

# Пример конфигурации "ASA/PIX 7.x and VPN Client IPSec Authentication, используя Digital Certificates with Microsoft CA"

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Родственные продукты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Конфигурация ASA](#)

[Сводная таблица конфигурации ASA](#)

[Конфигурация клиента VPN](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает, как вручную установить цифровой сертификат стороннего поставщика на устройстве защиты Cisco (ASA/PIX) 7.x, а также как обеспечить аутентификацию клиентов VPN IPsec на сервере центра сертификации Microsoft (CA).

## Предварительные условия

### Требования

Для выполнения действий, описанных в этом документе, необходимо иметь доступ к центру сертификации (CA) для регистрации сертификатов. Поддерживаемая третья сторона CA поставщики включают Балтимор, Cisco, Поручают, iPlanet/Netscape, Microsoft, RSA и VeriSign.

**Примечание:** Этот документ использует Windows 2003 Server в качестве сервера CA для сценария.

**Примечание:** В этом документе предполагается, что на устройстве ASA/PIX отсутствует

конфигурация VPN.

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ASA 5510, который работает под управлением ПО версии 7.2 (2) и версия 5.2 (2) ASDM.
- VPN-клиент, использующий программное обеспечение версии 4.x и более поздней версии.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Родственные продукты

Конфигурация ASA может также использоваться с Cisco PIX серии 500, который работает под управлением ПО версии 7. x.

## Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

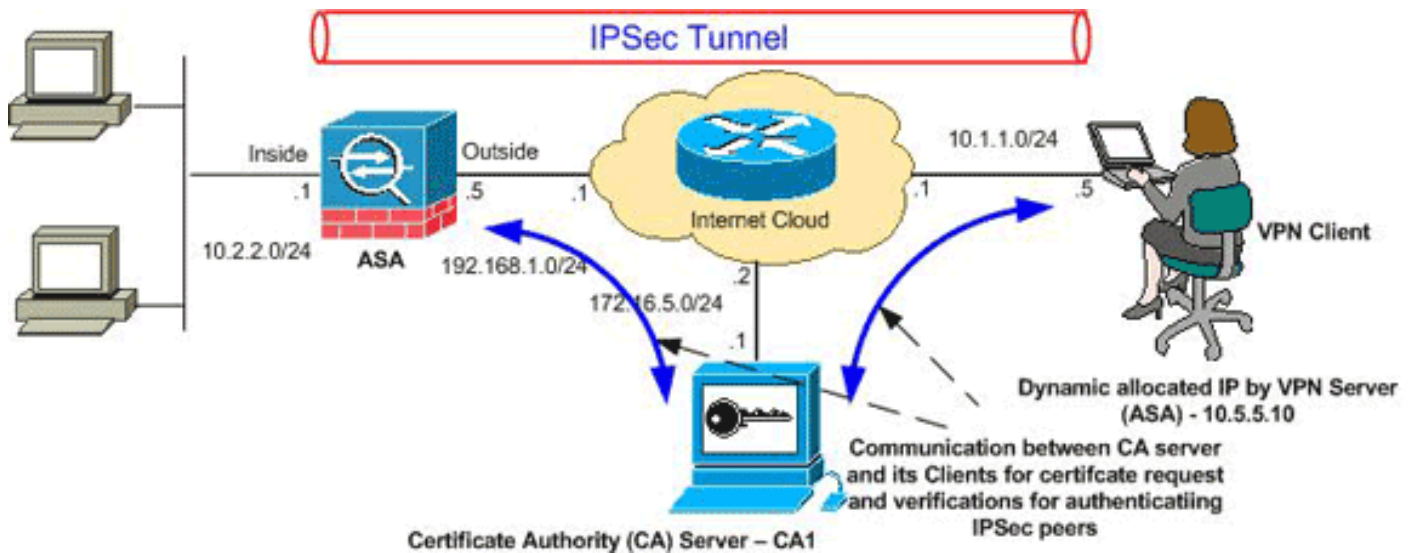
## Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.](#)

## Схема сети

В настоящем документе используется следующая схема сети:



**Примечание:** Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

## Конфигурации

Эти конфигурации используются в данном документе:

- [Конфигурация ASA](#)
- [Сводная таблица конфигурации ASA](#)
- [Конфигурация клиента VPN](#)

## Конфигурация ASA

Выполните эти шаги для установки цифрового сертификата поставщика третьей стороны на ASA:

[Шаг 1. Проверьте, что Дата, Время и Значения Часового пояса Точна](#)

[Шаг 2. Генерируйте открытые и секретные ключи криптосистемы RSA](#)

[Шаг 3. Создайте точку доверия.](#)

[Шаг 4. . Генерируйте хранилище сертификатов.](#)

[Шаг 5. . Аутентифицируйте точку доверия](#)

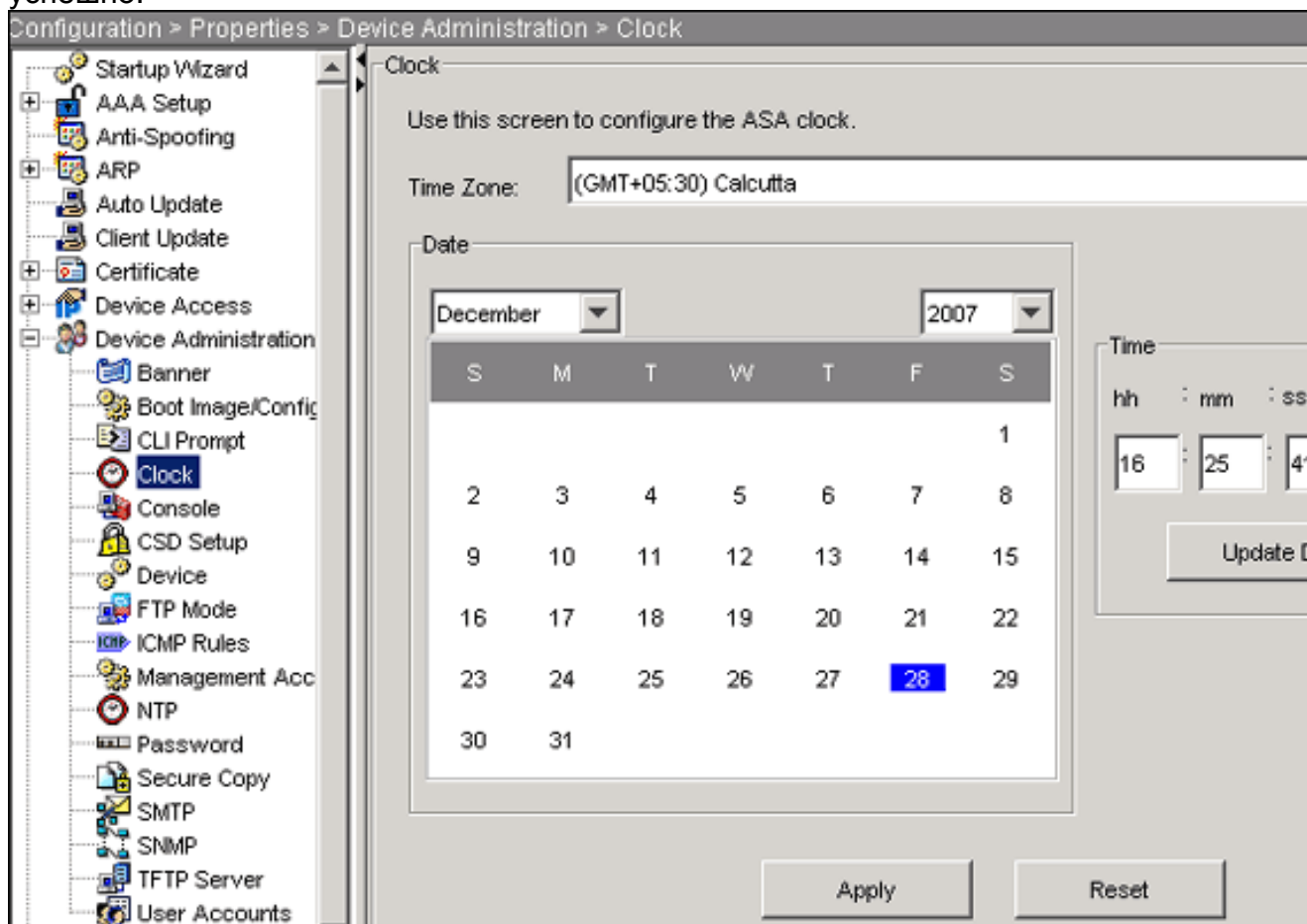
[Шаг 6. Установите сертификат](#)

[Шаг 7. Настройте VPN для удаленного доступа \(IPsec\) для Исполнения нового установленного сертификата](#)

[Шаг 1. Проверьте, что Дата, Время и Значения Часового пояса Точна](#)

Порядок действий в диспетчере ASDM

1. Нажмите **Configuration**, и затем нажмите **Properties**.
2. Разверните **Администрирование устройств** и выберите **Clock**.
3. Проверьте правильность отображаемой информации. Значения параметров Date, Time и Time Zone должны быть правильными, чтобы проверка сертификата прошла успешно.



#### Пример командной строки

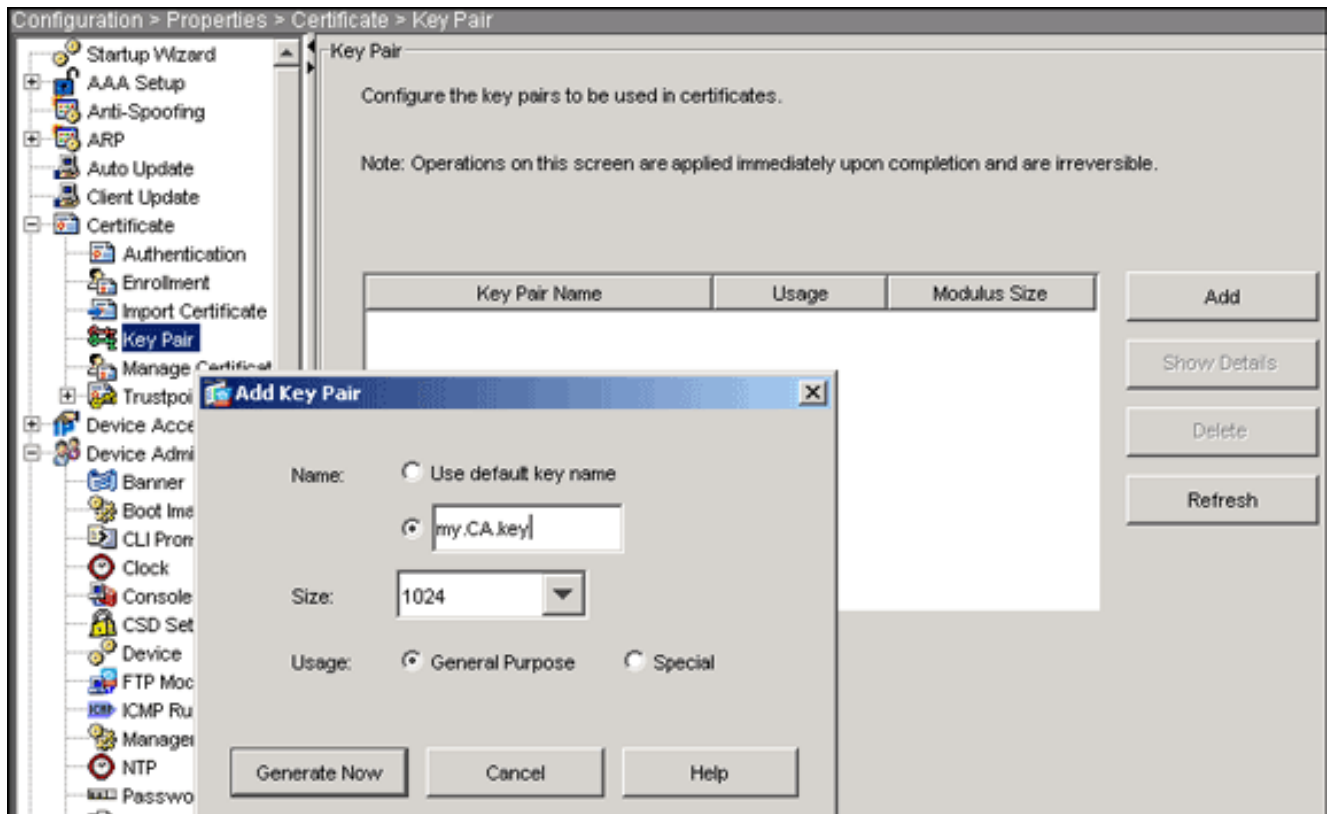
```
Cisco ASA
CiscoASA#show clock 16:25:49.580 IST Fri Dec 28 2007
```

### [Шаг 2. Генерируйте открытые и секретные ключи криптосистемы RSA](#)

Генерируемый открытый ключ RSA объединен с идентификационной информацией от ASA для формирования запроса сертификата PKCS#10. Необходимо отчетливо определить ключевое название с Точкой доверия, для которой вы создаете пару ключей.

#### Порядок действий в диспетчере ASDM

1. Нажмите **Configuration**, и затем нажмите **Properties**.
2. Разверните **Сертификат** и выберите **Key Pair**.
3. Нажмите **Add**.



4. Введите ключевое имя, выберите размер модуля и выберите тип использования. **Примечание:** Рекомендуемый размер пары ключей 1024.
5. **Нажмите кнопку Generate Now.** Пара ключей, которую вы создали, должна быть перечислена в столбце Key Pair Name.

