



RSA SecurID Ready Implementation Guide

Last Modified: March 25, 2009

Partner Information

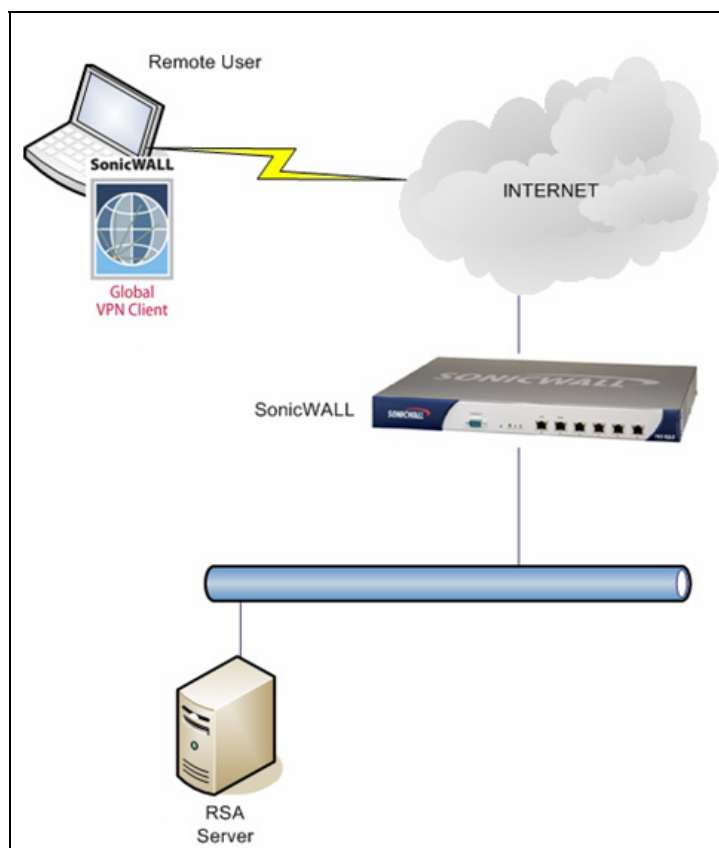
Product Information	
Partner Name	SonicWALL Inc.
Web Site	www.sonicwall.com
Product Name	SonicWALL TZ & PRO Products
Version & Platform	SonicOS Enhanced 4.0.0.12e
Product Description	SonicWALL TZ and PRO Unified Threat Management Firewalls integrate advanced security services for true multi-layered security, including Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Complete Anti-Virus and Content Filtering Service all manageable by SonicWALL's award-winning Global Management System. SonicOS Enhanced security operating system includes a streamlined Web GUI and comprehensive suite of easy-to-use configuration and management wizards that guide users through the configuration steps for common user network environments or scenarios, making it simple to set up in any network environment. SonicOS Enhanced supports RSA SecurID authentication via the RADIUS protocol.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (1)
RSA Authentication Agent Host Type for 6.1	Communication Server
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No





Product Requirements

Partner Product Requirements: <Partner Product (Component)>	
TZ Family	TZ 170, TZ 170 SP, TZ 170 SPW, TZ 170 W
PRO Family	PRO 1260, PRO 2040, PRO 3060 PRO 4060, PRO 4100, PRO 5060
Firmware Version	SonicOS Enhanced 4.0.0.12e

Additional Software Requirements	
SonicWALL Global VPN Client	4.0.0.842

Partner Product Requirements: SonicWALL Global VPN Client	
CPU	Intel x86 Compatible
Memory	32MB (Windows 98 SE/Me) 64MB (Windows NT 4.0) 128MB (Windows 2000/XP Home/Professional)
Storage	38MB

Operating System	
Platform	Required Patches
Microsoft Windows 98 SE/Me	All patch levels supported
Microsoft Windows NT 4.0	Service Pack 6.0 or greater
Microsoft Windows 2000 Professional	Service Pack 3.0 or greater
Microsoft Windows XP Home/Professional	All patch levels supported



Agent Host Configuration

! > Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.

! > Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.

