



## RSA Secured Implementation Guide For VPN Products

Last Modified: Thursday, March 09, 2006

### Partner Information

---

Product Information	
Partner Name	SonicWALL, Inc.
Web Site	<a href="http://www.sonicwall.com/">http://www.sonicwall.com/</a>
Product Name	PRO 2040 Enhanced
Version & Platform	SonicOS Enhanced 3.1.0.12-46e
Product Description	The SonicWALL PRO 2040 is part of SonicWALL's PRO Series, delivering complete business continuity for small to mid-sized networks. With integrated support for SonicWALL's Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, the PRO 2040 provides real-time protection against viruses, spyware, worms, Trojans and other malicious threats.
Product Category	Perimeter Defense (Firewalls, VPNs and ID)



## Solution Summary

---

The RSA Certificate Manager and the SonicWall PRO 2040 integrate utilizing x.509 standards to provide authentication and a secure connection to the enterprise within a public key infrastructure. RSA root signers, signed server certificates and end user end entity certificates are all supported by the SonicWall OS.



## Product Requirements

---

<b>SonicWall PRO 2040 Enhanced</b>	
Firmware	SonicOS Enhanced 3.1.0.12-46e

## Product Configuration

---

Proper configuration of the SonicWall PRO 2040 and the RSA Certificate Manager result in the successful authentication of end-users and the creation of a secure IPSEC tunnel utilizing x.509 certificates.

This guide assumes the reader has a fundamental working knowledge of the SonicWall PRO 2040 appliance and the RSA Security Certificate Manager software.

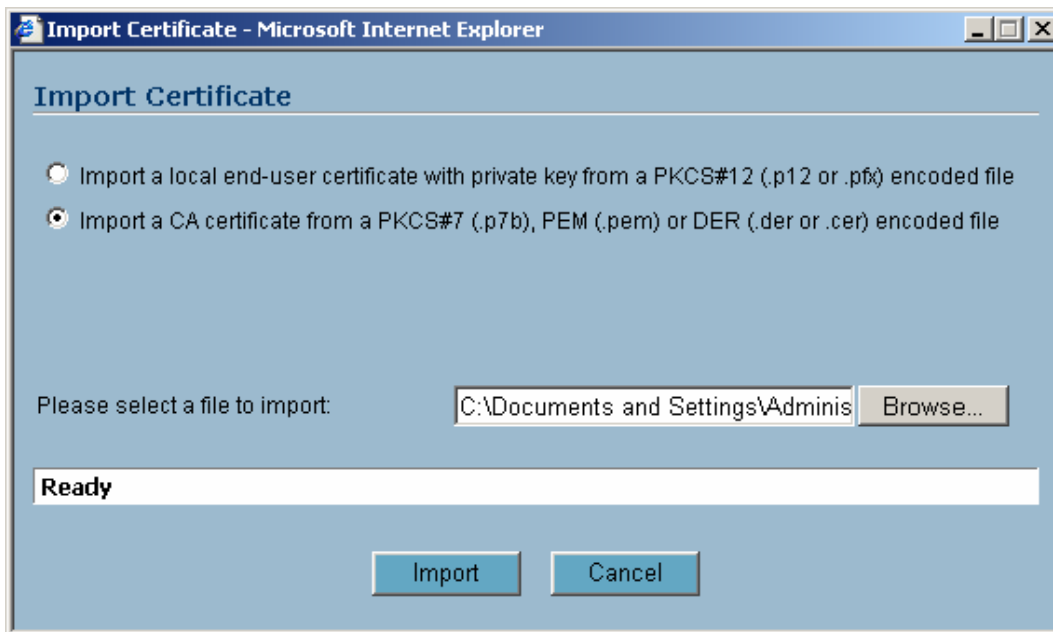
### ***RSA Authentication Manager Configuration***

Create a Jurisdiction on the RSA Certificate Manager. No certificate extensions are necessary for the root certificate but when you create the jurisdiction, ensure you include the necessary extension profiles for end entity certificates. This implementation will require the VPN/IPSEC profile. Additionally, enable CRL publishing as appropriate if you plan to query a repository via HTTP. Specifics on CRL configuration will be covered later in this guide. Export the jurisdiction root certificate for use in the SonicWall 2040 configuration.

