CRL-controle op HTTP op een Cisco VPN-concentratie 3000

Inhoud

Inleiding

Dit document beschrijft hoe u certificeringsinstanties (CRL) kunt inschakelen voor certificaten die in Cisco VPN 3000 Concentrator zijn geïnstalleerd via HTTP-modus.

Gewoonlijk wordt van een certificaat verwacht dat het geldig is gedurende de gehele geldigheidsduur. Als een certificaat echter ongeldig wordt vanwege bijvoorbeeld een naamswijziging, een wijziging in de associatie tussen het onderwerp en de CA en een compromis over de beveiliging, trekt de CA het certificaat in. Onder X.509 intrekken CA's certificaten door periodiek een ondertekend CRL af te geven, waarbij elk ingetrokken certificaat door het serienummer wordt geïdentificeerd. Het toestaan van CRL-controle betekent dat elke keer dat de VPN-Concentrator het certificaat voor authenticatie gebruikt, het ook de CRL controleert om te verzekeren dat het certificaat dat wordt geverifieerd niet is ingetrokken.

CA's gebruiken Lichtgewicht Directory Access Protocol (LDAP)/HTTP-databases om CRL's op te slaan en te distribueren. Ze kunnen ook andere middelen gebruiken, maar de VPN Concentrator is afhankelijk van LDAP/HTTP toegang.

HTTP CRL-controle wordt geïntroduceerd in VPN Concentrator versie 3.6 of hoger. In de eerdere versies van 3.x werd echter wel een op LDAP gebaseerde CRL-controle geïntroduceerd. In dit document worden alleen CRL-controles besproken met behulp van HTTP.

Opmerking: De CRL cache-grootte van VPN 3000 Series Concentrators is afhankelijk van het platform en kan niet volgens de wens van de beheerder worden ingesteld.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- U hebt met succes de IPsec-tunnel van de VPN 3.x hardwareclients ingesteld met certificaten voor IKE-verificatie (Internet Key Exchange (IKE) (zonder CRL-controle ingeschakeld).
- Uw VPN Concentrator heeft altijd connectiviteit op de CA server.
- Als uw CA-server is aangesloten op de openbare interface, hebt u de benodigde regels geopend in het openbare (standaard) filter.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- VPN 3000 Concentrator versie 4.0.1 C
- VPN 3.x hardwareclient
- Microsoft CA-server voor het genereren van certificaten en CRL-controle op een Windows 2000-server.

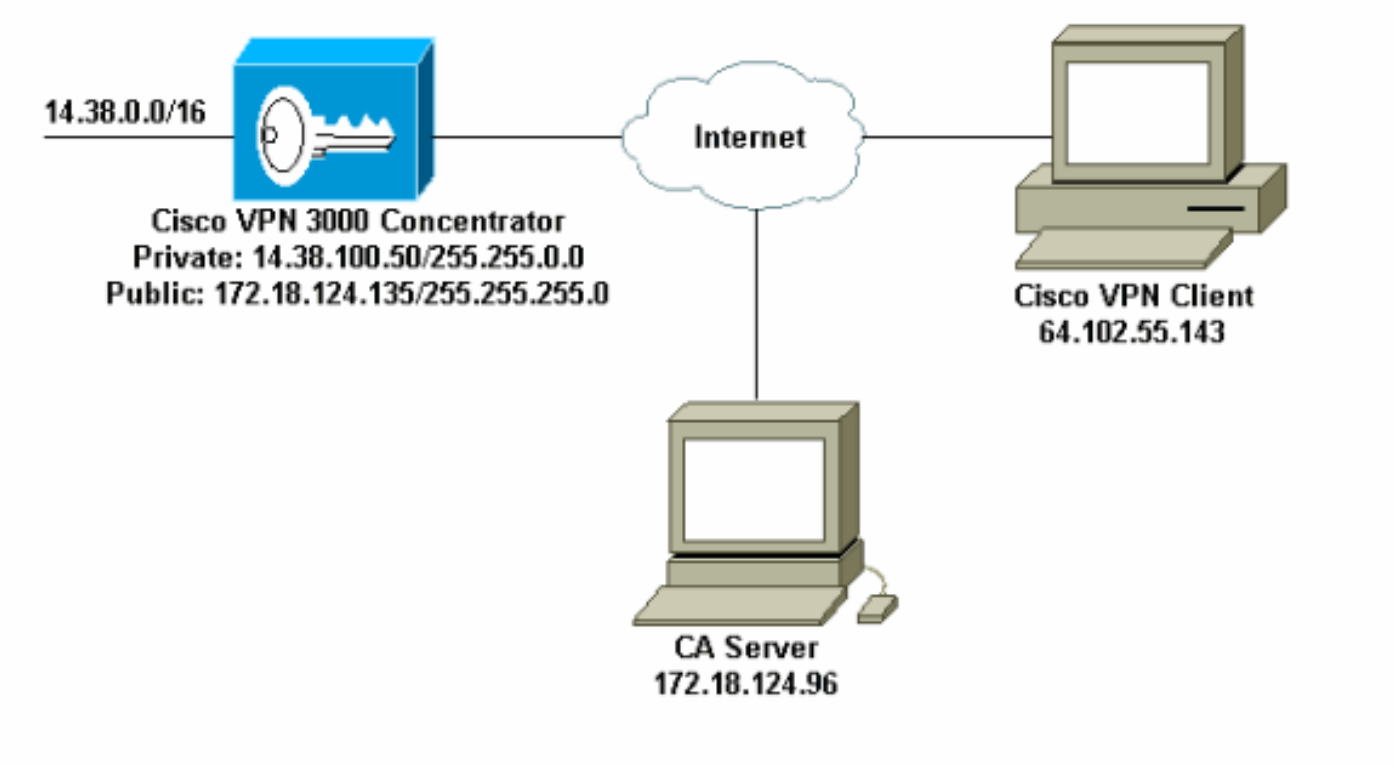
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

