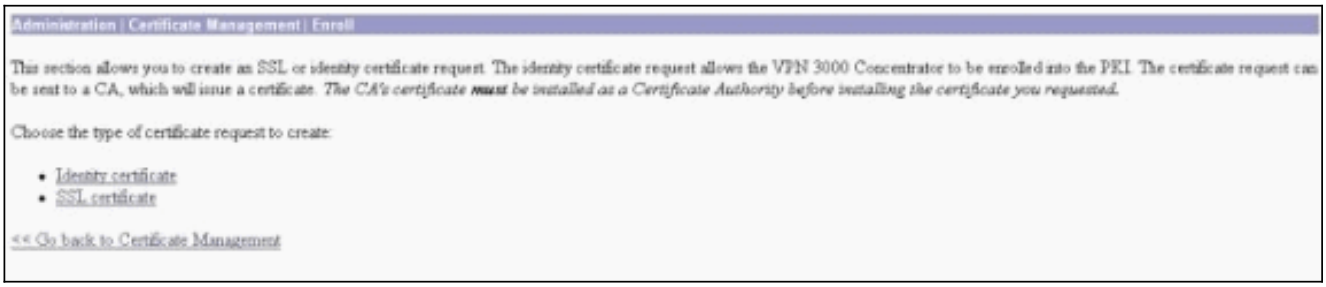


4. Geben Sie im SCEP-Fenster die vollständige URL des CA-Servers im Dialogfeld "URL" ein.In diesem Beispiel ist die IP-Adresse des CA-Servers 172.18.124.96. Da in diesem Beispiel der CA-Server von Microsoft verwendet wird, lautet die vollständige URL http://172.18.124.96/certsrv/mscep/mscep.dll. Geben Sie als Nächstes einen Deskriptor mit einem Wort in das Dialogfeld CA Descriptor ein. In diesem Beispiel wird CA verwendet.

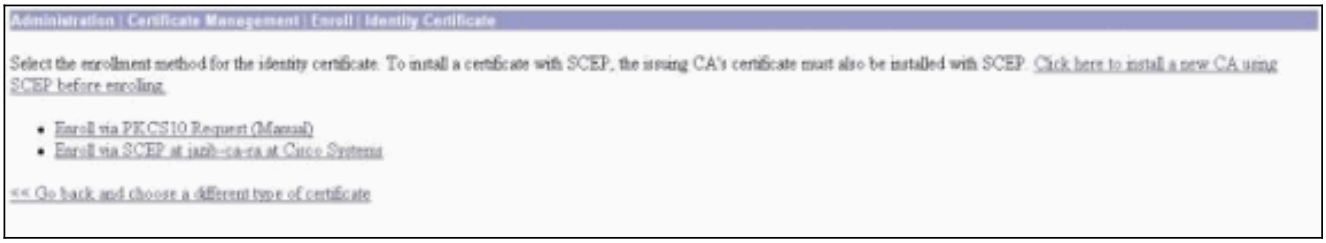


5. Klicken Sie auf **Abrufen**.Das Zertifizierungsstellenzertifikat sollte im Fenster Administration > Certificate Management (Verwaltung > Zertifikatsverwaltung) angezeigt werden. Wenn kein Zertifikat angezeigt wird, kehren Sie zu Schritt 1 zurück, und befolgen Sie das Verfahren erneut.

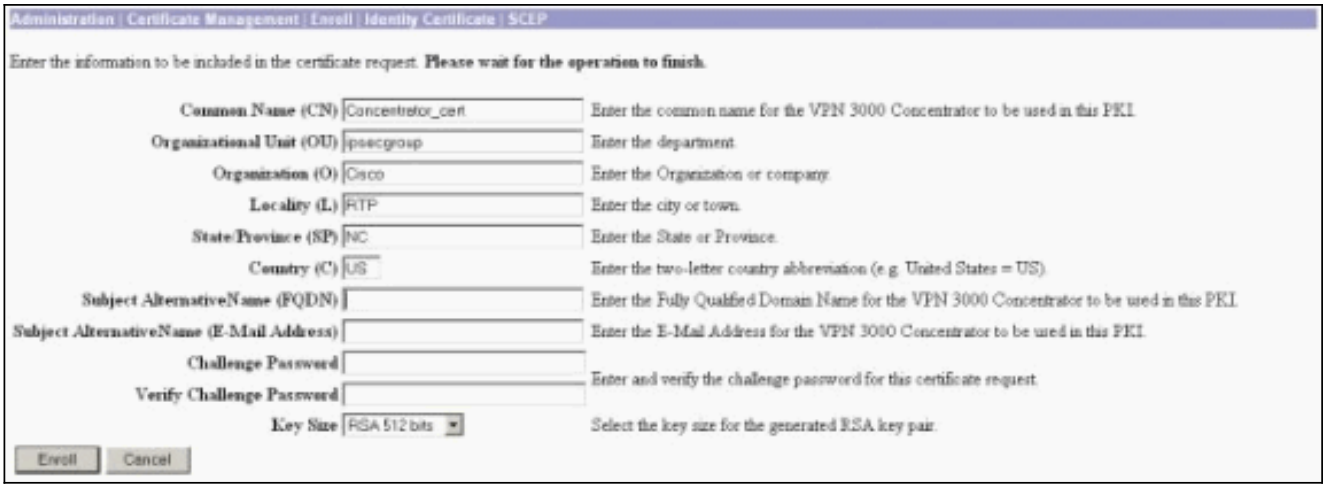
6. Wenn Sie das Zertifizierungsstellenzertifikat haben, wählen Sie **Administration > Certificate Management > Registrieren aus**, und klicken Sie dann auf **Identitätszertifikat**.



