SonicWall NSA Integration

Contents

SonicWall NSA PINsafe integration with SMS

The SonicWALL Network Security Appliance (NSA) Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and antispyware with the application-level control of SonicWALL Application Firewall.

The appliances have SSL VPN capability with which PINsafe can provide Two Factor Authentication using SMS with RADIUS authentication.

If Strong authentication is required using TURing, then the image needs to be displayed to the user such as the use of a Taskbar, Web page etc. The use of TURing is not covered in this document.

Overview

Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL Network Security Appliance configured for local authentication. Tested with 5.2 and 5.8

Baseline

PINsafe 3.x

NSA 240, SonicOS Enhanced 5.2.0.1-21o

Architecture

The NSA appliance was the firewall/SSL VPN device with the PINsafe server located within the DMZ.

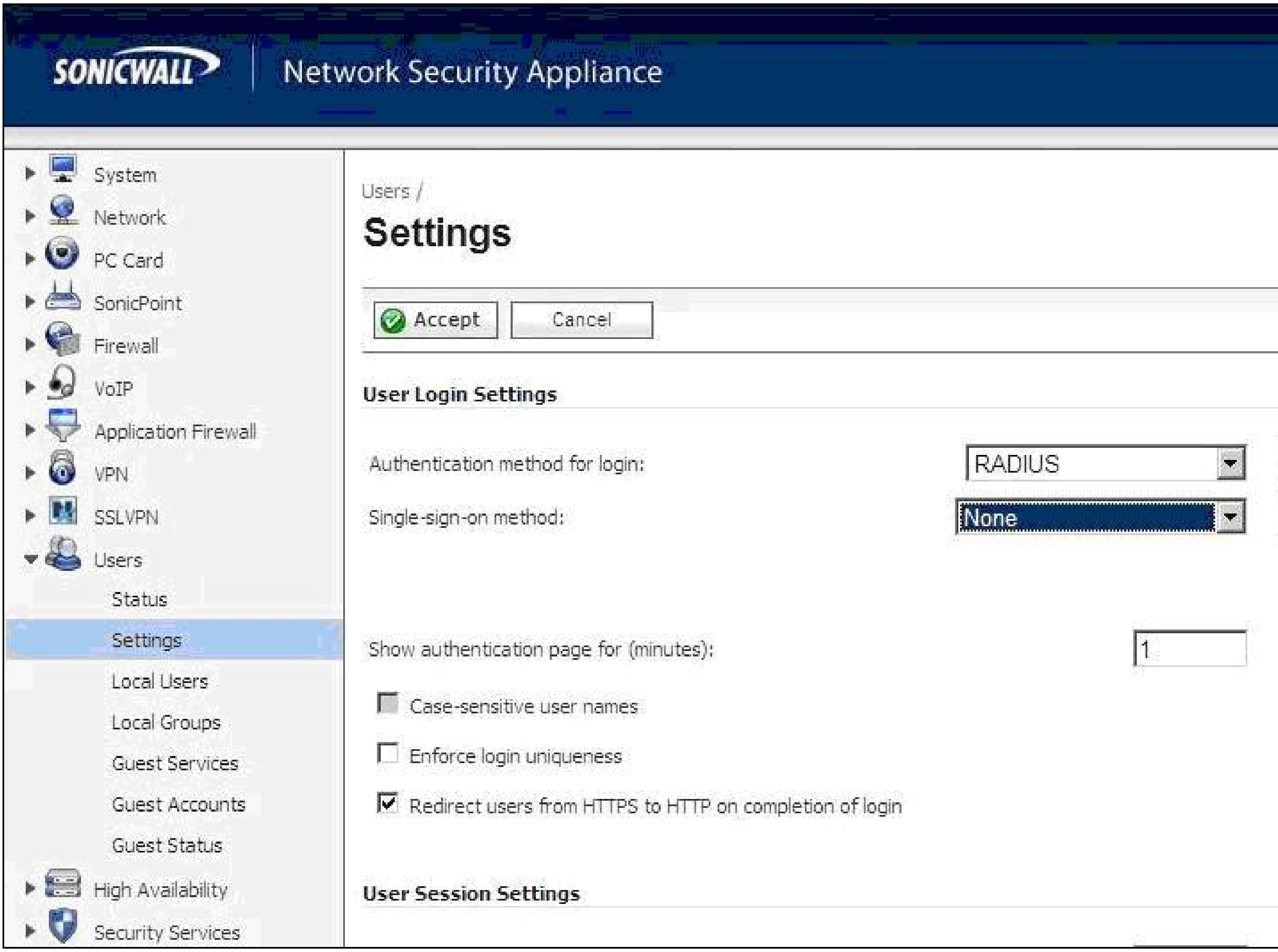
Installation

Configuring the PINsafe server

Configure PINsafe as a RADIUS server, from the RADIUS/server menu, enter the RADIUS server details and then select Enable RADIUS server. From the RADIUS/NAS menu enter a name for the SonicWALL NAS appliance and its IP address and a shared secret key.