Пример командной строки

```

Cisco ASA
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)#

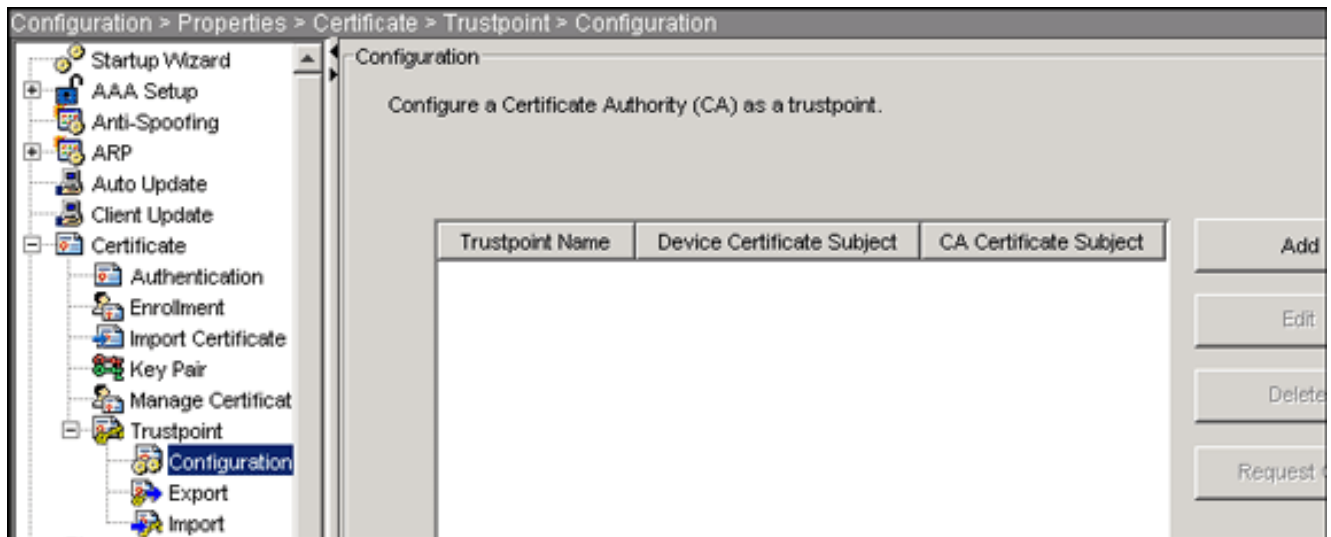
```

### Шаг 3. Создайте точку доверия

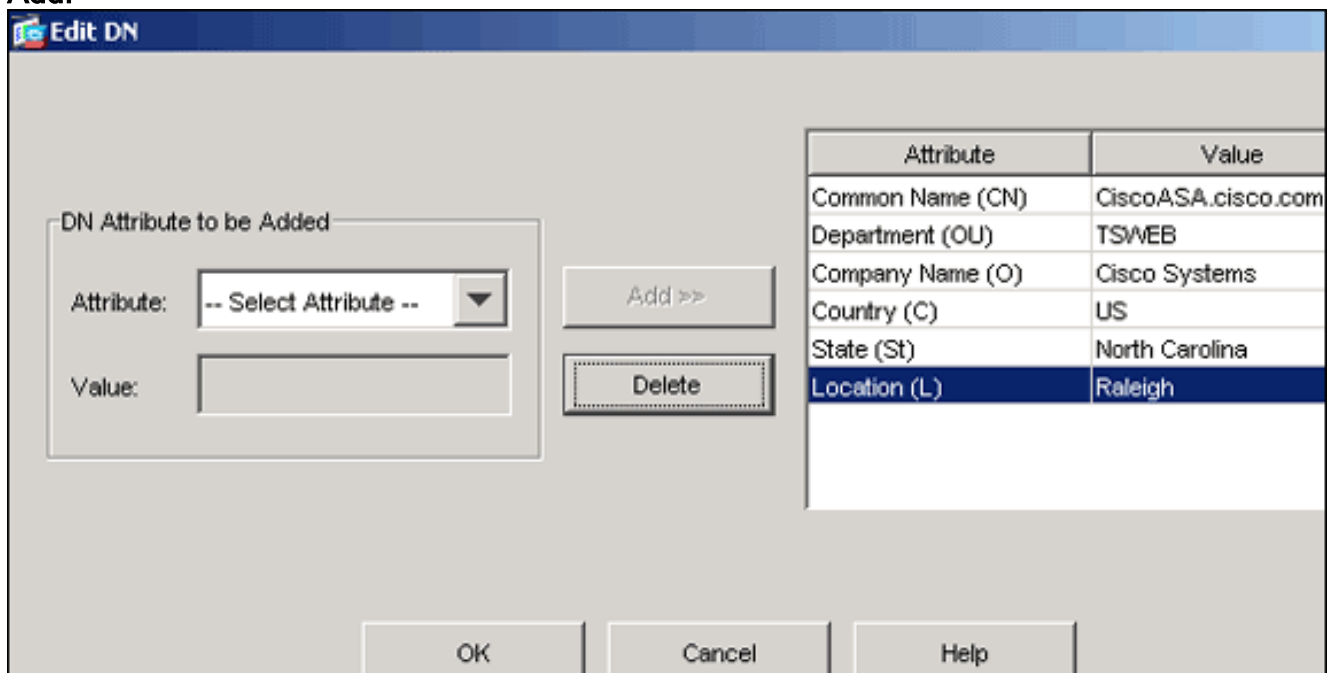
Точки доверия требуются, чтобы объявлять Центр сертификации (CA), который будет использовать ваш ASA.

#### Порядок действий в диспетчере ASDM

1. Нажмите **Configuration**, и затем нажмите **Properties**.
2. Разверните **Сертификат**, и затем разверните **Точку доверия**.
3. Выберите **Configuration**, и затем **нажмите Add**.



4. Настройте эти значения: **Название точки доверия:** название точки доверия должно относиться к предполагаемому использованию. (Данный пример использует CA1.) **Пара ключей:** Выберите пару ключей, генерируемую в [Share 2](#). (мой. CA.key)
5. Гарантируйте, что выбран Manual enrollment.
6. Нажмите **Certificate Parameters**. Диалоговое окно Certificate Parameters появляется.
7. Нажмите **Edit** и настройте атрибуты, перечисленные в этой таблице: **Чтобы настроить эти значения, выберите значение в раскрывающемся списке "Атрибут", введите его и щелкните Add.**



8. После добавления соответствующих значений нажмите кнопку **OK**.
9. В диалоговом окне Certificate Parameters введите FQDN в поле Specify FQDN. Это значение должно совпадать со значением FQDN, используемым для общего имени

**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

(CN).

10. **Нажмите кнопку OK.**
11. Проверьте, что корректная пара ключей выбрана, и нажмите кнопку с зависимой фиксацией **ручной регистрации Использования**.
12. **Нажмите кнопку OK, а затем нажмите Apply.**

**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

Пример командной строки

```

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=webvpn.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

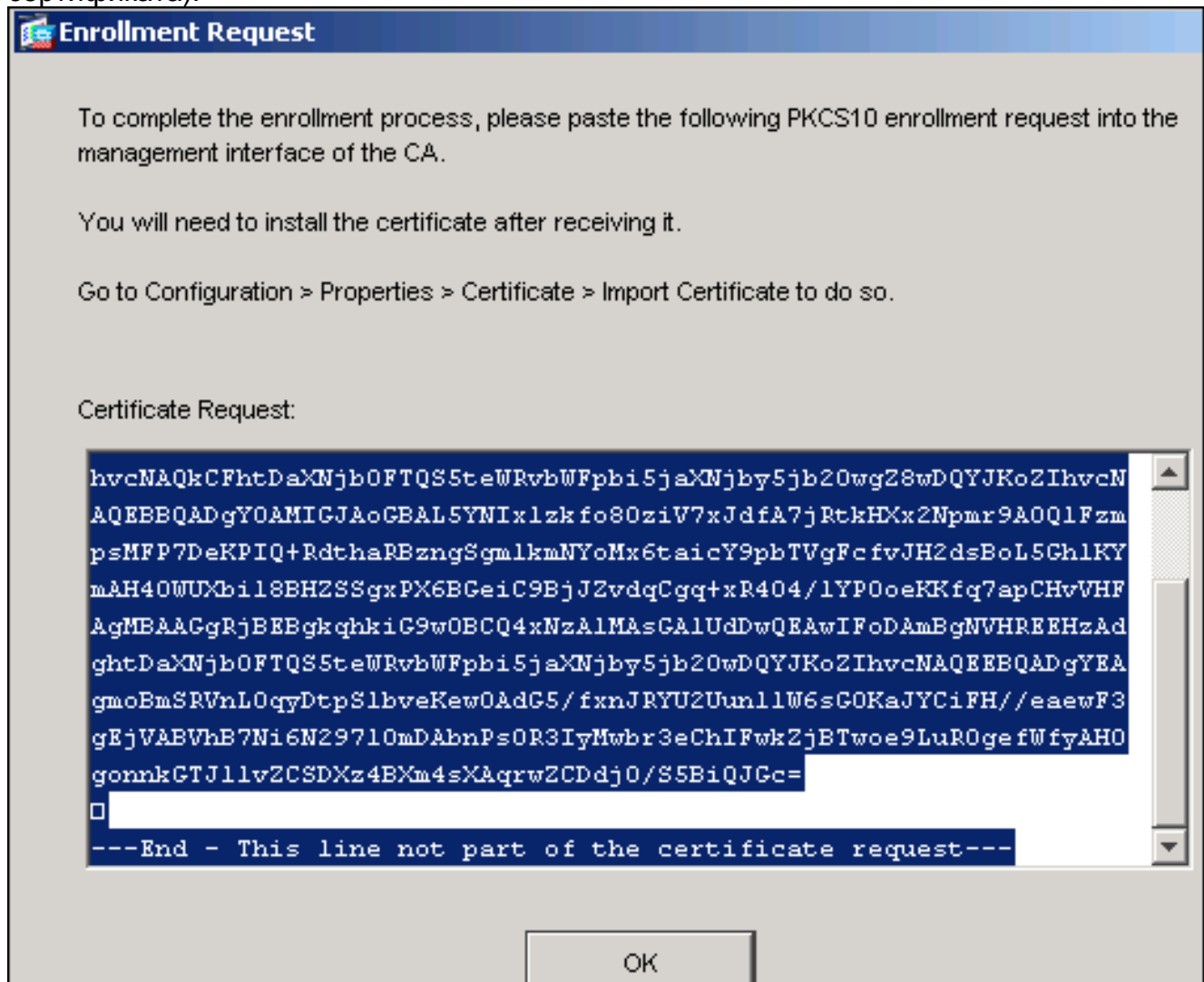
```

[Шаг 4. . Генерируйте хранилище сертификатов](#)