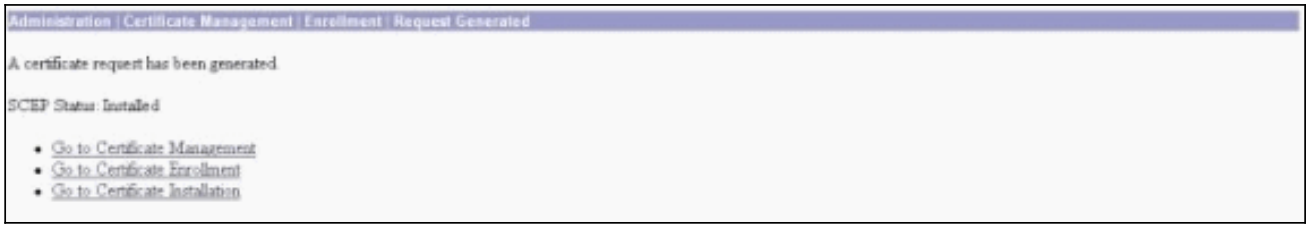
7. Klicken Sie auf **Über SCEP anmelden unter ...** um das Identitätszertifikat anzufordern.



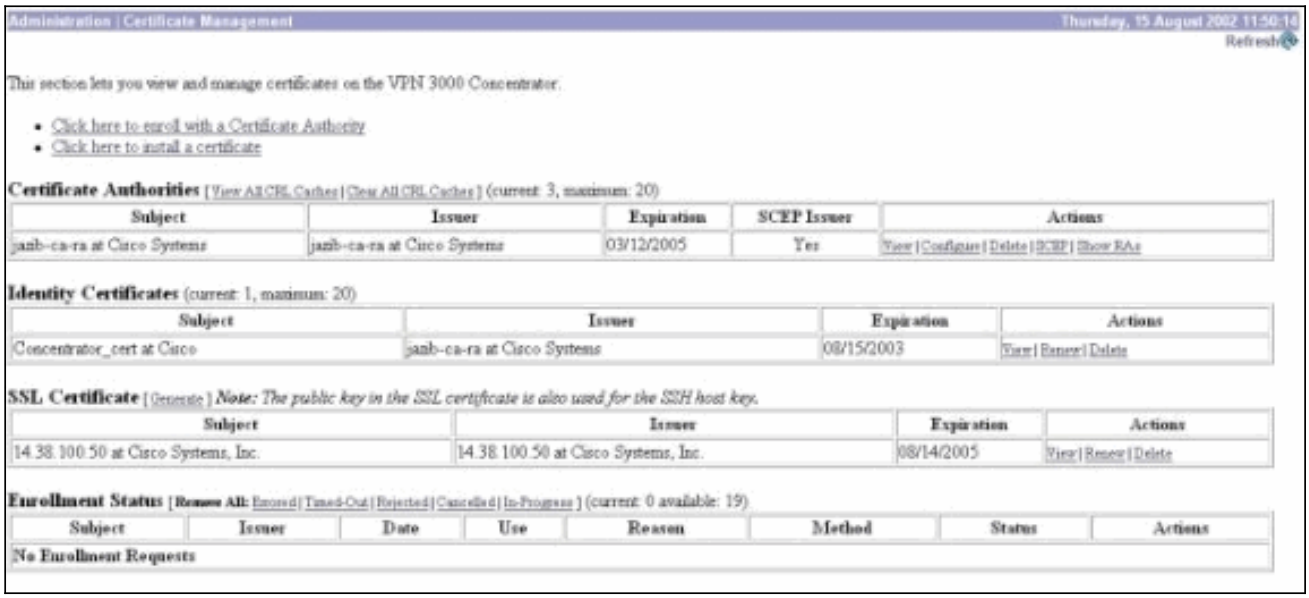
8. Gehen Sie wie folgt vor, um das Anmeldeformular auszufüllen:Geben Sie im Feld Common Name (CN) den allgemeinen Namen für den VPN Concentrator ein, der in der Public-Key-Infrastruktur (PKI) verwendet wird.Geben Sie Ihre Abteilung im Feld Organisationseinheit (OU) ein. Die OU muss mit dem konfigurierten IPsec-Gruppennamen übereinstimmen.Geben Sie Ihre Organisation oder Ihr Unternehmen in das Feld Organisation (O) ein.Geben Sie Ihre Stadt in das Feld "Locality" (L) ein.Geben Sie im Feld Bundesland Ihr Bundesland ein.Geben Sie Ihr Land in das Feld Land (C) ein.Geben Sie im Feld Fully Qualified Domain Name (FQDN) den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) für den im PKI zu verwendenden VPN Concentrator ein.Geben Sie im Feld Subject Alternative Name (E-Mail-Adresse) die E-Mail-Adresse für den im PKI zu verwendenden VPN Concentrator ein.Geben Sie im Feld Challenge Password (Kennwort) das Challenge-Kennwort für die Zertifikatsanforderung ein.Geben Sie das Challenge-Kennwort erneut im Feld Kennwort bestätigen ein.Wählen Sie in der Dropdown-Liste Key Size (Schlüsselgröße) die Schlüsselgröße für das generierte RSA-Schlüsselpaar aus.