Configuring the SonicWALL NSA Appliance User Settings

Select Users, then Settings, and on the menu for Authentication Method for Login: select RADIUS



Users /

Settings

User Login Settings

Authentication method for login: RADIUS

Single-sign-on method: None

Show authentication page for (minutes): 1

□ Case-sensitive user names

□ Enforce login uniqueness

☑ Redirect users from HTTPS to HTTP on completion of login

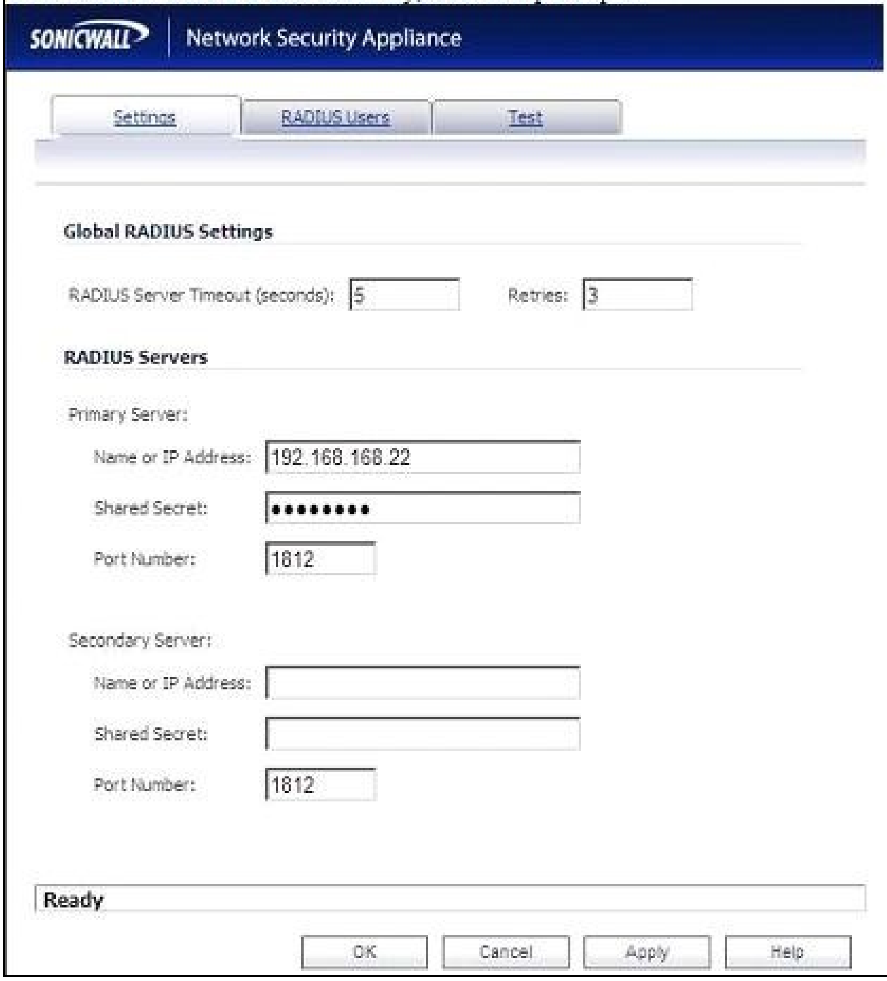
User Session Settings

Configuring the SonicWALL NSA Appliance RADIUS settings

From the Users\Settings menu click on Configure button next to the RADIUS option, then select the Settings tab and in the Primary Server IP Address field, enter the IP address of the PINsafe server and the shared secret key, and the required port.

Configuring the SonicWALL NSA Appliance RADIUS settings

From the Users\Settings menu click on Configure button next to the RADIUS option, then select the Settings tab and in the Primary Server IP Address field, enter the IP address of the PINsafe server and the shared secret key, and the required port.



