ASA configureren als een lokale CA-server en AnyConnect Head-end

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
<u>Achtergrondinformatie</u>
Configureren
Netwerkdiagram
ASA als lokale CA-server
Stap 1. De lokale CA-server op ASA configureren en inschakelen
Stap 2. Gebruikers maken en toevoegen aan de ASA-database
Stap 3. WebVPN inschakelen op de WAN-interface
Stap 4. Het certificaat op de clientmachine importeren
ASA als SSL-gateway voor AnyConnect-clients
ASDM AnyConnect-configuratiewizard
CLI voor AnyConnect configureren
Verifiëren
Problemen oplossen
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u een Cisco adaptieve security applicatie (ASA) kunt configureren als een CA-server (Certificate Authority) en als een SSL-gateway (Secure Sockets Layer) voor Cisco AnyConnect beveiligde mobiliteitsclients.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA basisconfiguratie die softwareversie 9.1.x in werking stelt
- ASDM 7.3 of hoger

Gebruikte componenten

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

- · Cisco 5500 Series ASA waarin softwareversie 9.1(6) wordt uitgevoerd
- AnyConnect Secure Mobility-clientversie 4.x voor Windows
- PC die een ondersteund besturingssysteem uitvoert volgens de compatibiliteitstabel.
- Cisco Adaptieve Security Device Manager (ASDM) versie 7.3

Opmerking: Download het AnyConnect VPN-clientpakket (AnyConnect-win*.pkg) van Cisco <u>Software Download</u> (alleen_<u>geregistreerde</u> klanten). Kopieer de AnyConnect VPN-client naar het flitsgeheugen van de ASA, dat moet worden gedownload naar de externe gebruikerscomputers om de SSL VPN-verbinding met de ASA tot stand te brengen. Raadpleeg het gedeelte <u>AnyConnect-client installeren</u> in de ASA-configuratiehandleiding voor meer informatie.

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.

Achtergrondinformatie

De certificeringsinstantie van de ASA biedt de volgende functies:

- Geïntegreerd basisbeheer van certificeringsinstanties op de ASA.
- Implementeert certificaten.
- Zorgt voor beveiligde herroepingscontrole van uitgegeven certificaten.
- Biedt een certificeringsinstantie op de ASA voor gebruik met op browser gebaseerde (WebVPN) en op client gebaseerde (AnyConnect) SSL VPN-verbindingen.
- Biedt betrouwbare digitale certificaten aan gebruikers, zonder dat ze hoeven te vertrouwen op externe certificaatautorisatie.
- Biedt een veilige, interne autoriteit voor certificaathandhaving en biedt eenvoudige inschrijving door gebruikers door middel van een websitelogin.

Richtlijnen en beperkingen

- Ondersteund in routed en transparante firewallmodus.
- Slechts één lokale CA-server tegelijk kan op een ASA worden geïnstalleerd.
- ASA als lokale CA-serverfunctie wordt niet ondersteund in een failover-instelling.
- De ASA fungeert vanaf nu als een Local CA-server en ondersteunt alleen het genereren van SHA1-certificaten.
- Lokale CA-server kan worden gebruikt voor browsergebaseerde en clientgebaseerde SSL VPN-verbindingen. Momenteel niet ondersteund voor IPSec.
- Ondersteunt geen VPN-taakverdeling voor de lokale CA.
- De lokale CA kan geen ondergeschikte instantie zijn van een andere CA. Het kan alleen fungeren als de wortel CA.
- Op dit moment kan de ASA zich niet inschrijven bij de lokale CA-server voor het

identiteitscertificaat.

 Wanneer een certificaatinschrijving wordt voltooid, slaat de ASA een PKCS12-bestand op met de sleutelpaar en de certificaatketen van de gebruiker, die ongeveer 2 KB aan flitsgeheugen of schijfruimte per inschrijving vereist. De feitelijke hoeveelheid schijfruimte is afhankelijk van de geconfigureerde RSA-sleutelgrootte en certificaatvelden. Houd deze richtlijn in gedachten wanneer u een groot aantal hangende certificaatinschrijvingen op een ASA toevoegt met een beperkte hoeveelheid beschikbaar flitsgeheugen, omdat deze PKCS12-bestanden in flitsgeheugen worden opgeslagen voor de duur van de geconfigureerde inschrijving ophalen tijd.

Configureren

In deze sectie wordt beschreven hoe u Cisco ASA kunt configureren als een lokale CA-server.

Opmerking: Gebruik de <u>Command Lookup Tool</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



ASA als lokale CA-server

Stap 1. De lokale CA-server op ASA configureren en inschakelen

- Navigeren naar Configuratie > Externe toegang VPN > Certificaatbeheer > Lokale certificeringsinstantie > CA-server. Controleer de optie Certificaatinstantie inschakelen.
- Wachtwoord configureren. Het wachtwoord moet minimaal 7 tekens lang zijn en wordt gebruikt om een PKCS12-bestand te coderen en op te slaan dat het lokale CA-certificaat en het sleutelpaar bevat. Het wachtwoord ontgrendelt het PKCS12-archief als het CA-certificaat of het sleutelpaar is verloren.