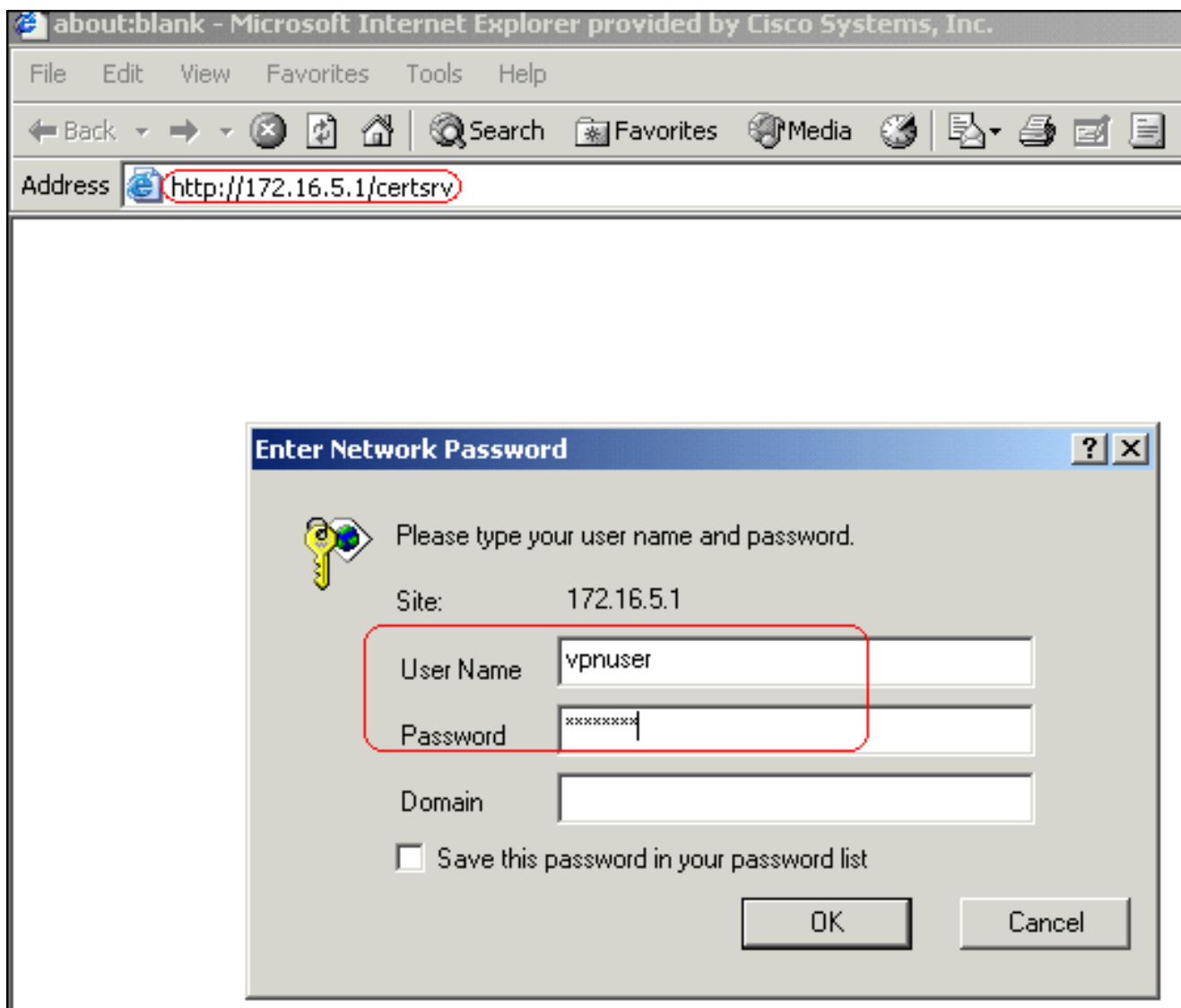


## Порядок действий в диспетчере ASDM

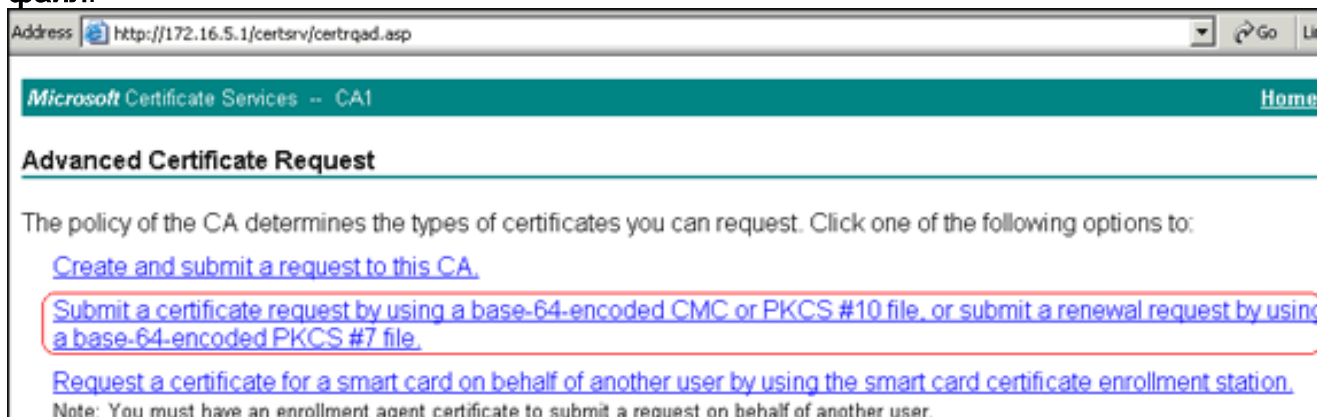
1. Нажмите **Configuration**, и затем нажмите **Properties**.
2. Разверните **Сертификат** и выберите **Enrollment**.
3. Проверьте, что Точка доверия, созданная в [Шаге 3](#), выбрана, и нажмите **Enroll**. Диалоговое окно появляется, который перечисляет запрос хранилища сертификатов (также называемый запросом подписи сертификата).



4. Скопируйте запрос регистрации PKCS#10 к текстовому файлу, и затем отправьте сохраненный CSR вашему поставщику третьей стороны (такому как Microsoft CA) как показано в этой процедуре: Войдите к серверу CA 172.16.5.1 с пользовательскими учетными данными, предоставленными серверу vpn.



**Примечание:** Удостоверьтесь, что у вас есть учетная запись пользователя для ASA (сервер vpn) с сервером CA.Нажмите **Request сертификат> усовершенствованный запрос сертификата**, и затем выберите **Submit запрос сертификата** при помощи **base-64-encoded CMC** или файла **PKCS#10** или отправьте запрос на обновление при помощи **base-64-encoded PKCS#7** файл.



Скопируйте и вставьте закодированную информацию в текстовое поле **Сохраненного запроса** и нажмите

## 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):

```
ivQVNB LmNpc2NvLmNvbTANBgkqhkiG9wOBAQQFAAO  
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8  
D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+  
t8Ux9emhFHpGHnQ/MpSfUOdQ==  
not part of the certificate request---
```

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

### Certificate Template:

IPSEC

### Additional Attributes:

Attributes:

Submit >

Submit.

Установите переключатель в положение Base 64 encoded и щелкните ссылку Download

Microsoft Certificate Services -- CA1

## Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



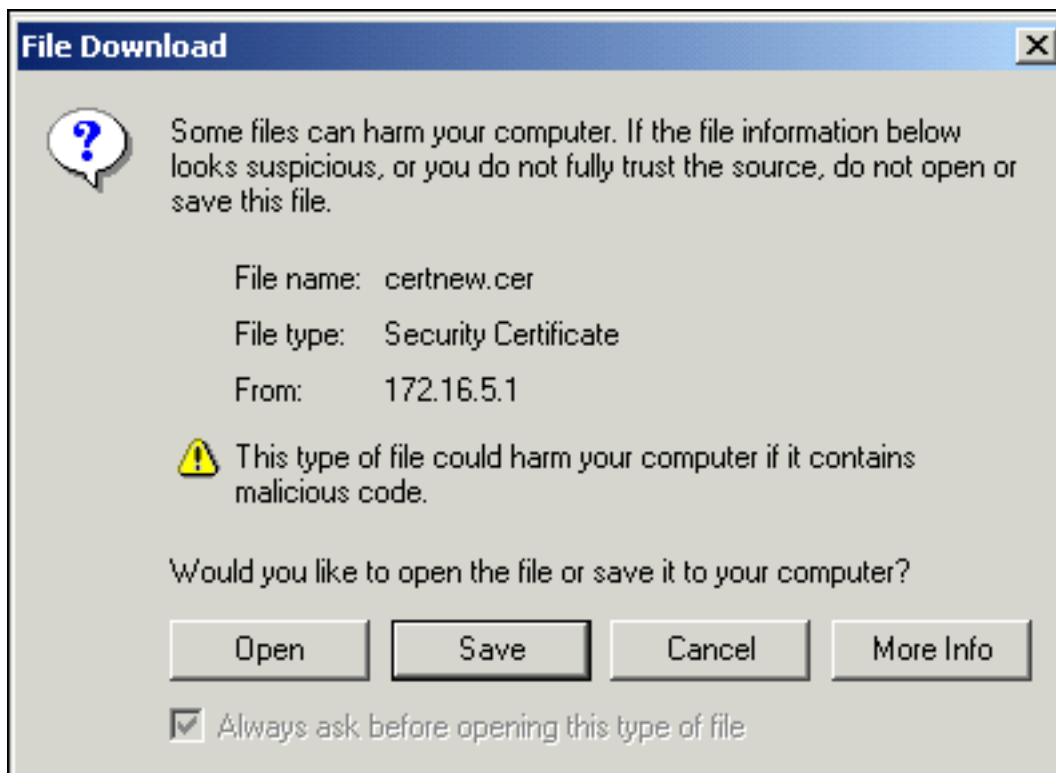
[Download certificate](#)

[Download certificate chain](#)

certificate.

Когда

Загрузка Файла dialog коробка появляется, сохраните его с названием **cert\_client\_id.cer**, который является сертификатом идентификации, который будет установлен на



ASA.

## Пример командной строки

### Cisco ASA

```
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:
MIICHjCCAYcCAQAwgAxEADA0BgNVBACTBlJhbGVpZ2gxZmZAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECXMVFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRip9cyQp/983pm5PfDD6/ho0nTktx0i+lcEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlarc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
```

```
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/  
Uo13yWce 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not  
part of the certificate request--- Redisplay enrollment  
request? [yes/no]: no ciscoasa(config)#
```

## Шаг 5. . Аутентифицируйте точку доверия

После получения идентификационного сертификата от стороннего поставщика можно перейти к этому шагу.

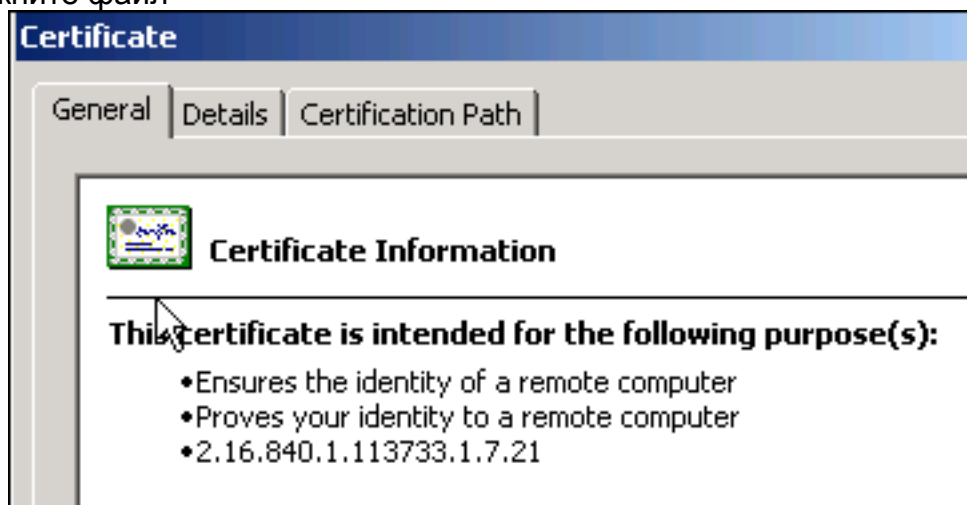
### Порядок действий в диспетчере ASDM

1. Сохраните идентификационный сертификат на локальном компьютере.
2. Если бы вы были предоставлены закодированный base64 сертификат, который не стал файлом, то необходимо скопировать сообщение base64 и вставить его в текстовый файл.
3. Переименуйте файл, изменив его расширение на .cer. **Примечание:** Как только файл переименован с .cer расширением, значок файла должен отобразиться как сертификат



как показано.

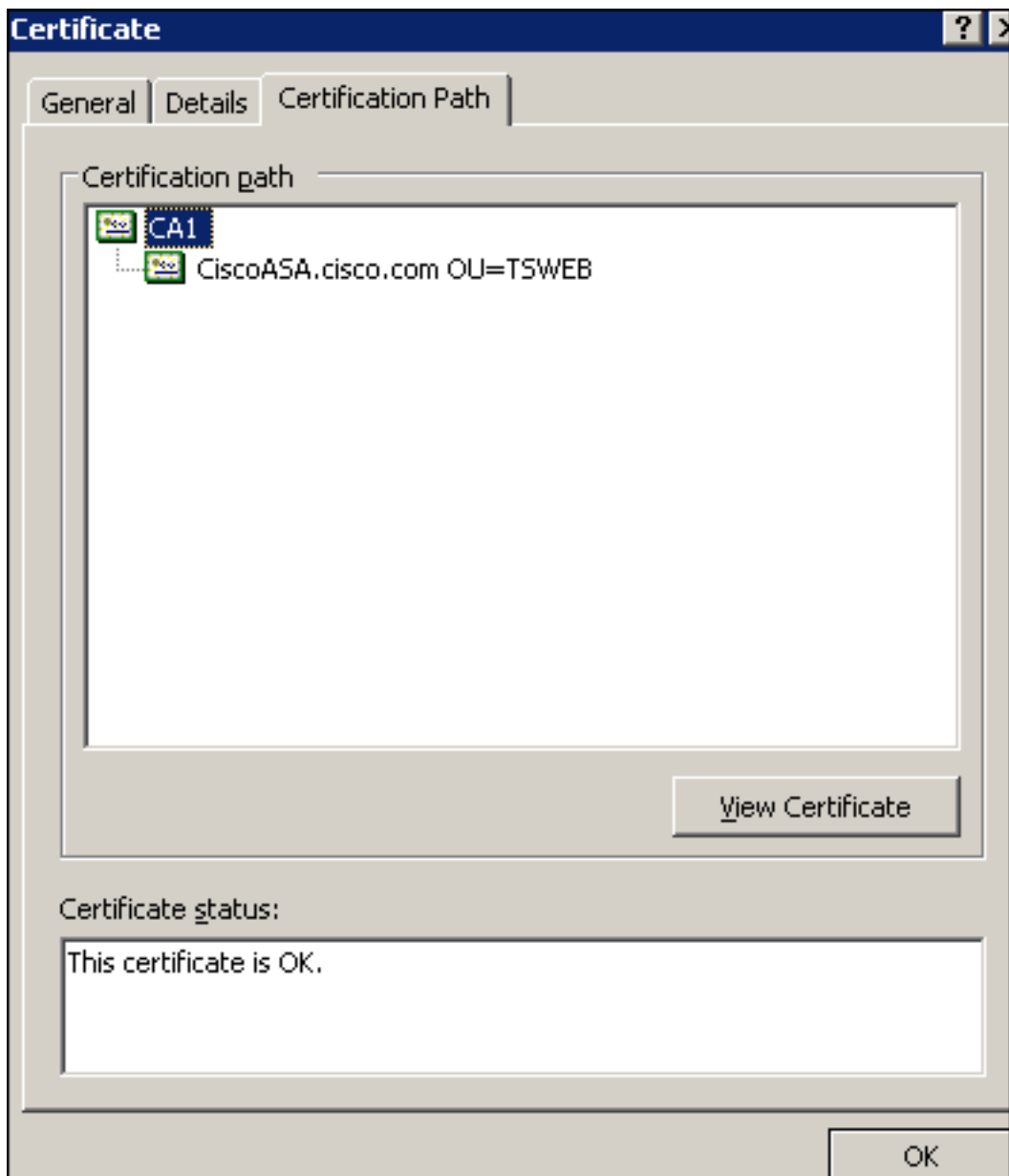
4. Дважды щелкните файл



сертификата. **Примечание:** Если на вкладке General появляется сообщение "Windows does not have enough information to verify this certificate", то для продолжения процедуры необходимо

получить корневой сертификат стороннего поставщика или промежуточный сертификат CA. Свяжитесь со своим сторонним поставщиком или администратором CA, чтобы получить корневой сертификат выпустившего его CA или промежуточный сертификат CA.

