

ASA/PIX 7.x- und VPN-Client IPSec-Authentifizierung mithilfe digitaler Zertifikate mit Microsoft CA - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Zugehörige Produkte](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfigurationen](#)

[ASA-Konfiguration](#)

[ASA-Konfigurationsübersicht](#)

[VPN-Client-Konfiguration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie ein digitales Zertifikat eines Drittanbieters manuell auf der Cisco Security Appliance (ASA/PIX) 7.x sowie auf VPN-Clients installieren, um die IPSec-Peers beim Microsoft Certificate Authority (CA)-Server zu authentifizieren.

Voraussetzungen

Anforderungen

Für dieses Dokument benötigen Sie Zugriff auf eine Zertifizierungsstelle (Certificate Authority, CA), um sich für Zertifikate zu registrieren. Zu den unterstützten Drittanbieter von CA gehören Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA und VeriSign.

Hinweis: In diesem Dokument wird Windows 2003 Server als CA-Server für dieses Szenario verwendet.

Hinweis: In diesem Dokument wird davon ausgegangen, dass die ASA/PIX keine bereits vorhandene VPN-Konfiguration enthält.

Verwendete Komponenten

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

- ASA 5510 mit Softwareversion 7.2(2) und ASDM Version 5.2(2).
- VPN-Client, auf dem die Softwareversion 4.x und höher 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.

Zugehörige Produkte

Die ASA-Konfiguration kann auch mit dem Cisco PIX der Serie 500 verwendet werden, auf dem die Softwareversion 7.x ausgeführt wird.

Konventionen

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

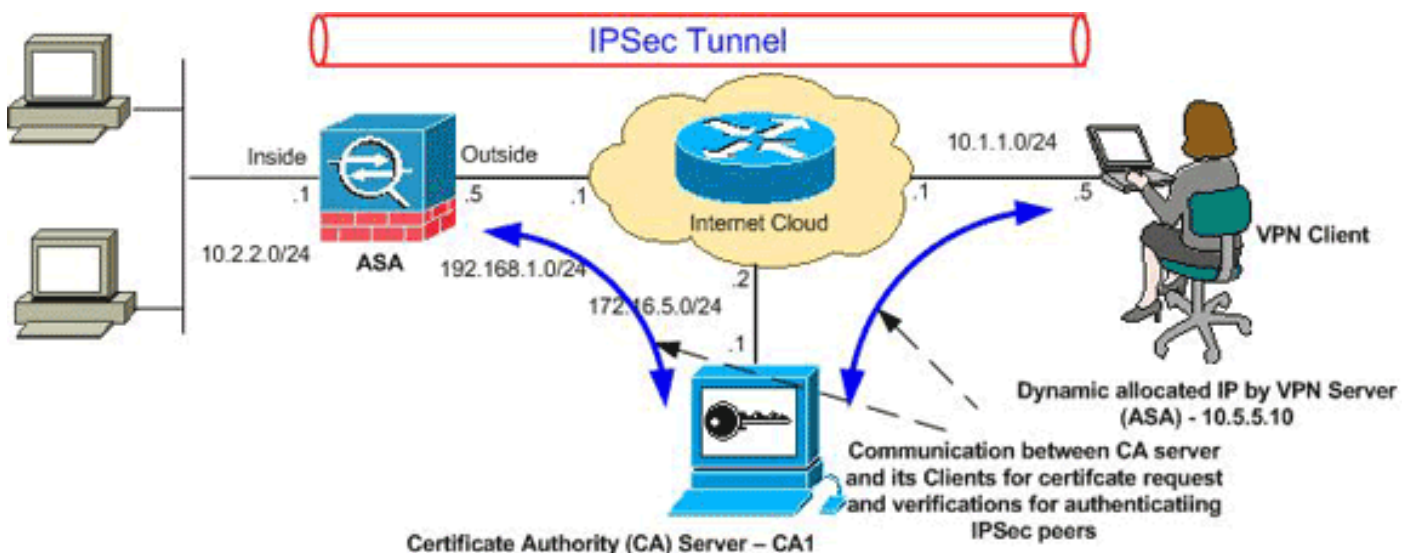
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht

rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- [ASA-Konfiguration](#)
- [ASA-Konfigurationsübersicht](#)
- [VPN-Client-Konfiguration](#)

ASA-Konfiguration

Gehen Sie wie folgt vor, um ein digitales Zertifikat eines Drittanbieters auf der ASA zu installieren:

[Schritt 1: Überprüfen der Genauigkeit der Werte für Datum, Uhrzeit und Zeitzone](#)

[Schritt 2: Generieren des RSA-Schlüsselpaars](#)

[Schritt 3: Erstellen Sie den Trustpoint.](#)

[Schritt 4: Generieren Sie die Zertifikatsregistrierung.](#)

[Schritt 5: Authentifizierung des Trustpoints](#)

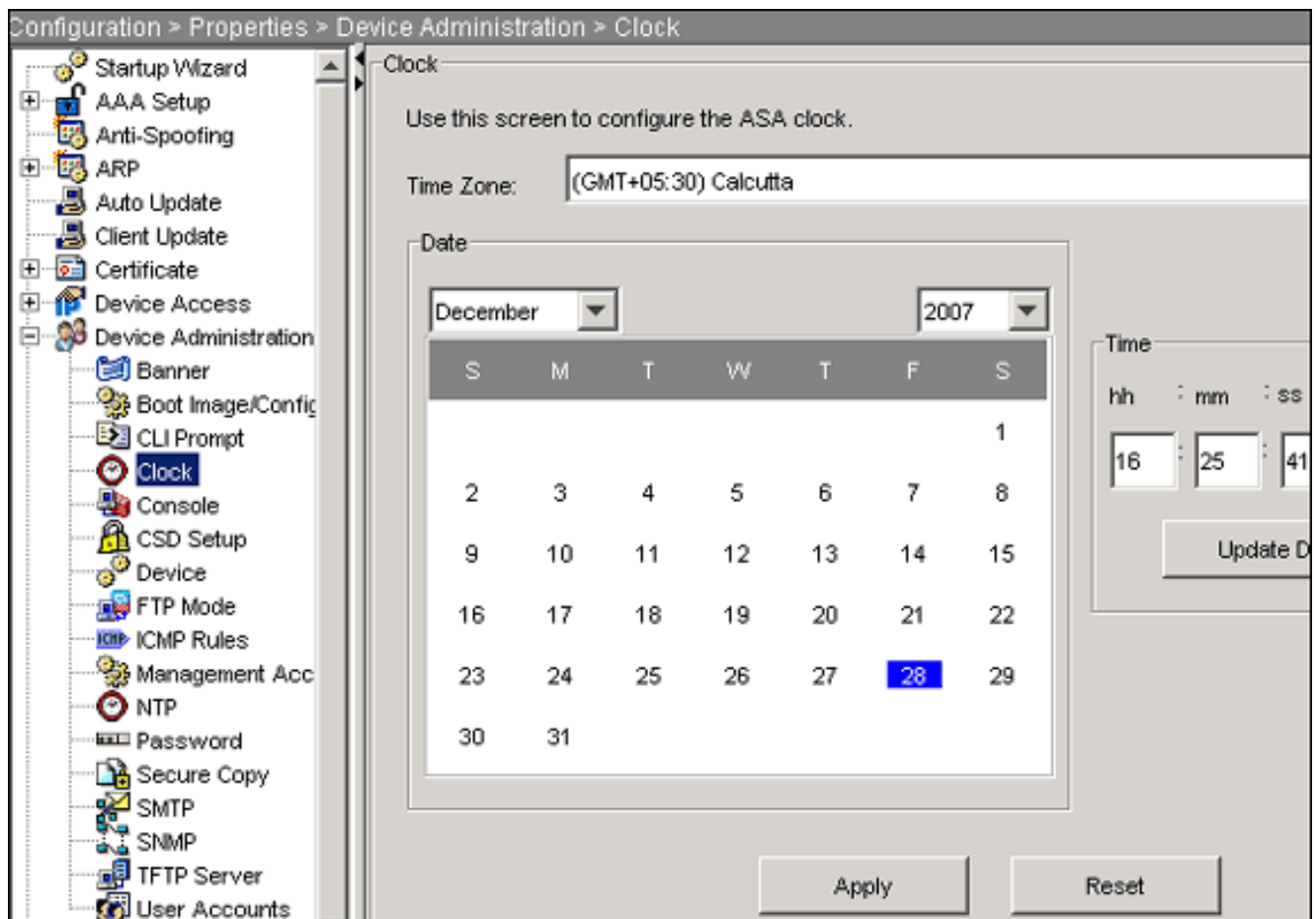
[Schritt 6: Installieren des Zertifikats](#)

[Schritt 7: Konfigurieren von Remote Access VPN \(IPSec\) zur Verwendung des neu installierten Zertifikats](#)

[Schritt 1: Überprüfen der Genauigkeit der Werte für Datum, Uhrzeit und Zeitzone](#)

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Device Administration (Geräteverwaltung)**, und wählen Sie **Clock** aus.
3. Überprüfen der Richtigkeit der angegebenen InformationenDie Werte für Datum, Uhrzeit und Zeitzone müssen genau sein, damit eine ordnungsgemäße Zertifikatsvalidierung erfolgt.



Befehlszeilenbeispiel

```

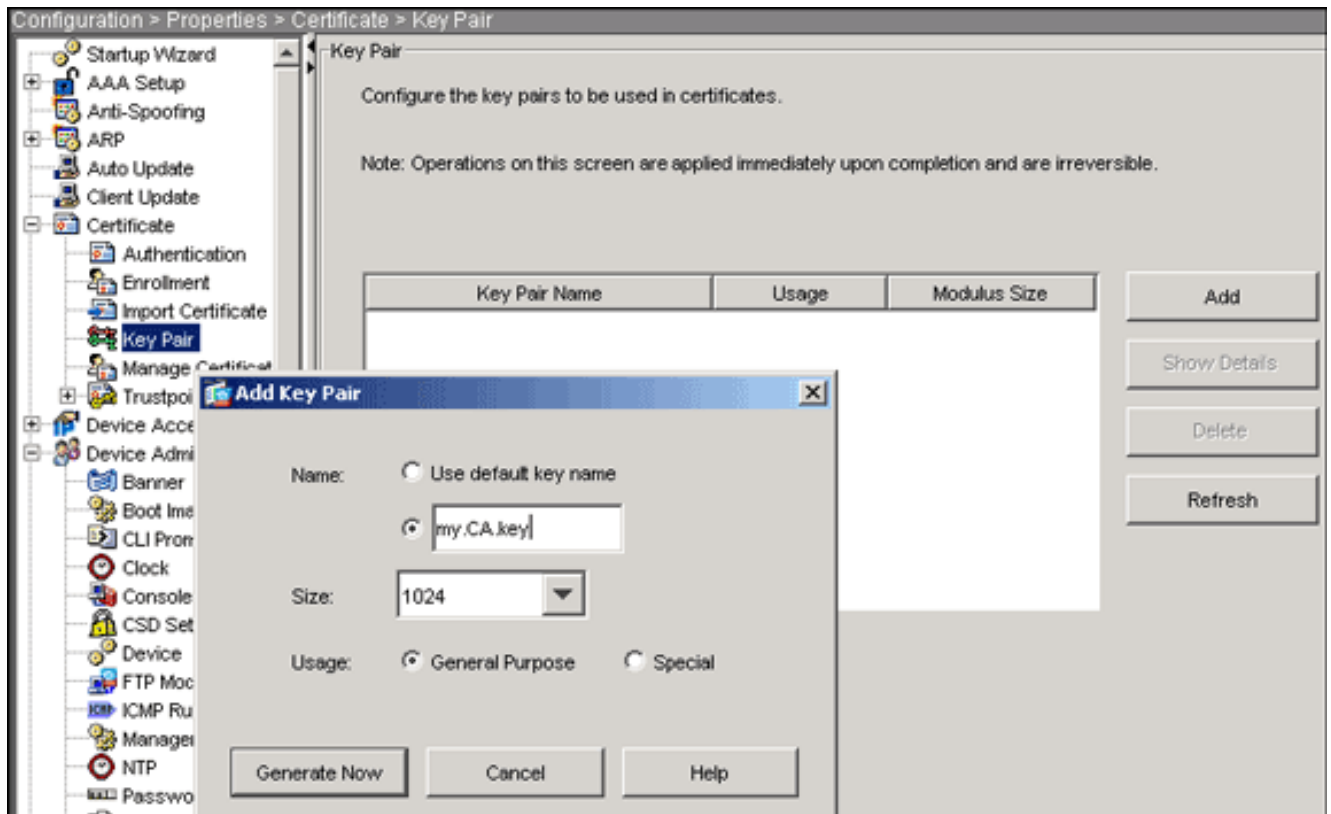
CiscoASA
-----
CiscoASA#show clock
16:25:49.580 IST Fri Dec 28 2007
  
```

[Schritt 2: Generieren des RSA-Schlüsselpaars](#)

Der generierte öffentliche RSA-Schlüssel wird mit den Identitätsinformationen der ASA kombiniert, um eine PKCS#10-Zertifikatsanforderung zu erstellen. Sie sollten den Schlüsselnamen deutlich mit dem Trustpoint identifizieren, für den Sie das Schlüsselpaar erstellen.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Schlüsselpaar aus**.
3. Klicken Sie auf **Hinzufügen**.



4. Geben Sie den Schlüsselnamen ein, wählen Sie die Modulusgröße aus, und wählen Sie den Verwendungsart aus. **Hinweis:** Die empfohlene Schlüsselpaargröße ist 1024.
5. Klicken Sie auf **Jetzt generieren**. Das von Ihnen erstellte Schlüsselpaar sollte in der Spalte Key Pair Name (Name des Schlüsselpaars) aufgeführt werden.

Befehlszeilenbeispiel

```

CiscoASA
-----
CiscoASA#configure terminal
CiscoASA(config)#crypto key generate rsa label my.CA.key
modulus 1024

!--- Generates 1024 bit RSA key pair. "label" defines
the name of the key pair. INFO: The name for the keys
will be: my.CA.key Keypair generation process begin.
Please wait... ciscoasa(config)#

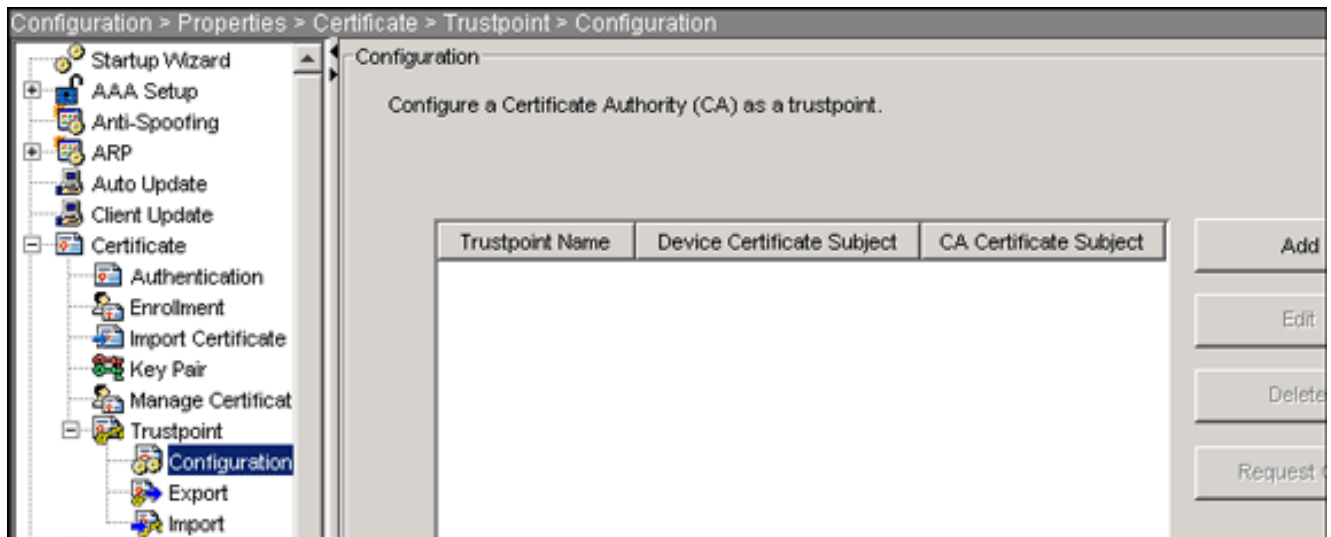
```

Schritt 3: Erstellen Sie den Trustpoint.