9. Wählen Sie **Registrieren**, und zeigen Sie den SCEP-Status im Abfragestatus an.
10. Rufen Sie den CA-Server auf, um das Identitätszertifikat zu genehmigen. Sobald er auf dem CA-Server genehmigt wurde, sollte der SCEP-Status installiert werden.



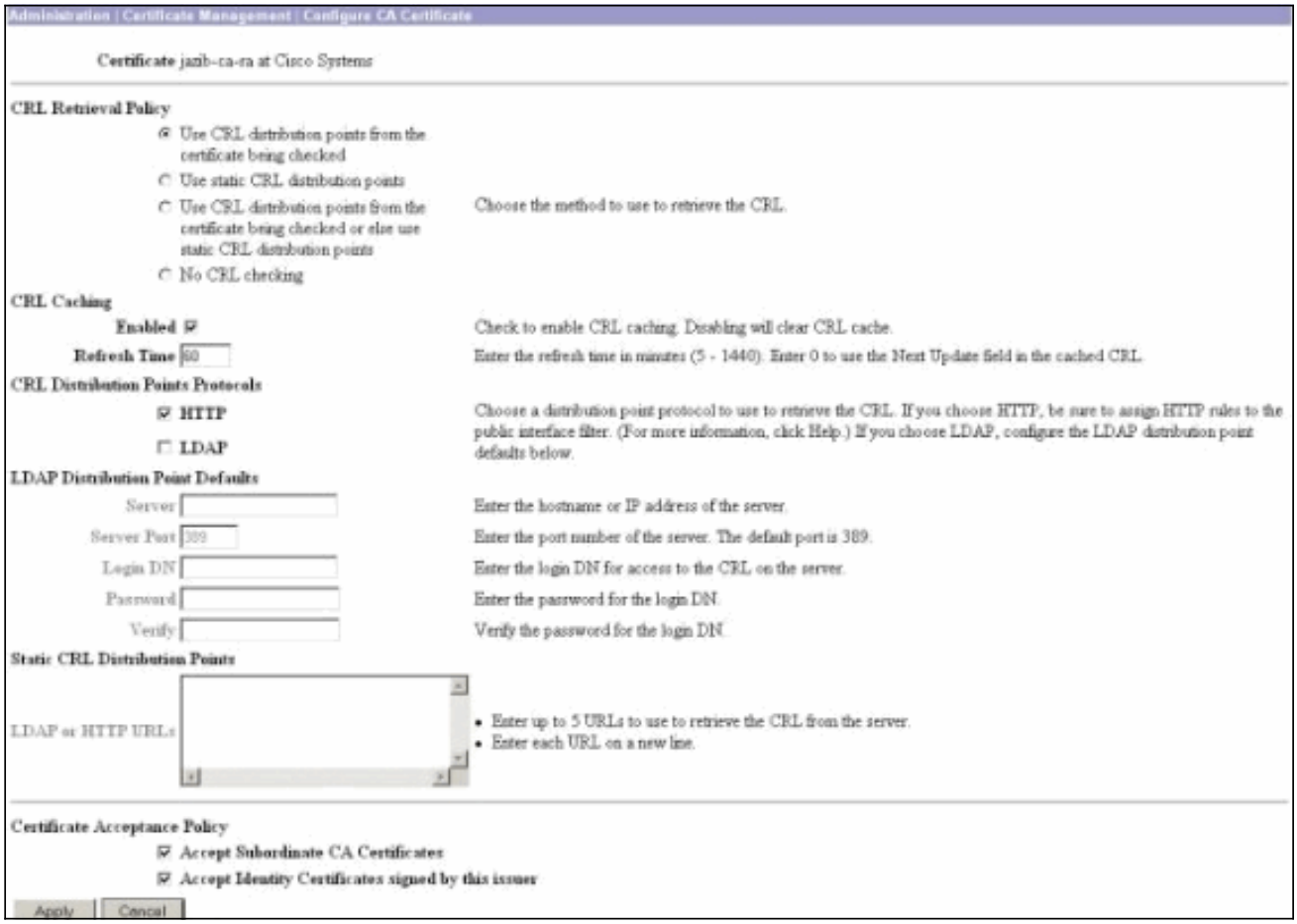
11. Unter Zertifikatsverwaltung sollten Sie Ihr Identitätszertifikat sehen.Falls nicht, überprüfen Sie die Protokolle auf Ihrem CA-Server, um weitere Fehlerbehebungsmaßnahmen zu erhalten.