- Configureer de afgevende naam. Dit veld wordt weergegeven als Root Certificate CN. Dit kan in de volgende indeling worden gespecificeerd: CN (algemene naam), OU (organisatieeenheid), O) organisatie, L (plaats), S (staat) en C (land).
- Optionele configuratie: Configureer de instellingen van de SMTP-server en e-mailserver om ervoor te zorgen dat de OTP kan worden ontvangen om clients via e-mail te ontvangen om de inschrijving te voltooien. U kunt hostnaam of IP-adres van uw lokale e-mail/SMTP-server configureren. U kunt ook configureren Van adres en Onderwerp veld van de e-mail die de klanten zouden ontvangen. Standaard is het Van adres admin@<ASA hostname>.null en is het onderwerp de uitnodiging voor certificaatinschrijving.
- Optionele configuratie: U kunt de optionele parameters configureren zoals grootte van de clientsleutel, grootte van de CA-serversleutel, levensduur van het CA-certificaat en levensduur van het clientcertificaat.

Device List	ΞΨ×	Configuration > Remote Access VPN	> Certificate Management > Local Certificate Authority > CA Server		
Add 📋 Delete 🚿 Connect					
Find: Go		Enable Certificate Authority Server			
10.105.130.69:4443					
		Passphrase:			
		Confirm Passphrase:	••••••• Specify the Passphrase		
		Issuer Name:	CN=ASA.local Specify the CN which will show as Issuer name		
		CA Server Key Size:	1024 🗸		
		Client Key Size:	1024 Specify the Server/Client key-size to be used		
		CA Certificate Lifetime:	1095 days		
			The CA certificate lifetime change will take effect after existing CA certs expire.		
Remote Access VPN	0 P	Client Certificate Lifetime:	365 days		
2 Introduction					
Network (Client) Access		SMTP Server & Email Settings			
Clientless SSL VPN Access		Server Name/IP Address:			
🕀 📷 AAA/Local Users					
Host Scan Image		From Address:	admin@ciscoasa.null		
E Secure Desktop Manager		Subject:	Certificate Enrollment Invitation		
Certificate Management					
CA Certificates		Mara OnFran			
Identity Certificates		More Options			
Trusted Certificate Pool					
Code Signer					
Local Certificate Authority					
CA Server					
Manage User Database					
manage User Certificates					

CLI-equivalent:

ASA(config)# crypto ca server ASA(config-ca-server)# issuer-name CN=ASA.local ASA(config-ca-server)# subject-name-default CN=ASA.local ASA(config-ca-server)# lifetime certificate 365 ASA(config-ca-server)# lifetime ca-certificate 1095 ASA(config-ca-server)# passphrase cisco123 ASA(config-ca-server)# no shutdown % Some server settings cannot be changed after CA certificate generation. Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

URL voor CRL- distributiepunt	Dit is de CRL locatie op de ASA. De standaardlocatie is <u>http://hostname.domain/+CSCOCA+/asa_ca.crl,</u> maar de URL kan worden gewijzigd.
Publish-CRL interface en poort	Om CRL voor de download van HTTP op een bepaalde interface en een haven beschikbaar te maken, kies een publiceren-CRL interface van de vervolgkeuzelijst. Voer vervolgens het poortnummer in, dat elk poortnummer van 1-65535 kan zijn. Het standaardpoortnummer is TCP- poort 80.
CRL-levensduur	De lokale CA werkt het CRL bij en geeft het opnieuw uit telkens als een gebruikerscertificaat wordt ingetrokken of niet ingetrokken, maar als er geen herroepingswijzigingen zijn, wordt het CRL automatisch opnieuw uitgegeven zodra elk CRL-leven, de periode die u met het levenslange bevel tijdens de lokale CA-configuratie specificeert. Als u geen CRL-leven specificeert, is de standaardtijdperiode zes uren.
Locatie voor databaseopslag	ASA heeft toegang tot en implementeert gebruikersinformatie, uitgegeven certificaten en herroepingslijsten met behulp van een lokale CA-database. Dit gegevensbestand verblijft in lokaal flitsgeheugen door gebrek, of kan worden gevormd om op een extern dossiersysteem te verblijven dat en toegankelijk voor ASA wordt opgezet.
Standaard onderwerpnaam	Voer een standaard onderwerp (DN-string) in om toe te voegen aan een gebruikersnaam op uitgegeven certificaten. De toegestane DN-kenmerken zijn in deze lijst opgenomen: ·CN (algemene naam)SN (familienaam) ·O (naam organisatie) ·L (Plaats) ·C (land) ·OU (organisatie-eenheid) ·EA (e-mailadres) ·ST (Staat/Provincie) ·T (titel)

Inschrijvingsperiode	Stelt de inschrijvingstijd in in uren waarbinnen de gebruiker het PKCS12- bestand van ASA kan ophalen. De standaardwaarde is 24 uur. Opmerking: Als de inschrijvingsperiode verloopt voordat de gebruiker het PKCS12-bestand met het gebruikerscertificaat ophaalt, is inschrijving niet toegestaan.
Vervaldatum van eenmalig wachtwoord	Bepaalt de hoeveelheid tijd in uren dat OTP voor gebruikersinschrijving geldig is. Deze tijdsperiode begint wanneer de gebruiker zich kan inschrijven. De standaardwaarde is 72 uur.
Herinnering voor verlopen certificaat	Specificeert het aantal dagen vóór het verlopen van het certificaat dat een eerste herinnering om opnieuw in te schrijven wordt verzonden naar de eigenaars van het certificaat.