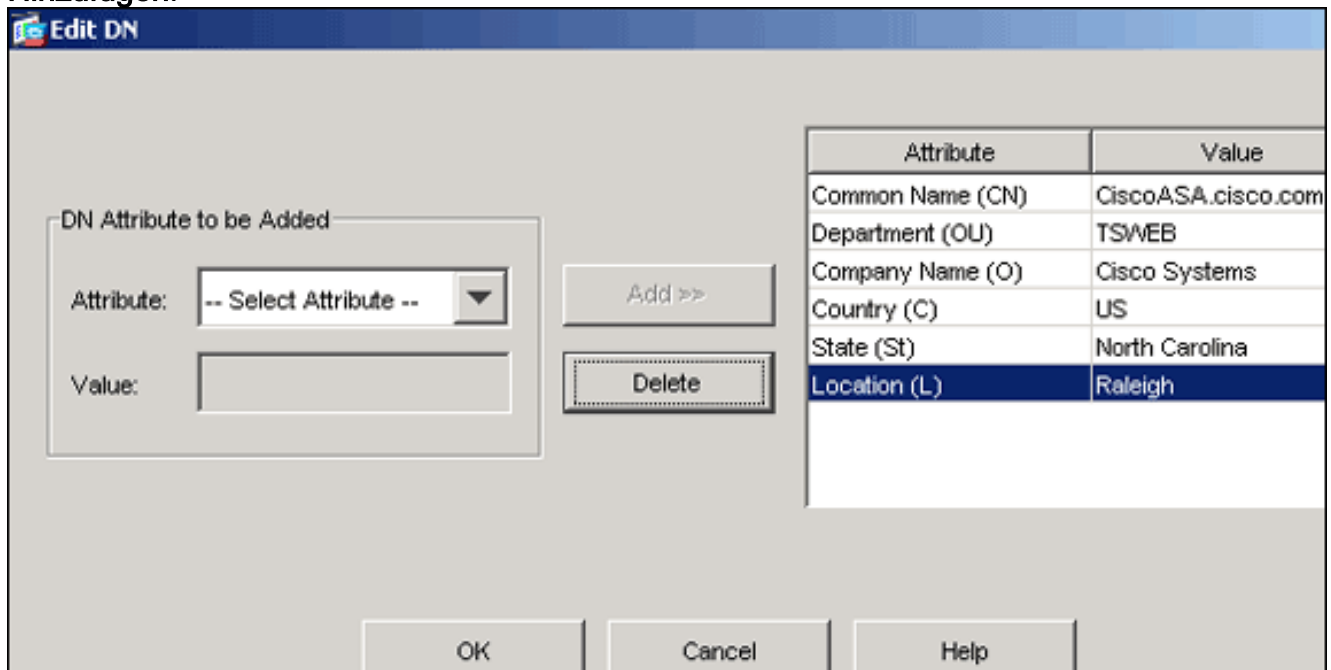
Trustpoints sind erforderlich, um die Zertifizierungsstelle (Certificate Authority, CA) zu deklarieren, die von Ihrer ASA verwendet wird.

ASDM-Verfahren

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Certificate**, und erweitern Sie dann **Trustpoint**.
3. Wählen Sie **Konfiguration aus**, und klicken Sie dann auf **Hinzufügen**.



4. Konfigurieren Sie die folgenden Werte:**Trustpoint-Name:** Der Trustpoint-Name sollte für die beabsichtigte Verwendung relevant sein. (In diesem Beispiel wird *CA1* verwendet.)**Schlüsselpaar:** Wählen Sie das in [Schritt 2](#) generierte Schlüsselpaar aus. (my.CA.key)
5. Stellen Sie sicher, dass die Option Manuelle Anmeldung ausgewählt ist.
6. Klicken Sie auf **Zertifikatsparameter**.Das Dialogfeld Zertifikatparameter wird angezeigt.
7. Klicken Sie auf **Bearbeiten**, und konfigurieren Sie die in dieser Tabelle aufgelisteten Attribute:Um diese Werte zu konfigurieren, wählen Sie in der Dropdown-Liste Attribute einen Wert aus, geben Sie den Wert ein, und klicken Sie auf **Hinzufügen**.



8. Klicken Sie nach dem Hinzufügen der entsprechenden Werte auf **OK**.
9. Geben Sie im Dialogfeld Zertifikatsparameter im Feld FQDN angeben den FQDN ein.Dieser Wert sollte der gleiche FQDN sein, den Sie für den Gemeinsamen Namen (CN) verwendet

Certificate Parameters

Enter the values for the parameters that are to be included in the certificate.

Subject DN:

Subject Alternative Name (FQDN)

Use FQDN of the device

Specify FQDN

Use none

E-mail:

IP Address:

Include device serial number

haben.

10. Klicken Sie auf **OK**.
11. Überprüfen Sie, ob das richtige Schlüsselpaar ausgewählt ist, und klicken Sie auf das Optionsfeld **Manuelle Anmeldung verwenden**.
12. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Add Trustpoint Configuration

Trustpoint Name:

Generate a self-signed certificate on enrollment
 If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP

Key Pair: Show Details New Key Pair...

Challenge Password: Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint

Enrollment Mode

Use manual enrollment

Use automatic enrollment

Enrollment URL: http://

Retry Period: minutes

Retry Count: (Use 0 to indicate unlimited retries)

Certificate Parameter

OK Cancel Help

Befehlszeilenbeispiel

```

CiscoASA
-----
CiscoASA(config)#crypto ca trustpoint CA1

!--- Creates the trustpoint. CiscoASA(config-ca-
trustpoint)#enrollment terminal

!--- Specifies cut and paste enrollment with this
trustpoint. CiscoASA(config-ca-trustpoint)#subject-name
CN=wepvpn.cisco.com,OU=TSWEB,
O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh

!--- Defines x.500 distinguished name. CiscoASA(config-

```



```
ca-trustpoint)#keypair my.CA.key

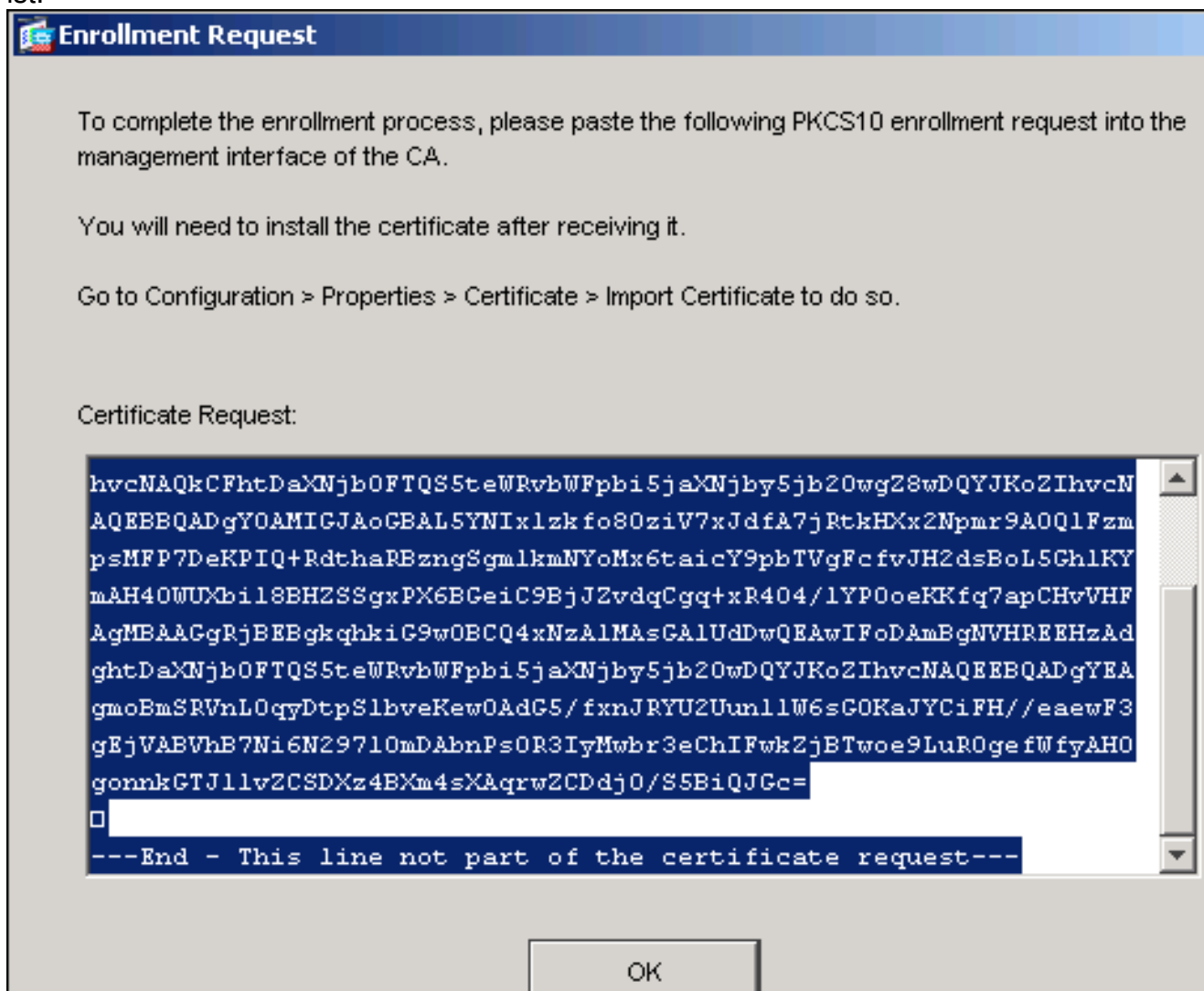
!--- Specifies key pair generated in Step 2.
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com

!--- Specifies subject alternative name (DNS:).
CiscoASA(config-ca-trustpoint)#exit
```

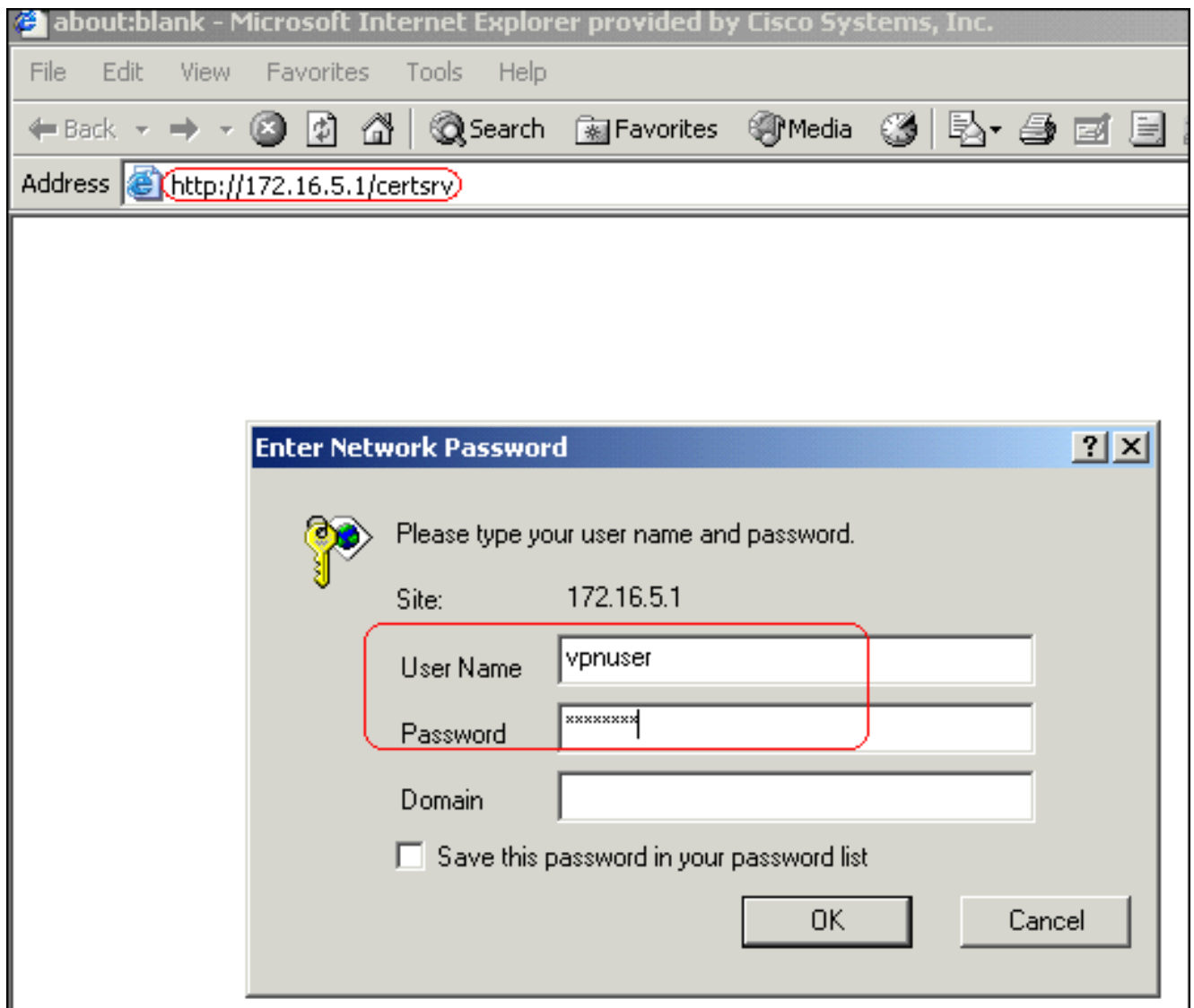
Schritt 4: Generieren der Zertifikatsregistrierung

ASDM-Verfahren

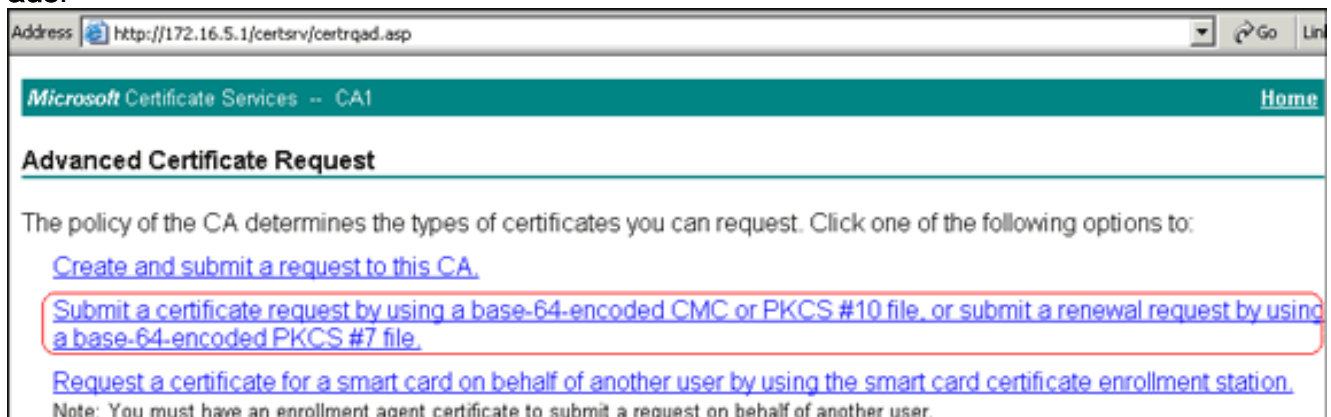
1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Registrierung** aus.
3. Überprüfen Sie, ob der in [Schritt 3](#) erstellte Trustpoint ausgewählt ist, und klicken Sie auf **Registrieren**. Es wird ein Dialogfeld angezeigt, in dem die Anforderung für die Zertifikatsregistrierung (auch als Zertifikatssignierungsanfrage bezeichnet) aufgeführt ist.



