Konfigurieren des VPN Client 3.x zum Abrufen eines digitalen Zertifikats

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren des VPN-Clients Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird veranschaulicht, wie der Cisco VPN Client 3.x so konfiguriert wird, dass er ein digitales Zertifikat erhält.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem PC, auf dem Cisco VPN Client 3.x 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 unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren des VPN-Clients

Führen Sie diese Schritte aus, um den VPN-Client zu konfigurieren.

 Wählen Sie Start > Programme > Cisco Systems Inc. VPN-Client > Certificate Manager aus, um den VPN Client Certificate Manager zu



2. Wählen Sie die Registerkarte Persönliche Zertifikate aus, und klicken Sie auf

A certificate authority (C/	A) is an organization that issues	certificates.
Enrollment requests are o	certificate requests that a CA h	as yet to approve.
Personal Certificates	CA Cartificatos Enrollment Ba	aquesta
Lennicate	Store	
Stores: <all></all>	<u>▼</u> <u>N</u> ew	<u>O</u> ptions 👻

: Computerzertifikate zur Authentifizierung von Benutzern für VPN-Verbindungen können nicht mit IPsec erstellt werden.

3. Wenn Sie vom VPN-Client zur Eingabe eines Kennworts aufgefordert werden, geben Sie ein Kennwort zum Schutz des Zertifikats an. Bei jeder Operation, die Zugriff auf den privaten Schlüssel des Zertifikats erfordert, muss das angegebene Kennwort eingegeben werden, um fortzufahren.

CISCO SYSTEMS	Password protecting your certificate provides an additional level of security. This password is optional.	
adhaadha.	By choosing to protect your certificate with a password, any operation that requires access to the certificate's private key will require the specified password to continue.	
	Note - File based enrollments require the password used here to be re-entered when the approved certificate is imported.	
Sec.	Password:	
	Confirmation Password:	

4. Wählen Sie **File (Datei)** aus, um ein Zertifikat im PKCS #10-Format auf der Anmeldeseite anzufordern. Klicken Sie anschließend auf

CISCO SYSTEMS	 The enrollment wizard allows you to request a personal identity certificate from a Certificate Authority (CA). Network based enrollment allows you to connect directly to a CA over a network connection. File based enrollment will produce a certificate request file which you need to submit to your administrator. 	
	Please select the method you wish to proceed with: Enrollment type: Network Eile	
	<u>Back Next></u> Cancel Help	

5. Klicken Sie auf Durchsuchen, und geben Sie einen Dateinamen für die

Zertifikatsanforderungsdatei an. Wählen Sie als Dateityp die Option **PEM Encoded Request File (*.req)** aus, und klicken Sie auf



6. Klicken Sie auf der Seite "VPN Client Enrollment" auf

	To create an enrollment red type of file you wish to gene	quest file, please select tł erate.	ne
CISCO SYSTEMS	Contact your network admi which encoded file type is r	nistrator if you are not sui required.	re
	When you select a file externa associated file type will be a	ension in the Browse diald selected on this page.	og the
	<u>F</u> ile name: *		
	C:\My Documents\client5.	.req Brows	e)
	File type:		
	Base 64 encoded (.re	eq)	
	C Bjnary encoded (.p10	D)	
		* Required	Field
< B.	ack Next>	Cancel He	lo

7. Füllen Sie die Felder im Anmeldeformular aus.Dieses Beispiel zeigt die Felder:Common Name = User1Abteilung = IPSECCERT (Dies muss mit der Organisationseinheit (OU) und dem Gruppennamen im VPN 3000-Konzentrator übereinstimmen.)Unternehmen = Cisco SystemsState = NorthCarolinaLand = USAE-Mail = User1@email.comIP-Adresse = (optional) wird verwendet, um die IP-Adresse auf der Zertifikatsanforderung anzugeben.)Domain = cisco.comKlicken Sie abschließend auf

CISCO SYSTEMS	Enter your certificate e provided below.	enrollment information in the fields
authorauthora	Department (ou):	IPSECCERT
	Company (o):	Cisco Systems
	<u>S</u> tate (st):	NorthCarolina
	Co <u>u</u> ntry (c):	US
	<u>E</u> mail (e):	User1@email.com
	IP Address:	
	Do <u>m</u> ain:	cisco.com
	2	* Required Fie

8. Klicken Sie auf **Fertig stellen**, um mit der Registrierung fortzufahren.

Enrollment - Summary	
CISCO SYSTEMS	This is a summary of the information you have provided for this certificate enrollment request. Select Finish to proceed with the enrollment or Back to make modifications.
	Enrollment: File - client5.reg Certificate Store: Cisco Common Name: User1 Department: IPSECCERT Company: Cisco Systems State: NorthCarolina Country: US Email: User1@email.com IP Address: Domain: cisco.com
</th <th>Back Finish Cancel Help</th>	Back Finish Cancel Help

9. Wählen Sie die Registerkarte Registrierungsanfragen aus, um die Anforderung im VPN Client Certificate Manager zu

Cisco Systems VPN Client Certific	
re signed by a certificate authority.	pie and hosts you communicate with an
certificate authority (CA) is an organiza	ation that issues certificates.
nrollment requests are certificate reque	ests that a CA has yet to approve.
Personal Certificates CA Certificates	Enrollment Requests
Certificate	Store
User5	Request
	<u>Ω</u> ptions ▼

überprüfen.