Stap 2. Gebruikers maken en toevoegen aan de ASA-database

 Navigeer naar Configuratie > Externe toegang VPN > Certificaatbeheer > Lokale certificeringsinstantie > Gebruikersdatabase beheren.Klik op Toevoegen.



· Gebruikersnaam, e-mail-id en onderwerpnaam, zoals in deze afbeelding.

🔄 Add User		x
Username:	user 1	
Email ID:	user 1@cisco.com	
Subject (DN String):	CN=user1,OU=TAC	Select
Allow enrollment		
	Add User Cancel Help	

- Zorg ervoor dat Toestaan de Inschrijving wordt gecontroleerd zodat u voor het certificaat mag inschrijven.
- Klik op Gebruiker toevoegen om de gebruikersconfiguratie te voltooien.

CLI-equivalent:

<#root>

ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com

 Nadat de gebruiker is toegevoegd aan de gebruikersdatabase, wordt de inschrijvingsstatus weergegeven als Toestaan om in te schrijven.

Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database						
Manage the	Manage the users in the user database for Local Certificate Authority Server.					
Username	E	imail	Subject Name	Enrollment Status	Certificate Holder	Add
user 1		user1@cisco.com	CN=user 1,OU=TAC	allowed	yes	Edit
						Delete
						Allow Enrollment
						Email OTP
						View/Re-generate OTP

CLI om de gebruikersstatus te verifiëren:



 Nadat de gebruiker is toegevoegd aan de gebruikersdatabase, kan het eenmalige wachtwoord (One Time Password) voor de gebruiker om de inschrijving te voltooien worden verstrekt met behulp van ofwel dit:

E-mail de OTP (Hiervoor moeten SMTP-server en e-mail-instellingen worden geconfigureerd onder de CA-serverconfiguratie).

OF

Bekijk direct de OTP en deel met de gebruiker door te klikken op View/Re-generation OTP. Dit kan ook worden gebruikt om de OTP te regenereren.



CLI-equivalent:

!! Email the OTP to the user ASA# crypto ca server user-db allow user1 email-otp !! Display the OTP on terminal ASA# crypto ca server user-db allow user1 display-otp Username: user1 OTP: 18D14F39C8F3DD84

Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016

Stap 3. WebVPN inschakelen op de WAN-interface

• Schakel Web Access op de ASA voor clients in om inschrijving aan te vragen.

```
!! Enable web-access on the "Internet" interface of the ASA
ASA(config)# webvpn
ASA(config-webvpn)#enable Internet
```

Stap 4. Het certificaat op de clientmachine importeren

- Open op het client werkstation een browser en navigeer naar de link om de inschrijving te voltooien.
- · De IP/FQDN die in deze link wordt gebruikt, moet het IP zijn van de interface waarop

webvpn is ingeschakeld in die stap, namelijk interface-internet.

<#root>
https://
< <u><></u>
IP/FQDN>/+CSCOCA+/enroll.html

• <u>Voer de gebruikersnaam in (geconfigureerd op de ASA onder Stap 2, optie A) en de OTP,</u> <u>die via e-mail of handmatig is verstrekt.</u>

ASA - Local Certificate Authority	
ASA - Local Certificate Authority Username user1 One-time Password ••••••••••••••••••••••••••••••••••••	

- Klik op Open om het clientcertificaat dat van de ASA is ontvangen, rechtstreeks te installeren.
- <u>Het wachtwoord voor het installeren van het clientcertificaat is hetzelfde als het eerder</u> <u>ontvangen OTP.</u>

File Down	load 🗾 🔀
Do you	want to open or save this file?
	Name: user1.p12 Type: Personal Information Exchange From: 10.105.130.214
2	Open Save Cancel While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

• Klik op Next (Volgende).

Certificate Import Wizard



X

• Laat het pad standaard staan en klik op Volgende.

Certificate Import Wizard
File to Import
Specify the file you want to import.
Eile namer
s\Temporary Internet Files\Content.IE5\SQT1AUGH\user1[1].p12 Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about certificate file formats
< Back Next > Cancel

- Voer de OTP in het veld Wachtwoord in.
- <u>U kunt de optie selecteren om deze toets als exporteerbaar te markeren, zodat de toets</u> indien nodig in de toekomst uit het werkstation kan worden geëxporteerd.
- Klik op Volgende

Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about <u>protecting private keys</u>
< Back Next > Cancel

- <u>U kunt het certificaat handmatig installeren in een bepaald certificaatarchief of het verlaten</u> om automatisch de winkel te kiezen.
- Klik op Next (Volgende).

ertificate Import Wizard	x
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Browse	
Learn more about <u>certificate stores</u>	
< Back Next > Cancel	

• Klik op Voltooien om de installatie te voltooien.