12. Wählen Sie **Auf** dem erhaltenen Zertifikat **anzeigen**, um festzustellen, ob das Zertifikat über einen CRL Distribution Point (CDP) verfügt.CDP listet alle CRL-Verteilungspunkte des Ausstellers dieses Zertifikats auf. Wenn Sie CDP auf Ihrem Zertifikat haben und einen DNS-Namen verwenden, um eine Abfrage an den CA-Server zu senden, stellen Sie sicher, dass Sie im VPN-Concentrator DNS-Server definiert haben, um den Hostnamen mit einer IP-Adresse aufzulösen. In diesem Fall ist der Hostname des CA-Beispielservers jazib-pc, der auf dem DNS-Server in eine IP-Adresse von 172.18.124.96 aufgelöst wird.

13. Klicken Sie auf **Konfigurieren** für das CA-Zertifikat, um die CRL-Überprüfung der empfangenen Zertifikate zu aktivieren.Wenn Sie CDP auf Ihrem empfangenen Zertifikat haben und dieses verwenden möchten, wählen Sie **Use CRL distribution points aus dem zu überprüfenden Zertifikat aus**.Da das System das CRL von einem Netzwerkverteilungspunkt abrufen und untersuchen muss, kann die Aktivierung der CRL-Überprüfung die Reaktionszeiten des Systems beeinträchtigen. Wenn das Netzwerk langsam oder überlastet ist, kann auch die CRL-Prüfung fehlschlagen. Aktivieren Sie CRL-Caching, um diese potenziellen Probleme zu beheben. Dadurch werden die abgerufenen CRLs im lokalen flüchtigen Speicher gespeichert, und der VPN Concentrator kann den Widerrufsstatus von Zertifikaten schneller überprüfen.Bei aktivierter CRL-Caching überprüft der VPN Concentrator zunächst, ob die erforderliche CRL im Cache vorhanden ist, und überprüft die Seriennummer des Zertifikats anhand der Liste der Seriennummern im CRL, wenn er den Widerrufsstatus eines Zertifikats überprüfen muss. Das Zertifikat gilt als widerrufen, wenn seine Seriennummer gefunden wird. Der VPN Concentrator ruft eine CRL von einem externen Server ab, wenn er die erforderliche CRL im Cache nicht findet, die Gültigkeitsdauer der zwischengespeicherten CRL abgelaufen ist oder wenn die konfigurierte Aktualisierungszeit abgelaufen ist. Wenn der VPN Concentrator ein neues CRL von einem externen Server empfängt, aktualisiert er den Cache mit dem neuen CRL. Der Cache kann bis zu 64 CRLs enthalten.**Hinweis:** Der CRL-Cache ist im Speicher vorhanden. Daher wird der CRL-Cache durch einen Neustart des VPN Concentrator gelöscht. Der VPN Concentrator repliziert den CRL-Cache mit aktualisierten CRLs, wenn er neue Peer-Authentifizierungsanforderungen verarbeitet.Wenn Sie **Statische CRL-Verteilungspunkte verwenden** auswählen, können Sie bis zu fünf statische CRL-Verteilungspunkte verwenden, wie in diesem Fenster angegeben. Wenn Sie diese Option wählen, müssen Sie mindestens eine URL eingeben.Sie können auch **CRL-Verteilungspunkte aus dem zu überprüfenden Zertifikat verwenden** auswählen oder **Statische CRL-Verteilungspunkte verwenden** auswählen. Wenn der VPN Concentrator im Zertifikat nicht fünf CRL-Verteilungspunkte finden kann, fügt er statische CRL-Verteilungspunkte hinzu (maximal fünf). Wenn Sie diese Option wählen, aktivieren Sie mindestens ein CRL Distribution Point Protocol. Sie müssen auch mindestens einen (und höchstens fünf) statischen CRL-Verteilungspunkt eingeben.Wählen Sie **Keine CRL-Überprüfung aus**, wenn Sie die CRL-Überprüfung deaktivieren möchten.Wählen Sie unter CRL Caching das Kontrollkästchen **Enabled (Aktiviert)** aus, damit der VPN-Concentrator abgerufene CRLs zwischenspeichern kann. Standardmäßig wird CRL-Caching nicht aktiviert. Wenn Sie die CRL-Zwischenspeicherung deaktivieren (das Feld deaktivieren), wird der CRL-Cache gelöscht.Wenn Sie eine CRL-Abrufrichtlinie konfiguriert haben, die