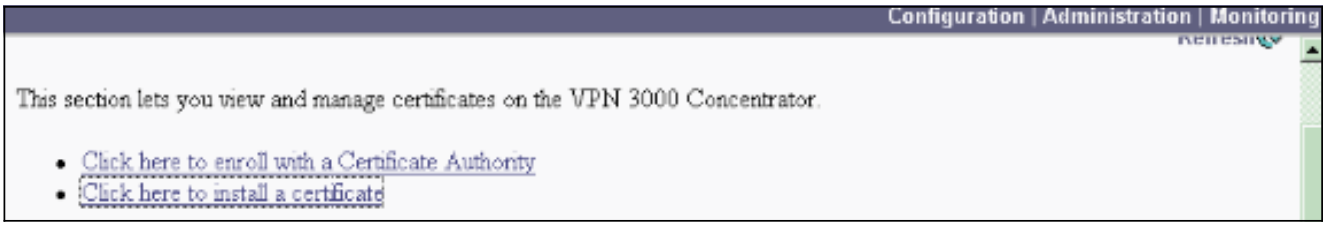


De VPN 3000-concentratie configureren

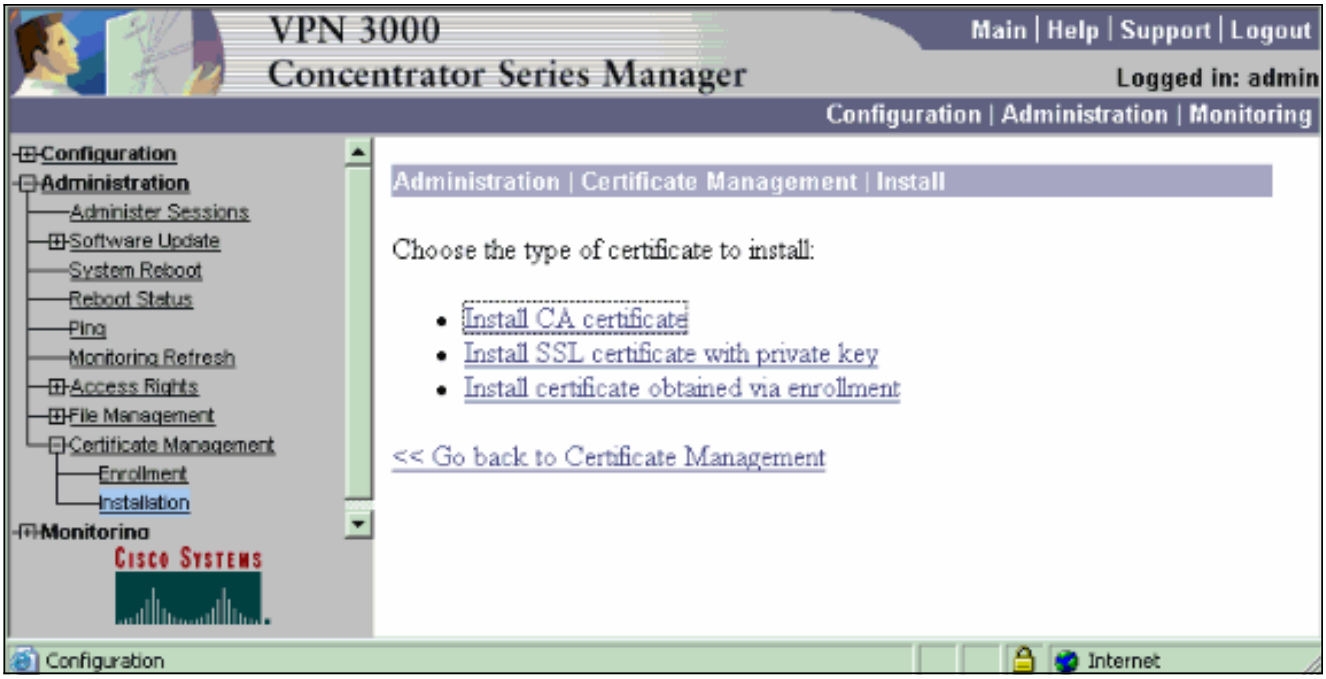
Stapsgewijze instructies

Volg deze stappen om de VPN 3000 Concentrator te configureren:

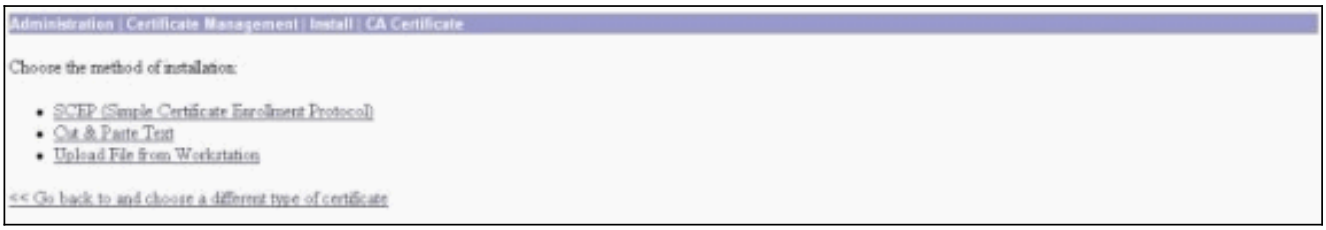