## SonicWall 2040 VPN Appliance Configuration

Create VPN policies to allow users to connect to Network resources with a username and password. Although this is a step for interoperability, details will not be covered as it is beyond the scope of this guide.

Import the root certificate into the SonicWall appliance by selecting System|Certificates|Import from the SonicWall administration page.



Create a certificate signing request (PKCS#10) on the SonicWall Appliance and submit it to the RSA Certificate Manager. Select "New Signing Request" from the System|Certificates page. Fill in the appropriate information and click "Generate".

**Generate Certificate Signing Request**

Certificate Alias: 192.168.78.71

Country: US

State:

Locality, City, or County:

Company or Organization: RSA

Department: PE

Group:

Team:

Common Name: 192.168.78.71

Subject Distinguished Name: C=US;O=RSA;OU=PE;CN=192.168.78.71

Subject Alternative Name (Optional):

Domain Name:

Subject Key Type: RSA

Subject Key Size: 1024 bits

Ready

Generate Cancel

Export and submit the request to the appropriate RSA Certificate Manager Jurisdiction.

**Export Certificate Request**

**Name:** 192.168.78.71

**Subject Distinguished Name:** C=US;O=RSA;OU=PE;CN=192.168.78.71

**Subject Key Identifier:** 0x90015E7EFC45A8D651D539A51D9AD3D87ED35A6

**Status:** Request Generated

A PKCS#10 Certification Request has been generated and is available for export. Save this file on your local disk for submission to a Registration or Certificate Authority. The file will be saved in PEM Certificate Request format, by default as '192.168.78.71.p10' (the file name can be changed at download as needed).

