



RSA SecurID Ready Implementation Guide

Last Modified: March 27, 2009

Partner Information

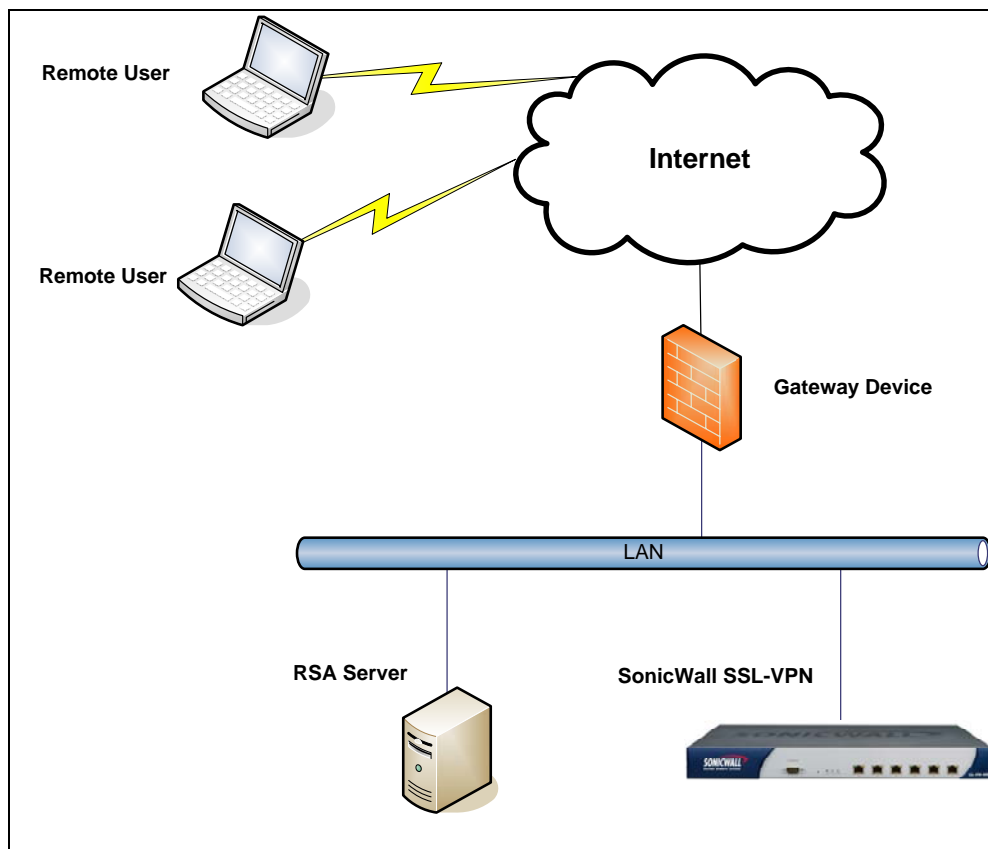
Product Information	
Partner Name	SonicWALL Inc.
Web Site	www.sonicwall.com
Product Name	SonicWALL SSL-VPN
Version & Platform	SonicOS SSL-VPN 3.5.0.0-15sv
Product Description	SonicWALL SSL-VPN appliances provide small and mid-size organizations an easy-to-use, secure and affordable remote access solution that requires no pre-installed client software. Utilizing a standard Web browser, authorized users such as employees, contractors, partners and customers, can easily and securely access e-mail, files, intranets, Web and legacy applications and remote desktops from any location. SonicOS 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 (2)
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: SonicWALL SSL-VPN	
Hardware Version	2000, 4000
Firmware Version	SonicOS SSL-VPN 3.5.0.0-15sv

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 SSL-VPN 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 SSL-VPN 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 SSL-VPN as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the SonicWall SSL-VPN 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

The SonicWALL SSL-VPN running SonicOS SSL-VPN supports secure two-factor authentication via the RADIUS protocol. This section provides the configuration steps required to enable such functionality.