Certificate Import Wizard



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected Content	Automatically determined by t PFX
File Name	C: \Users \mrsethi \AppData \Lo
•	- F
< Back	Finish Cancel

х



- Nadat het certificaat is geïnstalleerd, kunt u dit verifiëren.
- <u>Open IE en navigeer naar Gereedschappen > Internet-opties.</u>



• Navigeer naar het tabblad Inhoud en klik op Certificaten, zoals in deze afbeelding.

Internet Options				
General Security Privacy Content Connections Programs Advanced				
Parental Controls Control the Internet content that can Parental Controls be viewed.				
Content Advisor Ratings help you control the Internet content that can be viewed on this computer. Enable Settings				
Certificates Use certificates for encrypted connections and identification. Clear SSL state Certificates Publishers				
AutoComplete AutoComplete stores previous entries On webpages and suggests matches for you. Eeeds and Web Slices				
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.				
OK Cancel Apply				

• Onder de Persoonlijke winkel kunt u het certificaat zien dat u van de ASA hebt ontvangen.

Certificates				×
Intended pu	urpose: <a>All	>		
Personal	Other People	Intermediate Certification A	uthorities T	rusted Root Certification
Issued	То	Issued By	Expiratio	. Friendly Name
user	·1	asa.local	1/8/2017	ou=TAC,cn=user1
Import Certificate	. Export	. Remove		Advanced
Learn more	e about <u>certificate</u>	<u>:S</u>		Close

ASA als SSL-gateway voor AnyConnect-clients

ASDM AnyConnect-configuratiewizard

De AnyConnect Configuration Wizard/CLI kan worden gebruikt om de AnyConnect Secure Mobility Client te configureren. Zorg ervoor dat een AnyConnect-clientpakket is geüpload naar de flash/schijf van de ASA-firewall voordat u verdergaat.

Volg de volgende stappen om de AnyConnect Secure Mobility Client te configureren met de configuratiewizard:

1. Log in ASDM en navigeer naar Wizard > VPN Wizards > AnyConnect VPN Wizard om de Configuration Wizard te starten en klik op Volgende.

📑 AnyConnect VPN Connecti	ion Setup Wizard	23
VPN Wizard Image: Ima	Introduction Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the user's device when a VPN connection is established. VPN Remote Access Coal One of the Coal One	end
	< Back Next > Cancel H	eip

2. Voer de naam van het verbindingsprofiel in, kies de interface waarop het VPN wordt beëindigd in het vervolgkeuzemenu VPN-toegangsinterface en klik op Volgende.

TanyConnect VPN Connect	tion Setup Wizard	
Steps	Connection Profile Identification	
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN	
2. Connection Profile	connections.	
2 VPN Protocolo	Connection Profile Name: SSL_GRP	
4. Client Images		
5. Authentication Methods	VPN Access Interface: Internet	
6. Client Address Assignme		
7. Network Name Resolutio		
Servers		
8. NAT Exempt		
 AnyConnect Client Deployment 		
10. Summary		
	< Back Next > Cancel Help	

3. Controleer het SSL-aanvinkvakje om Secure Sockets Layer (SSL) in te schakelen. Het apparaatcertificaat kan een door een betrouwbare externe certificeringsinstantie (CA, zoals Verisign of Entrust) uitgegeven certificaat of een zelf-ondertekend certificaat zijn. Als het certificaat

1. Opmerking: dit certificaat is het serverzijcertificaat dat door ASA aan SSL-clients wordt aangeboden. Als er op dit moment geen servercertificaten op de ASA zijn geïnstalleerd dan moet er een zelfondertekend certificaat worden gegenereerd, klik dan op Beheren.

Om een certificaat van een externe partij te installeren moet u de stappen volgen die zijn beschreven in het Cisco-document <u>ASA 8.x: voorbeeld van handmatige installatie van certificaten van een externe leverancier voor gebruik bij een WebVPN-configuratie</u>.

- Schakel de VPN-protocollen en het apparaatcertificaat in.
- Klik op Next (Volgende).

Connect VPN Connect	tion Setup Wizard
Steps	VPN Protocols
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support. SSL IPSec Device Certificate Device Certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA. Device Certificate:None Manage
	< Back Next > Cancel Help

4. Klik op Add om het AnyConnect-clientpakket (.pkg-bestand) toe te voegen vanaf het lokale station of vanaf de flitser/schijf van ASA.

Klik op Bladeren Flash om de afbeelding toe te voegen van de flash drive, of klik op Upload om de afbeelding toe te voegen van de lokale schijf van de host machine.