4. Kopieren Sie die PKCS#10-Registrierungsanfrage in eine Textdatei und senden Sie die gespeicherte CSR an Ihren Drittanbieter (z. B. Microsoft CA), wie in diesem Verfahren gezeigt: Melden Sie sich beim CA-Server 172.16.5.1 an, wobei die dem VPN-Server bereitgestellten Benutzerkredite bereitgestellt werden.



Hinweis: Stellen Sie sicher, dass Sie über ein Benutzerkonto für ASA (VPN-Server) mit dem CA-Server verfügen. Klicken Sie auf **Zertifikat anfordern > Erweiterte Zertifikatsanforderung**, und wählen Sie dann **eine Zertifikatsanforderung mit einer Base-64-codierten CMC- oder PKCS#10-Datei einreichen** oder eine Verlängerungsanfrage mit einer Base-64-codierten PKCS#7-Datei einreichen aus.



Kopieren Sie die verschlüsselten Informationen, fügen Sie sie in das Textfeld **Gespeicherte Anforderung ein**, und klicken Sie auf **Senden**.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded certificate request (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
lvQVNBmNpc2NvLmNvbTANBgkqhkiG9w0BAQFAAQ...  
4BfcXd20LCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8...  
D6MEG6cu7Bxj/K1Z6MxafUvCHROPYWVU1wgRJGh+...  
t8Ux9emhFHpGHnQ/MpSfUOdQ==
```

not part of the certificate request---

[Browse for a file to insert.](#)

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Submit >

Klicken

Sie auf das Optionsfeld **Base 64-verschlüsseltes** Zertifikat, und klicken Sie auf **Zertifikat**

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



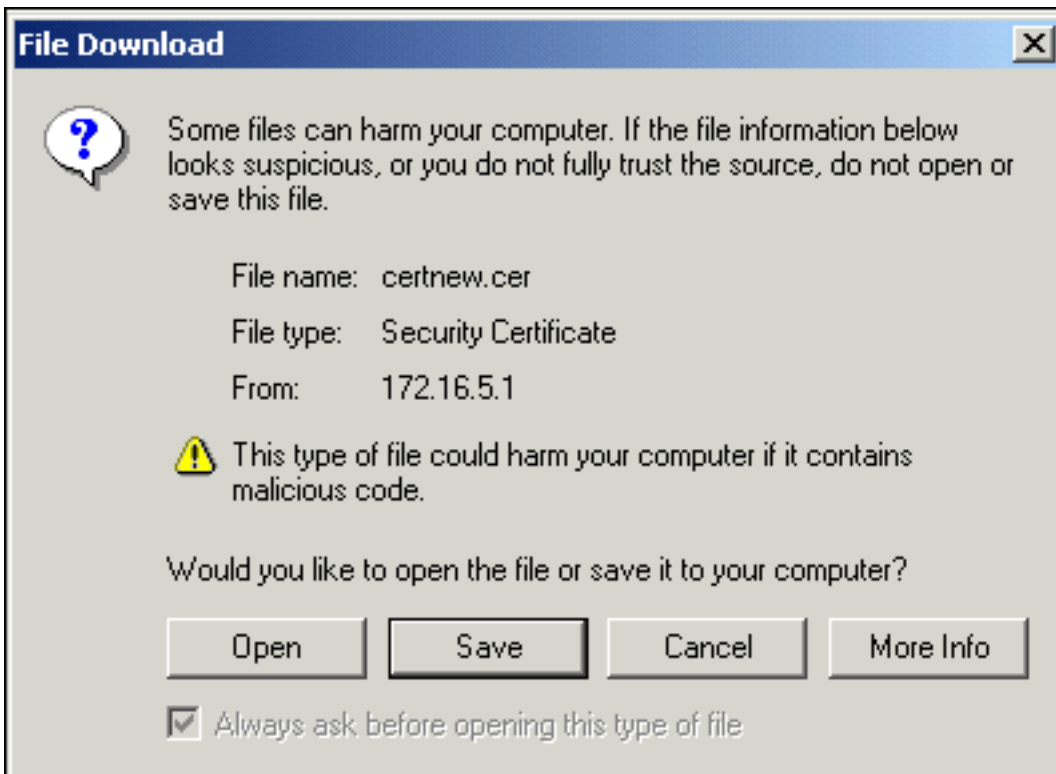
[Download certificate](#)

[Download certificate chain](#)

herunterladen.

Wenn

n das Dialogfeld Dateidownload angezeigt wird, speichern Sie es mit dem Namen **cert_client_id.cer**, dem Identitätszertifikat, das auf der ASA installiert werden



soll.

Befehlszeilenbeispiel

```

CiscoASA
CiscoASA(config)#crypto ca enroll CA1

!--- Initiates CSR. This is the request to be submitted
!--- via web or email to the 3rd party vendor. % Start
certificate enrollment .. % The subject name in the
certificate will be: CN=CiscoASA.cisco.com,OU=TSWEB,
O=Cisco Systems,C=US,St=North Carolina,L=Raleigh % The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: no

!--- Do not include the device's serial number in the
subject. Display Certificate Request to terminal?
[yes/no]: yes

!--- Displays the PKCS#10 enrollment request to the
terminal. !--- You will need to copy this from the
terminal to a text !--- file or web text field to submit
to the 3rd party CA. Certificate Request follows:
MIICHjCCAYcCAQAwwgAaxEDAObgNVBAcTB1JhbGVpZ2gxZzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxmFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBdfBSsejDOnBpFYzKsGf7TUMQB2m2RfaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw

```