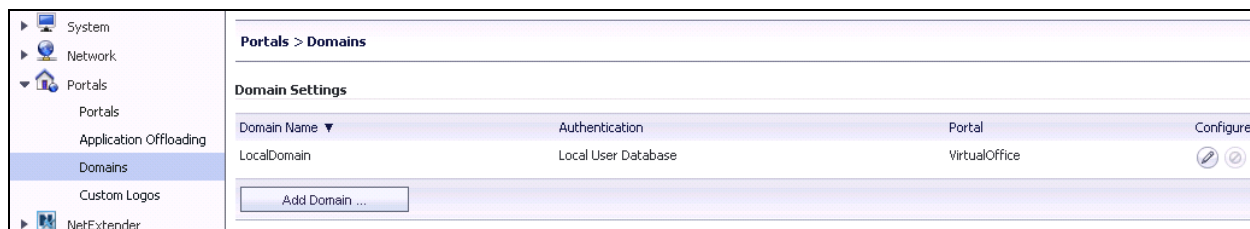
SonicOS SSL-VPN Firmware

First, make sure that the latest version of SonicOS SSL-VPN is running on the SonicWALL SSL-VPN.

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

Configuring the SSL-VPN Appliance for SecurID authentication

1. On the SonicWALL SSL-VPN, navigate to the **Portal > Domain** page.





2. Click on the **Add Domain** button.

Add Domain
Authentication type:
Domain name:
Authentication Protocol:
Primary Radius server
Radius server address:
Radius server port:
Secret password:
Radius Timeout (Seconds):
Max Retries:
Backup Radius server
Radius server address:
Radius server port:
Secret password:
 Use Filter-ID For RADIUS Groups
Portal name:
 Enable client certificate enforcement
 Delete external user accounts on logout
 One-time passwords

3. In the authentication type pull-down menu, select **Radius**.
4. Enter a descriptive name for the authentication domain in the **Domain Name** field. This is the domain name users will select in order to log into the SonicWALL SSL-VPN portal.
5. Enter the IP address of the RADIUS server in the **Radius Server Address** field.
6. Enter the Radius server port in the **Radius server port** field.
7. Enter a number (in seconds) for Radius timeout in the **Radius Timeout (Seconds)** field.
8. Enter the maximum number of retries in the **Max Retries** field.
9. Enter the authentication secret in the **Secret Password** field.
10. Click the name of the layout in the **Portal Name** pull-down menu.
11. Click **Add** to update the configuration. The domain will be added to the **Domain Settings** table.

Time Synchronization

Because two-factor authentication depends on time synchronization, it is important that the internal clocks for the SonicWALL SSL-VPN and the RSA Authentication Manager server are set correctly. On the SonicWALL SSL-VPN, set the time on the **System > Time** page.

System > Time Accept
System Time
Time (hh:mm:ss): : :
Date (mm:dd:yyyy): / /
Time Zone:
 Automatically synchronize with an NTP server
 Display UTC in logs (instead of local time)
NTP Settings
Update Interval (seconds):
NTP Server 1:
NTP Server 2 (Optional):
NTP Server 3 (Optional):



End-user Experience

After RSA SecurID has been enabled as an authentication method, navigate to the SonicWALL SSL-VPN device with a web browser. The following screens will be available for RSA SecurID authentication.

SONICWALL | SSL-VPN Login

Username: user

Password: ●●●●●●●●

Domain: RSA SecurID

Login

End-user login to SonicWALL SSL-VPN

SONICWALL | SSL-VPN Login

A new PIN is required. Do you want system to generate your new PIN?

Yes No

End-user prompted to accept System Generated PIN

SONICWALL | SSL-VPN Login

Are you satisfied with system generated PIN lzpt ?

Yes No

End-user prompted to confirm PIN

SONICWALL | SSL-VPN Login

 PIN accepted. Please wait for token to change, then login with the new passcode.

Username: user

Password: ●●●●●●●●

Domain: RSA SecurID

Login

End-user PIN change accepted

Certification Checklist for RSA Authentication Manager v6.x

Date Tested: 03/26/2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.3	Windows 2003 Server R2
SonicWALL SSL-VPN	2000	SonicOS 3.5.0.0-15sv

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 / PAR

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

Certification Checklist for RSA Authentication Manager 7.x

Date Tested: 03/26/3009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 Server R2
SonicWALL SSL-VPN	2000	SonicOS 3.5.0.0-15sv

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 / PAR

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



Known Issues

RADIUS Testing Tool

The RADIUS Testing Tool does not support New PIN and/or Next Tokencode modes. It is intended to be used to test standard RADIUS authentication and does not support RADIUS challenge/response.