- 10. Stellen Sie den CA-Server (Certification Authority) und die VPN-Client-Schnittstellen gleichzeitig ein, um die Anfrage zu senden.
- 11. Wählen Sie Zertifikat anfordern aus, und klicken Sie auf Weiter auf dem CA-



- Server.
- 12. Wählen Sie Erweiterte Anforderung für die Art der Anfrage aus, und klicken Sie auf Weiter

Microsoft Certificate Services - Microsoft Internet Explorer	_ 6 >
Elle Edit Yew Favorites Iods Help	
Back Fronted Stop Refersh Home Search Favories History Mail Print	
Addess 🕘 http://192.168.2.50/cettorv/cettigus.asp	💌 🖓 Go 🛛 Linka ?
	2
Microsoft Certificate Services - win2kserver	Home
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request.	
Web Browser Centificate	
E-Mail Protection Certificate	
L	
Advanced request	
	Next >
	-

13. Wählen Sie unter Erweiterte Zertifikatsanforderungen eine unter Base64 verschlüsselte PKCS #10-Datei oder eine Verlängerungsanfrage unter Verwendung einer Base64kodierten PKCS #7-Datei einreichen aus, und klicken Sie dann auf Weiter.

Miccosoft Certificate Services - Microsoft Internet Explorer	- 6 >
Ele Edit View Favorites Tools Help	
Hand Fronted Stop Refersh Home Search Favories History Mail Print	
Address 🙋 http://192.168.2.50/cettorv/cettrgad.asp	▼ 🖓 Go Links
entrane centrale centres - weignerve	TENIOR
Advanced Certificate Requests	
/ou can request a certificate for yourself, another user, or a computer using one of the following methods authority (CA) will determine the certificates that you can obtain.	s. Note that the policy of the certification
 Submit a certricate request to this CA using a form. 	
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a b	ase64 encoded PKCS #7 file.
C Request a certificate for a smart card on behalt of another user using the Smart Card Enrollment Sta You must have an enrollment agent certificate to submit a request for another user.	ation.
	Next>
Done	🔮 Internet

14. Markieren Sie die VPN Client-Anforderungsdatei, und fügen Sie sie unter "Gespeicherte Anforderung" auf den CA-Server ein. Klicken Sie anschließend auf **Senden**.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	. 8 ×
Elle Edit View Fgvorkes Icols Help	
Sack Fronter Stop Refeets Home Search Favorites History Mail Pint	
Address @ http://192.168.2.50/cettorv/cettigit.asp	¥ ∂Go j Links *
	<u>×</u>
Microsoft Cadificate Services - wezkserver	Hame
Submit A Saved Request	
Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an extension server) into the request field to submit the request to the certification authority (CA). Saved Request Base64 Encoded Certificate Request TELIAbc61UEBbRCdIM#xDARDgrbVQDFAdbyYIL02300 BQ6WDQYDVQQKFA2bbBRCdIM#xDARDgrbVDAcTC62y Certificate Request TELIAbc61UEBbRCdIM#xDARDgrbVDAcTC62y Certificate Request TELIAbc61UEBbRCdIM#xDARDgrbVDAcTC62y Certificate Request TELIAbc61UEBbRCdIM#xDARDgrbVDAcTC62y Base64 Encoded Bcowrag for a file to insert. Browrag for a file to insert.	emal application (such as a web
Additional Attributes:	
Attributes:	
	Submit >
a) Dove	-

15. Stellen Sie auf dem CA-Server das Identitätszertifikat für die VPN-Client-Anforderung

Tree	Request ID Bina	ry Request	Request Dis	position Message	Request Submission D	ate Requester Name	Request Country
Certification Authority (Local) Frahm-pc Revolved Certificates Sisued Certificates Pending Requests Failed Requests	257 and a	BEGIN NE AI Rof Hol	Taka Inde Tasks P resh P	Isue Deny	3)23/2001 9:13 AM	GHOST2KJUSR_	US

16. Laden Sie die Root- und Identitätszertifikate auf den VPN-Client herunter. Wählen Sie auf dem CA-Server die Option Auf ausstehendem Zertifikat prüfen aus, und klicken Sie dann auf

Weiter.	
Microsoft Certificate Services - jfrahim-pc	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other so will be able to securely identify yourself to other people over the web, sign your e-mail mes- depending upon the type of certificate you request.	ecure program. Once you acquire a certificate, you sages, encrypt your e-mail messages, and more
Select a task:	
C Retrieve the CA certificate or certificate revocation list	
Check on a pending certificate	
	Next>

17. Wählen Sie Base 64-verschlüsselt aus. Klicken Sie dann auf Zertifizierungsstellenzertifikat herunterladen auf dem CA-

Server.