```
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKulaRc783w4BMO5lulIEhHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5Q1Kx2Y/vrqs+Hg5SLHpbhj/
Uo13yWce 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no
ciscoasa(config)#
```

Schritt 5: Authentifizierung des Trustpoints

Sobald Sie das Identitätszertifikat des Fremdherstellers erhalten haben, können Sie mit diesem Schritt fortfahren.

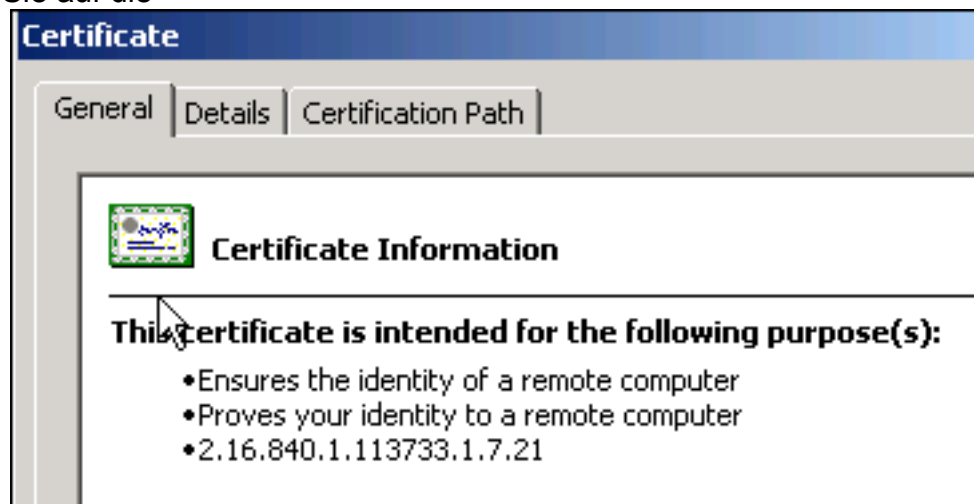
ASDM-Verfahren

1. Speichern Sie das Identitätszertifikat auf Ihrem lokalen Computer.
2. Wenn Ihnen ein Base64-kodiertes Zertifikat bereitgestellt wurde, das nicht als Datei geliefert wurde, müssen Sie die base64-Nachricht kopieren und in eine Textdatei einfügen.
3. Benennen Sie die Datei mit der Erweiterung .cer um. **Hinweis:** Sobald die Datei mit der Erweiterung .cer umbenannt wurde, sollte das Dateisymbol wie gezeigt als Zertifikat



angezeigt werden.

4. Doppelklicken Sie auf die

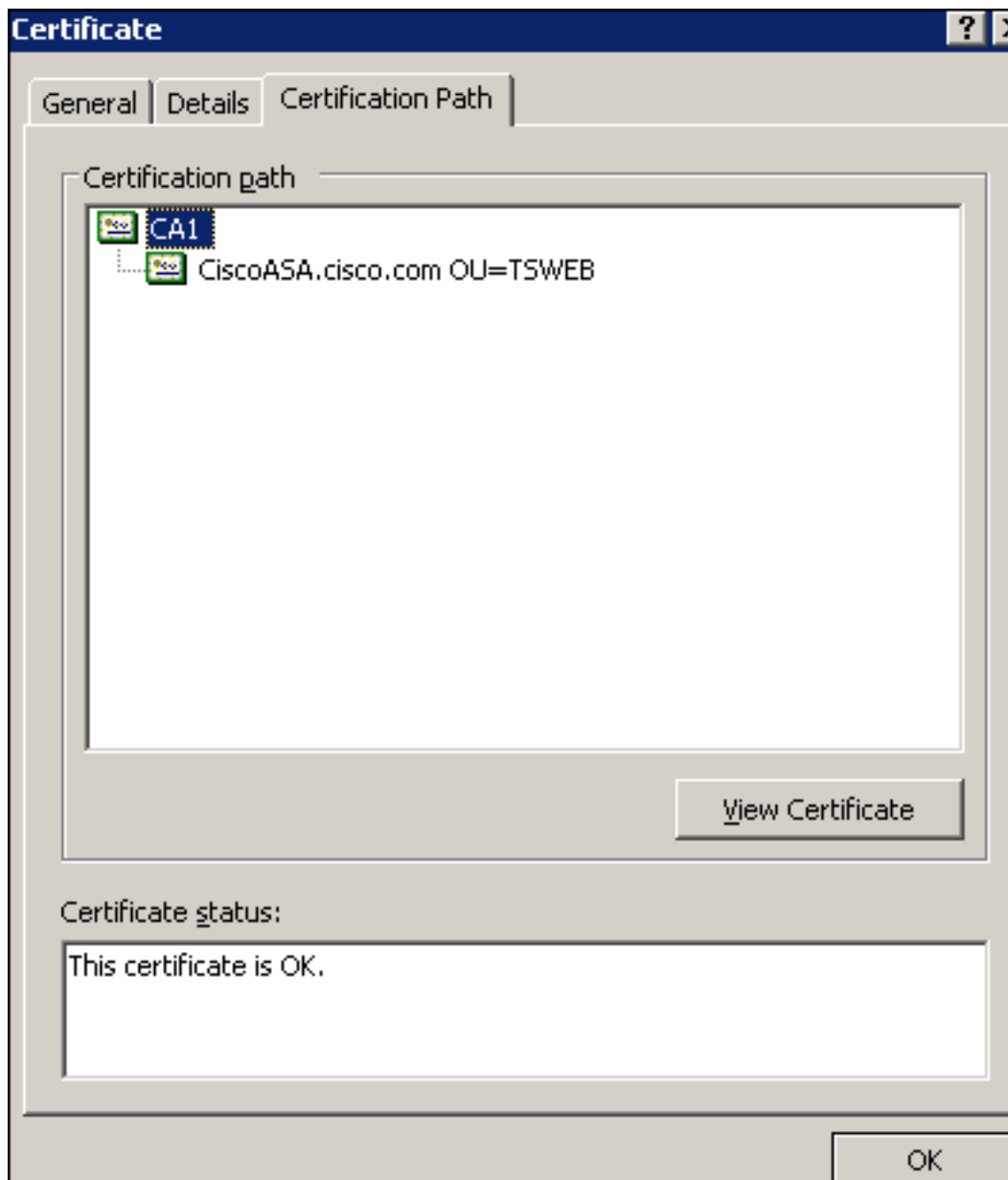


Zertifikatsdatei.

Hinweis:

Wenn die Meldung "Windows verfügt nicht über genügend Informationen, um dieses Zertifikat zu überprüfen" auf der Registerkarte "Allgemein" angezeigt wird, müssen Sie das Root-CA- oder Zwischenzertifikat des Fremdherstellers abrufen, bevor Sie mit diesem Verfahren fortfahren. Wenden Sie sich an Ihren Fremdhersteller oder CA-Administrator, um das ausstellende Root-CA- oder Zwischenzertifikat zu erhalten.

5. Klicken Sie auf die Registerkarte **Zertifikatspfad**.
6. Klicken Sie auf das Zertifizierungsstellenzertifikat oberhalb Ihres ausgestellten Identitätszertifikats, und klicken Sie auf **Zertifikat**

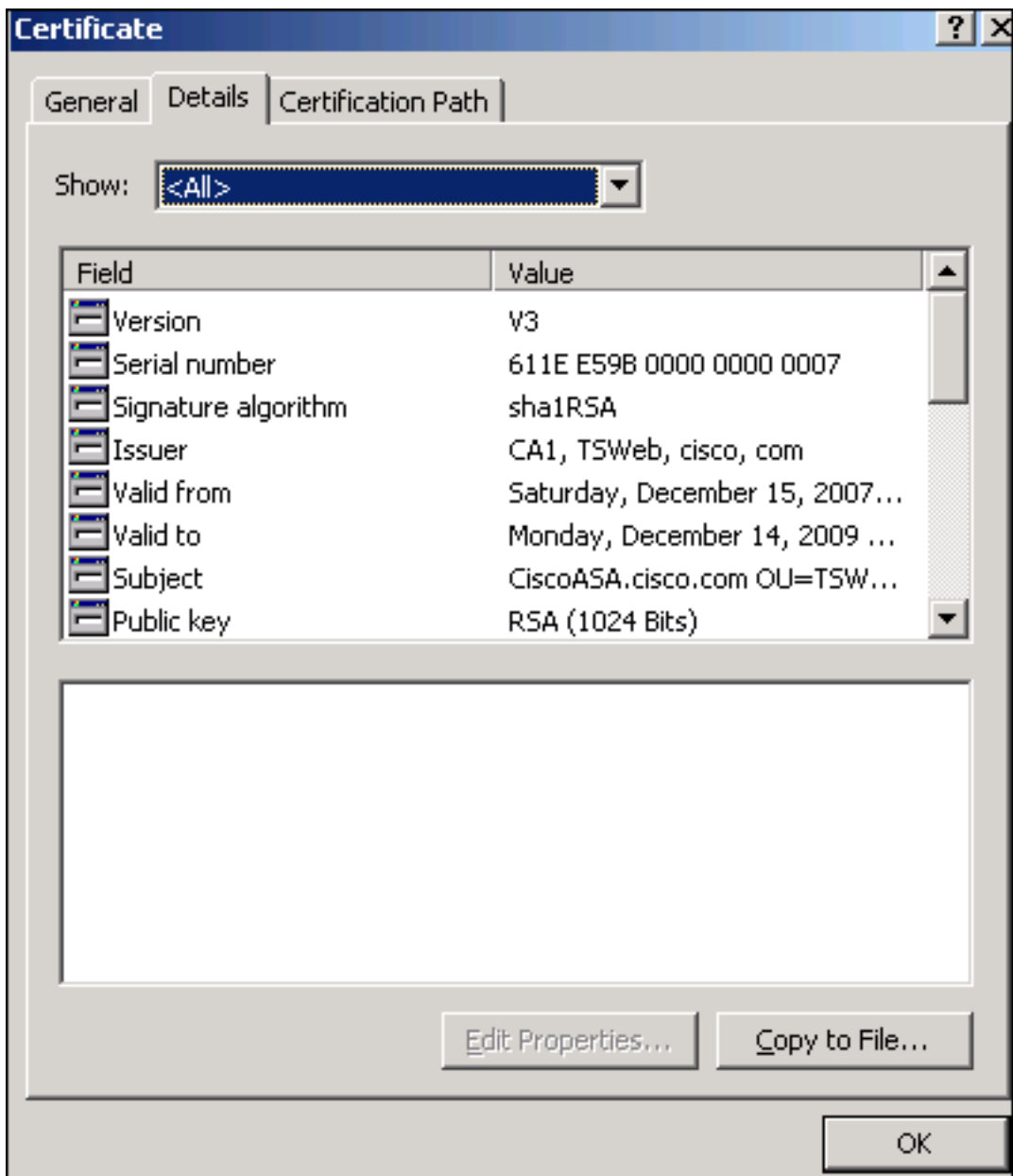


anzeigen.

Detaillier

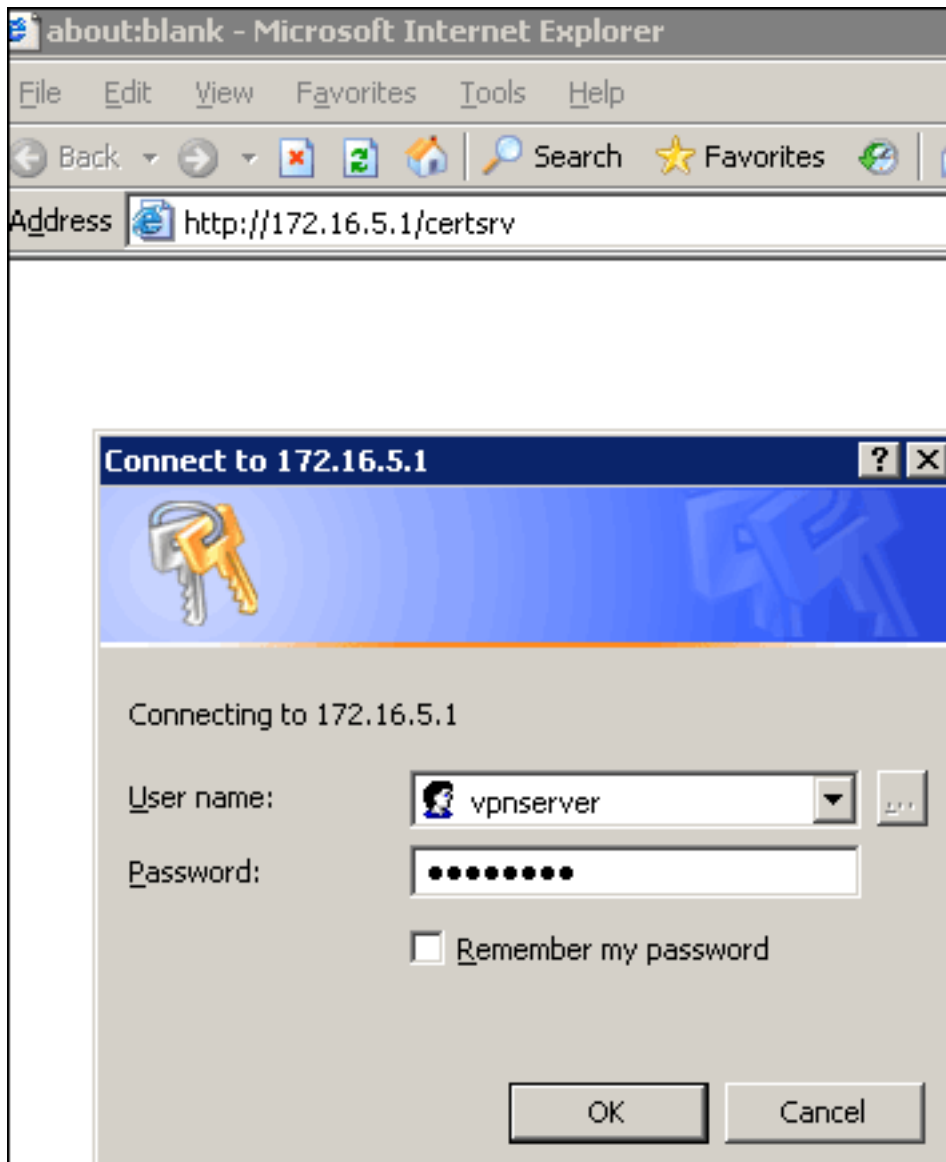
te Informationen zum Zertifizierungsstellenzertifikat werden angezeigt.

7. Klicken Sie auf **Details**, um weitere Informationen zum Identitätszertifikat zu



erhalten.

8. Bevor Sie das Identitätszertifikat installieren, muss das Zertifizierungsstellenzertifikat vom CA-Server heruntergeladen und in der ASA installiert werden. Gehen Sie wie folgt vor, um das Zertifizierungsstellenzertifikat vom CA-Server mit dem Namen *CA1* herunterzuladen: Melden Sie sich beim CA-Server 172.16.5.1 an, wobei dem VPN-Server eigene Gutschriften zur Verfügung gestellt



werden.

Klicken Sie auf **Zertifizierungsstellenzertifikat, Zertifikatskette oder CRL herunterladen** und wählen Sie dann das Optionsfeld **Base 64** aus, um die Kodierungsmethode anzugeben. Klicken Sie auf das **Zertifikat CA** herunterladen.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
 Base 64

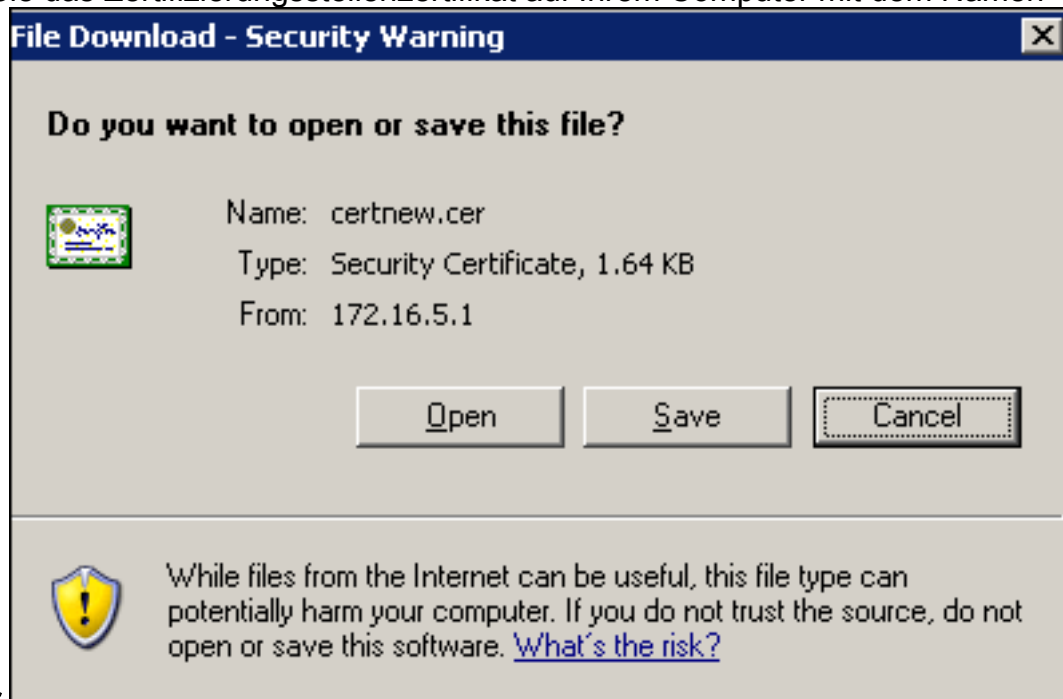
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Speichern Sie das Zertifizierungsstellenzertifikat auf Ihrem Computer mit dem Namen

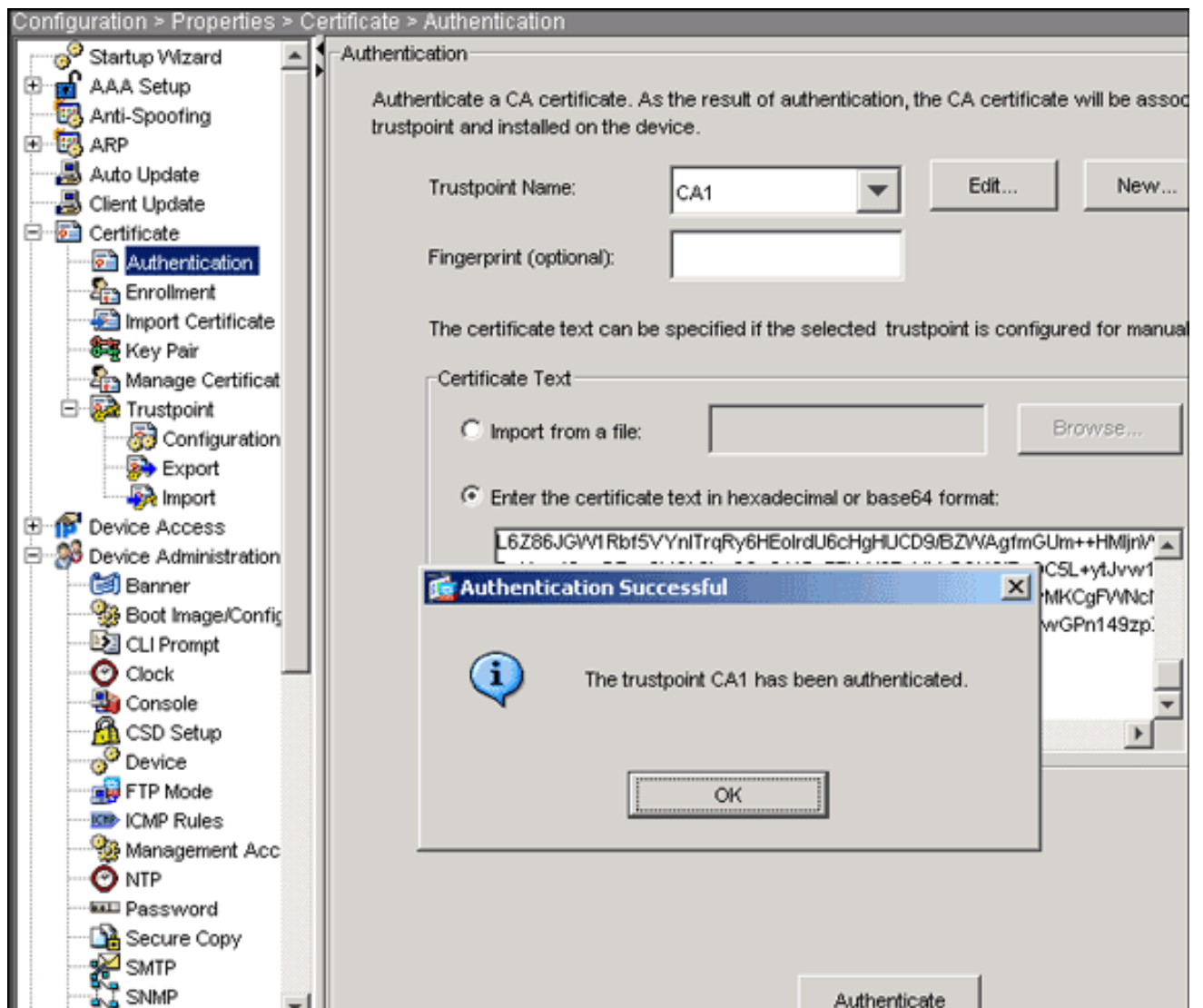


certnew.cer.

9. Navigieren Sie zu dem Speicherort, an dem Sie das Zertifizierungsstellenzertifikat gespeichert haben.
10. Öffnen Sie die Datei mit einem Texteditor, z. B. Notepad. (Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie **Senden an > Editor**.)
11. Die Base64-codierte Nachricht sollte ähnlich wie das Zertifikat in diesem Bild aussehen:

```
certnew.cer - Notepad
File Edit Format Help
-----BEGIN CERTIFICATE-----
MIIEntCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzy28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0XDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIXDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcqnwdoq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4u04xxQmr//Sct1tdwQcvk2V
UBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSSGAQQBgjCUAgQHgQAQwBBMAsGA1UdDwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ00ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZXk1MjBTZXJ2awNlcYxD
Tj1TZXJ2awNlcYxDTj1Db25mawd1cmF0aw9uLERDPVRTV2ViLERDPWNpc2NvLERD
PWNvbT9jZXJ0awZpY2F0ZVJldm9jYXRpb25maxN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNwh0dHA6Ly90cy13MmszLWFjcy50c3d1Yi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSsGAQQBgjcvAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5VynlTrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcnwxlQxsDT+n9Yok6bnG6uof4SgETNrN8EyyVrSGK0lE+OC5L+ytJvw19Gzh1ze
lOVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFWNCNItcufu0x1b
LXXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPN149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. Klicken Sie im ASDM auf **Konfiguration** und dann auf **Eigenschaften**.
13. Erweitern Sie **Zertifikat**, und wählen Sie **Authentifizierung** aus.
14. Klicken Sie auf das Optionsfeld **Zertifikatstext im Hexadezimal- oder Base64-Format eingeben**.
15. Fügen Sie das Base64-formatierte CA-Zertifikat aus dem Texteditor in den Textbereich ein.
16. Klicken Sie auf **Authentifizierung**.



17. Klicken Sie auf OK.

Befehlszeilenbeispiel

CiscoASA

```
CiscoASA(config)#crypto ca authenticate CA1
```

*!--- Initiates the prompt to paste in the base64 CA root
!--- or intermediate certificate. Enter the base 64
encoded CA certificate. End with the word "quit" on a
line by itself -----BEGIN CERTIFICATE-----*

```
MIIEntCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQGGRYDY29tMRUwEwYKZImiZPyLQGGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0EzMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgms
JomT8ixkARkWBWNpc2NvMRUwEwYKZImiZPyLQGGRYFVFNXZWIxDDAK
BgNVBAMT
A0NBMTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOUU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
```

```

cQnwdOq+
Kx+sWaeNCjs1rxeuahpIBTuaNOckueBUBjxgPJUNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wgwFrMBMGCSsGAQQBgjcUAQGHGQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTzrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMM1mJBLZXk1mJBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGw1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAghmGUm++HM1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGK0LE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNCNIt
cufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqT
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
quit

!--- Manually pasted certificate into CLI. INFO:
Certificate has the following attributes: Fingerprint:
98d66001 f65d98a2 b455fbce d672c24a Do you accept this
certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

% Certificate successfully imported
CiscoASA(config)#

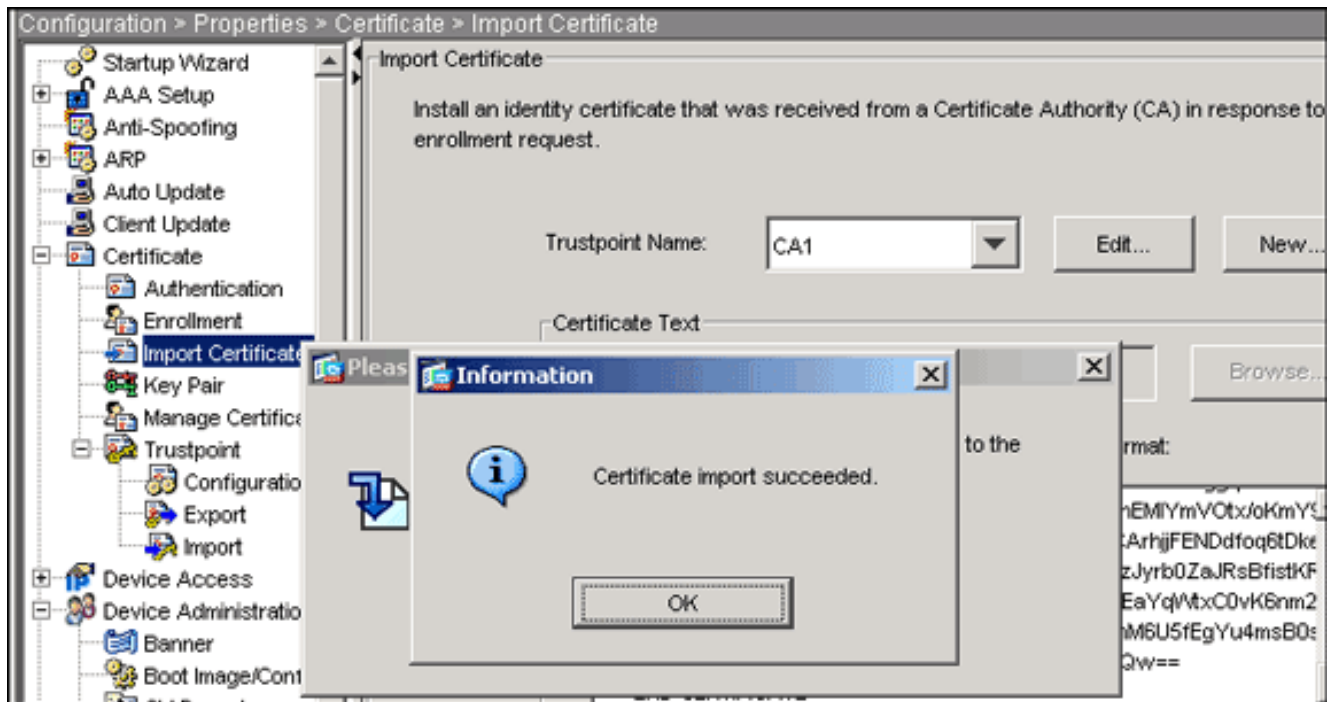
```

Schritt 6: Installieren des Zertifikats

ASDM-Verfahren

Führen Sie die folgenden Schritte mit dem vom Fremdhersteller bereitgestellten Identitätszertifikat durch:

1. Klicken Sie auf **Konfiguration** und dann auf **Eigenschaften**.
2. Erweitern Sie **Zertifikat**, und wählen Sie **Zertifikat importieren aus**.
3. Klicken Sie auf das Optionsfeld **Zertifikattext im Hexadezimalformat oder im Base64-Format eingeben**, und fügen Sie das Base64-Identitätszertifikat in das Textfeld ein.