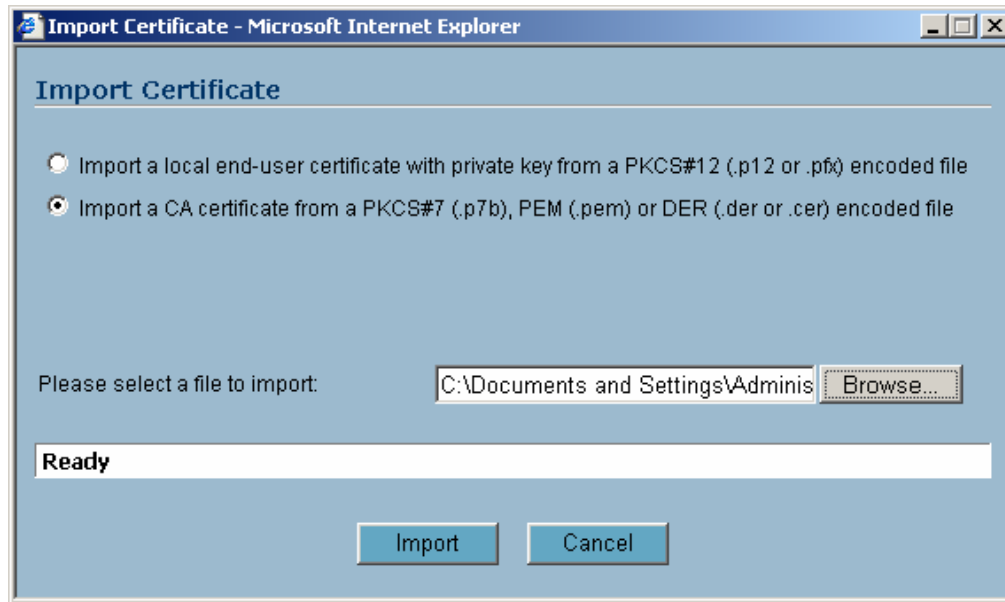
Ready

Export Cancel

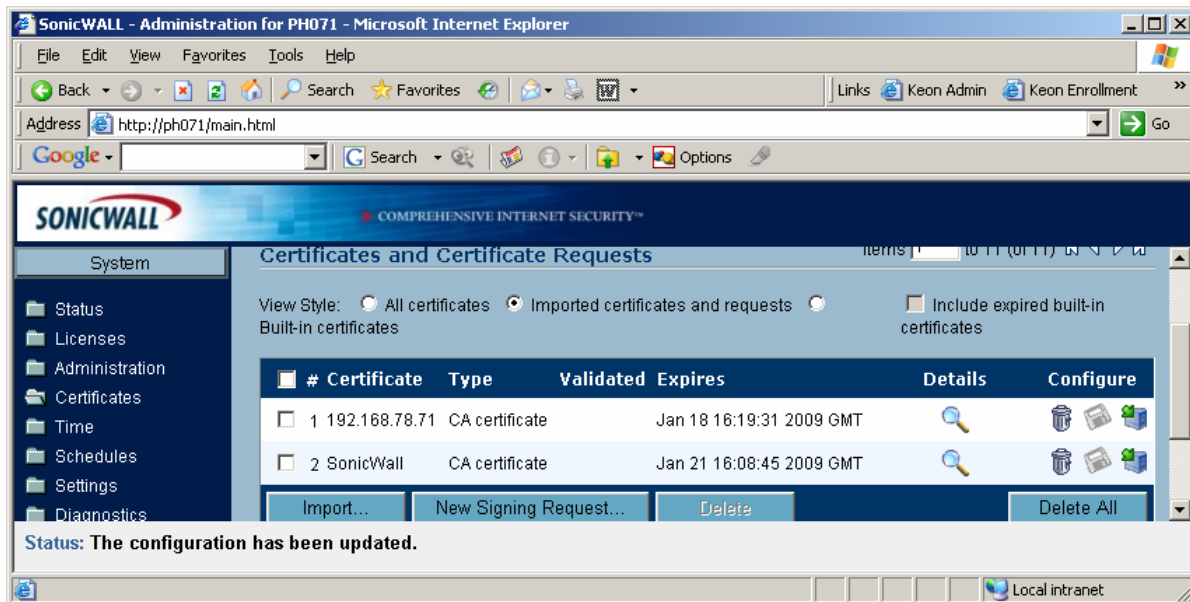
Obtain the signed request from your RSA Certificate Manager administrator.

**Note: If you have access to the RSA Certificate Manager Administration page, approve and download the certificate as a PKCS#7 containing the certificate chain.**

Import signed request (PKCS#7) into SonicWall Appliance.



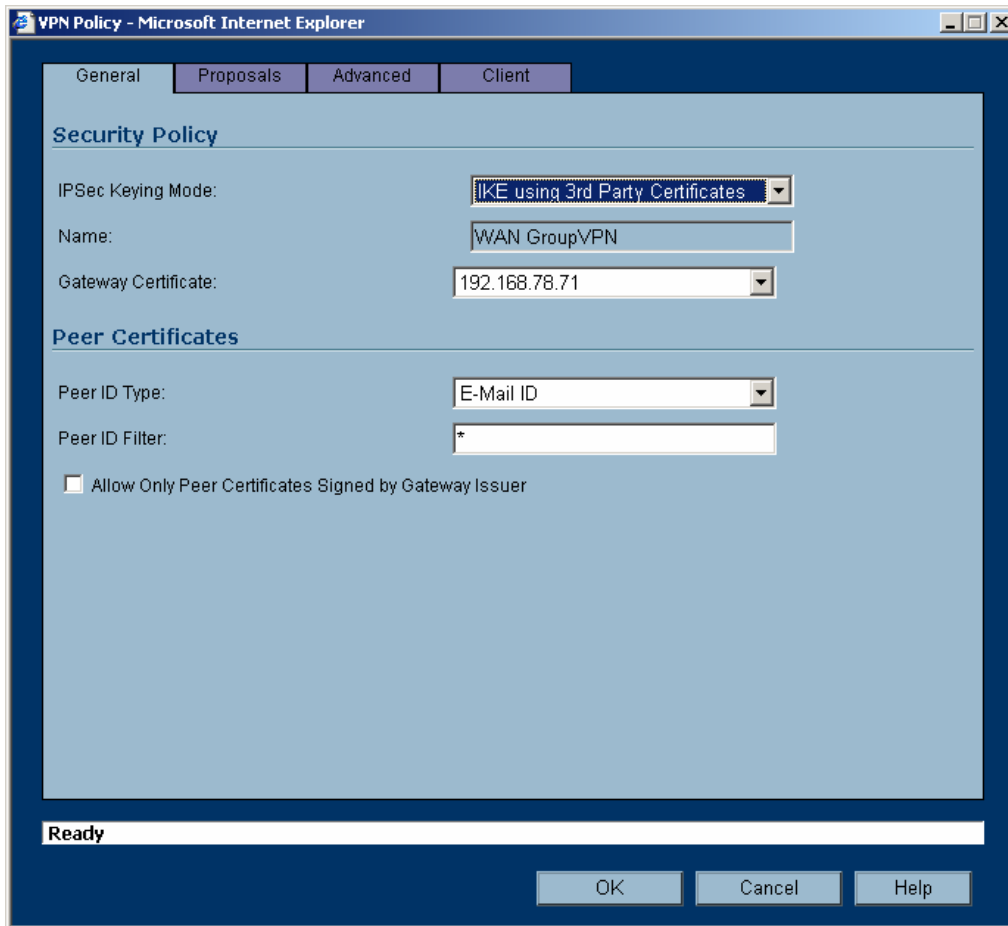
Once done, the SonicWall root CA certificate can be viewed at the SonicWall administration console.