5. Щелкните вкладку Путь к сертификату
6. Выберите сертификат CA, расположенный над вашим выпущенным идентификационным сертификатом, и нажмите View

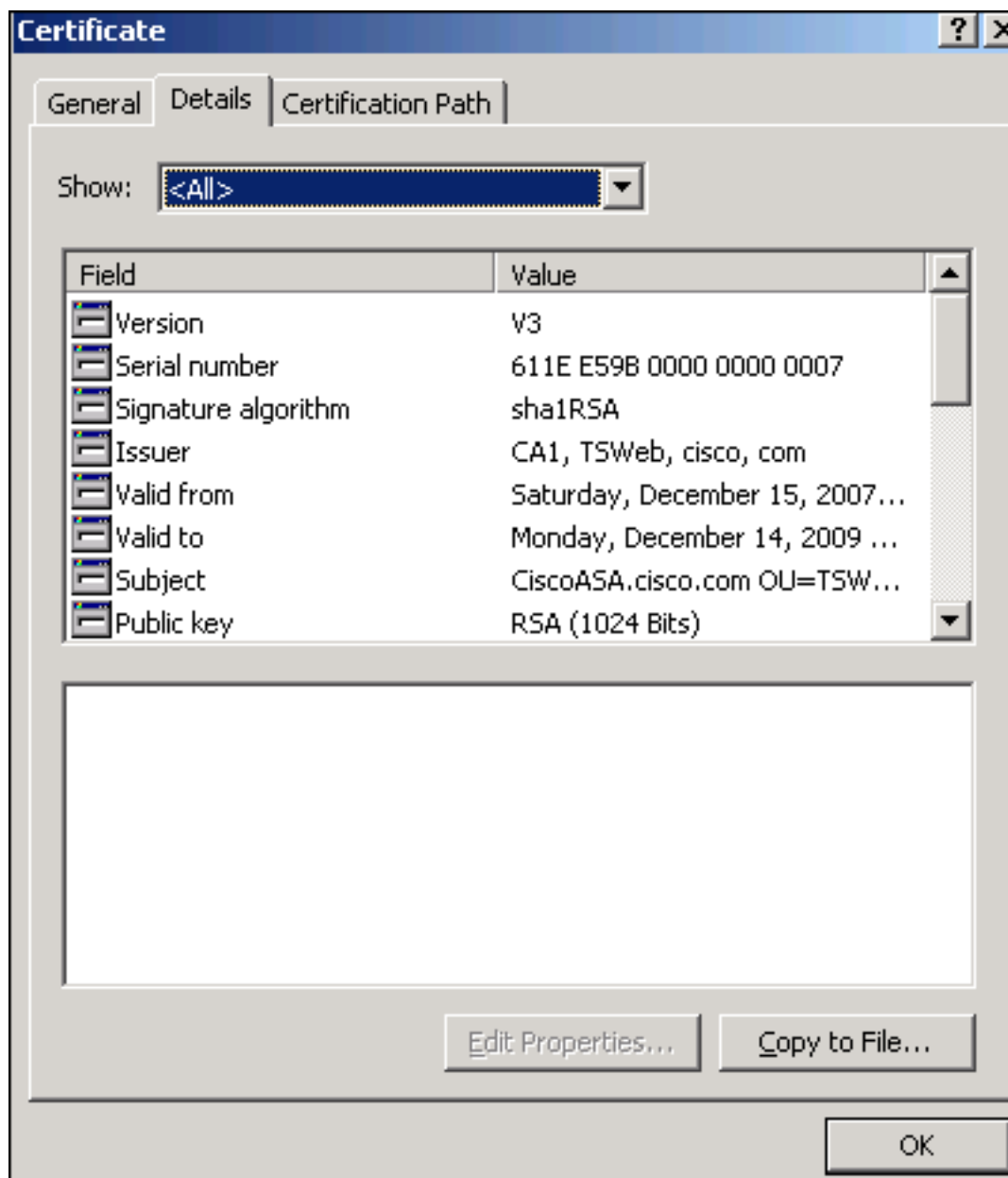


Certificate.

зится подробная информация о сертификате CA.

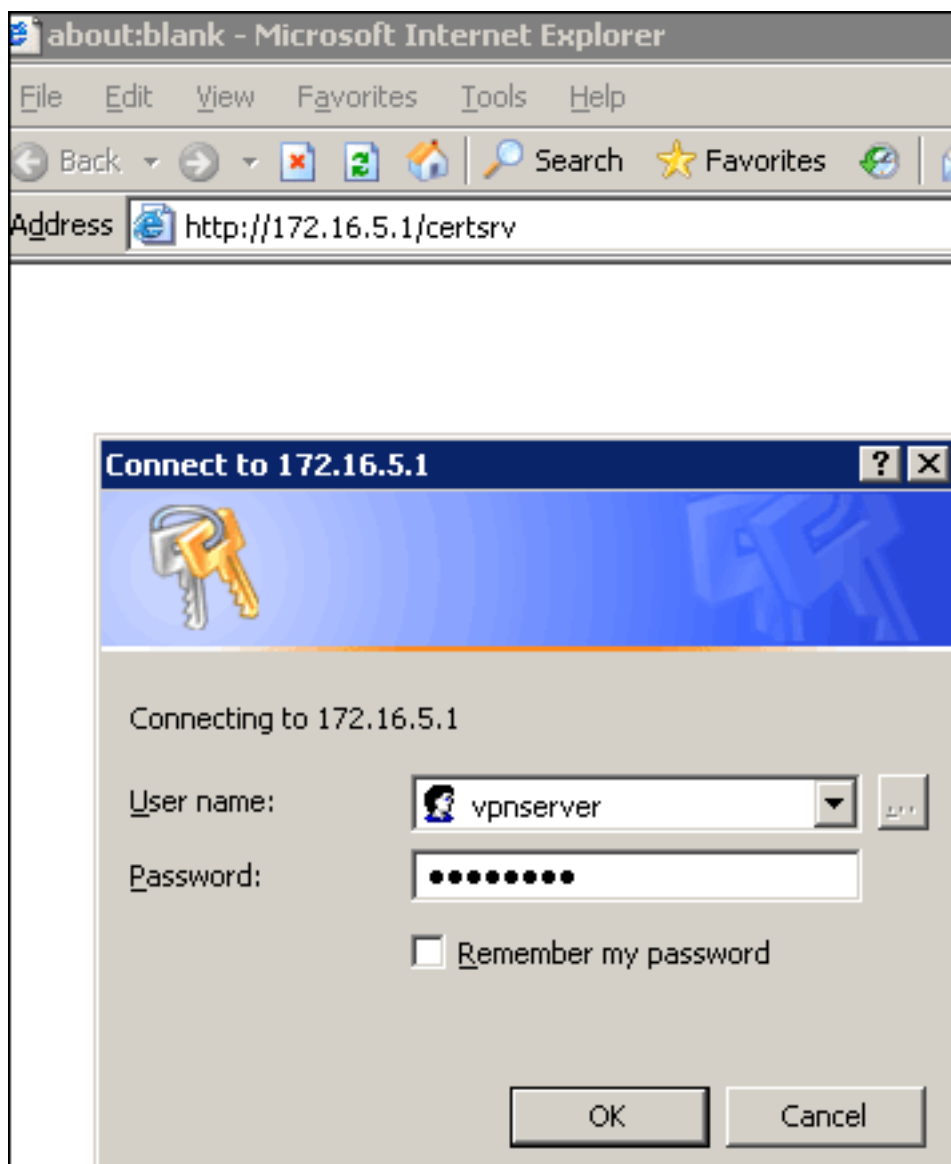
7. Нажмите кнопку Сведения, чтобы получить дополнительную информацию об идентификационном

Отобра



сертификате.

8. Перед установкой сертификата идентификации сертификат ЦС должен быть загружен от сервера CA и установлен в ASA. Выполните следующие шаги для загрузки сертификата CA с сервера CA с названием CA1: Войдите к серверу CA 172.16.5.1 с пользовательскими учетными данными, предоставленными серверу



vpn.

Нажмите **Download**

а **CA certificate**, цепочку сертификатов или **CRL**, и затем установите переключатель **Base 64** для определения способа кодирования. Нажмите **сертификат CA** **Загрузки**.

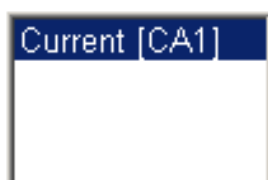


## Download a CA Certificate, Certificate Chain, or CRL

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

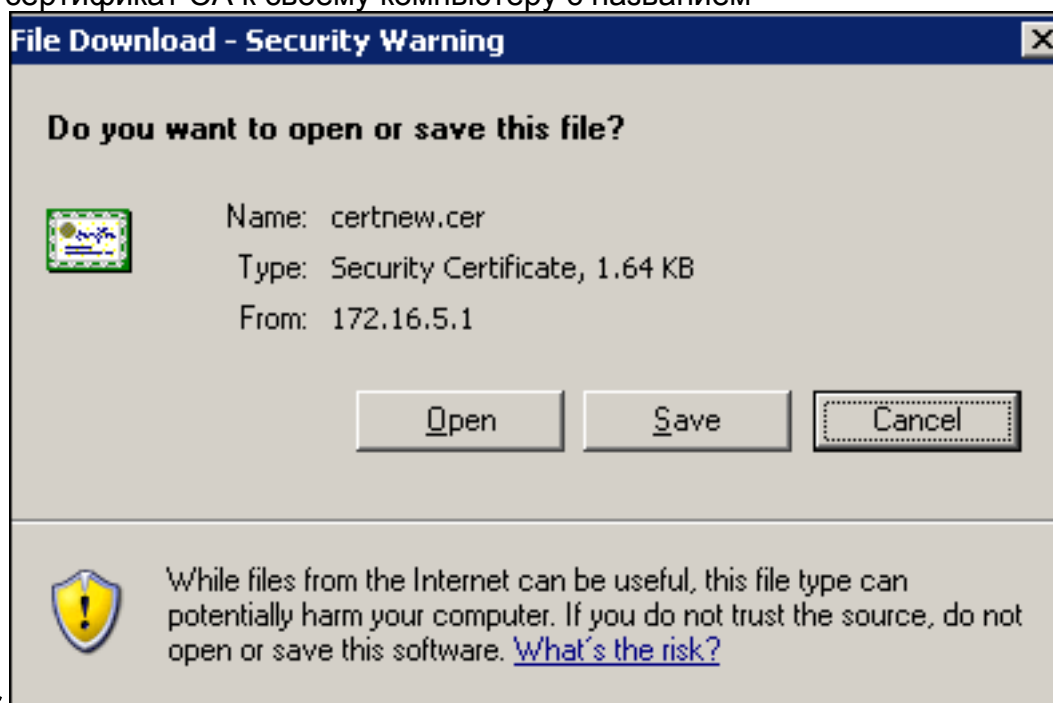
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Сохраните сертификат CA к своему компьютеру с названием

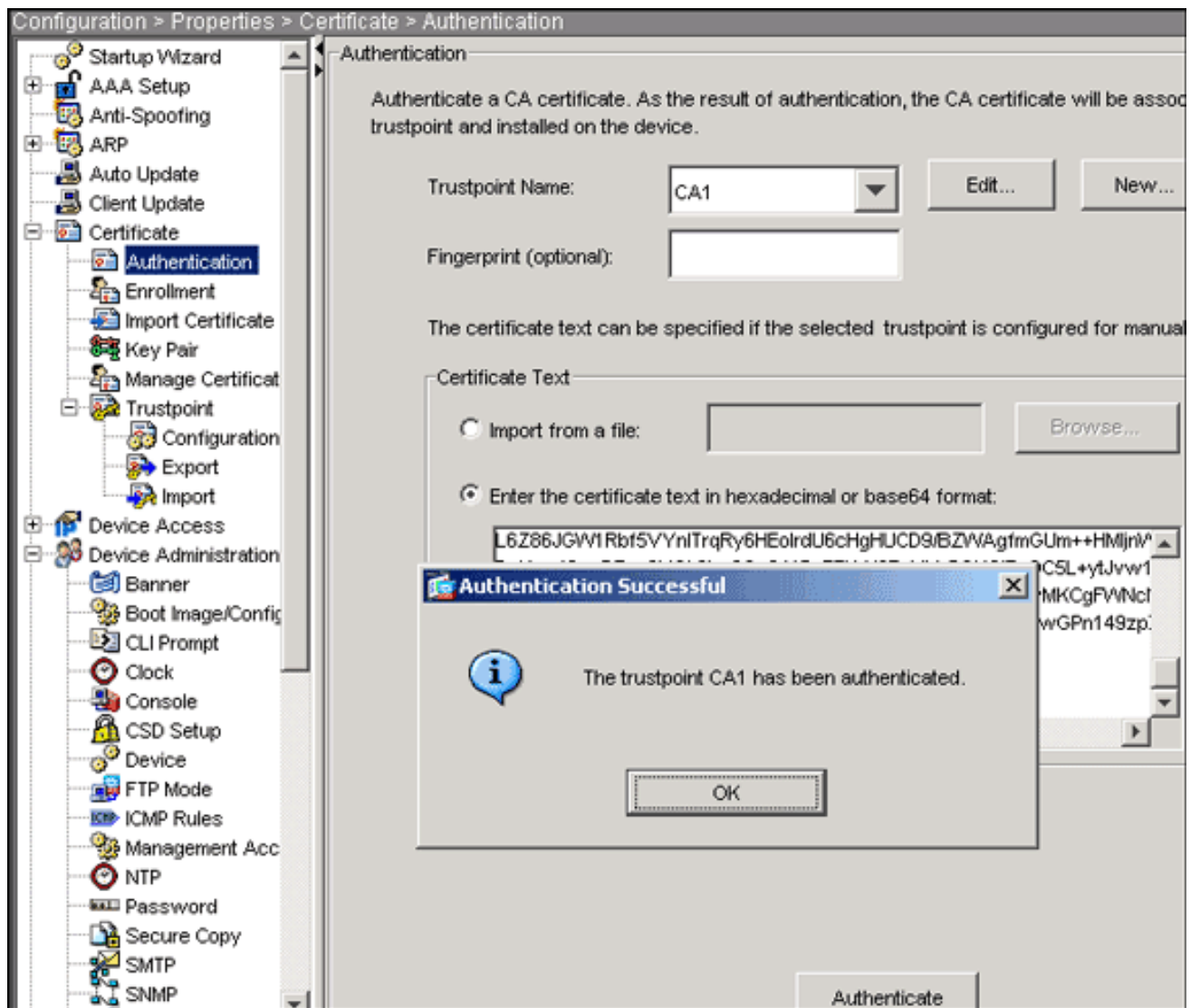


certnew.cer.

