SafeNet Authentication Service

Integration Guide

Protecting SonicWall Appliances with SAS

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012623-001, Rev A
Release Date	July 2009

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as SonicWall.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

By default, the SonicWall VPN requires that a user provide a correct user name and password to successfully log on. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password (OTP) generated by a SafeNet token using the provided instructions below.

Applicability

This guide is applicable to the following:

Security Partner Information	
Security Partner	SonicWall
Product Name and Version	SonicWall NSA
Protection Category	Remote Access

SAS Server	
Authentication Server	SafeNet Authentication Service
Version	3.2 or higher

Prerequisites

The following must be installed and operational prior to configuring SonicWall to use SafeNet Authentication Service:

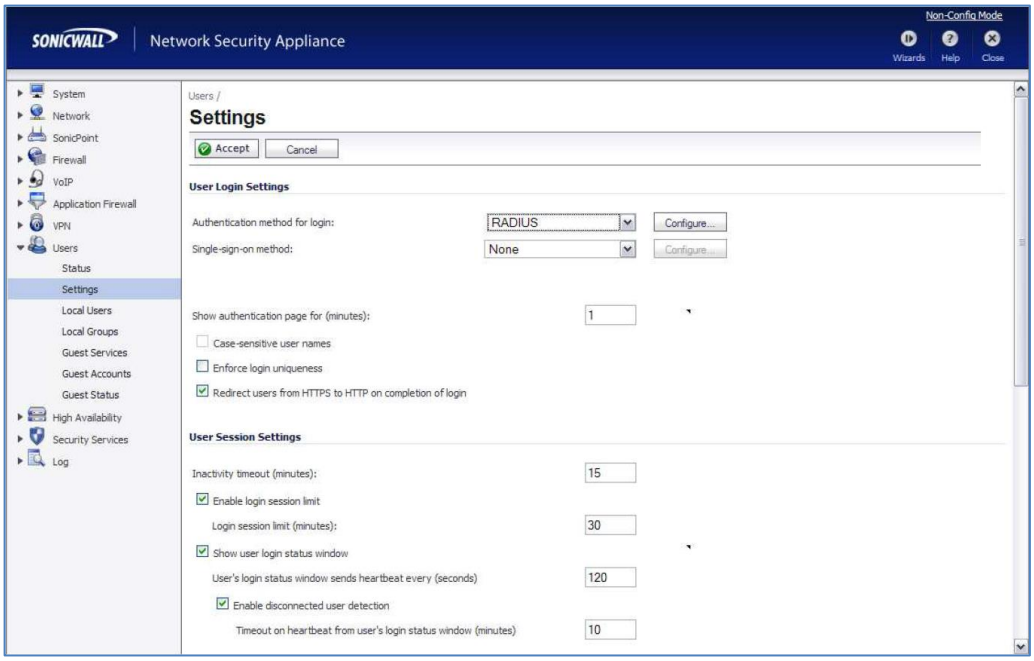
- SafeNet Authentication Service has been installed and configured, and a “Test” user account has been created.
- If the SAS server is installed and configured to use SQL only mode, then:
  - The SAS user name must be identical to the user name currently used by the end user
  - Ports 1812 and 1813 must be open between the SonicWall device and the SAS server.

Operation

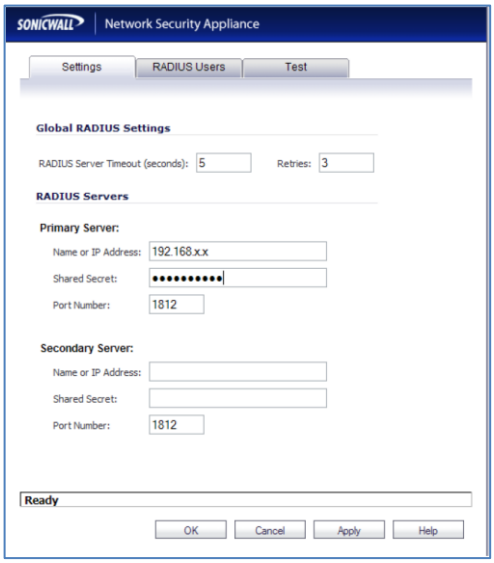
When a user attempts to log on using the SonicWall VPN Client, they will input their user name and a one-time password (OTP) generated from their token. Upon valid authentication, the SonicWall VPN connection will resume normal logon process flow.

Configuration

1. Go to **Users > Settings** and change the **Authentication method for Login** field to **RADUIS**.



2. Click **Configure**.
3. Enter the IP address of the SAS server and the Shared Secret that you entered in the RADIUS Clients of your NPS/IAS.



4. Click **OK**.

Troubleshooting

When troubleshooting RADIUS authentication issues refer to the logs on the SonicWall device.

All logging information for Internet Authentication Service (IAS) or Network Policy Server (NPS) can be found in the Event Viewer.

All logging information for the SAS IAS/NPS agent can be found in the following directory:

\Program Files\CRYPTOCard\BlackShield ID\IAS Agent\log

The following is an explanation of the logging messages that may appear in the event viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server.

Failed Logons

The following is an explanation of the logging messages that may appear in the Event Viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server.

Error Message	Solution
Packet DROPPED: A RADIUS message was received from an invalid RADIUS client.	Verify that a RADIUS client entry exists on the RADIUS server.
Authentication Rejected: Unspecified	This will occur when one or more of the following conditions occur: • The username does not correspond to a user on the SAS server. • The SafeNet token password does not match any tokens for that user. • The shared secret entered in SonicWall does not match the shared secret on the RADIUS server.
Authentication Rejected: The request was rejected by a third-party extension DLL file.	This will occur under one or more of the following conditions: • The SAS Agent for IAS/NPS cannot contact the SAS server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for IAS/NPS. • The SAS Agent for IAS/NPS Key file does not match the key file stored on the SAS server. • The username does not correspond to a user on the SAS server. • The SafeNet token password does not match any tokens for that user.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	