Enable certificate authentication for VPN Policies. Select the appropriate VPN policy from the VPN tab and select edit.



Configure the security policy to use 3rd party certificates and the appropriate gateway certificate. In the below example, the Peer ID is set to email address. This allows the VPN to extract the username from the email address specified with the Subject Alt Name extension within the certificate. End-User Certificate properties are covered later in this guide.



Optionally configure certificate status checking. From the SonicWall administration console select System|Certificates|Configure.

#	Certificate	Type	Validated	Expires	Details	Configure
<input type="checkbox"/>	1 192.168.78.71	Local certificate	Yes	Jan 18 16:12:16 2009 GMT		
<input type="checkbox"/>	2 SonicWall	CA certificate		Jan 21 16:08:45 2009 GMT		

Place either the url for the certificate revocation list (CRL) or import the CRL manually. Certificates serial numbers listed in this CRL will not be allowed to authenticate.

The SonicWall log shows the certificate being rejected if its serial number resides in the Certificate Revocation List.

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	03/06/2006 14:32:58.800	Error	VPN IKE	CERT -payload processing error	192.168.78.66, 500	192.168.78.71, 500		
2	03/06/2006 14:32:58.800	Alert	VPN PKI	Certificate on Revoked list(CRL)			Joe	
3	03/06/2006 14:32:58.736	Info	VPN IKE	IKE Responder: Received Aggressive Mode request (Phase 1)	192.168.78.66, 500	192.168.78.71, 500		
4	03/06/2006 14:32:58.736	Notice	Network Access	UDP packet dropped	192.168.78.66, 500, X1	192.168.78.71, 500	UDP ISAKMP	

## SonicWall Global VPN Client Configuration and Operation

Request end user certificates for authentication. The following certificate extensions were issued by the RSA Certificate Manager and used to authenticate to the appliance.