Microsoft Certificate Services - jfrahim-pc					Home
Certificate Issued					
The certificate you requested was issue	d to you.				
C DER encoded or C Ba Download CA certificate Download CA certification	٠	100			
	Saving centrew o	Col Darkton			<u>?ix</u>
	Estimated Download Transfer it Close1	My Documents My Computer My Network Places Cases Jazb			
	My Lonputer	File name: client_cert	cer-		Save
		Save as type: Security C	ertificate	-	Cancel

18. Wählen Sie eine Datei aus, die Sie von der Seite Zertifikat oder Zertifikatswiderrufliste abrufen möchten, um das Stammzertifikat auf dem CA-Server abzurufen. Klicken Sie anschließend auf

Microsoft Certific	cate Services - jfrahim-pc		ne en e					Heme
Retrieve The C	CA Certificate Or Certification path to allow	ficate Rev	ocation List	artificatas issi	ued from this c	entification	authority	
t is not necessa because the C/ Choose file to	ary to manually install th A certification path will the download:					licate from	n this certificatio	n authority
CA Cerbficate:	Current [frehim-pc(2)] Previous [frehim-pc(1)] Previous [frehim-pc] C DER encoded or Download CA certifica Download CA certifica Download latest certific	certnew.cor	Save As Save in: Save in: History History Desktop My Documents	My Documents My Documents My Computer My Network Pla Cases Jacb Vpn Client_cert.cer	aces	J	+ = -	212
			Ny Computer	File name Save as type:	Client_root_cert.cer Security Certificate	6	-	Save Cancel

19. Wählen Sie Certificate Manager > CA Certificate > Import on the VPN Client aus, und wählen Sie dann die Root CA-Datei aus, um die Root- und Identitätszertifikate zu installieren.

	Open	? X
ization that issues certificates. uests that a CA has yet to approve.	Look in: M Desktop	 3-
s Enrolment Requests Store	My Computer Client_root_cert.cer My Network Places Cases Cases Cases Vpn Vpn	
CISCO SYSTEMS	File name: client_root_cert.cer Files of type: X.509 DER Files (*.der;*.cer) osoft certificate:)pen ancel
File:	Browse	
< Back	Next > Cancel Help	

20. Wählen Sie **Zertifikatsmanager > Persönliche Zertifikate > Importieren aus**, und wählen Sie die Identitätszertifikatdatei

Import Certif	icate - Source	
	The certificate source identifies where the origination of the certificate imported from. Additionally, if the certificate importing is protected by a password, pleas below. Certificate source: Microsoft certificate: File: Import password:	eertificate is you are e enter it Browse
Open ^{ti} Look in:	Back Next> Cancel	Help ? 2
Open Look in: My Docu My Comp My Netw Cases jazib ypn	Back Next> Cancel Cancel Desktop Center Cient_cert.cer Couter Cient_root_cert.cer Cork Places	Help ?
Dpen Look in: My Docu My Comp My Netw Cases jazib ypn File name:	Back Next > Cancel Desktop ments client_cert.cer outer client_root_cert.cer	Help ?

21. Stellen Sie sicher, dass das Identitätszertifikat auf der Registerkarte "Persönliche Zertifikate" angezeigt

are signed by a certificate a	uthority.
A certificate authority (CA) is	s an organization that issues certificates.
Enrollment requests are cert	inicate requests that a CA has yet to approve.
Personal Certificates CA	Certificates Enrollment Requests
Certificate	Store
User5	Cisco

22. Stellen Sie sicher, dass das Stammzertifikat auf der Registerkarte Zertifizierungsstellen angezeigt

ares	signed by a certific	ate authority.	e and nosis you co	
A ce	rtificate authority (I	CA) is an organizal	ion that issues cert	ificates.
Enro	Ilment requests are	e certificate reques	sts that a CA has ye	et to approve.
Per	rsonal Certificates	CA Certificates	Enrollment Beque	oto
	Condi Contined(63		enrollment rieque	
	Certificate		Store	
i	jfrahim-pc		CA	

<u>Überprüfen</u>

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Wenn Sie versuchen, sich beim Microsoft CA Server anzumelden, kann diese Fehlermeldung generiert werden.

Initiating online request Generating key pair Generating self-signed Certificate Initiating online request Received a response from the CA Your certificate request was denied Wenn Sie diese Fehlermeldung erhalten, finden Sie weitere Informationen in den Microsoft CA-Protokollen oder in diesen Ressourcen.

- Windows kann keine Zertifizierungsstelle finden, die die Anforderung verarbeitet.
- XCCC: Wenn Sie ein Zertifikat für sichere Konferenzen anfordern, wird die Fehlermeldung "Ihre Zertifikatsanforderung wurde abgelehnt" angezeigt.

Zugehörige Informationen

- IPsec-Aushandlung/IKE-Protokolle
- <u>Technischer Support und Dokumentation Cisco Systems</u>