Introduction

This document describes how to manually install a third party vendor digital certificate on the Cisco Security Appliance (ASA/PIX) 8.x as well as VPN clients in order to authenticate the IPSec peers with the Microsoft Certificate Authority (CA) server.

Prerequisites

Requirements

This document requires that you have access to a certificate authority for certificate enrollment. Supported third party CA vendors are Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign.

This document assumes that there is no pre-existing VPN configuration in the ASA/PIX.

Note: This document uses a Microsoft Windows 2003 server as the CA server for the scenario.

Note: Refer to Configuring CA on Windows server for complete information on how to configure
a Windows 2003 server as a CA.

**Components Used**

The information in this document is based on these software and hardware versions:

- ASA 5510 that runs software version 8.0(2) and ASDM version 6.0(2)
- VPN client that runs software version 4.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

**Related Products**

The ASA configuration can also be used with the Cisco 500 Series PIX that runs software version 8.x.

**Conventions**

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

**Configure**

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the [Command Lookup Tool](#) (registered customers only) in order to obtain more information on the commands used in this section.

**Network Diagram**

This document uses this network setup:

![Network Diagram](image)

**Note:** The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which were used in a lab environment.
Configurations

This document uses these configurations:

- ASA Configuration
- ASA Configuration Summary
- VPN Client Configuration

ASA Configuration

In order to install a third party vendor digital certificate on the ASA, complete these steps:

- Step 1. Verify that the Date, Time, and Time Zone Values are Accurate
- Step 2. Generate a Certificate Signing Request
- Step 3. Authenticate the Trustpoint
- Step 4. Install the Certificate
- Step 5. Configure Remote Access VPN (IPSec) to Use the Newly Installed Certificate

Step 1. Verify that the Date, Time, and Time Zone Values are Accurate

ASDM Procedure

1. Click **Configuration**, and then click **Device Setup**.
2. Expand **System Time**, and choose **Clock**.
3. Verify that the information listed is accurate. The values for Date, Time, and Time Zone must be accurate in order for the proper certificate validation to occur.

![Command Line Example](Image)

Command Line Example

```
CiscoASA
CiscoASA#show clock
```
Step 2. Generate a Certificate Signing Request

A certificate signing request (CSR) is required in order for the third party CA to issue an identity certificate. The CSR contains your ASA’s distinguished name (DN) string along with the ASA’s generated public key. The ASA uses the generated private key to digitally sign the CSR.

ASDM Procedure

1. Click Configuration, and then click Device Management.
2. Expand Certificate Management, and choose Identity Certificates.
3. Click Add.
4. Click the Add a new identity certificate radio button.
5. For the Key Pair, click
6. Click the **Enter new key pair name** radio button. You must distinctly identify the key pair name for recognition purposes.

7. Click **Generate Now**. The key pair must now be created.

8. In order to define the Certificate Subject DN, click **Select**, and configure the attributes listed in this table:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name (CN)</td>
<td>Cisco/ASA.cisco.</td>
</tr>
<tr>
<td>Department (OU)</td>
<td>T5WEB</td>
</tr>
<tr>
<td>Company Name (O)</td>
<td>Cisco Systems</td>
</tr>
<tr>
<td>Country (C)</td>
<td>US</td>
</tr>
<tr>
<td>State (ST)</td>
<td>North Carolina</td>
</tr>
<tr>
<td>Location (L)</td>
<td>Raleigh</td>
</tr>
</tbody>
</table>

   In order to configure these values, choose a value from the Attribute drop-down list, enter the value, and click **Add**.

9. Once the appropriate values are added, click **OK**. The Add Identity Certificate dialog box appears with the Certificate Subject DN field populated.

10. Click **Advanced**.

11. In the FQDN field, enter the FQDN to be used to access the device from the internet. This value must be the same FQDN you used for the Common Name (CN).
12. Click OK, and then click Add Certificate. You are prompted to save the CSR to a file on your local machine.

13. Click Browse, choose a location in which to save the CSR, and save the file with the .txt extension. Note: When you save the file with a .txt extension, you can open the file with a text editor (such as Notepad) and view the PKCS#10 request.
14. Submit the saved CSR to your third party vendor such as Microsoft CA, as shown. Perform the web login into the CA Server 172.16.5.1 with the help of the user credentials supplied for the vpnsolver. 

---End - This line not part of the certificate request---
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

- Create and submit a request to this CA.
- Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Copy and paste the encoded information into the Saved Request box, and then click Submit.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 file (such as a Web server) in the Saved Request box.

Saved Request:

```
vQVNBLmNpc2NvLmNvbTANBkgkqhhkiG9wOBAQQFAAO48fcXxd2O1CbXaoP5L1KbPaEeaCkfN/Pp5mATAsG8D6MEG6cu7Bxj/KlZ6MxafUvCHRopYVvU1wgRJGh+8Ux9emhFHpGHnQ/MpSU2OdQ==
```

Browse for a file to insert.

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Click the Base 64 encoded radio button, and click Download.
The certificate you requested was issued to you.

[Image: Certificate Issued]

The File Download window appears. Save it with the `cert_client_id.cer` name, which is the identity certificate to be installed on the ASA.

**Command Line Example**

```plaintext
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)# crypto ca trustpoint CA1
   ciscoasa(config-ca-trustpoint)# subject-name CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh !--- Defines x.500 distinguished name. Use the attributes defined in table as a guide. ciscoasa(config-ca-trustpoint)# keypair my.CA.key !--- Specifies key pair generated in Step 3 ciscoasa(config-ca-trustpoint)# fqdn CiscoASA.cisco.com !--- Specifies the FQDN (DNS:) to be used as the subject alternative name
```
Step 3. Authenticate the Trustpoint

Once you receive the identity certificate from the third party vendor, you can proceed with this step.

ASDM Procedure

1. Save the identity certificate to your local computer.
2. If your were provided a base64-encoded certificate that did not come as a file, you must copy the base64 message and paste it into a text file.
3. Rename the file with a .cer extension
   - Note: Once the file is renamed with the .cer extension, the file icon displays as a certificate, as shown.
4. Double-click the certificate
Note: If the Windows does not have enough information to verify this certificate message appears in the General tab, you must obtain the third party vendor root CA or intermediate CA certificate before you continue with this procedure. Contact your third party vendor or CA administrator in order to obtain the issuing root CA or intermediate CA certificate.

5. Click the Certificate Path tab.
6. Click the CA certificate associated with your issued identity certificate, and click View.
7. Click **Details** in order to know more information about the identity certificate.

8. Before you install the identity certificate, the CA certificate must be downloaded from the CA server and installed in the ASA, as shown. Complete these steps in order to download the CA certificate from the CA server named **CA1**. Perform the web login into the CA server 172.16.5.1 with the help of the credentials supplied to the VPN.
Click **Download a CA certificate, certificate chain or CRL** in order to open the window, as shown. Click the **Base 64** radio button as the encoding method, and click **Download CA certificate**.
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:

<table>
<thead>
<tr>
<th>Current [CA1]</th>
</tr>
</thead>
</table>

Encoding method:

- DER
- Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Save the CA certificate with the certnew.cer name on your computer.

9. Browse to the location where you saved the CA certificate.
10. Open the file with a text editor, such as Notepad. Right-click the file, and choose Send To > Notepad.
11. The base64-encoded message similar to the certificate in this image appears:
12. Within ASDM, click **Configuration**, and then click **Device Management**.

13. Expand **Certificate Management**, and choose **CA Certificates**.

14. Click **Add**.

15. Click the **Paste certificate in PEM Format** radio button, and paste the base64 CA certificate provided by the third party vendor into the text field.

16. Click **Install Certificate**.
Dialog box appears that confirms the installation is successful.

**Command Line Example**

```
CiscoASA(config)#crypto ca authenticate CA1 !---
Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provided by the third party vendor. Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIEnTCCA4gAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYKCIimI2PyLgQBGRYDY29tMRUwEwYKCIimI2PyLgQBGRYFY1lz
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0EM4XDTA3MzExMDk5MDExM1oX
MDAwMDMwMBMGCgMS
JomT8ixkArkWBWncpc2NmRuwEwYKCIimI2PyLgQBGRYFYFNYZXWixDDAK
BgNVBAAM
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
```
Step 4. Install the Certificate

ASDM Procedure

Use the identity certificate provided by the third party vendor in order to complete these steps:

1. Click Configuration, and then click Device Management.
2. Expand Certificate Management, and then choose Identity Certificates.
3. Select the identity certificate you created in Step 2. Note: The Expiry Date displays Pending.
4. Click Install.
Click the **Paste the certificate data in base-64 format** radio button, and paste the identity certificate provided by the third party vendor into the text field.

5. Click **Install Certificate**. A dialog box appears in order to confirm the import is successful.

**Command Line Example**

```
CiscoASA
CiscoASA(config)# crypto ca import CA1 certificate
---
Initiates prompt to paste the base64 identity certificate provided by the third 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 third party vendor. ---BEGIN CERTIFICATE-----
[a-long base-64 certificate]
---END CERTIFICATE-----
```

Step 5. Configure Remote Access VPN (IPSec) to Use the Newly Installed Certificate

ASDM Procedure

Complete these steps in order to configure the remote access VPN:

1. Choose Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add in order to create a ISAKMP policy 65535, as shown.
Click OK and Apply.

2. Choose Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add in order to create the myset transform set, as shown. Click OK and Apply.

3. Choose Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add in order to create a crypto map with dynamic policy of priority 10, as shown.
Click OK and Apply. Note: ASA 8.0 does not support SHA 2. Also IPSec clients that use certificates with a 256 hash are not supported.

4. Choose Configuration > Remote Access VPN > Network (Client) Access > Advanced > Group Policies > Add in order to create a Defaultgroup group policy, as shown.

Click OK and Apply.

5. Choose Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add in order to configure the vpnpool address pool for the VPN client users to be assigned
dynamically. Click OK and Apply.

6. Choose Configuration > Remote Access VPN > AAA Setup > Local Users > Add in order to create the vpnuser user account for VPN client access. Also, make this user a member of DefaultRAGroup.

7. Choose Configuration > Remote Access VPN > Network (Client) Access > IPSec
Connection Profiles > Edit in order to edit the DefaultRAGroup, as shown. Choose the appropriate identity certificate from the drop down for IKE Peer Authentication field. Choose the server group as LOCAL for the User Authentication field. Choose vpnpool as the Client Address Pool for the Client Address Assignment field. Choose defaultgroup as the Group Policy for the Default Group Policy field.

Choose the appropriate identity certificate from the drop down for IKE Peer Authentication field. Choose the server group as LOCAL for the User Authentication field. Choose vpnpool as the Client Address Pool for the Client Address Assignment field. Choose defaultgroup as the Group Policy for the Default Group Policy field.

Click OK and Apply.

Command Line Example

```bash
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 dynmap 10 set transform-set myset CiscoASA(config)#crypto map mymap 10 ipsec-isakmp dynamic dynmap CiscoASA(config)#crypto map mymap 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
Cisco123 CiscoASA(config)#username vpnuser password CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit !--- Create a user account "vpnuser" and added to "DefaultGroup"
```
CiscoASA(config)#tunnel-group DefaultRAGroup general-attributes

--- The Security Appliance provides the default tunnel groups!--- for remote access

(DefautRAGroup). 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 Configuration Summary

CiscoASA

CiscoASA#show running-config

--- Saved
---
ASA Version 8.0(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
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
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
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
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:00
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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
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 dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap 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=Rale
serial-number
keypair my.CA.key
crl configure
crypto ca certificate chain CA1
certificate 611ee59b0000000000000007
   308205a7 3082048f a0030201 0202a61 1ee59b00
00000000 07300d06 092a8648
   86f7d01 01050500 30513113 3011060a 09922689
   93f22c64 01119160 363f6d31
   15301306 0a099226 8993f22c 64011916 05636973
   636f3115 3013060a 09922689
   93f22c64 01119160 54535765 62310c30 0a060355
   04031303 43413130 1e170d30
   37313231 35303833 3533395a 170d3039 31323134
   30383335 33395a30 76310b30
   09060355 04061302 55533117 30150603 55040813
   0e4e6f72 74686204 61726f6c
   6966131 10300e06 03550407 13075261 6c656967
   68311630 14060355 040a130d
   436f7363 6f205379 7374656d 73312430 22060355
   04031301 43697363 6f415341
   2e636973 6f6204f 553d5453 57454230
   819f200d 06092a86 4886f70d
   01010105 003818d 00308189 02818100 b8e20aa8
crypto isakmp enable outside
crypto isakmp policy 65535
  authentication rsa-sig
  encryption 3des
  hash md5
  group 2
  lifetime 86400
crypto isakmp identity auto
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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 esmtpl
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
policy-group defaultgroup internal
group-policy defaultgroup attributes
  default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
Complete these steps in order to configure the VPN client.

1. Choose Start > Programs > Cisco Systems VPN Client > VPN Client in order to launch the VPN client software.

2. Complete these steps in order to download the CA certificate from the CA server named CA1, and install it into Cisco VPN client. Perform the web login into the CA server 172.16.5.1 with the help of the credentials supplied to the
vpnuser.

Note: Make sure that you have a user account for the VPN client user with the CA server. Click Download a CA certificate, certificate chain or CRL in order to open the window, as shown. Click the Base 64 radio button as the encoding method, and click Download CA certificate.
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

Save the CA certificate with the certnew.cer name on your computer. By default, it stores in the C:\Program Files\Cisco Systems\VPN Client path.

In the VPN client, choose Certificates tab > Import, and click the Import from File radio button. Click Browse in order to import the CA certificate from the stored location C:\Program Files\Cisco Systems\VPN Client, as shown. Click Import. A success window appears, as shown.
In the Certificates tab, the CA Certificates CA1 appears, as shown.

**Note:** Make sure that the **Show CA/RA Certificates** option is chosen, as shown, otherwise the CA certificates must not appear in the certificate.
3. Complete these steps in order to download the Identity certificate and install it into the VPN client. In the CA server CA1, choose **Request a Certificate > advanced certificate request > Create and submit a request to this CA** in order to enroll for the identity certificate. Click **Submit**.
Certificate Template:

Key Options:

- Create new key set
- Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: Exchange

Key Size: 1024

- 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

Click Yes in order to proceed.

Certificate Issued

The certificate you requested was issued to you.
to proceed.

You must receive the certificate installed message, as shown. Exit the VPN client and re-launch it in order to make the installed identity certificate start to appear in the certificate tab of the VPN client, as shown.

4. In the Connection entries tab, click New in order to create connection entry vpnuser, as shown. Enter the remote peer IP address (routable) in the Host field. Click the Certificate Authentication radio button, and choose the identity certificate from the drop down list, as shown. Click
5. Click **Connect**.

6. When prompted, enter the Username and Password information for xauth, and click **OK** in order to connect to the remote.
network.

7. The VPN client connects with the ASA, as shown.

**Verify**

On the ASA you can issue several show commands at the command line in order to verify the status of a certificate.

Use this section in order to confirm that your configuration works properly.

- **The `show crypto ca trustpoint` command displays configured trustpoints.**
  CiscoASA# show crypto ca trustpoints
  Trustpoint CA1:
  Subject Name:
  cn=CA1
dc=TSWeb
dc=cisco
dc=com
  Serial Number: 7099f1994764e09c4651da80a16b749c
  Certificate configured.
- **The `show crypto ca certificate` command displays all the certificates installed on the system.**
  CiscoASA# show crypto ca certificate
  Certificate
  Status: Available
  Certificate Serial Number: 3f14b70b00000000000f
  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=Configuration,DC=TSWeb,DC=cisco,
  DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  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=Configuration,DC=TSWeb,DC=cisco,
      DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
Validity Date:
  start date: 06:01:43 UTC Dec 14 2007
  end   date: 06:10:15 UTC Dec 14 2012
Associated Trustpoints: CA1

Certificate
Subject Name:
  Name: CiscoASA.cisco.com
Status: Pending terminal enrollment
Key Usage: General Purpose
Fingerprint: 1a022cf2 9771e335 12c3a530 1f9a0345
Associated Trustpoint: CA1

- The `show crypto ca crls` command displays cached certificate revocation lists (CRL).
- The `show crypto key mypubkey rsa` command displays all generated crypto key pairs.

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
99e995d6c b5bdad625 777aebebe 6ee428e6 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d387c70 29031b76 6853c96f 36229b14 fef3d3298 69f9123c 37f6c43b
4f8384c4 a736426d 457665c7 f04cbaf1 29a95890 84d2c5d4 adefe2b4 01b1f68
2fe4b9b1 5fa12de0 7789ace45 55190e79 1364aba4 7b2b21ca defaf74d 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 00d8e20a
99e995d6c b5bdad625 777aebebe 6ee428e6 23c49f9a bea53224 0234b843 1c0c8541
f5a66eb1 6d387c70 29031b76 6853c96f 36229b14 fef3d3298 69f9123c 37f6c43b
4f8384c4 a736426d 457665c7 f04cbaf1 29a95890 84d2c5d4 adefe2b4 01b1f68
2fe4b9b1 5fa12de0 7789ace45 55190e79 1364aba4 7b2b21ca defaf74d b7020301 0001
Key pair was generated at: 07:35:18 UTC Dec 21 2007
CiscoASA#
The `show crypto isakmp sa` command displays the IKE 1 tunnel information.

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

The `show crypto ipsec sa` command displays the IPSec tunnel information.

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

The Output Interpreter Tool (registered customers only) (OIT) supports certain `show` commands. Use the OIT in order to view an analysis of `show` command output.

**Troubleshoot**

This section provides information you can use in order to troubleshoot your configuration.

Here are some possible errors that you can encounter:

- **ERROR: Failed to parse or verify imported certificate** This error can occur when you install
the identity certificate and do not have the correct intermediate or root CA certificate authenticated with the associated trustpoint. You must remove and reauthenticate with the correct intermediate or root CA certificate. Contact your third party vendor in order to verify that you received the correct CA certificate.

- **Certificate does not contain general purpose public key** This error can occur when you attempt to install your identity certificate to the wrong Trustpoint. You attempt to install an invalid identity certificate, or the key pair associated with the Trustpoint does not match the public key contained in the identity certificate. Issue the `show crypto ca certificates trustpointname` command in order to verify you installed your identity certificate to the correct trustpoint. Look for the line stating **Associated Trustpoints**: If the wrong trustpoint is listed, use the procedures described in this document in order to remove and reinstall the appropriate trustpoint. Also, verify the key pair has not changed since the CSR was generated.

- **ERROR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:** If you have authentication problems with certificates, this error message can appear in the VPN client. Use the command `crypto isakmp identity auto` in the ASA/PIX configuration in order to resolve the issue.

**Related Information**

- [Cisco Adaptive Security Appliance Support page](#)
- [Cisco VPN Client Support Page](#)
- [Configuring Microsoft Server as Certificate Authority (CA)](#)
- [Technical Support & Documentation - Cisco Systems](#)