AnyConnect VPN Connect	on Setup Wizard	22	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to		
3. VPN Protocols	the top of the list.		
4. Client Images			
5. Authentication Methods			
6. Client Address Assignme	Image	Regular expression to match user-agent	
 Network Name Resolutio Servers 			
8. NAT Exempt			
9. AnyConnect Client Deployment			
10. Summary			
	You can download ApyConnect Client packages from Cisco by coarchir	an 'ApyConnect VPN Client' or click here	
	Too can download Any-connect client packages from Cisco by searchin	ig Anyconnect very client of <u>click nere</u> ,	
	< Back Next >	Cancel Help	

- U kunt het AnyConnect.pkg-bestand uploaden vanaf ASA Flash/Disk (als het pakket al bestaat) of vanaf het lokale station.
- Blader door de flitser om het AnyConnect-pakket te selecteren in de ASA Flash/Disk.
- Upload om het AnyConnect-pakket te selecteren vanaf het lokale station van de hostmachine.
- Klik op OK.

Add AnyConnect	Client Image	22
AnyConnect Image:	disk0:/anyconnect-win-4.2.00096-k9.pkg Browse Flash	
		Upload
Regular expression	to match user-agent	*
	OK Cancel Help	

• Klik op Next (Volgende).

AnyConnect VPN Connect	tion Setup Wizard	×	
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.		
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to an image.		
3. VPN Protocols	the top of the list.		
4. Client Images			
5. Authentication Methods	Add 🖉 Replace 🛄 Delete 🎓 🔸		
6. Client Address Assignme	Image	Regular expression to match user-agent	
 Network Name Resolutio Servers 	disk0:/anyconnect-win-4.2.00096-k9.pkg		
8. NAT Exempt			
 AnyConnect Client Deployment 			
10. Summary			
	You can download AnyConnect Client packages from <u>Cisco</u> by searching	'AnyConnect VPN Client' or <u>click here</u> .	
	<back next=""></back>	Cancel Help	

5. De gebruikersverificatie kan worden voltooid via de servergroepen Verificatie, autorisatie en accounting (AAA). Als de gebruikers al zijn geconfigureerd, kies dan LOCAL en klik op Next. Voeg anders een gebruiker toe aan de lokale gebruikersdatabase en klik op Volgende.

Opmerking: in dit voorbeeld is LOKALE verificatie geconfigureerd, wat betekent dat de lokale gebruikersdatabase op de ASA zal worden gebruikt voor verificatie.

AnyConnect VPN Connect	tion Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignme 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Authentication Methods This step lets you specify the location of the authentication server. You can dick on the "New" button to create a new server group. AAA Server Group: LOCAL New Local User Database Details User to be Added Username: user1 Add >> Delete Confirm Password: ••••• Delete
	< Back Next > Cancel Help

6. Zorg ervoor dat de Adrespool voor de VPN-clients is geconfigureerd. Als een ip pool reeds wordt gevormd dan selecteer het uit het drop-down menu. Als dit niet het geval is, klikt u op Nieuw om de configuratie te starten. Klik op Volgende als u klaar bent.

TanyConnect VPN Connect	tion Setup Wizard
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool: Details of the selected address pool
	< Back Next > Cancel Help

Te Add IPv4 Pool		
Name:	VPN_Pool	
Starting IP Address:	10.10.10.1	
Ending IP Address:	10.10.200	
Subnet Mask:	255.255.0 ◄	
ОК	Cancel Help	

• Klik op Next (Volgende).

AnyConnect VPN Connect	tion Setup Wizard	
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. Client Address Assignment 7. Network Name Resolutio Servers 8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool: VPN_Pool New Details of the selected address pool Starting IP Address: 10.10.10.10.200 Subnet Mask: 255.255.255.0	
< Back Next > Cancel Help		

7. Configureer naar keuze de DNS-servers (Domain Name System) en DNS-servers in de velden DNS en Domain Name en klik vervolgens op Volgende.

anyConnect VPN Connec	tion Setup Wizard	x
Steps	Network Name Resolution Servers	
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.	
2. Connection Profile Identification	DNS Servers:	
3. VPN Protocols	WINS Servers:	
4. Client Images	Domain Name:	
5. Authentication Methods		
6. Client Address Assignme		
7. Network Name Resolution Servers		
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel H	elp

8. Zorg ervoor dat het verkeer tussen de client en het interne subnet moet worden vrijgesteld van elke dynamische netwerkadresomzetting (NAT). Schakel het selectievakje Uitzonderlijk VPN-verkeer van netwerkadresomzetting in en configureer de LAN-interface die voor de vrijstelling wordt gebruikt. Specificeer ook het lokale netwerk dat moet worden vrijgesteld en klik op Volgende.

anyConnect VPN Connection Setup Wizard			
AnyConnect VPN Connect Steps I. Introduction C. Connection Profile Identification VPN Protocols Client Images Authentication Methods Client Address Assignme	NAT Exempt If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation. If network address translation Inside Interface is the interface directly connected to your internal network. Inside Interface: Inside Interface:		
 Client Address Assignme Network Name Resolutio Servers NAT Exempt AnyConnect Client Deployment Summary 	Local Network is the network address(es) of the internal network that client can access. Local Network: 192.168.10.0/24 The traffic between AnyConnect client and internal network will be exempt from network address translation.		
	< Back Next > Cancel Help		