1. Selecteer **Beheer > certificaatbeheer** om een certificaat aan te vragen als u geen certificaat hebt.Selecteer **Klik hier om een certificaat te installeren** om het basiscertificaat op de VPN-centrator te installeren.



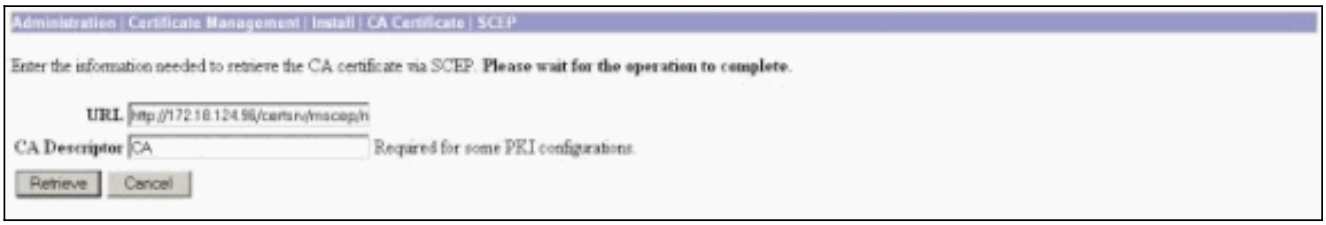
2. Selecteer **Installeer het CA-certificaat**.