To facilitate communication between the SonicWALL TZ & PRO Products and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the SonicWALL TZ & PRO Products within its database and contains information about communication and encryption. You will also need to configure a RADIUS client.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the SonicWALL TZ & PRO Products as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the SonicWALL TZ & PRO Products will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

 **Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host, and RADIUS client records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	N/A
Node Secret	N/A
sdstatus.12	N/A
sdopts.rec	N/A



Partner Product Configuration

Before You Begin


This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Documenting the Solution

SonicWALL TZ and PRO products running SonicOS Enhanced support secure two-factor authentication for Global VPN Client tunnels via the RADIUS protocol. The following configuration steps must be performed in order to implement this solution.

 **Note:** SonicWALL recommends that customers update to the latest version of SonicOS Enhanced prior to completing this configuration.

On the SonicWALL security appliance:

- Set up the User's Authentication Method
- Create new GroupVPN Policy for the Global VPN Client
- Verify that applications function properly through the tunnel

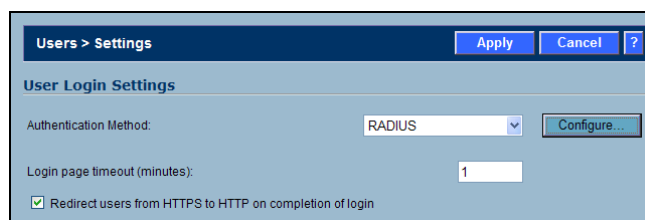
On the computer requiring secure remote access via SonicWALL Global VPN Client:

- Install SonicWALL Global VPN Client
- Create a Profile for Connecting to the SonicWALL security appliance

SonicOS Enhanced Configuration


Configuring RADIUS

1. In **Users > Settings** under **User Login Settings**, set the Authentication Method to **RADIUS** from the drop-down menu, and click the **Configure** button.

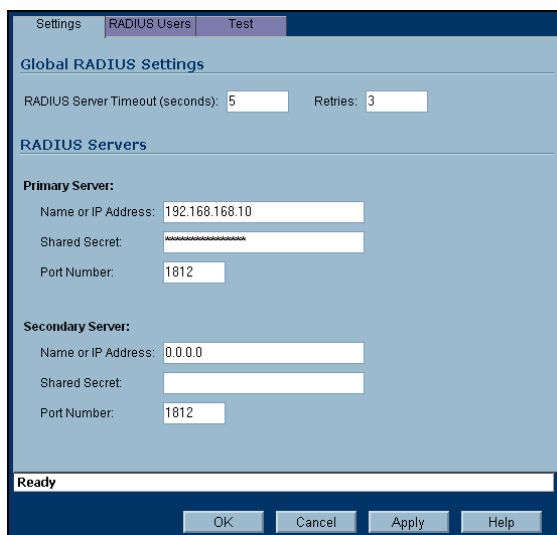


The screenshot shows the 'Users > Settings' configuration window. The 'User Login Settings' section is active. The 'Authentication Method' is set to 'RADIUS' in a dropdown menu, with a 'Configure...' button next to it. The 'Login page timeout (minutes)' is set to '1'. A checkbox labeled 'Redirect users from HTTPS to HTTP on completion of login' is checked. At the top right of the window are 'Apply', 'Cancel', and '?' buttons.



 **Note:** After the RADIUS authentication method is enabled the SonicWALL security appliance can only be accessed using HTTPS Management.

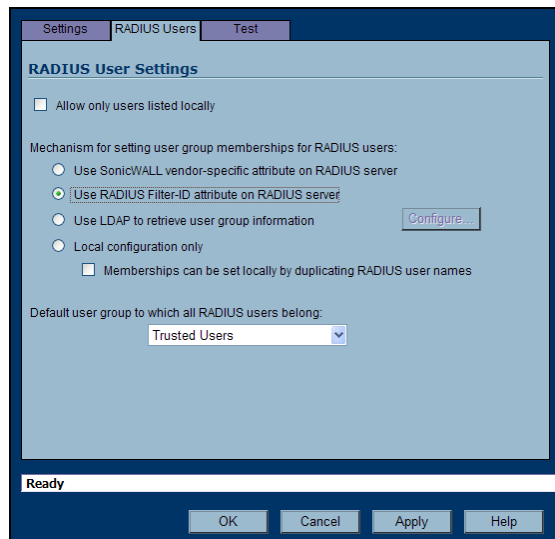
2. In the **Primary Server: Name or IP Address** field, enter the RSA Authentication Manager Servers IP Address.
3. Create a **Shared Secret** to authenticate the SonicWALL to the RSA Authentication Manager Server. This same secret will be used when you create the Agent Host records in the RSA Authentication Manager Server configuration.
4. Set the **Port Number** to 1812.