9. Klik op Volgende.

anyConnect VPN Connect	tion Setup Wizard	23		
Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols	AnyConnect Client Deployment AnyConnect client program can be installed to a client device by one of the following two methods: 1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed 2) Pre-deployment - Manually install the AnyConnect client package.	;		
 Client Images Authentication Methods Client Address Assignme Network Name Resolutio Servers NAT Exempt 				
9. AnyConnect Client Deployment 10. Summary				
	< Back Next > Cancel Help			

10. De laatste stap toont de samenvatting. Klik op Voltooien om de configuratie te voltooien.

AnyConnect VPN Connecti	ion Setup Wizard	22
VPN Wizard	Summary	
Branch	Here is the summary of the configuration.	
EET -	Name	Value
T ISP	Summary	
	Name/Alias of the Connection Profile	SSL_GRP
Home	VPN Access Interface	Internet
Carporate	Device Digital Certificate	none
Network	VPN Protocols Enabled	SSL only
	AnyConnect Client Images	1 package
GLAND IN ME	Authentication Server Group	LOCAL
and the second second	Address Pool for the Client	10.10.10.1 - 10.10.10.200
	DNS	Server: Domain Name:
	Network Address Translation	The protected traffic is not subjected to network address translation
TTHU		
There		
the state		
Not at		
(< Back Finish	Cancel Help

De configuratie van de AnyConnect-client is nu voltooid. Wanneer u AnyConnect echter configureert via de configuratiewizard, wordt de verificatiemethode standaard als AAA

geconfigureerd. Om de clients te verifiëren via certificaten en gebruikersnaam/wachtwoord, moet de tunnelgroep (Verbindingsprofiel) worden geconfigureerd om certificaten en AAA als verificatiemethode te gebruiken.

- Navigeer naar Configuration > Remote Access VPN > Network (client) Access > AnyConnect Connection-profielen.
- U moet het nieuwe toegevoegde verbindingsprofiel SSL_GRP zien.

Device List 🗗 🖓 🗡	Configuration >	Remote Access VP	N > Network (Client	Access > AnyConne	ect Connection Profiles				
	The security app tunnel with Data	pliance automatically de agram Transport Layer	eploys the Cisco AnyCo Security (DTLS) tunnel	nnect VPN Client to rem ing options.	ote users upon connection. The	initial di	ent deployment requires end	-user administrative rights. The Cisco AnyConne	ct VPN Client supports IPsec (IKEv2) tunnel as well as SSL
	Access interfaces								
	Enable Cisco	o AnyConnect VPN Clier	nt access on the interfa	aces selected in the tabl	e below				
	SSL access must	SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).							
		SSL Access	tess IPsec (IKEv2		2) Access				
	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services		Device Certificate		
Remote Access VPN	Inside						Port Settings		
2 Introduction	Internet								
Network (Client) Access	Outside					-			
Any Correct Connection Profiles Any Connect Cost Profiles Any Connect Cost Profiles Any Connect Clear Profile Any Connect Clear Profile Any Connect Clear Software Any Connect Seentals Any Connect Seentals	Bypass Inter Access lists from Login Page Setting Allow user t Shutdown p Connection Profile Connection pro & Add I f	rface access lists for int n group policy and user a	bound VPN sessions policy always apply to file on the login page.	the traffic.	meters. You can configure the ase	napping	from certificate to connection	profile <u>bere</u> .	
ACL Manager	Name		SSL Enabled	IPs	ec Enabled		Aliases	Authentication Method	Group Policy
Clientless SSL VPN Access	DefaultRAGrou	p			V			AAA(LOCAL)	DfltGrpPolicy
Connection Profiles	DefaultWEBVPN	VGroup						AAA(LOCAL)	DfltGrpPolicy
Portal	ssl-grp						ssl-grp	AAA(LOCAL)	DfltGrpPolicy
	SSL_GRP		V				SSL_GRP	AAA(LOCAL)	GroupPolicy_SSL_GRP

- Als u AAA-verificatie en certificaatverificatie wilt configureren, selecteert u het verbindingsprofiel SSL_GRP en klikt u op Bewerken.
- Selecteer onder Verificatiemethode de optie Beide.