9. Перейдите к месту размещения сохраненного сертификата CA.
10. Откройте файл в текстовом редакторе, например, в "Блокнот". **Щелкните его правой кнопкой, а затем выберите Отправить > Блокнот.**)
11. Должно появиться сообщение в кодировке base64, которое похоже на сертификат на следующем рисунке:

```
certnew.cer - Notepad
File Edit Format Help
-----BEGIN CERTIFICATE-----
MIIE nTCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYK CZImiZPyLGQBGRYDY29tMRUwEwYK CZImiZPyLGQBGRYFY2IzY28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0xDTExMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYK CZImiZPyLGQBGRYFVFNXZWIXDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgntjX
bt6czaHpbuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcqnwdoq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhDbMivwqYBXWkh4uc04xxQmr//sct1tdwQcvk2V
UBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSSGAQQBgjCUAgQHgQAQwBBMAsgA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ0E9Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZxk1MjBTZXJ2awN1cyxD
Tj1TZXJ2awN1cyxDTj1Db25mawd1cmF0aw9uLERDPVRTV2ViLERDPwnpc2NvLERD
Pwnvbt9jZXJ0awZpY2F0ZVJldm9jYXRpb25maxN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNwh0dHA6Ly90cy13MmszLWwFjcy50c3dlYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGC5sGAQQBgjCVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MicbXJekr
L6Z86JGw1Rbf5vyn1TrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcNwx1QxsDT+n9YOK6bnG6uof4SgETNrN8EyyVrSGK01E+OC5L+ytJvw19Gzh1ze
1OVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCgFwNcNItcufu0x1b
LXXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPN149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. В ASDM нажмите **Configuration**, и затем нажмите **Properties**.
13. Разверните **Сертификат** и выберите **Authentication**.
14. Нажмите **Enter** текст сертификата в **шестнадцатеричном** или кнопке с зависимой фиксацией **формата base64**.
15. Вставьте отформатированный **base64** Сертификат CA от своего текстового редактора в область для текста.
16. Нажмите **Authenticate**.



17. Нажмите кнопку ОК.

Пример командной строки

### Cisco ASA

```
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-----
MIIEEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUDqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
MRMwEQYKCZImiZPyLQGGRYDY29tMRUwEwYKCZImiZPyLQGGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQGGRYFVFNXZWIxDDAK
BgNVBAMT
A0NBMTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbdosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaenCjs1rxuuaHpIBTuaNOckueBUBjxgPJuNPAk1G8YwBfaTV4M7
kZf4dbQI
```

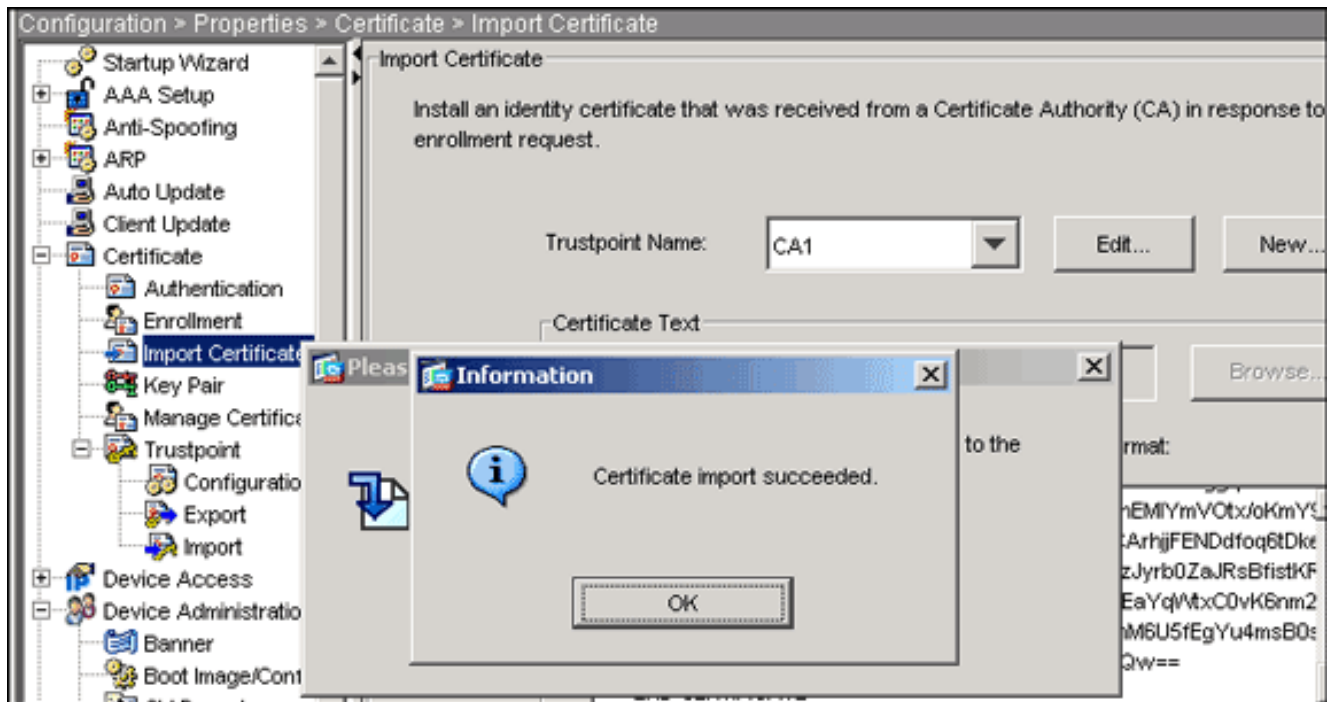
```
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvWqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Qlo+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wgGFrMBMGCSsGAQQBgjcUAQGHGQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwsB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcysZmtQUNTLENOPUNEUCxDTj1QdWJsaWMLmjBLZXk1MjBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIB3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGw1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAqfmGUm++HM1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOLE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNcNI
tcfu0xlb
lXXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqt 9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+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)#
```

## Шаг 6. Установите сертификат

### Порядок действий в диспетчере ASDM

Для выполнения этих шагов используйте идентификационный сертификат, предоставленный сторонним поставщиком:

1. Нажмите **Configuration**, и затем нажмите **Properties**.
2. Разверните **Сертификат**, и затем выберите **Import Certificate**.
3. Нажмите **Enter** текст сертификата в шестнадцатеричном или кнопке с зависимой фиксацией формата **base64**, и вставьте сертификат идентификации base64 в текстовое поле.



4. Нажмите **Import**, и затем нажмите **OK**.

#### Пример командной строки

##### Cisco ASA

```

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+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR
MRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKZImiZPyLGQBGRYFY2lZy28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoxDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxMzUzAVBgNVBAGTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAyDVQQKEw1DaXNjaXN0
ZW1ZMSQw
IgdYDVQDExtDaXNjaXN0FTQ5jaXNjaXN0Y20gT1U9VFNXRUlwgZ8wDQYJ
KoZlhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmFXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVRORBBywFIISQ2lZ
Y29BU0Eu
Y2lZy28uY29tMB0GA1UdDgQWBBSJC3bSQzeGv4tY+MeH7KML0xCFjAF
BgnVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
aWMLMjBLZXk1MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdl
cmF0aW9u

```