3. Selecteer **SCEP (Eenvoudig protocol voor certificaatinschrijving)** om de CA-certificaten op te halen.

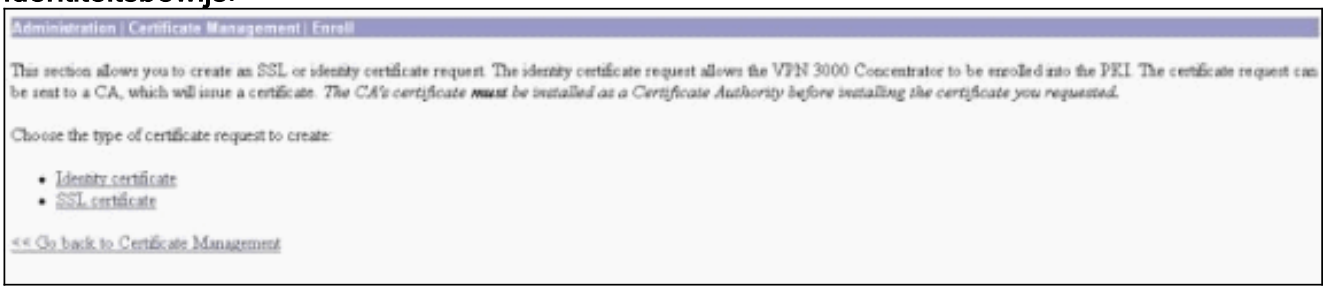


4. Voer vanuit het SCEP-venster de volledige URL van de CA-server in het dialoogvenster URL.In dit voorbeeld is het IP-adres van de CA-server 172.18.124.96. Aangezien dit voorbeeld de CA-server van Microsoft gebruikt, is de volledige URL http://172.18.124.96/certsrv/mscep/mscep.dll. Typ vervolgens een woord beschrijver in het dialoogvenster CA-beschrijving. Dit voorbeeld gebruikt
CA.

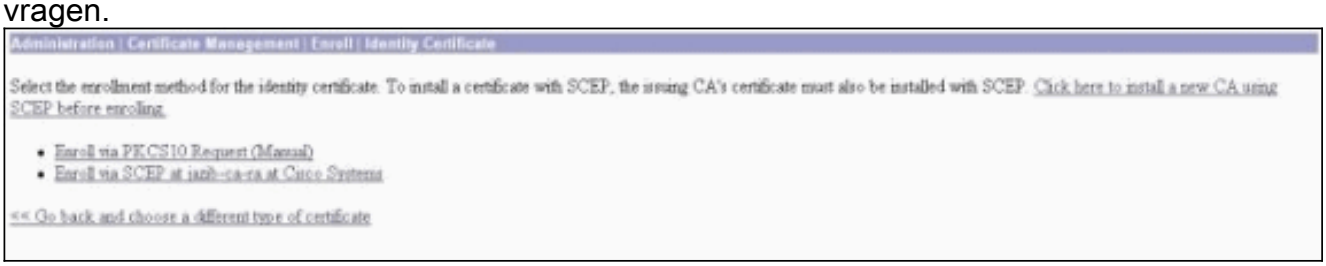


5. Klik op **Ophalen**.Uw CA-certificaat dient te worden weergegeven onder het venster Administration > certificaatbeheer. Als u geen certificaat ziet, gaat u terug naar Stap 1 en volgt u de procedure
opnieuw.