---

**Note: The subject Alt Name extension is a critical element of this implementation.**

---

### EXTENSIONS:

*CRL Distribution Points:*

*Distribution point 1:*

*Uniform Resource ID: http://ps021.pe.rsa.net:447/SonicWall.crl*

*Extended Key Usage: IPSec User*

*Key Usage: Critical Key Agreement*

*Subject Alt Name:*

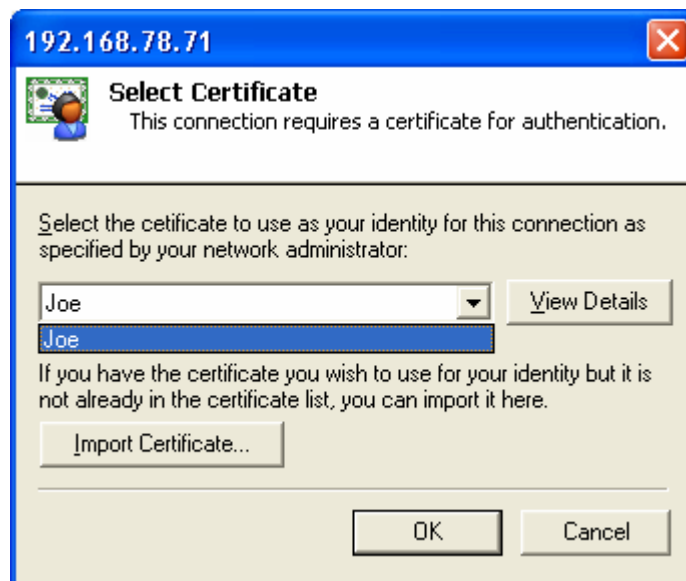
*RFC Name: Joe@ps026.pe.rsa.net*

*Authority Key Identifier:*

*Key ID: 0xe17c4146 416ccb0e e47852b4 45f3173d 5361b85e*

*Subject Key Identifier: 0x614eef6e 9852162e af491c01 d6183c70 3ebc61e8*

The SonicWall VPN client will prompt you to present a certificate for authentication (a password will also be requested if XAuth is required by the SonicWall 2040).



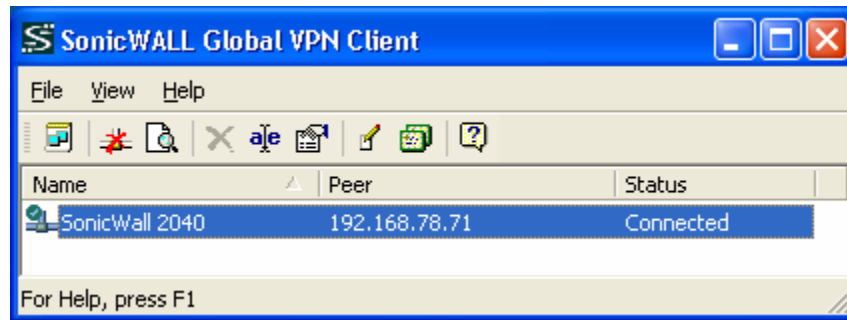
The SonicWall Global VPN Client will enumerate certificates exposed by the Microsoft Crypto API, including those stored in the RSA Sign-On Manager CSP.

---

**NOTE: The RSA Sign-On Manager CSP is only accessible by the SonicWall Global VPN Client when using the RSA Sign-On Manager Client version 4.53 builds 41 or above. The RSA Authentication Utility is not supported at this time.**

---

Once connected, the users have access to those network resources made available by the VPN policy.



# Certification Checklist for VPN Products

Date Tested: Thursday, March 09, 2006

Product	Operating System	Tested Version
RSA Certificate Manager	Microsoft Windows 2003 SP1	V 6.6 Build 301
RSA Sign-On Manager Client	Microsoft Windows XP SP2	V 4.53 Build 41
RSA Authentication Utility	Microsoft Windows XP SP2	V 1.0 Build 25
SonicWall VPN	PRO 2040 Enhanced	SonicOS Enhanced 3.1.0.12-46e
<b>SonicWall Global VPN Client</b>	Microsoft Windows XP SP2	V 3.1.0.559

Gateway Test Case	Result
Certificate Uses	
Import CA Root Certificate	✓
PKCS#10 Certificate Request	✓
PKCS#7 Response installed correctly	✓
PKCS#7 Response installed correctly w/chain	✓
SCEP Certificate Request	N/A
SCEP Response installed correctly	N/A
Certificate Status Checking	
CRL Manual Import	✓
CRL Retrieval via HTTP	✓
CRL Retrieval via LDAP	✓
VPN Client Authenticates Successfully with CRL checking enabled	✓
VPN Client Denied Access with Revoked Certificate	✓

VPN Client Test Case	w/RAU	w/SOM	Standalone VPN Client
Certificate Import			
Import PKCS#12 envelope			✓
Utilize x.509 Certificate			
Enumerate and Access Certificate in Local CSP via MSCAPI	✗	✓	✓
Authenticate with Certificate stored in Local CSP	✗	✓	✓

JRV

✓ = Pass ✗ = Fail N/A = Non-Available Function

## Known Issues

---

The RSA Sign-On Manager CSP is only accessible by the SonicWall Global VPN Client when using the RSA Sign-On Manager Client version 4.53 builds 41 or above. The RSA Authentication Utility is not supported at this time.