```
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnsG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEPMIIBCzCBQQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDtj1BSUESQ049UHVibGljJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBIAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtzh5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnFlzCnqfcyHcETieZtS
tlnwLpsc 1L5nuPsd8MaexBc= -----END CERTIFICATE----- quit
INFO: Certificate successfully imported
CiscoASA(config)#
```

## [Шаг 7. Настройте VPN для удаленного доступа \(IPSec\) для использования нового установленного сертификата](#)

### Порядок действий в диспетчере ASDM

Выполните эти шаги, чтобы настроить удаленный доступ через сеть VPN:

1. Выберите **Configuration> VPN> IKE> Policies> Add** для создания Политики ISAKMP 65535 как показано в этом образе.

**Add IKE Policy**

Priority: 65535      Authentication: rsa-sig

Encryption: 3des      D-H Group: 2

Hash: md5      Lifetime:  Unlimited  
 86400 seconds

OK      Cancel      Help

2. Нажмите кнопку OK, а затем нажмите Apply.
3. Выберите **Configuration> VPN> IPSec> Transform Sets> Add** для создания набора преобразований (*myset*) как показано в этом

**Add Transform Set**

Set Name: myset

Properties

Mode:  Tunnel       Transport

ESP Encryption: 3DES

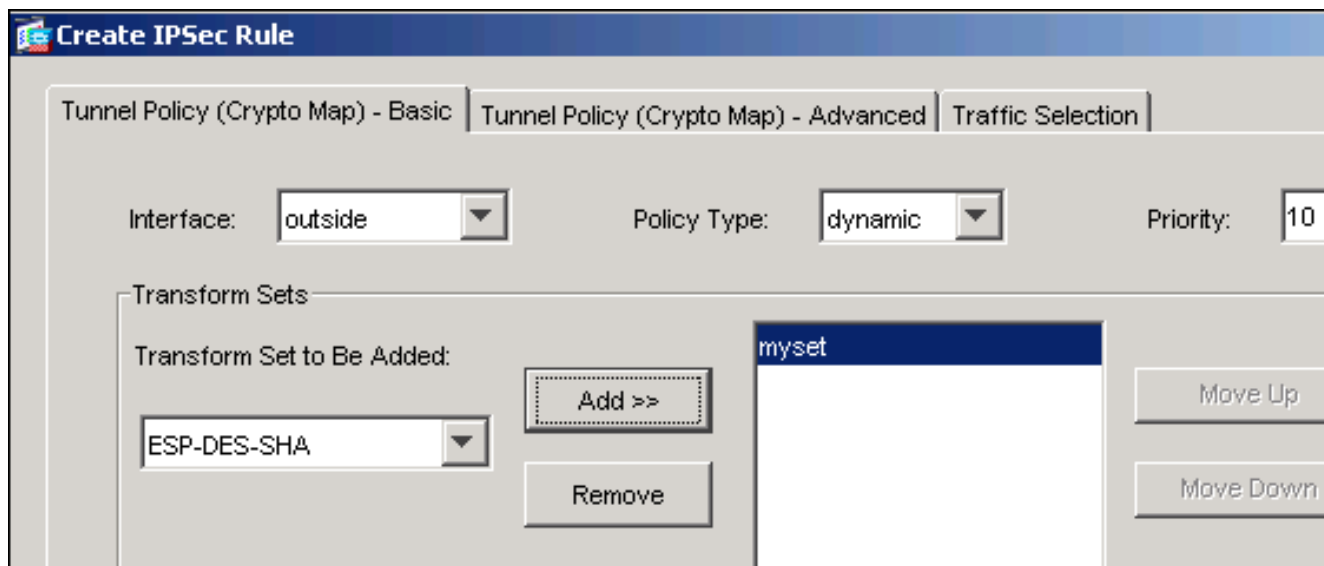
ESP Authentication: MD5

OK      Cancel      Help

образе:

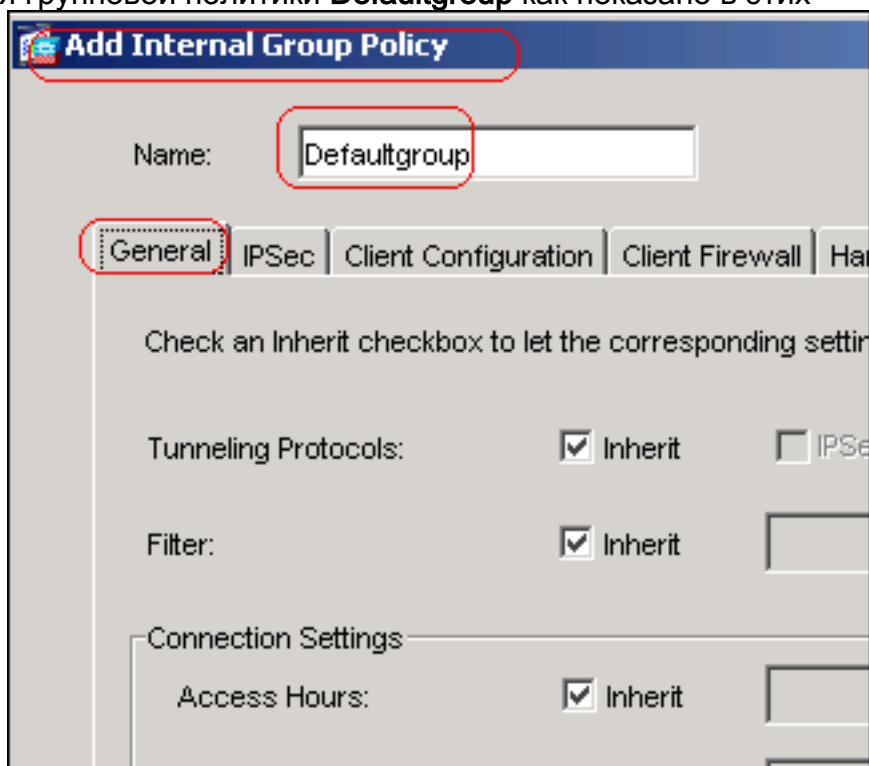
4. Нажмите кнопку OK, а затем Apply
5. Выберите **Configuration> VPN> IPSec> IPSec Rules> Add** для создания криптокарты с динамической политикой приоритета 10 как показано в этом образе:





6. Нажмите кнопку OK, а затем Apply

7. Выберите **Configuration > VPN > General > Group Policy > Add Internal Group Policy** для создания групповой политики **Defaultgroup** как показано в ЭТИХ



образом.



**Add Internal Group Policy**

Name:

General | IPsec | **Client Configuration** | Client Firewall | Hardware Client | NAC | WebV

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

General Client Parameters | Cisco Client Parameters | Microsoft Client Parameters

Banner:  Inherit

Default Domain:  Inherit

8. Нажмите кнопку OK, а затем Apply

9. Выберите **Configuration> VPN> IP Address Management> IP Pools> Add** для настройки пула адресов vpnpool для Пользователей VPN-клиента, которые будут назначены

**Add IP Pool**

Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

динамично.

10. Нажмите кнопку OK, а затем Apply

11. Выберите **Configuration> VPN>,> Users General> Добавляет** для создания учетной записи пользователя vpnuser для доступа клиента

**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

VPN.

12. Добавьте этого пользователя к **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

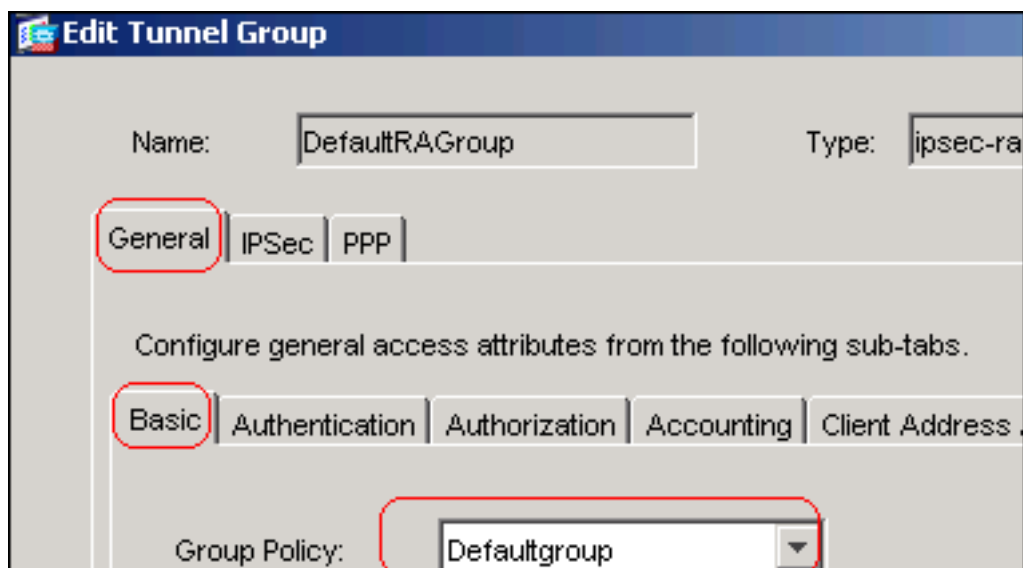
Tunneling Protocols:  Inherit  IPsec  WebVPN

Filter:  Inherit

Tunnel Group Lock:  Inherit DefaultRAGroup

Store Password on Client System:  Inherit  Yes  No

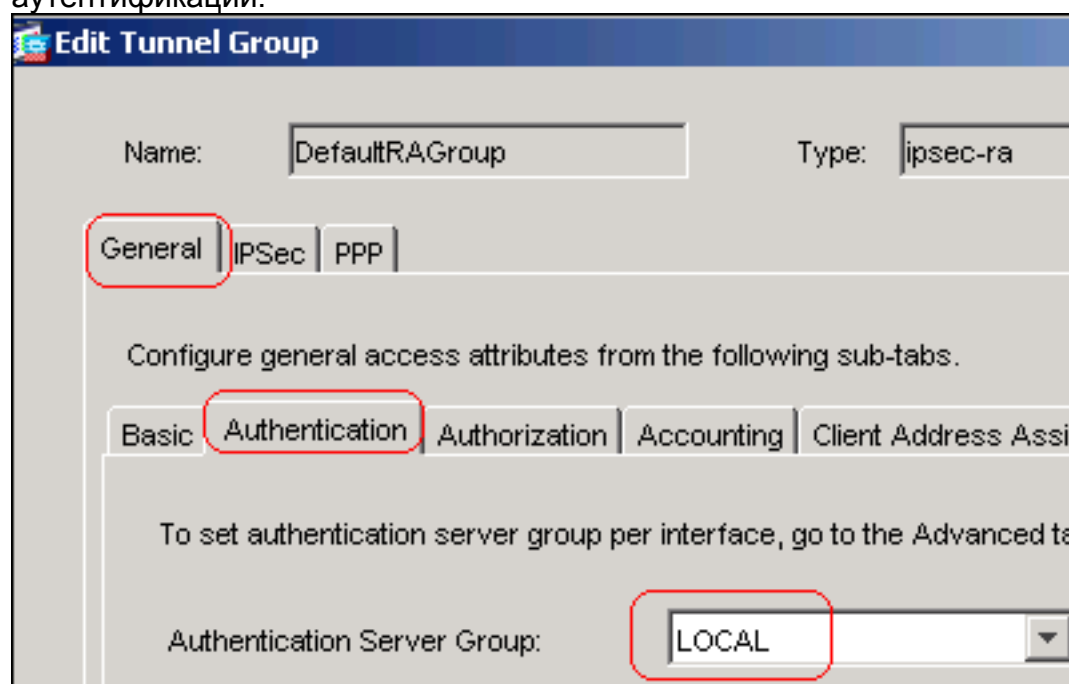
13. Нажмите кнопку **OK**, а затем **Apply**
14. Отредактируйте **DefaultRAGroup**, как описано в этой процедуре: Выберите **Configuration > VPN > General > Tunnel Group > Edit**. Выберите **Defaultgroup** из выпадающего списка Групповой



политики.

Выберит

е LOCAL из выпадающего списка Группы сервера аутентификации.



Выберите

vrpools из выпадающего списка Присвоения Адреса

**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, go to 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"/>

клиента.

15. Нажмите кнопку ОК, а затем Apply.

Пример командной строки

```

Cisco ASA
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

```

## [Сводная таблица конфигурации ASA](#)

### Cisco ASA

```

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 a0030201 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
```

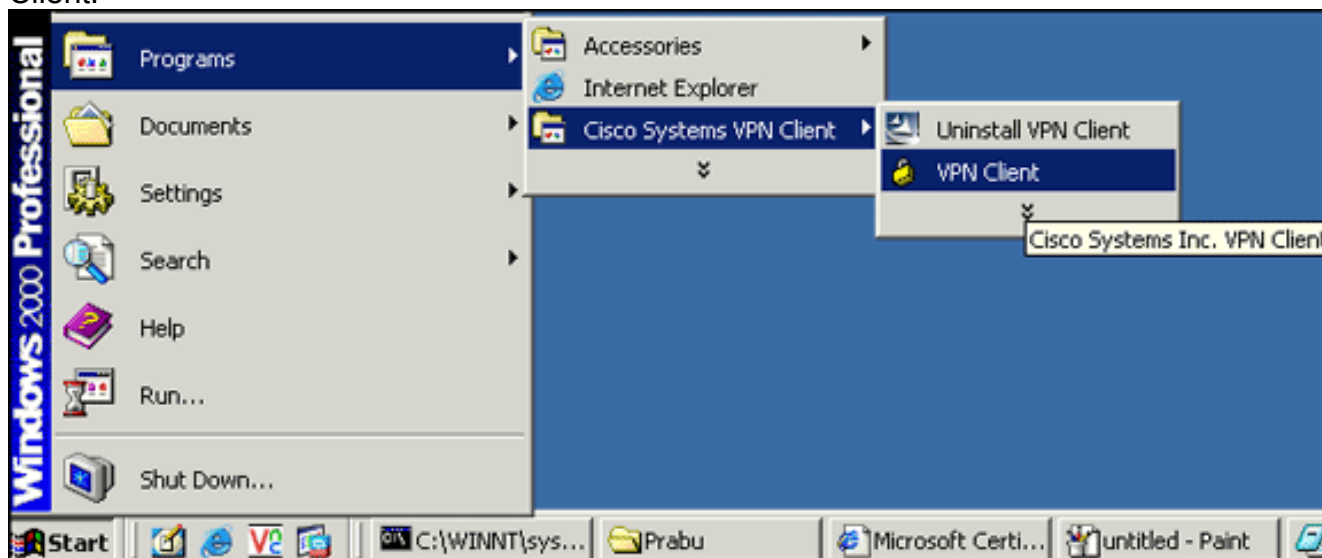
0d030730 0d06092a 864886f7 0d010105 05000382 010100bf  
99b9daf2 e24f1bd6 ce8271eb 908fad3 772df610 0e78b198  
f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e  
20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427  
fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1  
2355c358 a22af8bb e5194b42 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 a1e906ec  
88b32a19 38e5353e 6c0032e8 8c003fa6 2fd22a4d b9dda2c2  
5fcbb621 876bd678 c8a37109 f074eabe 2b1fac59 a78d0a3b  
35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4 9b8d3c09  
351bc630 05f69357 833b9197 f875b408 cb71a814 69a1f331  
bleb2b35 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 526fbc1c 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  
bl699c76 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#
```

## Конфигурация клиента VPN

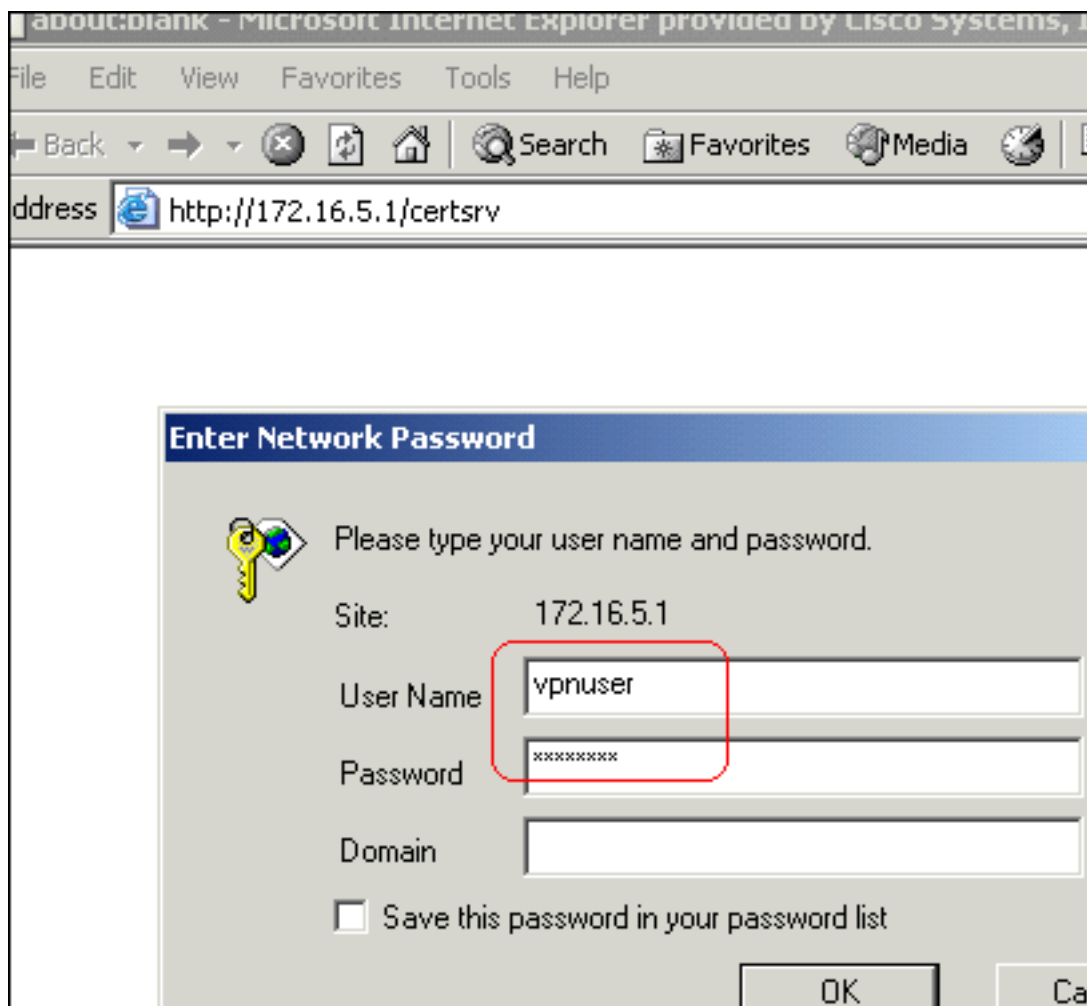
Выполните эти шаги, чтобы настроить VPN-клиент:

1. Выберите **Start> Programs> Cisco Systems VPN Client> VPN Client** для запуска ПО Cisco VPN Client.



2. Выполните следующие шаги, чтобы загрузить сертификат CA с сервера CA с названием CA1 и установить его на Cisco VPN Client: Войдите к серверу CA 172.16.5.1 с пользовательскими учетными данными, предоставленными





vpnuser.

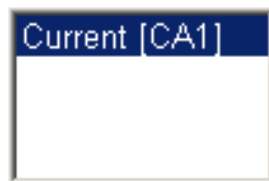
**Примечание:** Удостоверьтесь, что у вас есть учетная запись пользователя для Пользователя VPN-клиента с сервером CA. Нажмите **Download a CA certificate, цепочку сертификатов или CRL**, и затем установите переключатель **Base 64** для определения способа кодирования. Нажмите **сертификат CA Загрузки**.

## 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

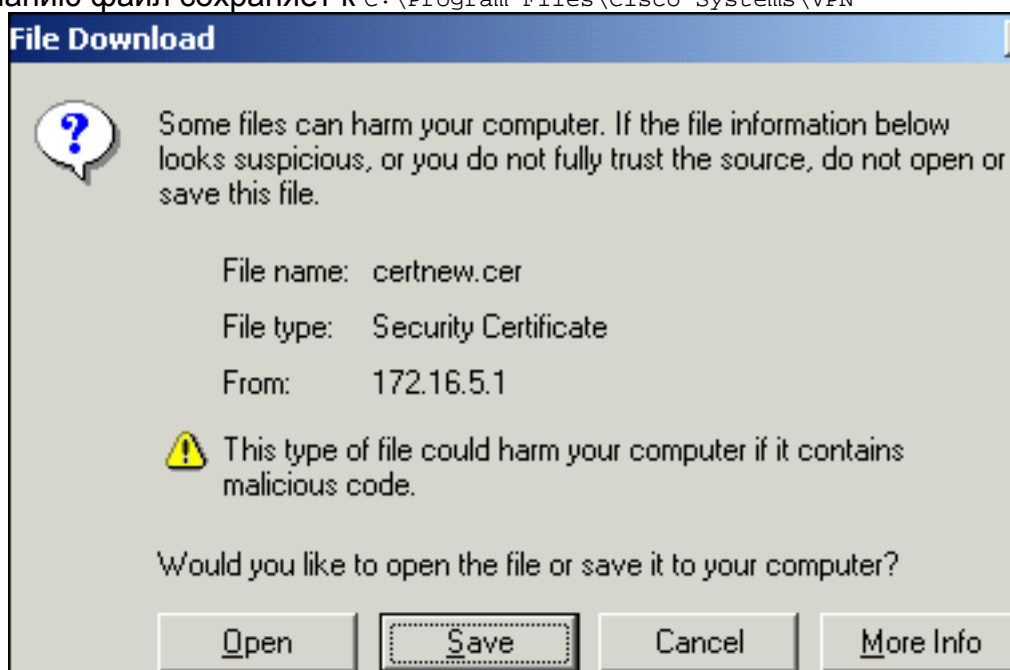
[Download CA certificate](#)

[Download CA certificate chain](#)

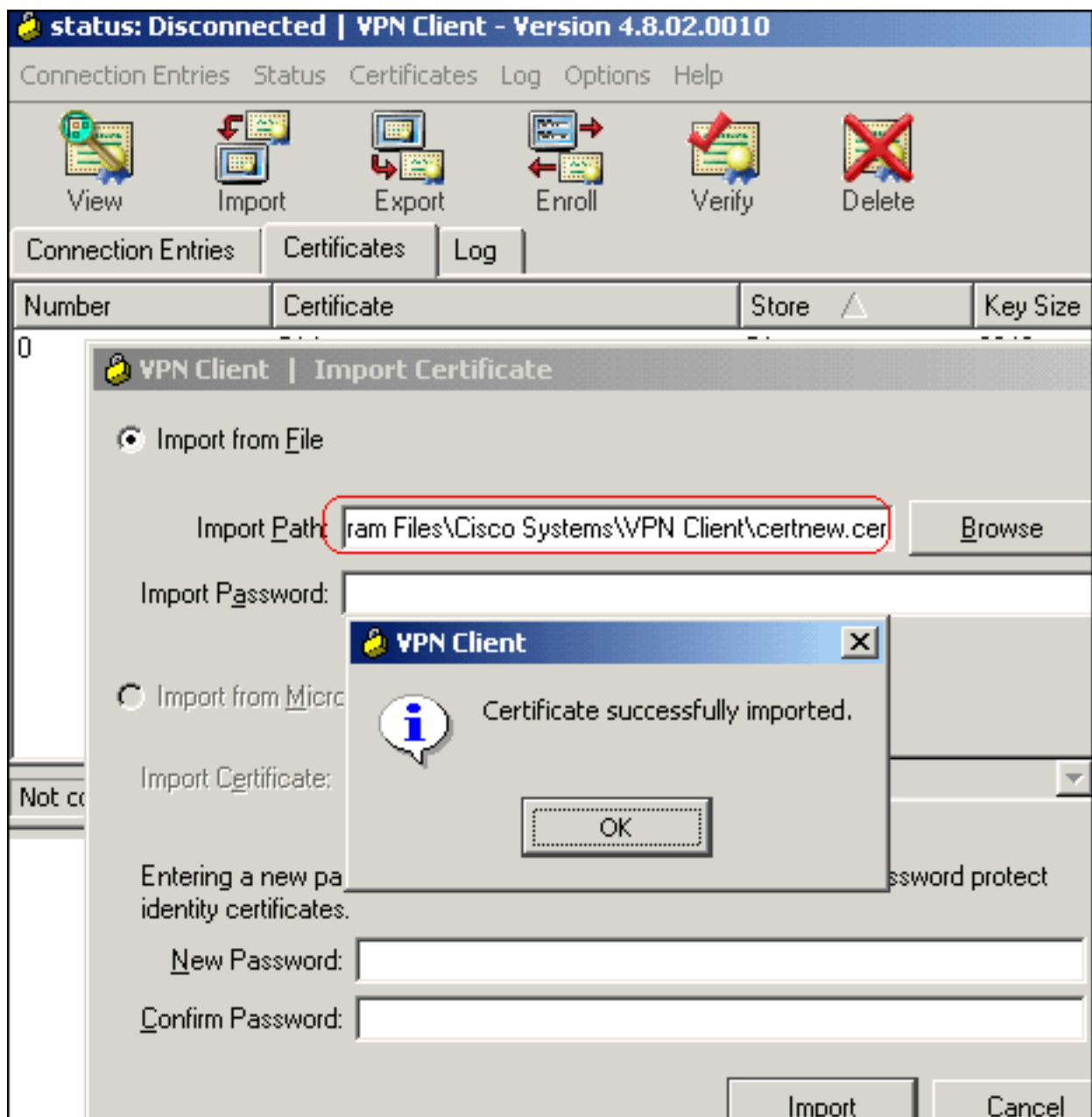
[Download latest base CRL](#)

[Download latest delta CRL](#)

Сохраните сертификат CA к своему компьютеру с названием **certnew.cer**. По умолчанию файл сохраняет к C:\Program Files\Cisco Systems\VPN



Client. В клиенте VPN нажмите вкладку **Certificates**, и затем выберите **Import**. Нажмите кнопку с зависимой фиксацией **Import from File**, и затем нажмите **Browse** для импорта сертификата CA из сохраненного местоположения C:\Program Files\Cisco Systems\VPN Client. **Нажмите кнопку Import (Импортировать)**. Диалоговое окно появляется, который сообщает, что был успешно импортирован сертификат.

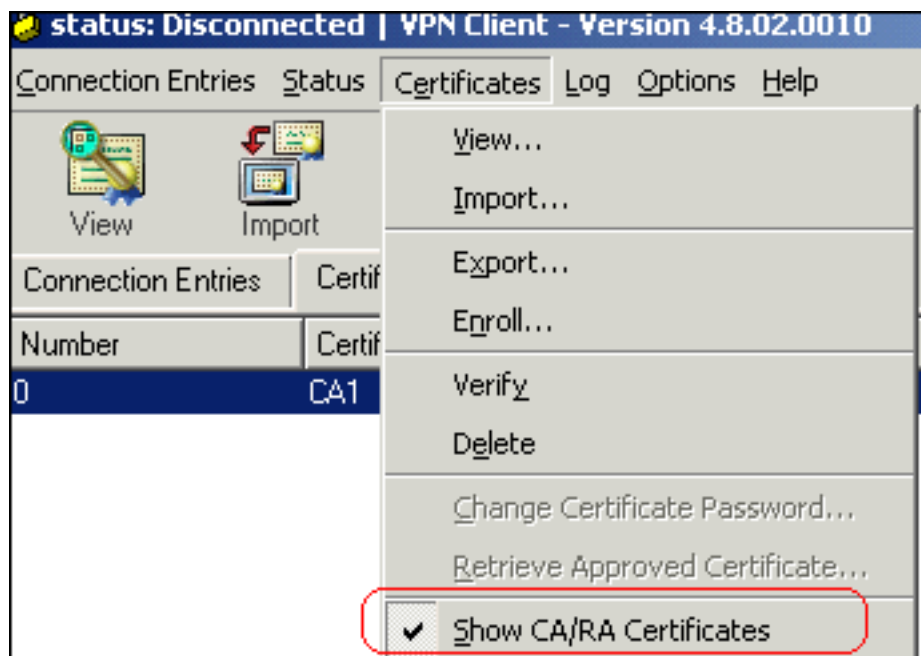


CA1

Сертификатов CA появляется во вкладке Certificates.



**Примечание:** Удостоверьтесь, что выбрана опция **Show CA/RA Certificates**; иначе, сертификаты CA не появятся в окне



сертификата.

3. Выполните следующие шаги для загрузки идентификационного сертификата и установки его на клиент VPN: На сервере CA "CA1" последовательно выберите **Request a Certificate > advanced certificate request > Create and submit a request to this CA**, чтобы зарегистрировать идентификационный сертификат. Нажмите кнопку **Submit (Отправить)**.

### 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:

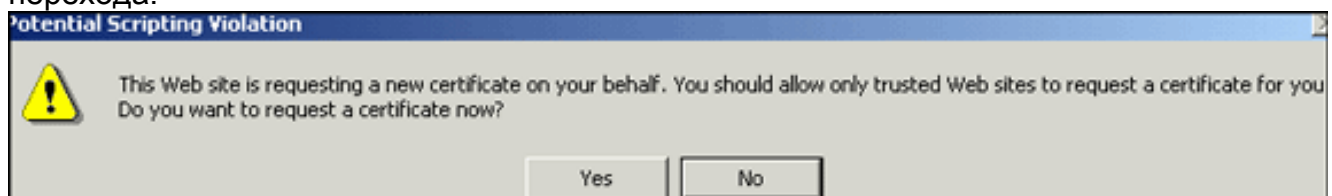
Request Format:  CMC     PKCS10

Hash Algorithm: MD5 ▼

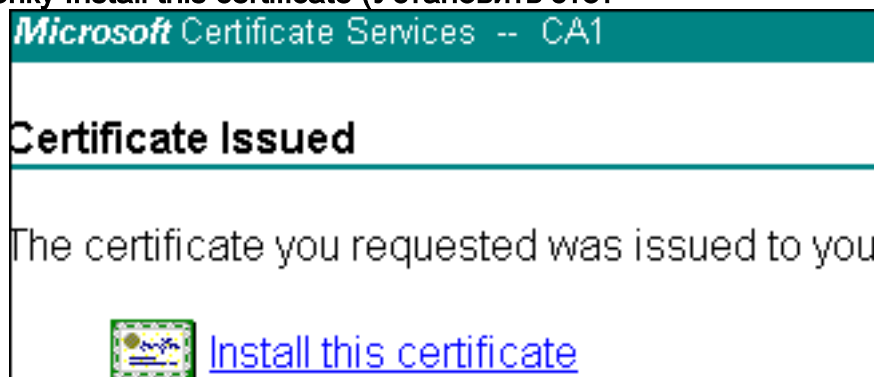
*Only used to sign request.*

Save request to a file

Нажмите **Yes** для  
перехода.



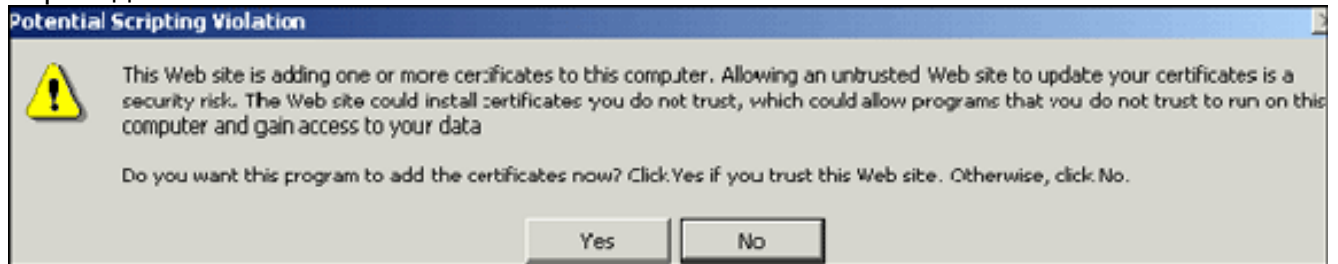
Нажмите кнопку **Install this certificate** (Установить этот



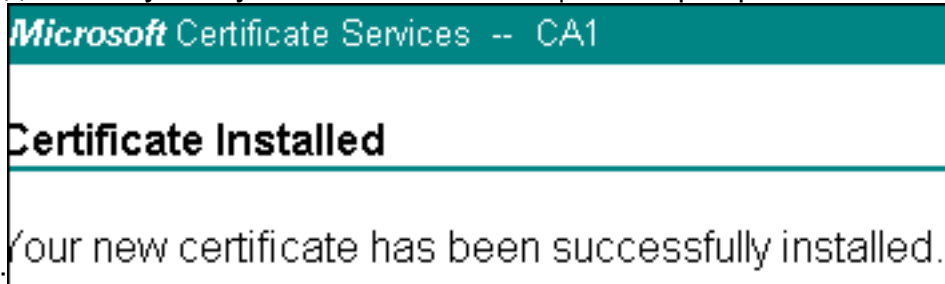
сертификат).