Edit AnyC	onnect Connection Profile: SSL_GRP		×
Basic	Name	SCI CDD	
	Alizensi		
	Alldses:	SSL_GRP	
	Authentication		
	Method:	AAA Certificate South	
	AAA Server Group:	LOCAL V	nage
		Use LOCAL if Server Group fails	
	Client Address Assignment -		
	DHCP Servers:		
		None OHCP Link OHCP Subnet	
	Client Address Pools:	VPN_Pool Se	elect
	Client IPv6 Address Pools:	: Se	elect
	Default Group Policy		
	Group Policy:	GroupPolicy_SSL_GRP	nage
	(Following field is an attrib	ute of the group policy selected above.)	
	Enable SSL VPN dier	nt protocol	
	Enable IPsec(IKEv2)) client protocol	
	DNS Servers:		
	WINS Servers:		
	Domain Name:		
Find:	Ne	ext O Previous	
	ОК	Cancel Help	

CLI voor AnyConnect configureren

<#root>

!! *****Configure the VPN Pool*****
ip local pool VPN_Pool 10.10.10.10.10.10.200 mask 255.255.255.0
!! *****Configure Address Objects for VPN Pool and Local Network*****
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0

```
object network NETWORK_OBJ_192.168.10.0_24
 subnet 192.168.10.0 255.255.255.0
 exit
!! *****Configure WebVPN*****
webvpn
enable Internet
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
 tunnel-group-list enable
 exit
!! *****Configure User*****
username user1 password mb02jYs13AX1IAGa encrypted privilege 2
!! *****Configure Group-Policy*****
group-policy GroupPolicy_SSL_GRP internal
group-policy GroupPolicy_SSL_GRP attributes
vpn-tunnel-protocol ssl-client
 dns-server none
wins-server none
 default-domain none
 exit
!! *****Configure Tunnel-Group*****
tunnel-group SSL_GRP type remote-access
tunnel-group SSL_GRP general-attributes
authentication-server-group LOCAL
 default-group-policy GroupPolicy_SSL_GRP
address-pool VPN_Pool
tunnel-group SSL_GRP webvpn-attributes
 authentication aaa certificate
 group-alias SSL_GRP enable
exit
!! *****Configure NAT-Exempt Policy*****
```

nat (Inside, Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24 destination of the state of

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Opmerking: De <u>Output Interpreter Tool</u> (alleen geregistreerde klanten) ondersteunt bepaalde show opdrachten. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

Zorg ervoor dat de CA-server is ingeschakeld.

crypto ca server tonen

<#root>

ASA(config)# show crypto ca server Certificate Server LOCAL-CA-SERVER:

Status: enabled

State: enabled Server's configuration is locked (enter "shutdown" to unlock it)

Issuer name: CN=ASA.local

CA certificate fingerprint/thumbprint: (MD5) 32e868b9 351a1b07 4b59cce5 704d6615 CA certificate fingerprint/thumbprint: (SHA1) 6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d Last certificate issued serial number: 0x1 CA certificate expiration timer: 19:25:42 UTC Jan 8 2019 CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016 Current primary storage dir: flash:/LOCAL-CA-SERVER/

Auto-Rollover configured, overlap period 30 days Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved !!

Zorg ervoor dat de gebruiker voor inschrijving na het toevoegen wordt toegestaan:

<#root>

*****Before Enrollment*****

ASA#

show crypto ca server user-db

username: user1
email: user1@cisco.com
dn: CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll

>>> Shows the status "Allowed to Enroll"

*****After Enrollment*****

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:05:14 UTC Thu Jan 14 2016 notified: 1 times

enrollment status: Enrolled

, Certificate valid until 19:18:30 UTC Tue Jan 10 2017, Renewal: Allowed

U kunt de details van de AnyConnect-verbinding controleren via CLI of ASDM.

Via CLI

toon vpn-sessiondb detail anyconnect

<#root>

ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed Username : user1 Index : 1 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol : AnyConnect Essentials License Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 13822 Bytes Rx : 13299 Pkts Tx : 10 Pkts Rx : 137 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_SSL_GRP Tunnel Group : SSL_GRP Login Time : 19:19:10 UTC Mon Jan 11 2016 : 0h:00m:47s Duration Inactivity : 0h:00m:00s NAC Result : Unknown VLAN VLAN Mapping : N/A : none AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 1.1 Public IP : 10.142.189.181 Encryption : none Hashing : none TCP Src Port : 52442 TCP Dst Port : 443 : Certificate and userPassword Auth Mode Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096

Bytes Tx : 6911 Bytes Rx : 768 Pkts Rx Pkts Tx : 5 : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 1.2 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Hashing : SHA1 Encryption : RC4 Encapsulation: TLSv1.0 TCP Src Port : 52443 TCP Dst Port : 443 Auth Mode : Certificate and userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 : 152 : 6911 Bytes Rx Bytes Tx : 2 Pkts Tx : 5 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 1.3 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Encryption : AES128 : SHA1 Hashing Encapsulation: DTLSv1.0 UDP Src Port : 59167 UDP Dst Port : 443 Auth Mode : Certificate and userPassword Idle TO Left : 30 Minutes Idle Time Out: 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 0 Bytes Rx : 12907 Pkts Tx : 0 Pkts Rx : 142 Pkts Tx Drop : 0 Pkts Rx Drop : 0 NAC: Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds SQ Int (T) : 0 Seconds EoU Age(T) : 51 Seconds Hold Left (T): 0 Seconds Posture Token: Redirect URL :

Via ASDM

- Navigeer naar Monitoring > VPN > VPN-statistieken > Sessies.
- · Kies het filter door als Alle externe toegang.
- U kunt een van de acties voor de geselecteerde AnyConnect-client uitvoeren.