4. Klicken Sie auf **Importieren** und anschließend auf **OK**.

Befehlszeilenbeispiel

CiscoASA

```
CiscoASA(config)#crypto ca import CA1 certificate

!--- Initiates prompt to paste the base64 identity
certificate !--- provided by the 3rd party vendor. % The
fully-qualified domain name in the certificate will be:
CiscoASA.cisco.com Enter the base 64 encoded
certificate. End with the word "quit" on a line by
itself !--- Paste the base 64 certificate provided by
the 3rd party vendor. -----BEGIN CERTIFICATE-----
MIIFPzCCBI+gAwIBAgIKYR71mwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLQQBGRYDY29tMRUwEwYKCZImiZPyLQQBGRYFY21zY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0EzMB4XDTA3MTIxNTA4MzUz
OV0XDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxZjZzAVBgNVBAGTDk5vbnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWx1aWdoMRYwFAYDVQQKEw1DaXNjaXJybyBT
eXN0
ZW1zMSQw
IgwYDVQDExtDaXNjaXJybyBFTQS5jaXNjaXJyby5jb20gT1U9VFNXRU
IwgZ8wDQYJ
KoZlhcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2Yac1AI03NdI8UpW5JHK14C
qB9j3HpX
BmFXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/0SQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QU5KMgWqBT7EXiRkgGBvjKf/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBAwHQYDVR0RBBywFIISQ21z
Y29BU0Eu
Y21zY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3myfNQJpAP1WCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0EzLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
```

```
aWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnsG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3d1Yi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEggEPMIIBCzCBQQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHVibG1jJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1d1YixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3d1Yi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UUy1XMkszLUFDUy5UU1d1Yi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFCAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtz5vBjG1cROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc
1L5nuPsd8MaexBc=
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
CiscoASA(config)#
```

[Schritt 7: Konfigurieren von Remote Access VPN \(IPSec\) zur Verwendung des neu installierten Zertifikats](#)

ASDM-Verfahren

Gehen Sie wie folgt vor, um das VPN für den Remote-Zugriff zu konfigurieren:

1. Wählen Sie **Configuration > VPN > IKE > Policies > Add**, um eine ISAKMP-Richtlinie 65535 zu erstellen, wie in diesem Bild gezeigt.

Add IKE Policy

Priority: Authentication:

Encryption: D-H Group:

Hash: Lifetime: Unlimited

2. Klicken Sie auf **OK** und dann auf **Übernehmen**.

3. Wählen Sie **Configuration > VPN > IPSec > Transform Sets > Add**, um einen Transformationssatz (*myset*) wie in diesem Bild gezeigt zu

Add Transform Set

Set Name:

Properties

Mode: Tunnel Transport

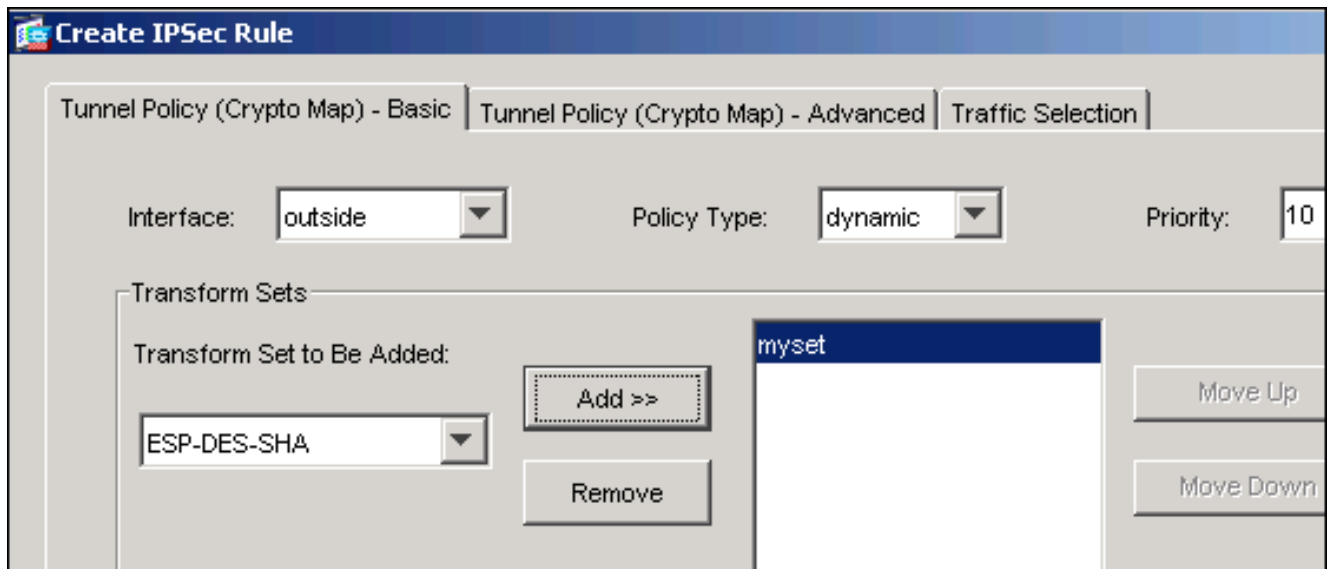
ESP Encryption:

ESP Authentication:

erstellen:

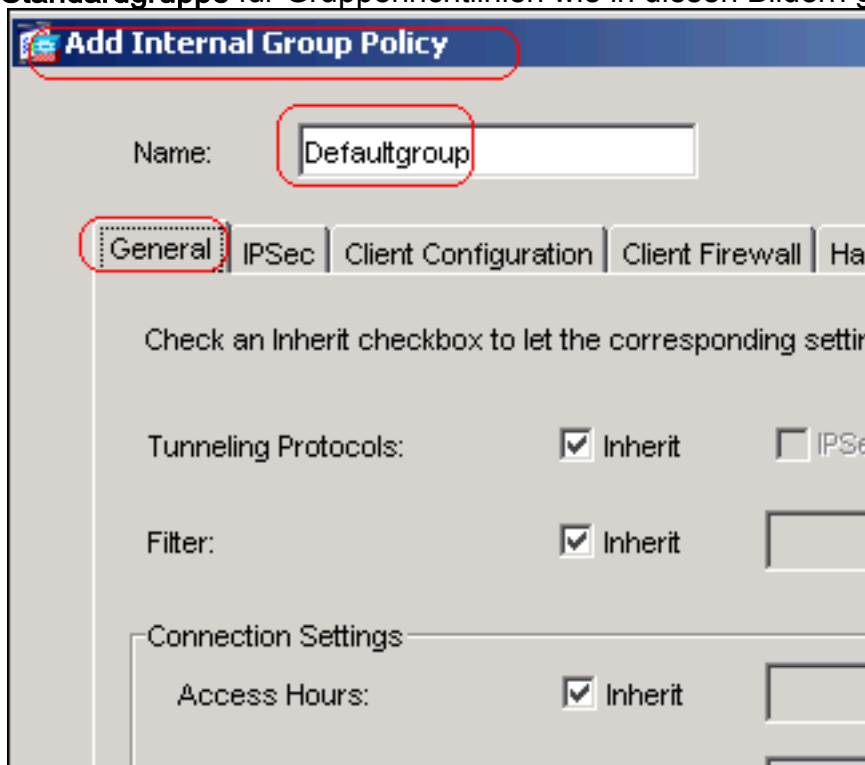
4. Klicken Sie auf **OK** und dann auf **Übernehmen**.

5. Wählen Sie **Configuration > VPN > IPSec > IPSec Rules > Add**, um eine Crypto Map mit dynamischer Richtlinie der Priorität 10 zu erstellen, wie in diesem Bild gezeigt:



6. Klicken Sie auf **OK** und dann auf **Übernehmen**.

7. Wählen Sie **Configuration > VPN > General > Group Policy > Add Internal Group Policy** (**Konfiguration > VPN > Allgemein > Gruppenrichtlinie > Interne Gruppenrichtlinie** hinzufügen), um eine **Standardgruppe** für Gruppenrichtlinien wie in diesen Bildern gezeigt zu



erstellen.

The screenshot shows the 'Add Internal Group Policy' dialog box with the 'Client Configuration' tab selected. The 'Name' field contains 'Defaultgroup'. Below the tabs, there is a note: 'Check an Inherit checkbox to let the corresponding setting take its value from the def'. Underneath, there are three sub-tabs: 'General Client Parameters', 'Cisco Client Parameters', and 'Microsoft Client Parameters'. In the 'Cisco Client Parameters' section, the 'Banner' field has an 'Inherit' checkbox checked, and the 'Default Domain' field has an 'Inherit' checkbox unchecked and the value 'cisco.com' entered. Red circles highlight the 'Client Configuration' tab and the 'cisco.com' text.

8. Klicken Sie auf **OK** und dann auf **Übernehmen**.

9. Wählen Sie **Configuration > VPN > IP Address Management > IP Pools > Add (Konfiguration > VPN > IP-Adressenverwaltung > IP-Pools > Add** aus, um den Adresspool für die dynamische Zuweisung der VPN-Client-Benutzer zu

The screenshot shows the 'Add IP Pool' dialog box. The 'Name' field contains 'vpnpool'. The 'Starting IP Address' field contains '10.5.5.10'. The 'Ending IP Address' field contains '10.5.5.20'. The 'Subnet Mask' field contains '255.255.255.0'. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

konfigurieren.

10. Klicken Sie auf **OK** und dann auf **Übernehmen**.

11. Wählen Sie **Configuration > VPN > General > Users > Add (Konfiguration > VPN > Allgemein > Benutzer > Hinzufügen**, um ein Benutzerkonto **vpnuser** für den VPN-Clientzugriff zu

Add User Account

Identity | VPN Policy | WebVPN

Username: vpnuser

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

erstellen.

12. Fügen Sie diesen Benutzer der **DefaultRAGroup**

Add User Account

Identity | VPN Policy | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the group

Group Policy: Inherit

Tunneling Protocols: Inherit IPSec WebVPN

Filter: Inherit

Tunnel Group Lock: Inherit DefaultRAGroup

Store Password on Client System: Inherit Yes No

hinzu.

13. Klicken Sie auf **OK** und dann auf **Übernehmen**.

14. Bearbeiten Sie die DefaultRAG-Gruppe wie in diesem Verfahren beschrieben: Wählen Sie **Configuration > VPN > General > Tunnel Group > Edit aus**. Wählen Sie **DefaultGroup** (Standardgruppe) aus der Dropdown-Liste Group Policy (Gruppenrichtlinie)

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | Client Address

Group Policy:

aus. Wählen Sie **LOCAL** aus der Dropdown-Liste Authentication Server Group (Authentifizierungsserver-Gruppe)

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | **Authentication** | Authorization | Accounting | Client Address Assign

To set authentication server group per interface, go to the Advanced ta

Authentication Server Group:

aus. Wählen Sie **vpnpool** aus der Dropdown-Liste Client Address Assignment (Client-Adressenzuweisung)

Edit Tunnel Group

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | **Client Address Assignment**

To specify whether to use DHCP or address pools for address assignment > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab

Available Pools	Assigned
<input type="text"/>	<input type="text" value="vpnpool"/>

aus.

15. Klicken Sie auf **OK** und dann auf **Übernehmen**.

Befehlszeilenbeispiel

```

CiscoASA
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)#exit
CiscoASA(config)#crypto isakmp identity auto

!--- Phase 1 Configurations CiscoASA(config)#crypto
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map outside_dyn_map 10

```

```

set transform-set myset
CiscoASA(config)#crypto map outside_map 65535 ipsec-
isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map interface
outside

!--- Phase 2 Configurations CiscoASA(config)#group-
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com
CiscoASA(config-group-policy)#exit

!--- Create a group policy "Defaultgroup" with domain
name !--- cisco.com CiscoASA(config)#username vpnuser
password password123
CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#group-lock value
DefaultRAGroup
CiscoASA(config-username)#exit

!--- Create an user account "vpnuser" and added to
"DefaultRAGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes

!--- The Security Appliance provides the default tunnel
groups !--- for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)#address-pool vpnpool

!--- Associate the vpnpool to the tunnel group using the
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup

!--- Associate the group policy "Defaultgroup" to the
tunnel group. CiscoASA(config-tunnel-general)#exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)#trust-point CA1
CiscoASA(config-tunnel-ipsec)#exit

!--- Associate the trustpoint CA1 for IPSec peer
authentication

```

[ASA-Konfigurationsübersicht](#)

CiscoASA

```

CiscoASA#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname CiscoASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.5 255.255.255.0