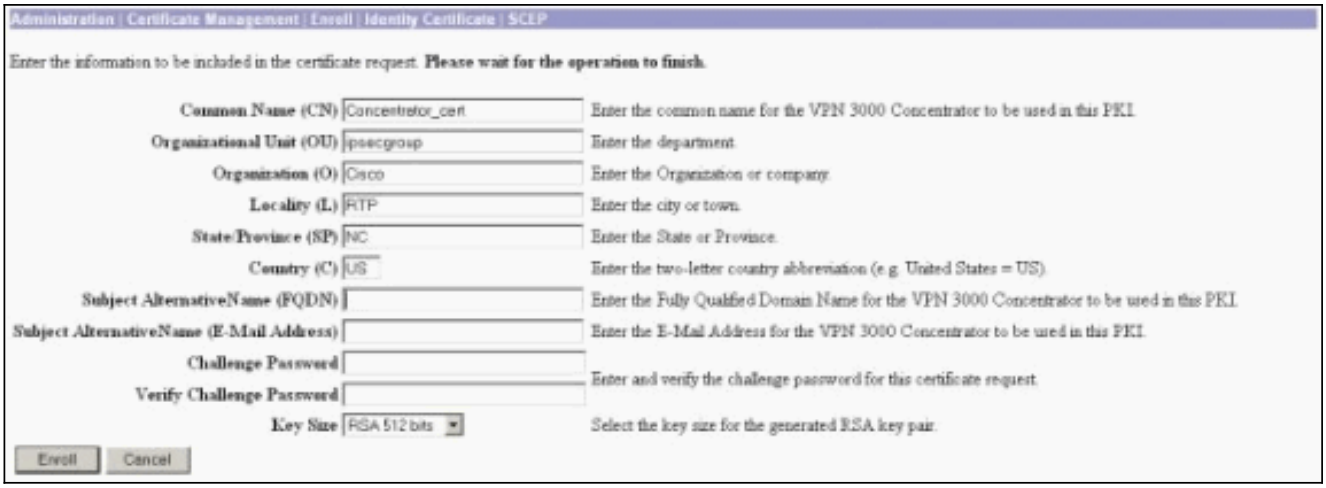
6. Nadat u het CA-certificaat hebt, selecteert u **Administratie > certificaatbeheer > Inschrijven** en vervolgens klikt u op **identiteitsbewijs**.



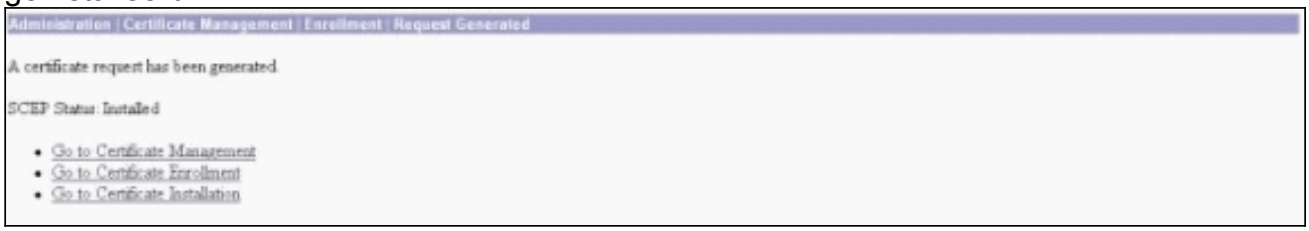
7. Klik op **Inschrijven via SCEP op ...** om het identiteitsbewijs aan te vragen.