The screenshot shows the 'RADIUS Users' configuration window. At the top, there are tabs for 'Settings', 'RADIUS Users', and 'Test'. Below the tabs is the 'Global RADIUS Settings' section with 'RADIUS Server Timeout (seconds): 5' and 'Retries: 3'. The 'RADIUS Servers' section contains two server configurations. The 'Primary Server' has 'Name or IP Address: 192.168.168.10', a masked 'Shared Secret', and 'Port Number: 1812'. The 'Secondary Server' has 'Name or IP Address: 0.0.0.0', a masked 'Shared Secret', and 'Port Number: 1812'. At the bottom, there is a 'Ready' status bar and buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

 **Note:** RSA recommends a RADIUS Server Timeout of 60 seconds or greater.

5. Select the **RADIUS Users** tab, and select the **Use Radius Filter-ID** attribute on Radius Server.
6. Select **Trusted User** from the drop-down box under **Default user group** to which all RADIUS users belong.

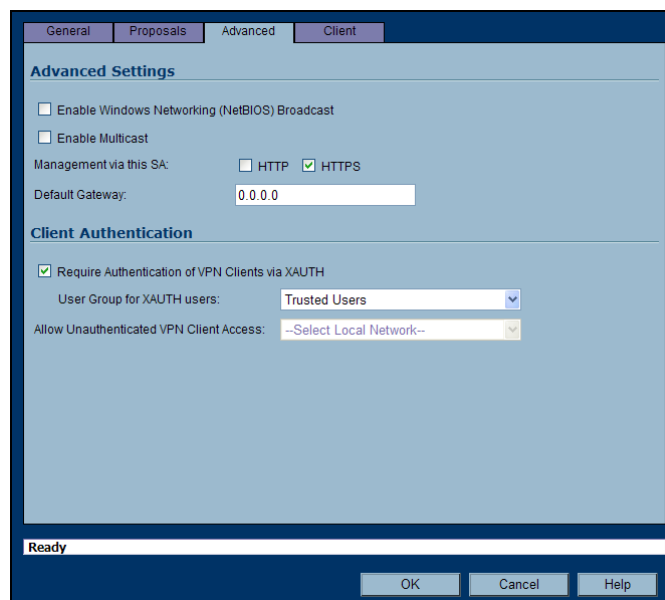


7. Click **OK**.

 **Note:** The RADIUS testing tool may not work due to encryption type mismatches. Please use the RSA Log Monitor application for testing and debugging purposes.

Configuring Global VPN Client Settings

1. In **VPN > Settings**, click the **Configure** icon for the **WAN GroupVPN**, and select the **Advanced** Tab.
2. Select **Require Authentication of VPN Clients via XAUTH**, and select the **Trusted Users** group as the User Group for XAUTH users.



3. Select the **Client** Tab, and set the following parameters:



- Set **Cache XAUTH User Name and Password on Client** to **Single Session**.
- Set **Virtual Adapter settings** to **DHCP Lease** (or **DHCP Lease** or **Manual Config** if you wish to statically address the virtual adapter).
- Select the **Use Default Key for Simple Client Provisioning** checkbox.

4. Click **OK**.

Configuring DHCP over VPN

1. Select **VPN > DHCP over VPN** and click the **Configure** icon for Central Gateway.
2. Select the **Use Internal DHCP Server** and **For Global VPN Client** check boxes.

3. Click **OK**.



Configuring User Group Settings

1. Select **Users > Local Groups** and click the **Configure** icon for Trusted Users.
2. Select the **Members** tab, and confirm **All RADIUS Users** is in the **Members Users and Groups**.

Settings Members VPN Access CFS Policy

Group Memberships

Non-Member Users and Groups:

- Content Filtering Bypass
- Guest Services
- Limited Administrators

Member Users and Groups:

- All RADIUS Users

Add All > < Remove All

Ready

OK Cancel

3. Select **VPN Access** tab, and add the **LAN Primary Subnet**.

Settings Members VPN Access CFS Policy

VPN Client Access Networks

Networks:

- All Interface IP
- All WAN IP
- All X0 Management IP
- All X1 Management IP
- All X2 Management IP

Access List:

- LAN Primary Subnet

> < Remove All

Ready

OK Cancel

4. Click **OK**.

Enable Global VPN Client Connections

1. Select **VPN > Settings**.
2. Select the **Enable VPN** checkbox.
3. Select the **Enable** checkbox for the **WAN GroupVPN** policy.

VPN > Settings VPN Policy Wizard... Apply Cancel ?

VPN Global Settings

Enable VPN

Unique Firewall Identifier: 0006B1020E6B

VPN Policies

Items 1 to 10 (of 10)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Co
1	WAN GroupVPN			ESP AES-256 HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	
2	LAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	

SonicWALL Global VPN Client Configuration

Download and install the SonicWALL Global VPN Client by logging in to your mySonicWALL account at www.mysonicwall.com. Once installed, simply use the New Connection Wizard to create a connection to your SonicWALL as detailed below.

1. Create a new VPN Connection using the New Connection Wizard. Select the **File > New Connection item** to launch the wizard. Click **Next** to continue to the next screen of the wizard.



2. Select the **Remote Access** radio button and click the **Next** button.





3. Enter the WAN IP Address or the DNS address of the SonicWALL that you are going to connect to. Click the **Next** button when finished.

New Connection Wizard

Remote Access
To use the remote access scenario, specify the gateway's domain name or IP address.

Specify the domain name or IP address of the security gateway.
IP Address or Domain Name:

You may also specify a name for this connection.
Connection Name:

To continue, click Next.

< Back Next > Cancel

4. Click the **Finish** button to complete the wizard.

New Connection Wizard

Completing the New Connection Wizard

Your new connection is ready to be added to your configuration. You can set the following options for this new connection:

- Create a desktop shortcut for this connection
- Enable this connection when the program is launched

To complete this wizard, click Finish.

SONICWALL

< Back Finish Cancel

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: 03/24/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.3	Windows 2003 Server R2
SonicWALL Pro 2040	4.0.0.12e	SonicOS Enhanced
SonicWALL GlobalVPN Client	4.0.0.842	Windows XP Professional SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
User Selectable	N/A	User Selectable	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Password	N/A	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
Name Locking Enabled	N/A	Name Locking Enabled	
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

BSD

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 03/23/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 Server R2
SonicWALL Pro 2040	4.0.0.12e	SonicOS Enhanced
SonicWALL GlobalVPN Client	4.0.0.842	Windows XP Professional SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny Numeric PIN	N/A	Deny Numeric PIN	✓
PIN Reuse	N/A	PIN Reuse	✓
Passcode			
16 Digit Passcode	N/A	16 Digit Passcode	✓
4 Digit Fixed Passcode	N/A	4 Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

BSD

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



Known Issues

New PIN Rejection

Upon New PIN rejection the SonicWALL Global VPN Client software will close out the authentication attempt with an error if the user enters a response that contains only null characters (spaces) to the question of whether or not to try a different PIN.

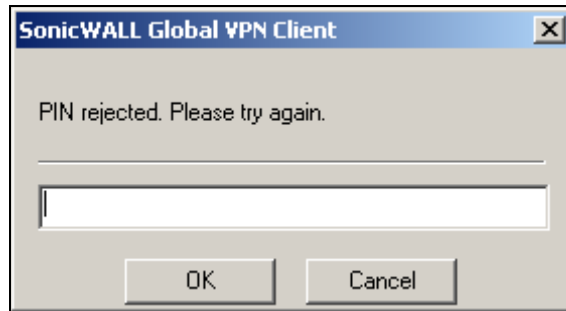


Fig 1. A null response is sent by the user to the Authentication Manager server.

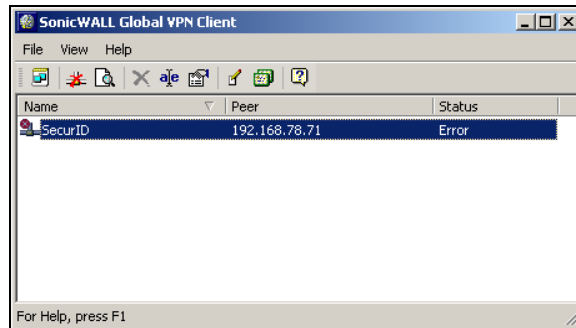


Fig 2. The authentication attempt is closed out with an error message.