```

```
!  
interface Ethernet0/1  
  shutdown  
  nameif inside  
  security-level 100  
  ip address 10.2.2.1 255.255.255.0  
!  
interface Ethernet0/2  
  nameif DMZ  
  security-level 90  
  ip address 10.77.241.142 255.255.255.192  
!  
interface Ethernet0/3  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Management0/0  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
passwd 2KFQnbNIdI.2KYOU encrypted  
boot system disk0:/asa722-k8.bin  
ftp mode passive  
dns server-group DefaultDNS  
  domain-name cisco.com  
access-list 100 extended permit ip 10.2.2.0  
255.255.255.0 10.5.5.0 255.255.255.0  
pager lines 24  
mtu outside 1500  
mtu inside 1500  
mtu DMZ 1500  
ip local pool vpnpool 10.5.5.10-10.5.5.20 mask  
255.255.255.0  
no failover  
icmp unreachable rate-limit 1 burst-size 1  
asdm image disk0:/asdm-522.bin  
no asdm history enable  
arp timeout 14400  
nat (inside) 0 access-list 100  
route outside 10.1.1.0 255.255.255.0 192.168.1.1 1  
route outside 172.16.5.0 255.255.255.0 192.168.1.1 1  
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1  
timeout xlate 3:00:00  
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00  
icmp 0:00:02  
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp  
0:05:00 mgcp-pat 0:05:00  
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00  
sip-disconnect 0:02:00  
timeout uauth 0:05:00 absolute  
group-policy Defaultgroup internal  
group-policy Defaultgroup attributes  
  default-domain value cisco.com  
username vpnuser password TXttW.eFqbHusJQM encrypted  
username vpnuser attributes  
  group-lock value DefaultRAGroup  
http server enable  
http 0.0.0.0 0.0.0.0 outside  
http 0.0.0.0 0.0.0.0 DMZ  
no snmp-server location
```

```
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 10 set transform-set
myset
crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto ca trustpoint CA1
  enrollment terminal
  subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco
Systems,
          C=US,St=North Carolina,L=Raleigh
keypair my.CA.key
crl configure
crypto ca certificate chain CA1
  certificate 3f14b70b00000000001f
    308205eb 308204d3 a030201 02020a3f 14b70b00
00000000 1f300d06 092a8648
    86f70d01 01050500 30513113 3011060a 09922689
93f22c64 01191603 636f6d31
    15301306 0a099226 8993f22c 64011916 05636973
636f3115 3013060a 09922689
    93f22c64 01191605 54535765 62310c30 0a060355
04031303 43413130 1e170d30
    37313232 37313430 3033365a 170d3038 31323236
31343030 33365a30 67311330
    11060a09 92268993 f22c6401 19160363 6f6d3115
3013060a 09922689 93f22c64
    01191605 63697363 6f311530 13060a09 92268993
f22c6401 19160554 53576562
    310e300c 06035504 03130555 73657273 31123010
06035504 03130976 706e7365
    72766572 30819f30 0d06092a 864886f7 0d010101
05000381 8d003081 89028181
    00b8e20a a8332356 b75b6600 735008d3 735d23c5
295b9247 2b5e02a8 1f63dc7a
    570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3
94f80d01 a14cc01d 98b1320e
    9fe84905 5ab94b18 ef308eb1 2f22ab1a 8edb38f0
2c2cf78e 07197f2d 52d3cb73
    91a9ccb2 d903f722 bd414b0a 3205aa05 3ec45e24
6480606f 8e417f09 a7aa9c64
    4d020301 0001a382 03313082 032d300b 0603551d
0f040403 02052030 34060355
    1d11042d 302ba029 060a2b06 01040182 37140203
a01b0c19 76706e73 65727665
    72405453 5765622e 63697363 6f2e636f 6d301d06
03551d0e 04160414 2c242ddb
    490cde1a fe2d63e3 1e1fb28c 974c4216 301f0603
551d2304 18301680 14d9adbf
    08f23a88 f114432f 79987cd4 09a403e5 58308201
03060355 1d1f0481 fb3081f8
    3081f5a0 81f2a081 ef8681b5 6c646170 3a2f2f2f
434e3d43 41312c43 4e3d5453
    2d57324b 332d4143 532c434e 3d434450 2c434e3d
5075626c 69632532 304b6579
    25323053 65727669 6365732c 434e3d53 65727669
6365732c 434e3d43 6f6e6669
    67757261 74696f6e 2c44433d 54535765 622c4443
3d636973 636f2c44 433d636f
    6d3f6365 72746966 69636174 65526576 6f636174
696f6e4c 6973743f 62617365
```

3f6f626a 65637443 6c617373 3d63524c 44697374
72696275 74696f6e 506f696e
74863568 7474703a 2f2f7473 2d77326b 332d6163
732e7473 7765622e 63697363
6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131
2e63726c 3082011d 06082b06
01050507 01010482 010f3082 010b3081 a906082b
06010505 07300286 819c6c64
61703a2f 2f2f434e 3d434131 2c434e3d 4149412c
434e3d50 75626c69 63253230
4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
3d636f6d 3f634143 65727469 66696361 74653f62
6173653f 6f626a65 6374436c
6173733d 63657274 69666963 6174696f 6e417574
686f7269 7479305d 06082b06
01050507 30028651 68747470 3a2f2f74 732d7732
6b332d61 63732e74 73776562
2e636973 636f2e63 6f6d2f43 65727445 6e726f6c
6c2f5453 2d57324b 332d4143
532e5453 5765622e 63697363 6f2e636f 6d5f4341
312e6372 74301506 092b0601
04018237 14020408 1e060045 00460053 300c0603
551d1301 01ff0402 30003015
0603551d 25040e30 0c060a2b 06010401 82370a03
04304406 092a8648 86f70d01
090f0437 3035300e 06082a86 4886f70d 03020202
0080300e 06082a86 4886f70d
03040202 00803007 06052b0e 03020730 0a06082a
864886f7 0d030730 0d06092a
864886f7 0d010105 05000382 010100bf 99b9daf2
e24f1bd6 ce8271eb 908fad3
772df610 0e78b198 f945f379 5d23a120 7c38ae5d
8f91b3ff 3da5d139 46d8fb6e
20d9a704 b6aa4113 24605ea9 4882d441 09f128ab
4c51a427 fa101189 b6533eef
adc28e73 fcfed3f1 f4e64981 0976b8a1 2355c358
a22af8bb e5194b42 69a7c2f6
c5a116f6 d9d77fb3 a7f3d201 e3cff8f7 48f8d54e
243d2530 31a733af 0e1351d3
9c64a0f7 4975fc66 a017627c cfd0ea22 2992f463
9412b388 84bf8b33 bd9f589a
e7087262 a4472e69 775ab608 e5714857 4f887163
705220e3 aca870be b107ab8d
73faf76d b3550553 1a2b873f 156f9dff 5386c839
1380fda8 945a7f6c c2e9d5c8
83e2e761 394dd4da 63eaefc6 a44df5
quit
certificate ca 7099f1994764e09c4651da80a16b749c
3082049d 30820385 a0030201 02021070 99f19947
64e09c46 51da80a1 6b749c30
0d06092a 864886f7 0d010105 05003051 31133011
060a0992 268993f2 2c640119
1603636f 6d311530 13060a09 92268993 f22c6401
19160563 6973636f 31153013
060a0992 268993f2 2c640119 16055453 57656231
0c300a06 03550403 13034341
31301e17 0d303731 32313430 36303134 335a170d
31323132 31343036 31303135
5a305131 13301106 0a099226 8993f22c 64011916
03636f6d 31153013 060a0992
268993f2 2c640119 16056369 73636f31 15301306


```
0a099226 8993f22c 64011916
  05545357 6562310c 300a0603 55040313 03434131
30820122 300d0609 2a864886
  f70d0101 01050003 82010f00 3082010a 02820101
00ea8fee c7ae56fc a22e603d
  0521b333 3dec0ad4 7d4c2316 3bleea33 c9a6883d
28ece906 02902f9a d1eb2b8d
  f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
ale906ec 88b32a19 38e5353e
  6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621
876bd678 c8a37109 f074eabe
  2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7
24b9e054 063c60a4 9b8d3c09
  351bc630 05f69357 833b9197 f875b408 cb71a814
69alf331 b1eb2b35 0c469443
  1455c210 db308bf0 a9805758 a878b82d 38c71426
afffd272 dd6d7564 1cbe4d95
  b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67
94b97ac7 63249009 fa05ca4d
  6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b
5f020301 0001a382 016f3082
  016b3013 06092b06 01040182 37140204 061e0400
43004130 0b060355 1d0f0404
  03020186 300f0603 551d1301 01ff0405 30030101
ff301d06 03551d0e 04160414
  d9adbf08 f23a88f1 14432f79 987cd409 a403e558
30820103 0603551d 1f0481fb
  3081f830 81f5a081 f2a081ef 8681b56c 6461703a
2f2f2f43 4e3d4341 312c434e
  3d54532d 57324b33 2d414353 2c434e3d 4344502c
434e3d50 75626c69 63253230
  4b657925 32305365 72766963 65732c43 4e3d5365
72766963 65732c43 4e3d436f
  6e666967 75726174 696f6e2c 44433d54 53576562
2c44433d 63697363 6f2c4443
  3d636f6d 3f636572 74696669 63617465 5265766f
63617469 6f6e4c69 73743f62
  6173653f 6f626a65 6374436c 6173733d 63524c44
69737472 69627574 696f6e50
  6f696e74 86356874 74703a2f 2f74732d 77326b33
2d616373 2e747377 65622e63
  6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f
4341312e 63726c30 1006092b
  06010401 82371501 04030201 00300d06 092a8648
86f70d01 01050500 03820101
  001abc5a 40b32112 22da80fb bb228bfe 4bf8a515
df8fc3a0 4e0c89c6 d725e2ab
  2fa67ce8 9196d516 dfe55627 953aea47 2e871289
6b754e9c 1e01d408 3f7f0595
  8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
  ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
  94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
  c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
  aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76
13018f9f 5e3dce95 efe6da93
  f4cb3b00 102efa94 48a22fc4 7e342031 2406165e
39edc207 eddc6554 3fa9f396 ad
quit
crypto isakmp enable outside
crypto isakmp policy 65535
```

```

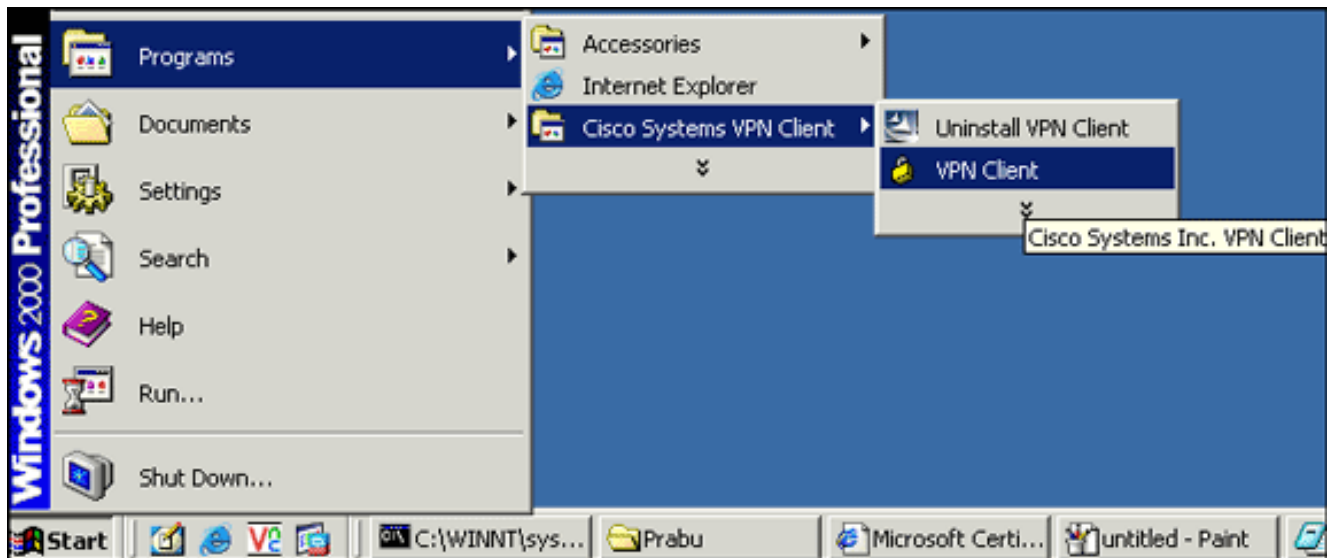
authentication rsa-sig
encryption 3des
hash md5
group 2
lifetime 86400
crypto isakmp identity auto
tunnel-group DefaultRAGroup general-attributes
  address-pool vpnpool
  default-group-policy Defaultgroup
tunnel-group DefaultRAGroup ipsec-attributes
  trust-point CA1
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0
: end
CiscoASA#

```

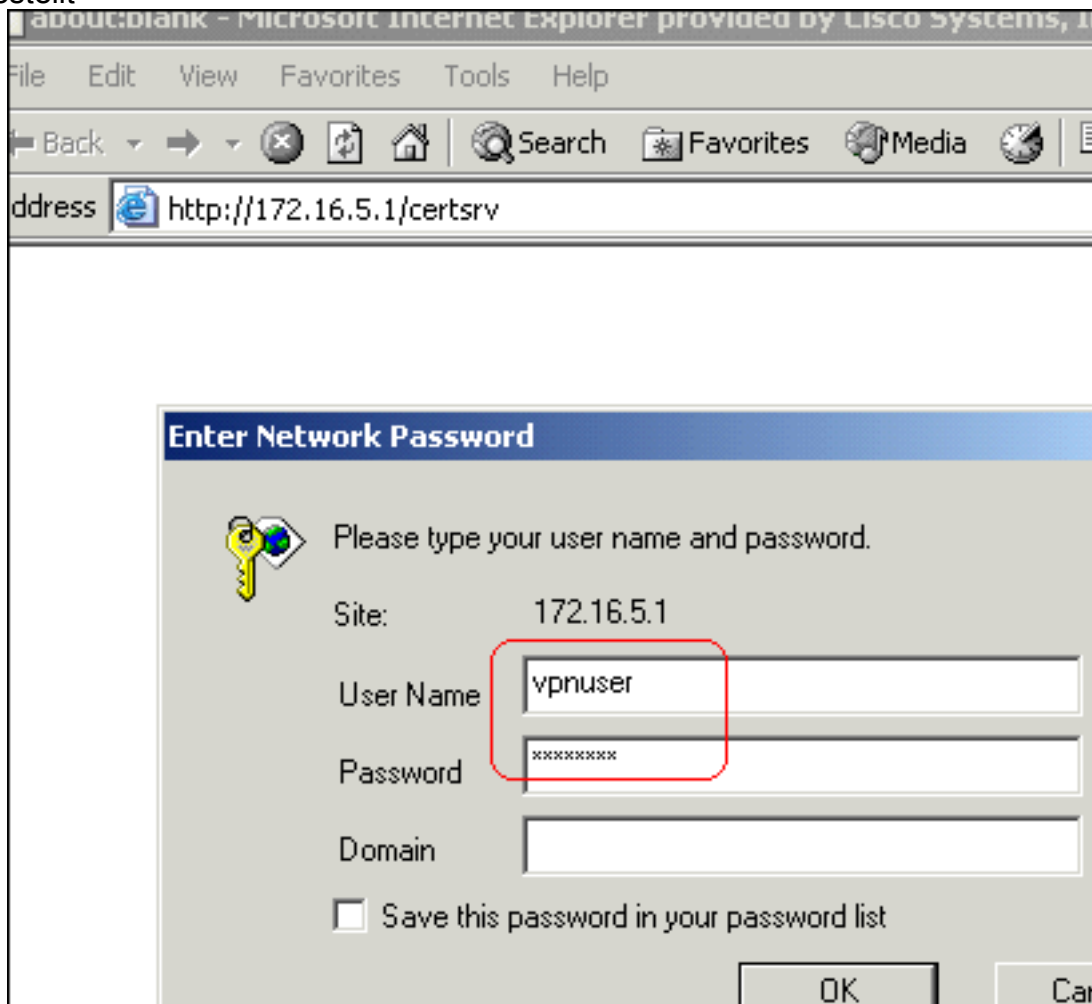
VPN-Client-Konfiguration

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

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client** aus, um die VPN-Client-Software zu starten.