CRL-Verteilungspunkte aus dem zu überprüfenden Zertifikat verwendet, wählen Sie ein Verteilungspunkt-Protokoll aus, das zum Abrufen der CRL verwendet werden soll. Wählen Sie **HTTP** in diesem Fall aus, um die CRL abzurufen. Weisen Sie dem öffentlichen Schnittstellenfilter HTTP-Regeln zu, wenn sich der CA-Server in Richtung der öffentlichen Schnittstelle
befindet.



Überwachung

Wählen Sie **Administration > Certificate Management** aus, und klicken Sie auf **View All CRL caches (Alle CRL-Caches anzeigen)**, um festzustellen, ob der VPN Concentrator CRLs vom CA-Server zwischengespeichert hat.

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Protokolle vom Concentrator

Aktivieren Sie diese Ereignisse auf dem VPN Concentrator, um sicherzustellen, dass die CRL-Überprüfung funktioniert.

1. Wählen Sie **Configuration > System > Events > Classes** aus, um die Protokollierungsebenen festzulegen.
2. Wählen Sie unter Klassenname entweder **IKE**, **IKEDBG**, **IPSEC**, **IPSECDBG** oder **CERT**

aus.

3. Klicken Sie entweder auf **Hinzufügen** oder **Ändern**, und wählen Sie **Option Schweregrad zu Protokoll 1-13 aus**.
4. Klicken Sie auf **Übernehmen**, wenn Sie Änderungen vornehmen möchten, oder auf **Hinzufügen**, wenn Sie einen neuen Eintrag hinzufügen möchten.

Erfolgreiche Concentrator-Protokolle

Wenn die CRL-Überprüfung erfolgreich ist, werden diese Meldungen in Filterable Event Logs (Ereignisprotokolle mit Filterbaren) angezeigt.

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

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

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

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

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

Unter Successful Concentrator Logs finden Sie die vollständige Ausgabe eines erfolgreichen Konzentrator-Protokolls.

Fehlgeschlagene Protokolle

Wenn die CRL-Eincheckfunktion nicht erfolgreich war, werden diese Meldungen in den Filterable Event Logs (Ereignisprotokolle) angezeigt.

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

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

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

Unter Revoked Concentrator Logs finden Sie die vollständige Ausgabe eines fehlgeschlagenen Konzentrator-Protokolls.

Unter Erfolgreiche Clientprotokolle finden Sie die vollständige Ausgabe eines erfolgreichen Clientprotokolls.

Die vollständige Ausgabe eines fehlgeschlagenen Clientprotokolls finden Sie unter Revocked Client Logs.

Fehlerbehebung

Weitere Informationen zur Fehlerbehebung finden Sie unter Beheben von Verbindungsproblemen im VPN 3000 Concentrator.

Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrators der Serie 3000
- Cisco VPN 3000 Client Support-Seite
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems