

## Introduction

This technote will detail how to use the open source program 'OpenSSL' (<http://www.openssl.org>) to create a private Certificate Authority, and use it to process certificate requests for server and client certificates. Please note that this process should only be used for testing purposes and not for production environments. OpenSSL is available on a number of platforms, and path references will change depending upon the platform that OpenSSL is being run on. Please ensure that the OpenSSL working directory contains the 'openssl\_config.txt' file before beginning this process.

In the examples below, any OpenSSL user-input commands shown below will be italicized. Replace any prompt field marked with '[ ]' with your site-specific information.

At the end of this technote, we'll also detail how to configure a SonicWALL so that it can accept Global VPN connections using third-party certificates as the authentication mechanism.

## Creating a Certificate Authority (CA)

The steps below detail how to use OpenSSL to create all the materials you will need to create a private CA that can be used to process client and server certificate requests. When done, be sure to store the CA's key in a secure location.

1. Create a working directory:
  - Make sure you have a directory called '\certs' before you begin.
2. Generate the CA's private/public keypair:
  - Start the OpenSSL program.
  - OpenSSL> *genrsa -des3 -out \certs\cakey.key 1024*
  - Enter a complex passphrase to protect the CA's key.
3. Generate the CA's certificate signing request:
  - OpenSSL> *req -new -key \certs\cakey.key -config openssl\_config.txt -out \certs\cacsr.csr*
  - Enter the passphrase used to protect the CA's key.
  - Fill in the following fields with your info: Country [ ]: State or Province [ ]: Locality [ ]: Organization Name [ ]: Organizational Unit Name [ ]: Domain Name [ ]: test@email.address [ ]:
4. Using a text editor, create an 'extension' file with the following attributes:
  - subjectAltName = DNS :[ ] basicConstraints = critical,CA:TRUE,pathlen:0 nsCertType = sslCA,emailCA,objCA nsComment = "This certificate was issued for testing purposes"
  - Save this file as: \certs\caext.txt
5. Self-sign the CA's certificate:
  - OpenSSL> *x509 -req -days 1095 -in \certs\cacsr.csr -signkey \certs\cakey.key -extfile \certs\caext.txt -out C:\certs\cacert.pem*
  - Enter the passphrase used to protect the CA's key.

The current version of the SonicWALL Global VPN Client does not have any mechanisms for creating a public/private keypair, or a certificate signing request (CSR). In order to use third-party certificates with the SonicWALL Global VPN Client, you must use an external utility to generate these items, and then convert the private key and client certificate into PKCS#12 (.pfx) format before importing them. The steps below detail how to use OpenSSL to create a keypair for the client, generate a CSR based upon that keypair, process the

## Tech Note

CSR with your private CA, and convert the client's key and cert into proper format for import into the Global VPN Client. For this example, we'll be attaching a unique user email address field to the final client certificate via the use of a special 'extensions' file entry called "SubjectAltName". Each time you create a unique client certificate, be sure to modify this entry in the extensions file with the user's unique email address. We'll be using this entry as a filtering mechanism later on (see page xx).

1. Generate the client's private/public keypair:

-OpenSSL> genrsa -des3 -out \certs\clientkey.key 1024

2. Generate the client's certificate signing request (CSR): OpenSSL> req -new -key \certs\clientkey.key -config openssl\_config.txt -out \certs\clientcsr.csr Fill in the following fields with your info:

Country [ ]: State or Province [ ]: Locality [ ]: Organization Name [ ]: Organizational Unit Name [ ]:

Domain Name [ ]:test@email.address [ ]:

2 Using a text editor, create an 'extension' file with the following attributes:

```
subjectAltName = email:[ ] basicConstraints = critical,CA:FALSE nsCertType = client,email  
nsComment = "This certificate was issued for testing purposes"
```

- Save the file as: \certs\clientext.txt

4. Sign the client's CSR with the CA and apply the extension file:

- OpenSSL> x509 -req -days 365 -CA \certs\cacert.pem -CAkey \certs\cakey.key -CAcreateserial -in \certs\clientcsr.csr -extfile \certs\clientext.txt -out \certs\clientcert.pem

- Enter the passphrase used to protect the CA's key.

5. Convert the client's key and certificate into PKCS#12 format:

- OpenSSL> pkcs12 -export -clcerts -in \certs\clientcert.pem -inkey \certs\clientkey.key -out \certs\clientpkcs12.pfx

- Enter the passphrase used to protect the client's key.

- Enter a complex export passphrase, and enter it again to confirm.

6. Import 'clientpkcs12.pfx' and 'cacert.pem' into the SonicWALL Global VPN Client

- Start the SonicWALL Global VPN Client.

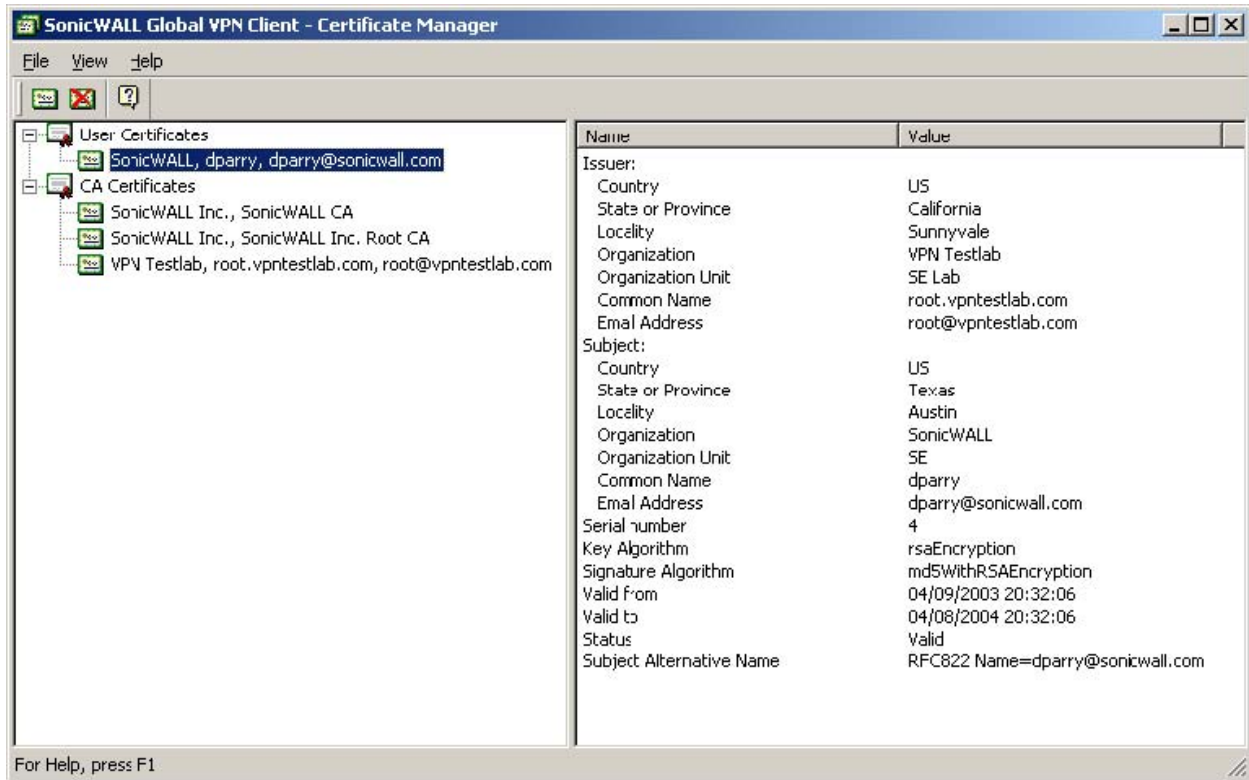
- From the 'View Menu', select 'Certificate Manager'.

- From the 'File Menu' of the Certificate Manager, Select 'Import Certificate'.

- Navigate to where the 'cacert.pem' and 'clientpkcs12.pfx' files are located and import them both; you will be prompted to enter the export passphrase created in step five.

## Tech Note

If the import was successful, you should be able to view the client cert and the CA cert. An example is below:



### **Signing a SonicWALL's Certificate Signing Request (CSR)**

The SonicWALL GUI for firmware 6.3.x.x and later include keypair and CSR generation tools. To create a keypair and a CSR to process with your private CA, open the SonicWALL device GUI, click on the 'VPN' button, and select the 'Local Certificates' tab.

1. Fill out CSR form in SonicWALL device and click on 'Generate'

- For the most part, you can leave the drop-down boxes to their defaults and fill out each field as suggested by its corresponding drop-down box. An example is below:

# Tech Note

SonicWALL Administration - Microsoft Internet Explorer provided by SonicWALL, INC.

Address: https://juniper.vpntestlab.com/management.html

**Generate Certificate Signing Request**

Import

SONICWALL

General  
Log  
Filter  
Tools  
Access  
Advanced  
DHCP  
VPN  
Anti-Virus  
High Availability

Logout

STATUS: The configuration has been updated.

Certificate Name:	Juniper
Country	US
State	California
Locality, City, or County	Sunnyvale
Company or Organization	SonicWALL
Department	
Group	
Team	
Common Name	juniper.vpntestlab.com
Subject Distinguished Name:	C=US,ST=California,L=Sunnyvale,O=SonicWALL,CN=juniper.vpntestlab.com
Subject Alternative Name (Optional):	
Domain Name	
Subject Key Type:	RSA
Subject Key Size:	1024 bits

Generate

-In the 'Country' field, put the country code abbreviation instead of spelling out the name of the country. In the 'State' field, put the full name of the state instead of the abbreviation. In the 'Common Name' field, put the name for the SonicWALL device. For the 'Subject Key Size' drop-down box, we suggest a key size of '1024 bits'. If you do not fill out these fields correctly, your OpenSSL may reject the certificate request.

- The optional 'Subject Alternate Name' field can be used to simplify VPN tunnel setup. Select "Domain Name" or "Email-ID" from the drop-down box and enter in the name or Email-ID of the SonicWALL device. This will allow you to identify peers with only their 'Subject Alternative Name' instead of having to paste in the full 'Subject Distinguished Name'. Please note that you must use this alternative name as the peer ID if the peer's local certificate shows one - you can't use Subject Distinguished Name.

2. Save the exported file to \certs directory

-For example, the CSR was exported from the SonicWALL as 'juniper.p10'.

3. Using a text editor, create an 'extension' file with the following attributes:

basicConstraints = critical,CA:FALSE nsCertType = serversComment = "This certificate was issued for testing purposes"

- Save the file as: \certs\fwext.txt

4. Sign the client's CSR with the CA and apply the extensions:

- OpenSSL> x509 -req -days 365 -CA \certs\cacert.pem -CAkey \certs\cakey.key -CAcreateserial -in \certs\juniper.p10 -extfile \certs\fwext.txt -out \certs\fwcert.pem

- Enter the passphrase used to protect the CA's key.

5. (Optional) Convert the cert to DER format to prepare for import:

- Only necessary if SonicWALL is running 6.3.x.x firmware; 6.4.x.x can import



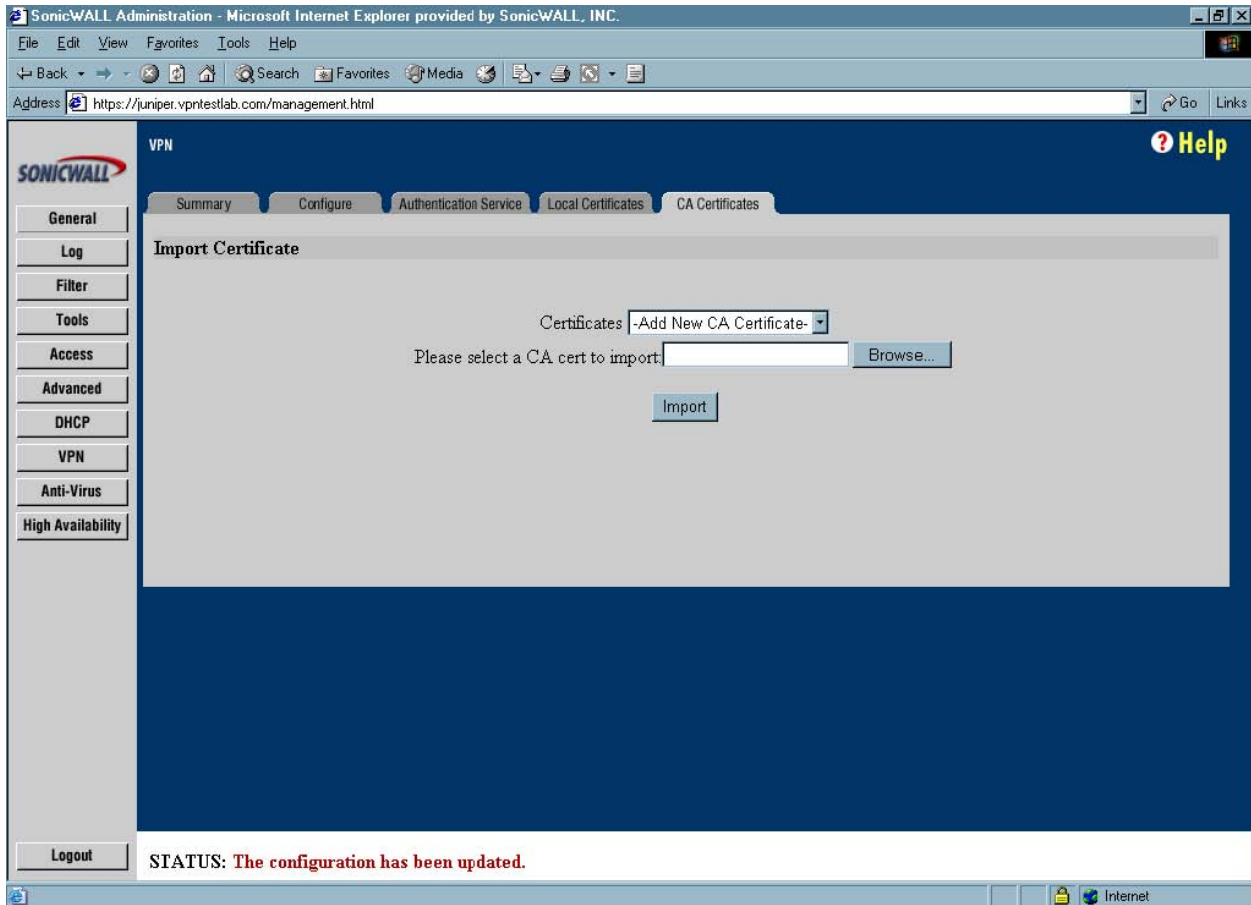
# Tech Note

PEM and DER.

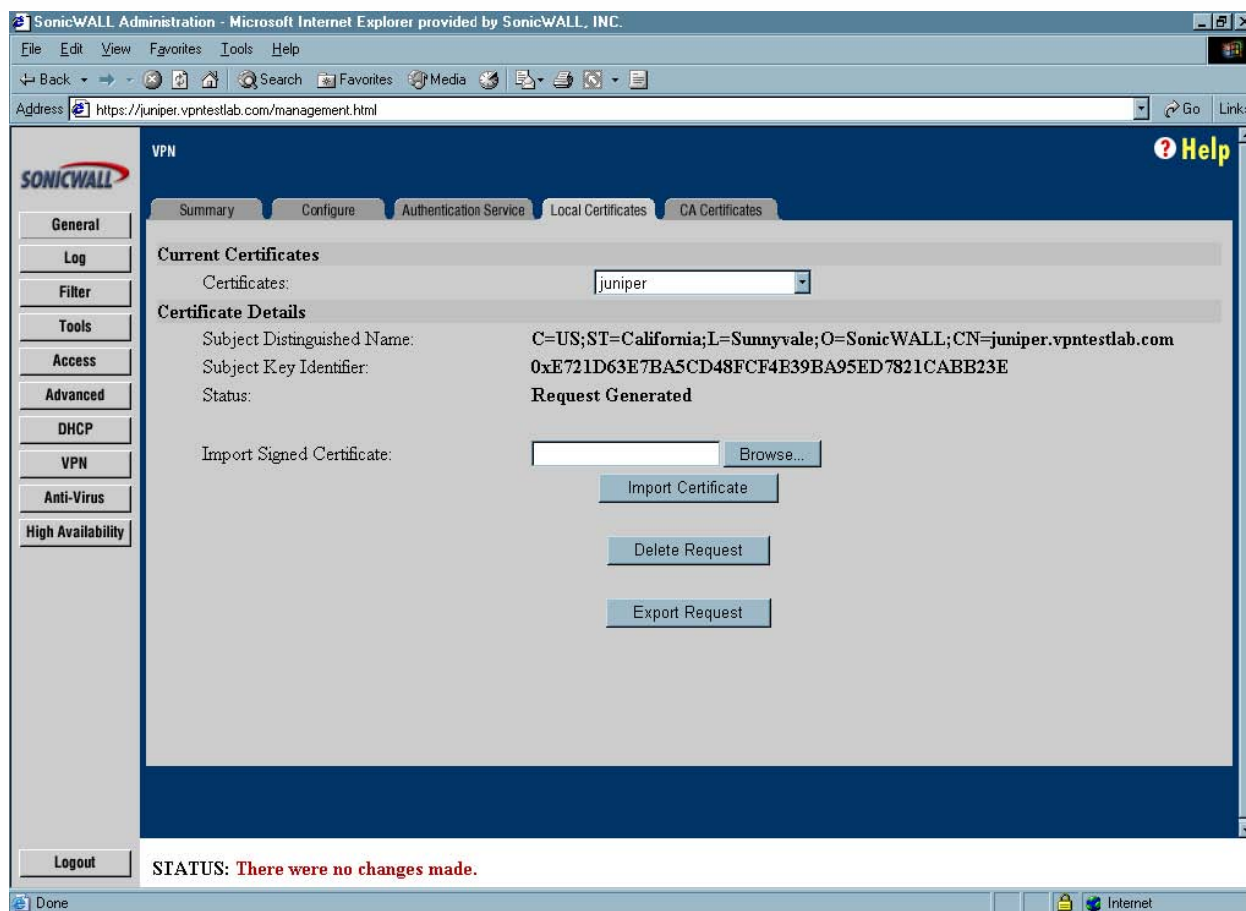
- OpenSSL> x509 -inform pem -outform der -in \certs\fwcert.pem -out \certs\fwcert.der

6. Import CA's cert and the server's cert into the SonicWALL

- In the SonicWALL GUI, click on the 'VPN' button and then the 'CA Certificates' tab.
- From the 'Certificates' drop-down box, select "-Add New CA Certificate-".
- Navigate to the directory where the CA's cert is located and click the 'Import' button.
- An example is below:
- In the SonicWALL GUI, click on the 'VPN' button and then the 'Local Certificates' tab.
- From the 'Certificates' drop-down box, select the name of your in-process certificate.
- Navigate to the directory where the firewall cert is located and click the 'Import Certificate' button.
- An example is below:



# Tech Note



## Configuring a SonicWALL to authenticate incoming Global VPN Client connections using third-party certificates

Before you begin, you must first load a copy of the CA certificate that was used to sign the client certificates. The firewall must also have its own certificate installed. Details on how to do this are on pages 4-7 of this document.

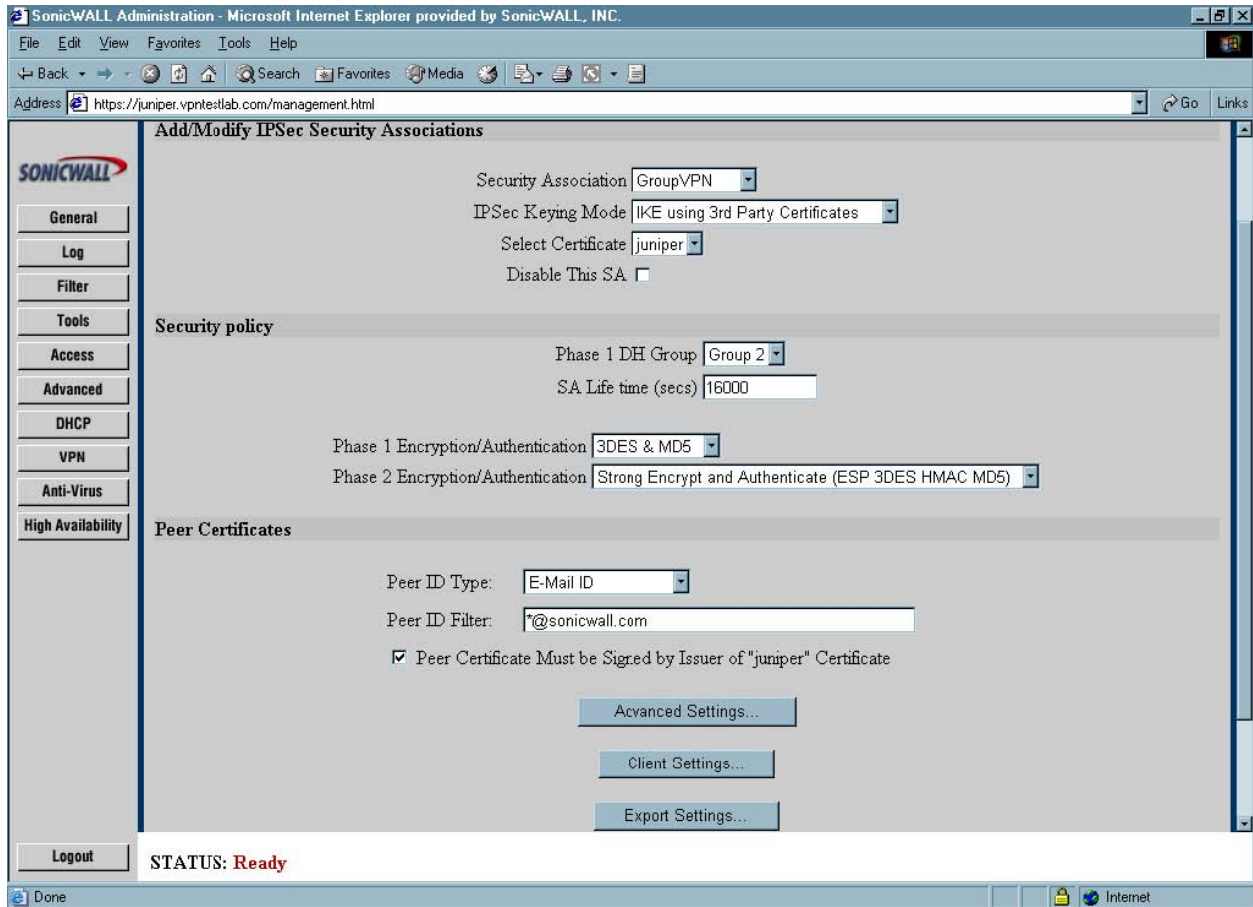
- Log into the SonicWALL GUI, click on the 'VPN' button, and then the 'Configure' tab.
- From the 'Security Association' drop-down box, select 'GroupVPN'.
- From the 'IPSec Keying Mode' drop-down box, select 'IKE using 3<sup>rd</sup> Party Certificates'.
- From the 'Select Certificate' drop-down box, select your firewall's certificate.
- Uncheck the box next to 'Disable This SA' (by default, it is checked).
- In the 'Security Policy' section, enter in your custom security policy.
- From the 'Peer ID Type' drop-down box, select 'E-Mail ID'.
- In the 'Peer ID Filter' dialog box, enter in the string you wish to use to filter against incoming client certificates. This feature will cause the SonicWALL to scan through the 'SubjectAltName' field on the incoming client certificates and match against this string. Wildcards are permitted. In the example on the next page, we are allowing any incoming client cert that contains '@sonicwall.com'.
- Check the box next to 'Peer Certificate Must be Signed by Issuer of \_\_\_\_ Certificate'. This feature will cause the SonicWALL to only accept incoming client certificates that have been signed by the same CA as the firewall's own certificate.
- Click on the 'Advanced Settings' box and enter in your custom security policy. It is strongly recommended that you enforce the use of XAUTH for incoming Global VPN Connections. If you

# Tech Note

choose to do this, you will need to enter in user accounts and passwords via the 'Access' button, 'Users' tab, or pass the requests to a RADIUS server.

- Click on the 'Client Settings' box and enter in your custom security policy. Do NOT check the box next to 'Use Default Key for Simple Client Provisioning'.
- When done, click on the 'Update' button at the bottom of the screen.

Example of GroupVPN setup using third-party certs:



**Prepared by SonicWALL, Inc.**  
**04/11/2003**  
**Last Edited: May 2008**