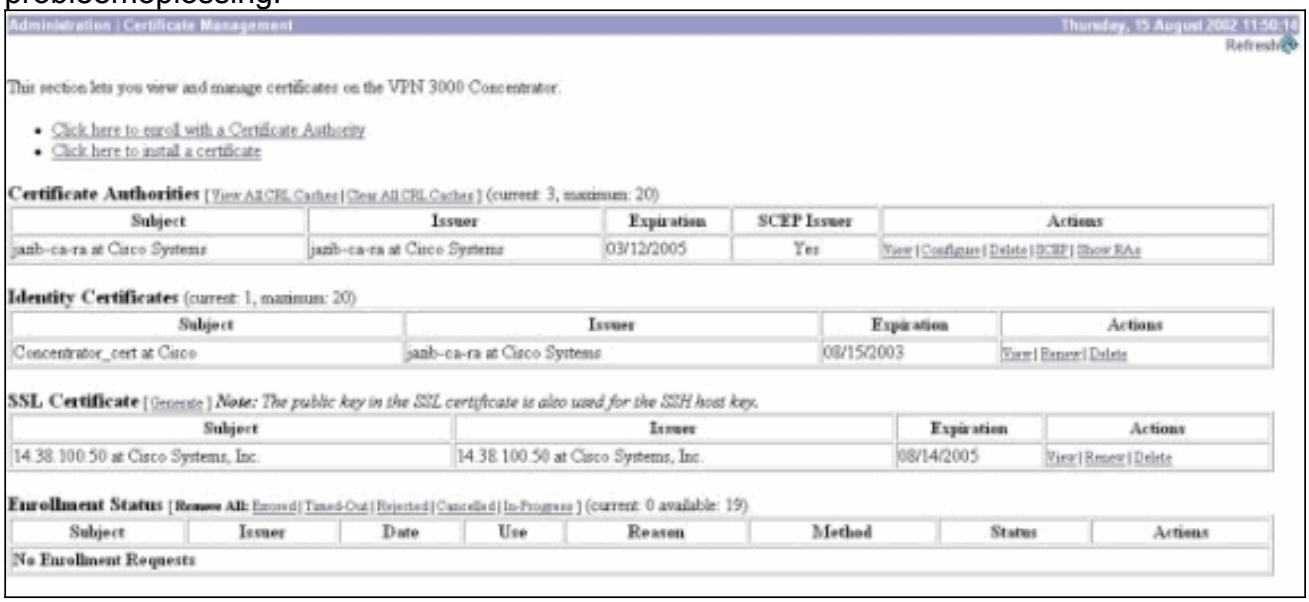
8. Voltooi deze stappen om het inschrijvingsformulier in te vullen:Voer de gezamenlijke naam in voor de VPN-centrator die in het veld Naam (GN) moet worden gebruikt in de PKI-infrastructuur (public-key infrastructure).Voer uw afdeling in het veld Organisatorische eenheid in. De U dient de ingesteld IPsec groepsnaam te selecteren.Voer uw organisatie of bedrijf in het veld Organisatie (O) in.Voer de stad in in het veld Locality (L).Voer de staat of provincie in het veld Land/Provincie (SP).Voer in het veld Land (C) uw land in.Voer de Full Qualified Domain Name (FQDN) in voor de VPN-concentrator die in PKI in het veld Full Qualified Domain Name (FQDN) wordt gebruikt.Voer het e-mailadres in voor de VPN-centrator die in PKI moet worden gebruikt in het veld Alternatieve naam (e-mailadres) voor onderwerp.Voer het uitdagingswachtwoord in voor de certificaataanvraag in het veld Wachtwoord voor uitdaging.Voer het uitdagingswachtwoord opnieuw in in het veld Wachtwoord voor uitdaging controleren.Selecteer de sleutelgrootte voor het gegenereerde RSA-sleutelpaar in de vervolgkeuzelijst
Toetformaat.



9. Selecteer **Inschrijven** en bekijk de SCEP status in de stemtoestand.
10. Ga naar uw CA server om het identiteitsbewijs goed te keuren. Zodra het op de CA server is goedgekeurd, moet uw SCEP status worden geïnstalleerd.