2. Gehen Sie wie folgt vor, um das Zertifizierungsstellenzertifikat vom CA-Server mit dem Namen **CA1** herunterzuladen und in Cisco VPN Client zu installieren: Melden Sie sich beim CA-Server 172.16.5.1 an, wobei die dem vpnuser bereitgestellten Benutzerkredite bereitgestellt



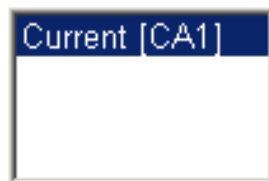
werden. **Hinweis**: Stellen Sie sicher, dass Sie über ein Benutzerkonto für den VPN-Client-Benutzer mit dem CA-Server verfügen. Klicken Sie auf **Zertifizierungsstellenzertifikat, Zertifikatskette oder CRL herunterladen** und wählen Sie dann das Optionsfeld **Base 64** aus, um die Kodierungsmethode anzugeben. Klicken Sie auf das **Zertifikat CA herunterladen**.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
 Base 64

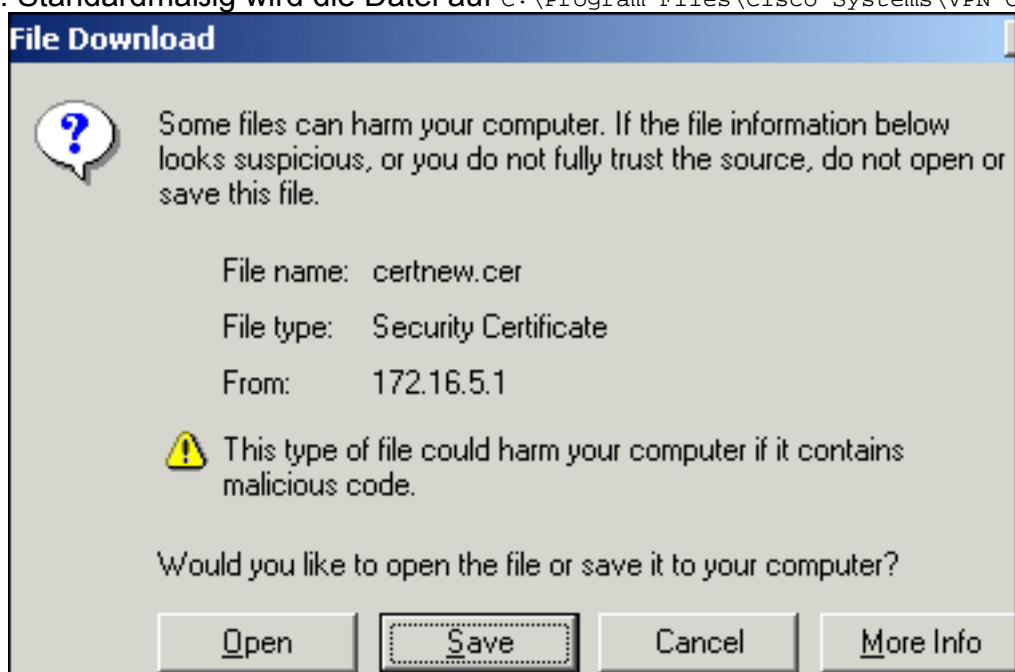
[Download CA certificate](#)

[Download CA certificate chain](#)

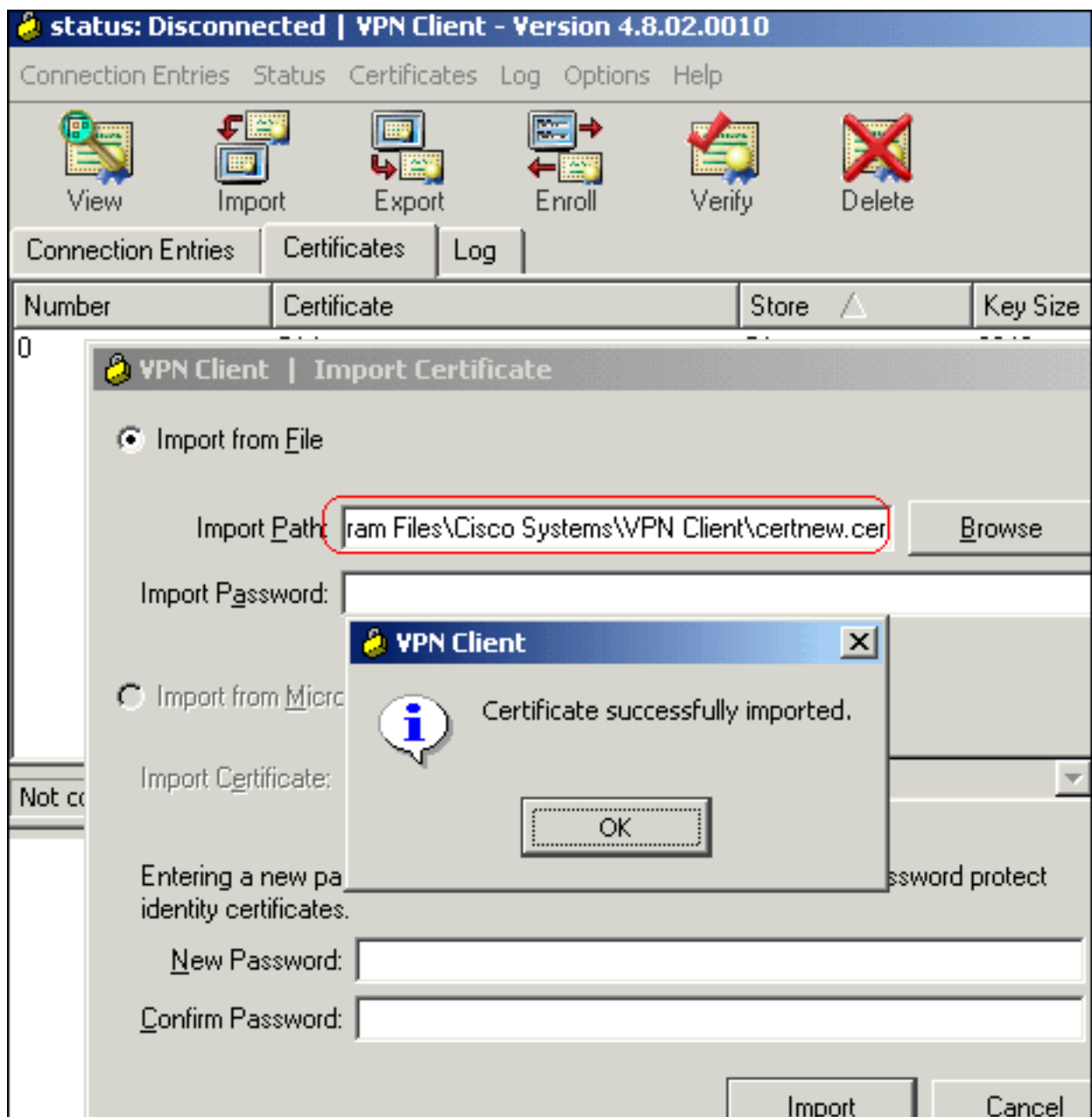
[Download latest base CRL](#)

[Download latest delta CRL](#)

Speichern Sie das Zertifizierungsstellenzertifikat auf Ihrem Computer mit dem Namen **certnew.cer**. Standardmäßig wird die Datei auf `C:\Program Files\Cisco Systems\VPN Client`

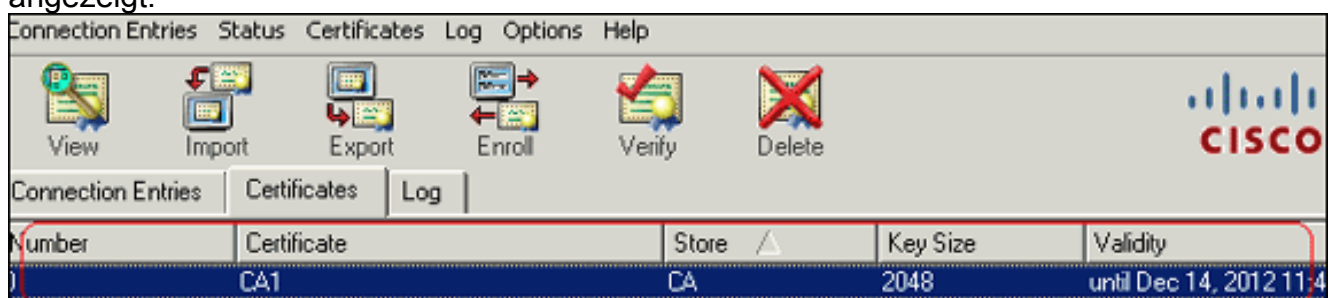


gespeichert. Klicken Sie im VPN-Client auf die Registerkarte **Zertifikate** und wählen Sie **Importieren**. Klicken Sie auf das Optionsfeld **Import from File (Aus Datei importieren)** und anschließend auf **Browse (Durchsuchen)**, um das Zertifizierungsstellenzertifikat vom gespeicherten Speicherort `C:\Program Files\Cisco Systems\VPN Client` zu importieren. Klicken Sie auf **Importieren**. Es wird ein Dialogfeld angezeigt, das angibt, dass das Zertifikat erfolgreich importiert wurde.

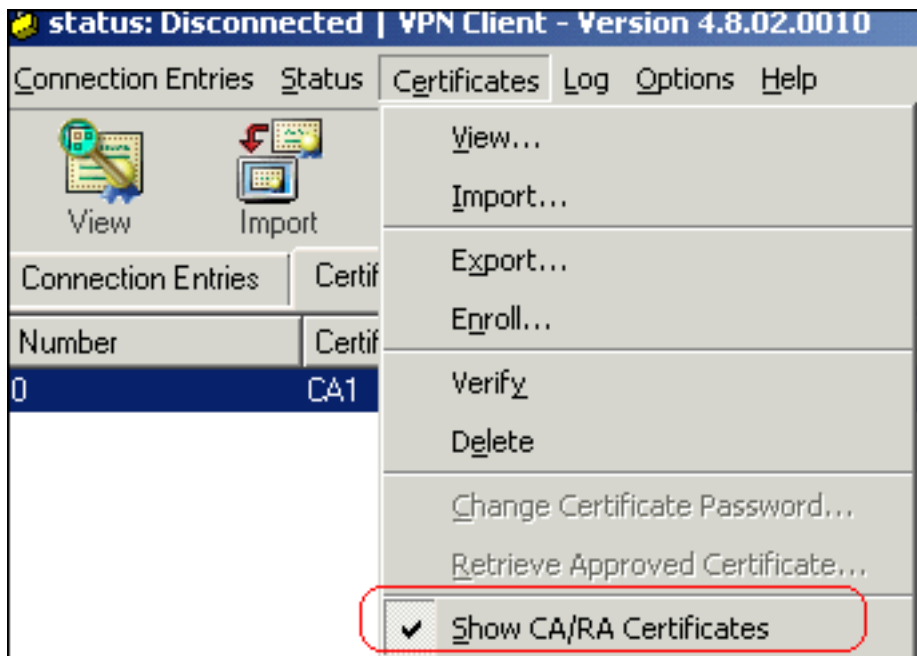


Die

CA Certificates CA1 wird auf der Registerkarte Certificates (Zertifikate) angezeigt.



Hinweis: Stellen Sie sicher, dass die Option **CA/RA-Zertifikate anzeigen** aktiviert ist. Andernfalls werden die Zertifizierungsstellenzertifikate nicht im Zertifikatsfenster



angezeigt.

3. Gehen Sie wie folgt vor, um das Identitätszertifikat herunterzuladen und im VPN-Client zu installieren: Wählen Sie auf dem CA-Server CA1 die Option **Zertifikat anfordern > Erweiterte Zertifikatsanforderung > Erstellen aus**, und senden Sie eine Anfrage an diese **Zertifizierungsstelle**, um sich für das Identitätszertifikat anzumelden. Klicken Sie auf **Senden**.

Certificate Template:

User ▼

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

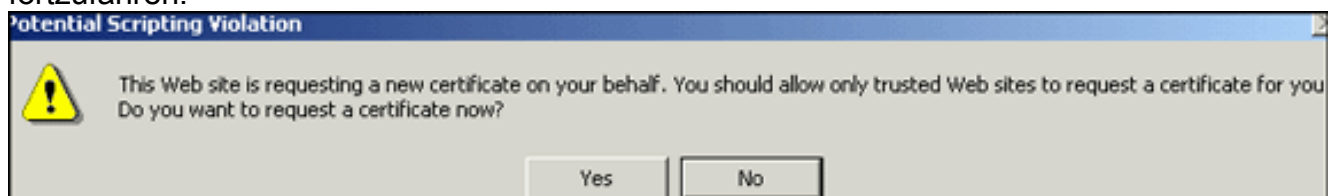
Request Format: CMC PKCS10

Hash Algorithm: MD5 ▼

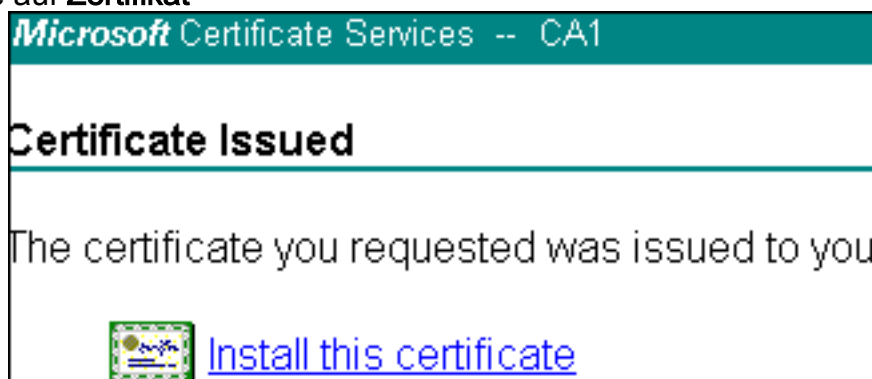
Only used to sign request.

Save request to a file

Klicken Sie auf **Ja**, um fortzufahren.



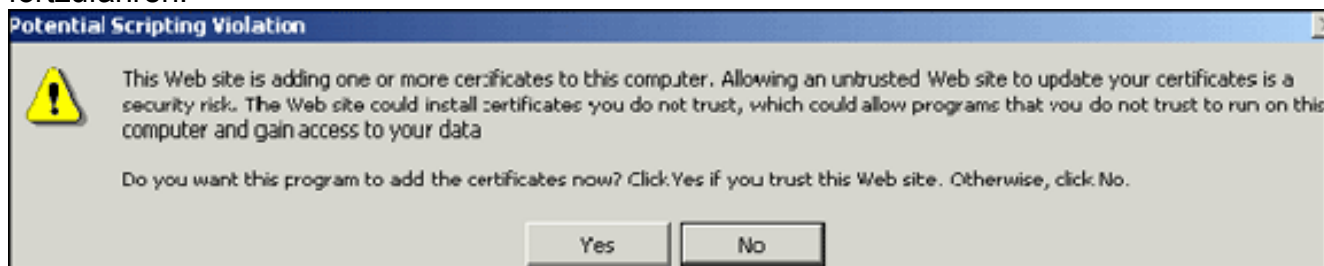
Klicken Sie auf **Zertifikat**



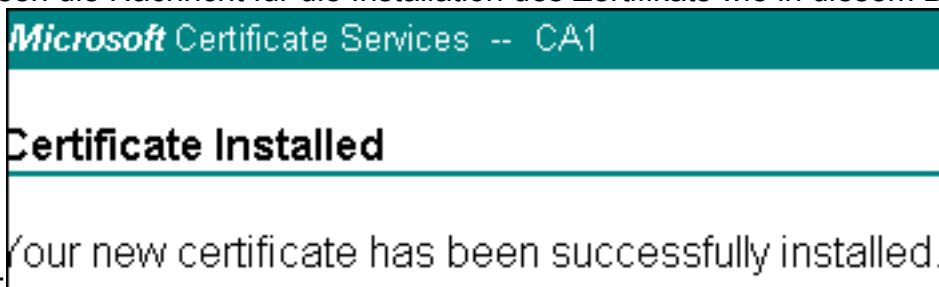
installieren.

Klicken Sie auf **Ja**,

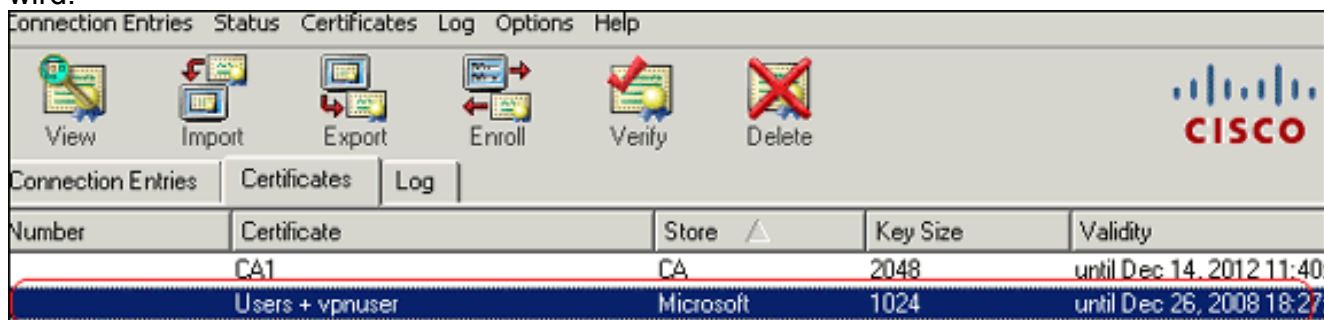
um
fortzufahren.



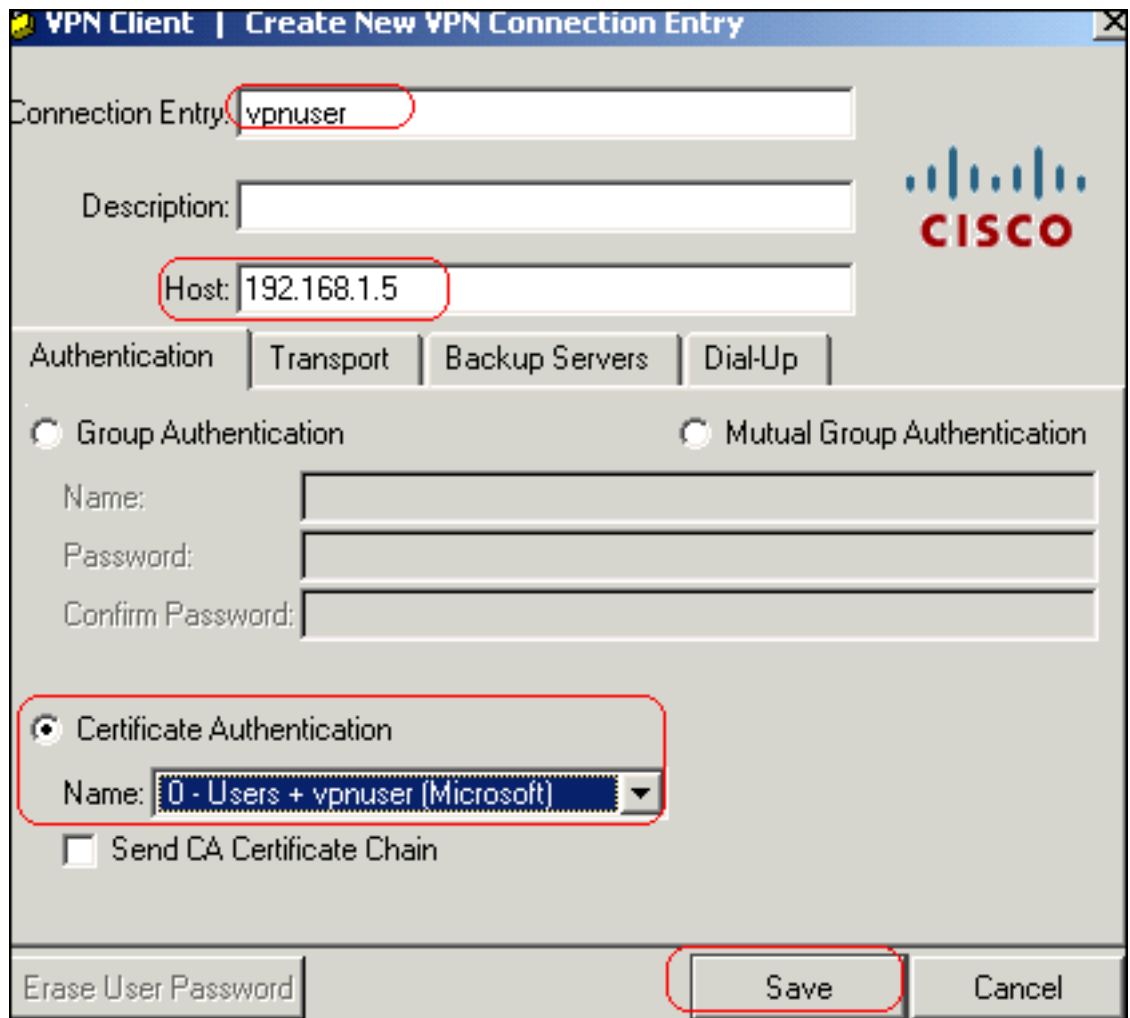
Sie müssen die Nachricht für die Installation des Zertifikats wie in diesem Bild gezeigt



erhalten: Beenden Sie den VPN-Client, und starten Sie ihn neu, damit das installierte Identitätszertifikat wie in diesem Bild gezeigt auf der Registerkarte Certificates (Zertifikate) des VPN-Clients angezeigt wird:

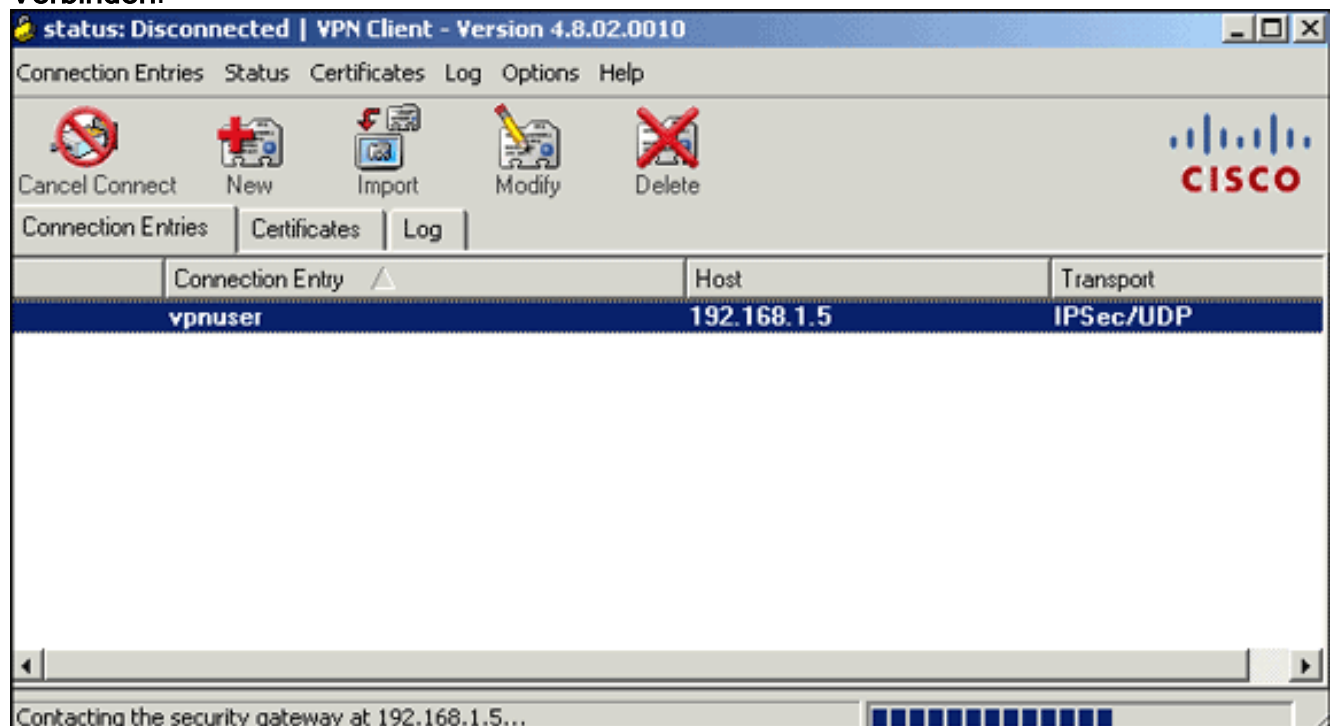


4. Gehen Sie wie folgt vor, um einen Verbindungseintrag (*vpnuser*) zu erstellen: Klicken Sie auf die Registerkarte Verbindungseinträge und anschließend auf **Neu**. Geben Sie die IP-Adresse des Remote-Peers (routingfähig) in das Feld Host ein. Wählen Sie die Optionsschaltfläche **Certificate Authentication** (Zertifikatsauthentifizierung) aus, und wählen Sie das Identitätszertifikat aus der Dropdown-Liste aus. Klicken Sie auf

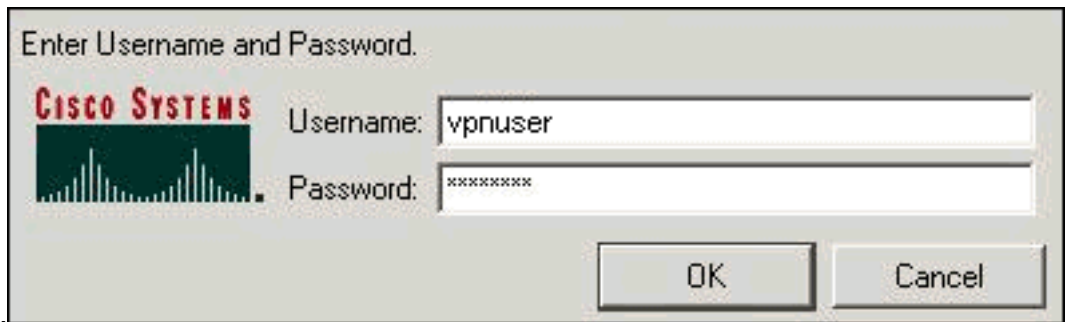


Speichern.

5. Klicken Sie auf **Verbinden**.



6. Geben Sie bei Aufforderung den Benutzernamen und das Kennwort für xauth ein, und klicken Sie auf **OK**, um eine Verbindung zum Remote-Netzwerk



herzustellen.

7. Der VPN-Client stellt eine Verbindung mit der ASA her, wie in diesem Bild



gezeigt:

Überprüfen

Auf der ASA können Sie mehrere Befehle zur Anzeige in der Befehlszeile verwenden, um den Status eines Zertifikats zu überprüfen.

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

- **show crypto ca trustpoint:** Zeigt konfigurierte Trustpoints an.

```
CiscoASA#show crypto ca trustpoints
```

```
Trustpoint CA1:
```

```
Subject Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Serial Number: 7099f1994764e09c4651da80a16b749c
```

```
Certificate configured.
```

- **show crypto ca certificate:** Zeigt alle Zertifikate an, die auf dem System installiert sind.

```
CiscoASA#show crypto ca certificates
```

```
Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 3f14b70b00000000001f
```

```
Certificate Usage: Encryption
```

```
Public Key Type: RSA (1024 bits)
```

```
Issuer Name:
```

```
cn=CA1
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
Subject Name:
```

```
cn=vpnserver
```

```
cn=Users
```

```
dc=TSWeb
```

```
dc=cisco
```

```
dc=com
```

```
PrincipalName: vpnserver@TSWeb.cisco.com
```

```
CRL Distribution Points:
```

```
[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuratio
```

```
n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
```

```
[2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl
```

```
Validity Date:
```

start date: 14:00:36 UTC Dec 27 2007
end date: 14:00:36 UTC Dec 26 2008
Associated Trustpoints: CA1

CA Certificate

Status: Available
Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Issuer Name:

cn=CA1
dc=TSWeb
dc=cisco
dc=com

Subject Name:

cn=CA1
dc=TSWeb
dc=cisco
dc=com

CRL Distribution Points:

[1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,
CN=Services,CN=Configuratio
n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
[2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl

Validity Date:

start date: 06:01:43 UTC Dec 14 2007
end date: 06:10:15 UTC Dec 14 2012

Associated Trustpoints: CA1

- **show crypto ca crls:** Zeigt zwischengespeicherte Zertifikatswiderruflisten (CRL) an.
- **show crypto key mypubkey rsa:** Zeigt alle generierten Krypto-Schlüsselpaare an.

CiscoASA#**show crypto key mypubkey rsa**

Key pair was generated at: 01:43:45 UTC Dec 11 2007

Key name: <Default-RSA-Key>

Usage: General Purpose Key

Modulus Size (bits): 1024

Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001

Key pair was generated at: 06:36:00 UTC Dec 15 2007

Key name: my.CA.key

Usage: General Purpose Key

Modulus Size (bits): 1024

Key Data:

30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001

Key pair was generated at: 07:35:18 UTC Dec 21 2007

CiscoASA#

- **show crypto isakmp sa:** Zeigt die Informationen zum IKE 1-Tunnel an.

CiscoASA#**show crypto isakmp sa**

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

```
1 IKE Peer: 10.1.1.5
   Type      : user           Role      : responder
   Rekey     : no             State     : MM_ACTIVE
```

- **show crypto ipsec sa** - Zeigt die IPSec-Tunnelinformationen an.

```
CiscoASA#show crypto ipsec sa
interface: outside
  Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0)
  current_peer: 10.1.1.5, username: vpnuser
  dynamic allocated peer ip: 10.5.5.10

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5

  path mtu 1500, ipsec overhead 58, media mtu 1500
  current outbound spi: FF3EEE7D

inbound esp sas:
  spi: 0xEFDF8BA9 (4024404905)
    transform: esp-3des esp-md5-hmac none
    in use settings = {RA, Tunnel, }
    slot: 0, conn_id: 4096, crypto-map: dynmap
    sa timing: remaining key lifetime (sec): 28314
    IV size: 8 bytes
    replay detection support: Y
outbound esp sas:
  spi: 0xFF3EEE7D (4282314365)
    transform: esp-3des esp-md5-hmac none
    in use settings = {RA, Tunnel, }
    slot: 0, conn_id: 4096, crypto-map: dynmap
    sa timing: remaining key lifetime (sec): 28314
    IV size: 8 bytes
    replay detection support: Y
```

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show** anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hier einige mögliche Fehler, die Sie möglicherweise feststellen:

- **FEHLER: Importiertes Zertifikat konnte nicht analysiert oder verifiziert werden.** Dieser Fehler kann auftreten, wenn Sie das Identitätszertifikat installieren und nicht das richtige Zwischen- oder Stammzertifikat der CA mit dem zugehörigen Vertrauenspunkt authentifiziert haben. Sie müssen das richtige Zwischen- oder Stammzertifikat der CA entfernen und erneut authentifizieren. Wenden Sie sich an Ihren Fremdhersteller, um zu überprüfen, ob Sie das richtige Zertifizierungsstellenzertifikat erhalten haben.
- **Das Zertifikat enthält keinen allgemeinen öffentlichen Schlüssel.** Dieser Fehler kann auftreten,

wenn Sie versuchen, Ihr Identitätszertifikat auf dem falschen Trustpoint zu installieren. Sie versuchen, ein ungültiges Identitätszertifikat zu installieren, oder das Schlüsselpaar, das dem Trustpoint zugeordnet ist, stimmt nicht mit dem öffentlichen Schlüssel überein, der im Identitätszertifikat enthalten ist. Verwenden Sie den Befehl **show crypto ca certificate trustpointname**, um zu überprüfen, ob Sie Ihr Identitätszertifikat auf dem richtigen Vertrauenspunkt installiert haben. Suchen Sie nach dem Posten, der **Associated Trustpoints** angibt. Wenn der falsche Vertrauenspunkt aufgeführt ist, verwenden Sie die in diesem Dokument beschriebenen Verfahren, um den entsprechenden Vertrauenspunkt zu entfernen und neu zu installieren. Überprüfen Sie außerdem, ob das Schlüsselpaar seit der Generierung der CSR-Nummer nicht geändert wurde.

- **FEHLER: ASA/PIX Sev=Warning/3 IKE/0xE300081 Ungültige Remote-Zertifikat-ID:**Dieser Fehler wird möglicherweise im VPN-Client angezeigt, wenn bei der Authentifizierung ein Problem mit den Zertifikaten auftritt. Um dieses Problem zu beheben, verwenden Sie den Befehl **crypto isakmp identity auto** in der ASA/PIX-Konfiguration.

Zugehörige Informationen

- [Support-Seite für Cisco Adaptive Security Appliance](#)
- [Support-Seite für Cisco VPN-Clients](#)
- [Cisco Security Appliances der Serie PIX 500](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Problemhinweise zu Sicherheitsprodukten \(einschließlich PIX\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)