Details - Meer informatie geven over de sessie

Uitloggen - De gebruiker handmatig uitloggen vanaf Head-end

Ping-to-ping van de AnyConnect-client vanuit de head-end

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Opmerking: raadpleeg Belangrijke informatie over debug-opdrachten voordat u debugopdrachten gebruikt.

Let op: op de ASA kunt u verschillende debugniveaus instellen, standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de hoeveelheid debug-informatie toenemen. Wees hier voorzichtig mee, vooral in productieomgevingen.

- · debug crypto ca
- · debug crypto ca server
- debug crypto ca-berichten
- · debug crypto ca-transacties
- debug webvpn anyconnect

Deze debug uitvoer toont wanneer de CA server is ingeschakeld met de opdracht no shut.

<#root>

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255 CRYPTO_CS: input signal enqueued: no shut >>>> Command issued to Enable the CA server Crypto CS thread wakes up! CRYPTO_CS: enter FSM: input state disabled, input signal no shut CRYPTO_CS: starting enabling checks CRYPTO_CS: found existing serial file. CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019 CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: DB version 1 CRYPTO_CS: last issued serial number is 0x4 CRYPTO_CS: closed ser file CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists. CRYPTO_CS: Read 220 bytes from crl file. CRYPTO_CS: closed crl file CRYPTO_PKI: Storage context locked by thread Crypto CA Server CRYPTO_PKI: inserting CRL CRYPTO_PKI: set CRL update timer with delay: 20250 CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016 CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016 CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016 CRYPTO_PKI: CRL cache delay being set to: 20250000

CRYPTO_PKI: Storage context released by thread Crypto CA Server

CRYPTO_CS: Inserted Local CA CRL into cache!

CRYPTO_CS: shadow not configured; look for shadow cert CRYPTO_CS: failed to find shadow cert in the db CRYPTO_CS: set shadow generation timer CRYPTO_CS: shadow generation timer has been set CRYPTO_CS: Enabled CS. CRYPTO_CS: exit FSM: new state enabled CRYPTO_CS: cs config has been locked.

```
Crypto CS thread sleeps!
```

Deze debug uitvoer toont de inschrijving van de client

<#root>

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255

CRYPTO_CS: writing serial number 0x2. CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO_CS: Writing 32 bytes to ser file CRYPTO_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

De inschrijving van de klant kan onder deze voorwaarden mislukken:

Scenario 1.

 De gebruiker wordt aangemaakt in de CA-serverdatabase zonder de toestemming om in te schrijven.

🔄 Add User		×
Username:	user 1	
Email ID:	user1@cisco.com	
Subject (DN String):	CN=user1,OU=TAC	Select
Allow enrollment		
	Add User Cancel Help	

CLI-equivalent:

<#root>		
ASA(config	g)# show crypto ca server user-db	
username: email: dn: allowed: notified:	user1 user1@cisco.com CN=user1,OU=TAC <not allowed=""> 0 times</not>	
enrollment	status: Not Allowed to Enroll	

• In het geval dat de gebruiker niet mag inschrijven, wordt deze foutmelding gegenereerd door te proberen de OTP voor de gebruiker te genereren/e-mailen.



Scenario 2.

• Controleer de poort en interface waarop het inschrijvingsportal beschikbaar is met de opdracht webvpn voor show-run. De standaardpoort is 443, maar kan worden aangepast.

 Zorg ervoor dat de client netwerkbereikbaarheid heeft naar het IP-adres van de interface waarop webvpn is ingeschakeld op de poort die wordt gebruikt om met succes toegang te krijgen tot het inschrijvingsportal.

In deze gevallen heeft de klant mogelijk geen toegang tot het inschrijvingsportal van ASA:

- 1. Als een tussenapparaat de inkomende verbindingen van de client naar de webvpn IP van de ASA op de opgegeven poort blokkeert.
- 2. De status van de interface is beneden waarop webvpn is ingeschakeld.
- Deze output toont aan dat het inschrijvingsportaal op het IP adres van de interface Internet op aangepaste poort 4433 beschikbaar is.

```
<#root>
```

ASA(config)# show run webvpn

webvpn

port 4433

enable Internet

```
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Scenario 3.

- De standaardlocatie van CA Server Database Storage is Flash-geheugen van de ASA.
- Zorg ervoor dat het flitsgeheugen vrije ruimte heeft om pkcs12-bestand te genereren en op te slaan voor de gebruiker tijdens de inschrijving.
- In het geval dat het flitsgeheugen niet genoeg vrije ruimte heeft, ASA er niet in slaagt om het inschrijvingsproces van de client te voltooien en genereert deze debug logboeken:

<#root>

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

CRYPTO_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1. CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1. CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1

Gerelateerde informatie

- Adaptieve security applicaties van Cisco ASA 5500 Series
- <u>Probleemoplossingsgids AnyConnect VPN-client veelvoorkomende problemen</u>
- AnyConnect-sessies beheren, bewaken en oplossen van problemen
- Technische ondersteuning en documentatie Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.