Нажмите **Yes**

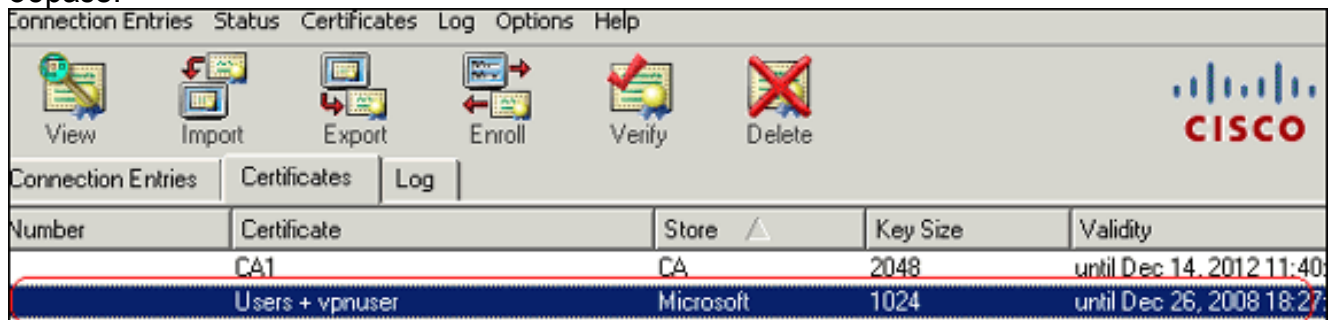
для  
перехода.



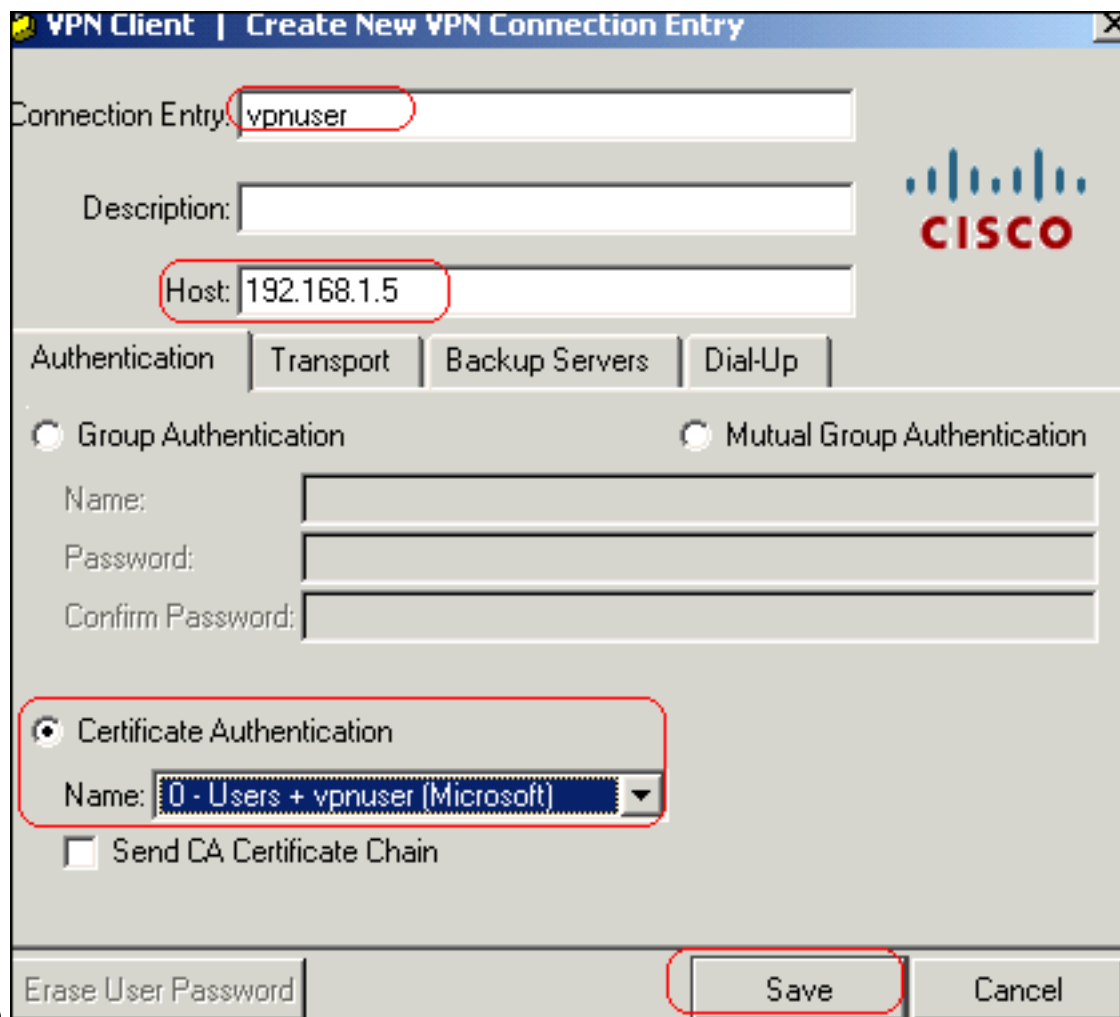
Необходимо получить установленное сообщение сертификата как показано в этом



образе: Выход и затем повторно запускает клиент VPN, чтобы позволить установленному сертификату идентификации появляться во вкладке Certificates клиента VPN как показано в этом образе:

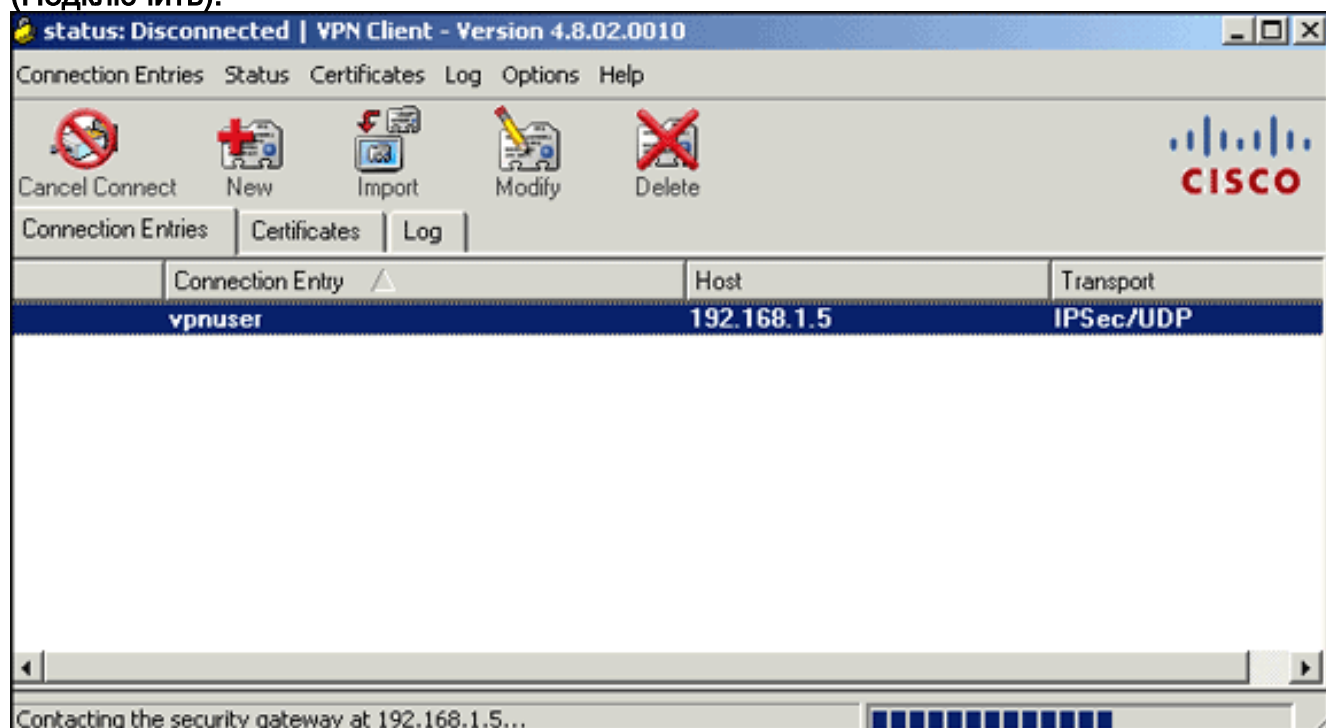


4. Выполните эти шаги для создания соединения (*vpnuser*): Нажмите вкладку Connection Entries, и затем нажмите **New**. Введите IP-адрес (маршрутизируемый) удаленного узла в поле "Host". Установите переключатель **Certificate Authentication** и выберите сертификат идентификации из выпадающего списка. **Нажмите**



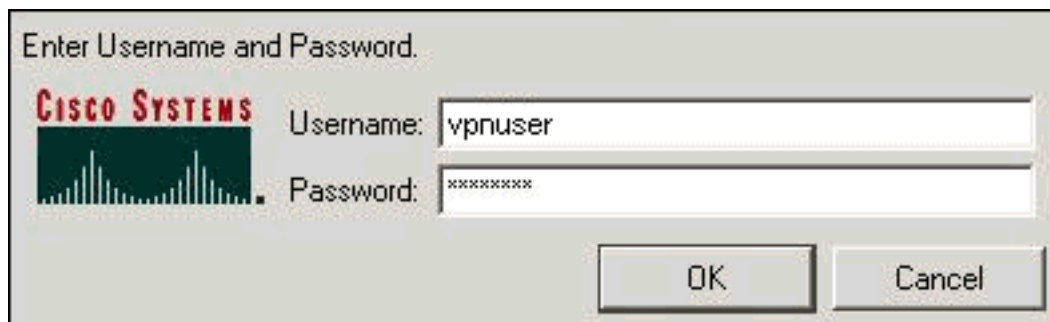
Save.

5. Нажмите кнопку Connect (Подключить).



6. При появлении соответствующего запроса введите имя пользователя и пароль для аутентификации Xauth и нажмите OK для подключения к удаленной





сети.

7. Клиент VPN соединяется с ASA как показано в этом



образе:

## Проверка

На ASA можно использовать несколько команд показа в командной строке для проверки статуса сертификата.

Этот раздел позволяет убедиться, что конфигурация работает правильно.

- **show crypto ca trustpoint** Отображает настроенные точки доверия. 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** Отображает все сертификаты, установленные в СИСТЕМЕ. 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=vpnservers cn=Users dc=TSWeb dc=cisco dc=com PrincipalName: vpnservers@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-ac.s.tsw eb.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-ac.s.tsw eb.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** Отображает списки отзыва кэшированных сертификатов (CRL).
- **show crypto key mypubkey rsa** Отображает все сгенерированные пары криптоключей. 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** сведения о туннеле IKE 1. 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** информация о Туннеле IPsec. 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

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

## Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Здесь приведен ряд сообщений об ошибках, с которыми можно столкнуться:

- **Ошибка: Failed to parse or verify imported certificate (Не удалось обработать или проверить импортированный сертификат)** Эта ошибка может возникнуть тогда, когда был установлен идентификационный сертификат, но не было правильного сертификата промежуточного или корневого СА, удостоверенного связанной точкой доверия. Необходимо удалить и произвести повторную аутентификацию с помощью правильного сертификата промежуточного или корневого СА . Свяжитесь со своим сторонним поставщиком, чтобы убедиться в получении правильного сертификата СА.
- **Certificate does not contain general purpose public key (Сертификат не содержит открытых ключей общего назначения)** Эта ошибка может возникнуть при попытке установить идентификационный сертификат на неверную точку доверия. Вы пытаетесь установить неверный идентификационный сертификат или пара ключей, связанная с точкой доверия, не подходит открытому ключу, содержащемуся в идентификационном сертификате. Воспользуйтесь командой **show crypto sa certificates** имя точки доверия, чтобы удостовериться, что ваш идентификационный сертификат установлен в правильную точку доверия. Обратите внимание на строку **Associated Trustpoints**. Если указана неверная точка доверия, используйте процедуры, описанные в этом документе, чтобы удалить и установить подходящую точку доверия. Также проверьте, не изменилась ли пара ключей с момента создания запроса CSR.
- **Ошибка: ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id: (Sev=Предупреждение/3 IKE/0xE3000081 Неверный идентификатор удаленного сертификата):** Если проблема происходит с сертификатами во время аутентификации, вы могли бы получить эту ошибку в клиенте VPN. Для решения этого вопроса используйте команду **crypto isakmp identity auto** в конфигурации ASA/PIX.

## Дополнительные сведения

- [Страница поддержки устройств адаптивной защиты Cisco](#)
- [Страница поддержки Cisco VPN Client](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Справочники по командам для межсетевого экрана PIX Cisco Secure](#)
- [Уведомления о дефектах продуктов по безопасности \(включая PIX\)](#)
- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)