Global RADIUS Settings

RADIUS Server Timeout (seconds): 5   Retries: 3

RADIUS Servers

Primary Server:

Name or IP Address: 192.168.168.22

Shared Secret: ●●●●●●●●●

Port Number: 1812

Secondary Server:

Name or IP Address:

Shared Secret:

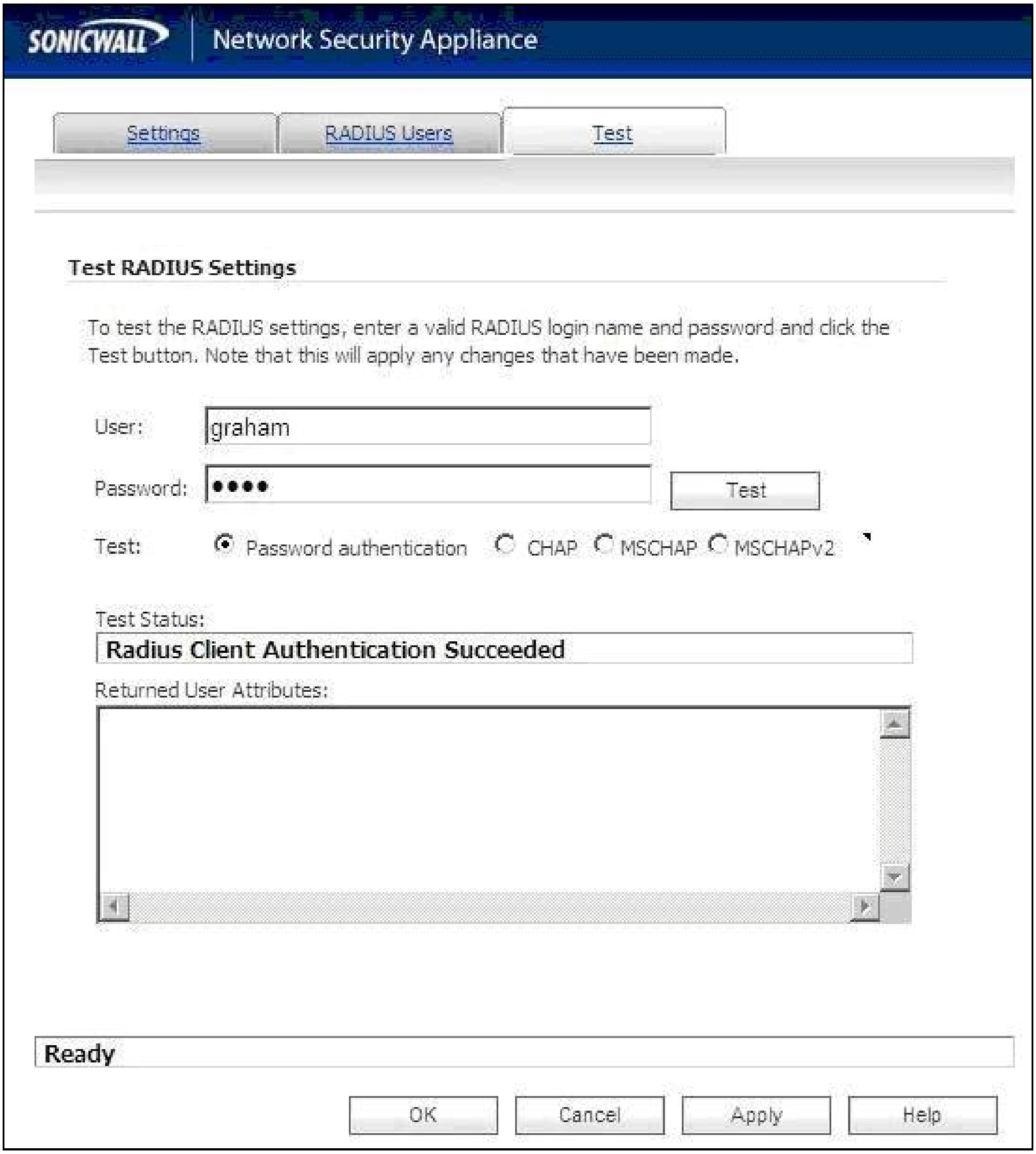
Port Number: 1812

Ready

Select the RADIUS Users tab, and ensure there is no tick in the allow only users listed locally box. Enter any other required information.

Testing SonicWALL NSA Appliance RADIUS configuration

Select the Test tab, and enter a Username and a One Time Code in the password field from the users SMS, click on the Test button (Once only), and the returned attributes will verify if the test has worked, or alternatively, enter 1234, and check for a Authentication Rejected message.



Test RADIUS Settings

To test the RADIUS settings, enter a valid RADIUS login name and password and click the Test button. Note that this will apply any changes that have been made.

User: graham

Password: ●●●●

Test: ● Password authentication ○ CHAP ○ MSCHAP ○ MSCHAPv2

Test Status: Radius Client Authentication Succeeded

Returned User Attributes:

Ready

Known Issues and Limitations

It is not currently possible to embed the Turing image into the login page, however other options such as the Taskbar utility or a web page can be used.

Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com or the local SonicWALL office http://www.sonicwall.com/emea/Support.html.