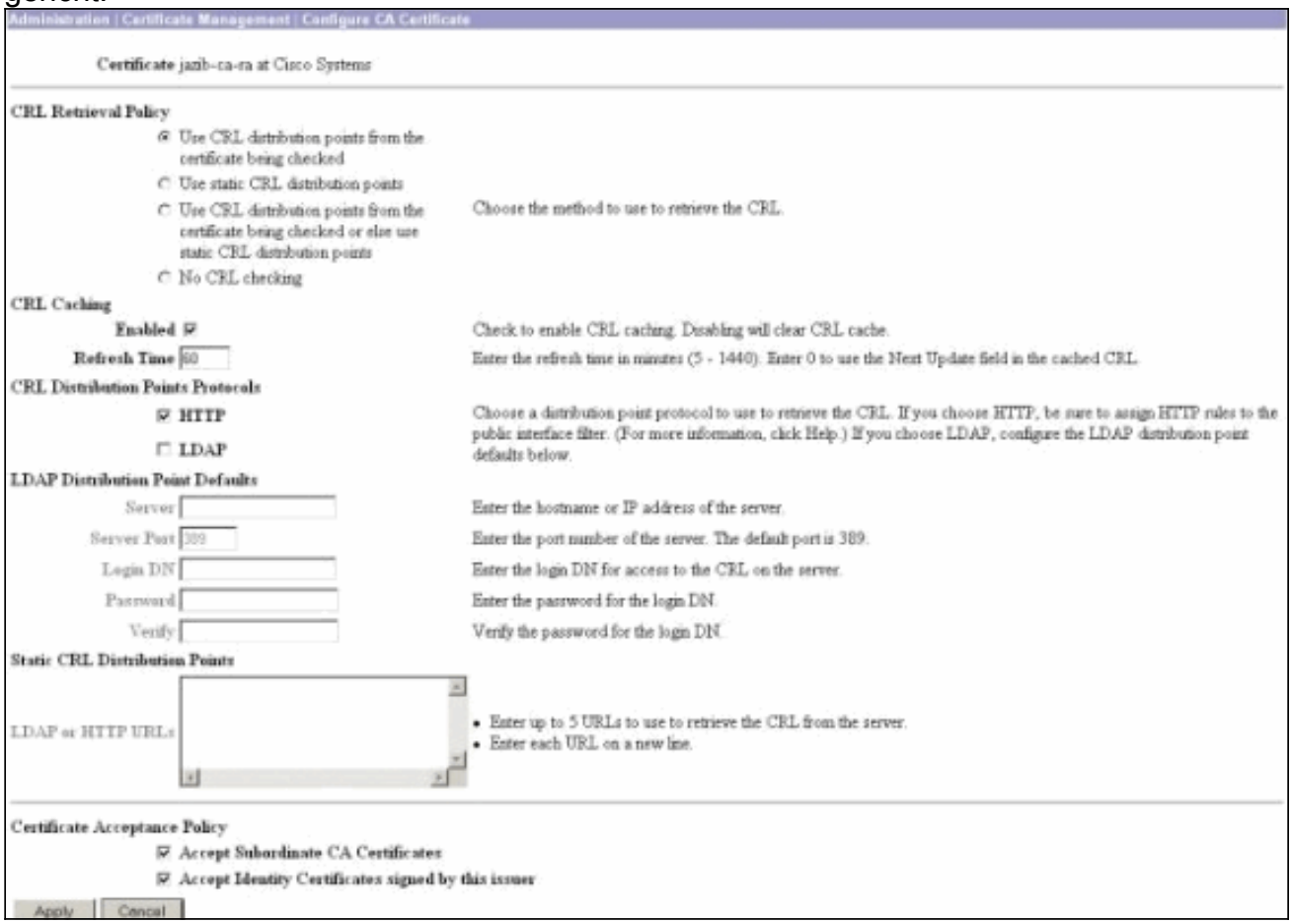
11. Raadpleeg onder certificaatbeheer uw identiteitsbewijs.Als u dit niet doet, controleert u de logbestanden op uw CA-server voor meer informatie over de probleemoplossing.



12. Selecteer **Beeld** op uw ontvangen certificaat om te zien of uw certificaat een CRL Distribution Point (CDP) heeft.CDP noemt alle CRL distributiepunten van de uitgever van dit certificaat. Als u CDP op uw certificaat hebt, en u gebruikt een DNS naam om een vraag naar de CA server te verzenden, zorg er dan voor dat u DNS servers hebt die in uw VPN Concentrator zijn gedefinieerd om de hostnaam met een IP-adres op te lossen. In dit geval is de host-naam van de CA-server jazib-pc, die oplost tot een IP-adres van 172.18.124.96 op de DNS-server.

13. Klik op **Configureren** op uw CA-certificaat om CRL-controle in te schakelen op de ontvangen certificaten.Als u CDP op het ontvangen certificaat hebt en u dit wilt gebruiken, selecteert u **CRL-distributiepunten gebruiken vanuit het certificaat dat wordt gecontroleerd**.Aangezien het systeem de CRL van een netwerkdistributiepunt moet terugvinden en onderzoeken, kan het inschakelen van CRL-controle de responsietijden van het systeem vertragen. Ook, als het netwerk langzaam of verstopt is, zou de controle van CRL kunnen mislukken. Laat CRL caching om deze potentiële problemen te verzachten. Dit slaat de opgehaalde CRL's op in een lokaal vluchtig geheugen en laat de VPN-Concentrator daarom de herroepingsstatus van certificaten sneller controleren.Als CRL-caching ingeschakeld is, controleert de VPN-Concentrator eerst of het vereiste CRL in het cachegeheugen aanwezig is en controleert u het serienummer van het certificaat aan de hand van de lijst met serienummers in het CRL wanneer het de herroepingsstatus van een certificaat moet controleren. Het certificaat wordt als ingetrokken beschouwd indien het serienummer van het certificaat is gevonden. De VPN Concentrator haalt een CRL van een externe server op wanneer het niet de vereiste CRL in het cache vindt, wanneer de geldigheidsperiode van het gecached CRL is verlopen of wanneer de geconfigureerde verfristijd is verstreken. Wanneer de VPN Concentrator een nieuw CRL van een externe server ontvangt, werkt het cache bij met de nieuwe CRL. De cache kan maximaal 64 CRL's bevatten.**Opmerking:** de CRL cache bestaat in het geheugen. Daarom moet u de VPN Concentrator opnieuw opstarten om het CRL cache te reinigen. De VPN Concentrator verwerkt het CRL cache met bijgewerkte CRL’s terwijl het nieuwe peer-verificatieverzoeken verwerkt.Als u **statische CRL-**distributiepunten selecteert, kunt u maximaal vijf statische CRL-distributiepunten gebruiken, zoals in dit venster gespecificeerd is. Als u deze optie kiest, moet u minimaal één URL invoeren.U kunt ook **CRL-distributiepunten gebruiken vanuit het certificaat dat wordt gecontroleerd**, of **statische CRL-distributiepunten gebruiken**. Als de VPN Concentrator geen vijf CRL-distributiepunten in het certificaat kan vinden, voegt het statische CRL-distributiepunten toe, tot een grens van vijf. Als u deze optie kiest, schakelt u ten minste één CRL-distributieprotocol in. U moet ook minimaal één (en maximaal vijf) statische CRL distributiepunten invoeren.Selecteer **Geen CRL-controle** als u CRL-controle wilt uitschakelen.Selecteer onder CRL Caching het **Ingeschakelde** vakje om de VPN Concentrator toe te staan teruggewonnen CRLs in het geheugen te stoppen. De standaardinstelling is dat CRL-caching niet wordt ingeschakeld. Wanneer u CRL caching uitschakelt (de doos niet selecteren), wordt het CRL cache gewist.Als u een CRL-herkenningsbeleid hebt ingesteld dat gebruikmaakt van CRL-distributiepunten uit het certificaat dat wordt gecontroleerd, kiest u een protocol van het distributiepunt om het CRL-systeem op te halen. Kies **HTTP** in dit geval om de CRL terug te halen. Pas HTTP-regels

aan het openbare interfacefilter toe als uw CA-server naar de openbare interface is gericht.



Controleren

Selecteer **Beheer > certificaatbeheer** en klik op **Alle CRL-caches** bekijken **om** te zien of uw VPN-Concentrator CRLs heeft gecached van de CA-server.

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Logs van Concentrator

Schakel deze gebeurtenissen in op de VPN-concentratie om er zeker van te zijn dat de CRL-controle werkt.

1. Selecteer **Configuration > System > Events > Classes** om de logniveaus in te stellen.
2. Selecteer onder Class Name **IKE**, **IKEDBG**, **IPSEC**, **IPSECDBG** of **CERT.**
3. Klik op **Add** of **Change**, en kies **Severity to Log optie 1-13**.
4. Klik op **Toepassen** als u wilt wijzigen of **Toevoegen** als u een nieuwe ingang wilt toevoegen.

Succesvolle Concentrator-vastlegging

Als uw CRL-controle succesvol is, worden deze berichten in de Logs van de gebeurtenis van

Filterable gezien.

```
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)
```

Raadpleeg Succesvolle Concentrator Logs voor de volledige uitvoer van een succesvol concentratorlogboek.

Logs mislukt

Als uw CRL-controle niet succesvol is, worden deze berichten in de Logs van de gebeurtenis van Filterable gezien.

```
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.
```

Raadpleeg Ingetrokken Concentrator Logs voor de volledige uitvoer van een mislukte concentratorlog.

Raadpleeg Succesvolle clientvastlegging voor de volledige uitvoer van een succesvol clientlogboek.

Raadpleeg de ingetrokken clientlogboek voor de volledige uitvoer van een mislukt clientlogboek.

Problemen oplossen

Raadpleeg verbindingsproblemen met probleemoplossing in de VPN 3000-centrator voor meer informatie over probleemoplossing.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrators
- Cisco VPN 3000 clientondersteuningspagina
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems