External authentication with SonicWall SSL VPN Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	
	With special thanks to: Jakob Voss-Eliasson & Thomas Weisdorf of Infinigate Denmark	

SonicWall SSl VPN (Radius) Integration Guide

This document describes how to integrate a SonicWall SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

The SonicWall SSL VPN appliance provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as SonicWall SSL VPN appliance), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of your PIN and your Phone to receive the onetime passcode. This can be either via SMS, email or using a SecurEnvoy Soft Token installed upon the phone.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

SonicWall
SonicWall SSL VPN appliance v5.8.1.3-3a

SecurEnvoy
Windows 2008 server R2 64bit
IIS installed with SSL certificate (required for remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v6.1.501

© 2012 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites 3
2.0 Configuration of SonicWall SSL VPN 4
3.0 Test Logon (Using Pre Load Passcodes or Soft Token) 5
4.0 Configuration of Real Time passcodes 5
4.0 Configuration of SecurEnvoy 6

1.0 Pre Requisites

It is assumed that the SonicWall SSL VPN appliance *is setup and operational. An existing Domain user can authenticate using a Domain password and access applications, your users can access through SSL VPN using Domain accounts.*

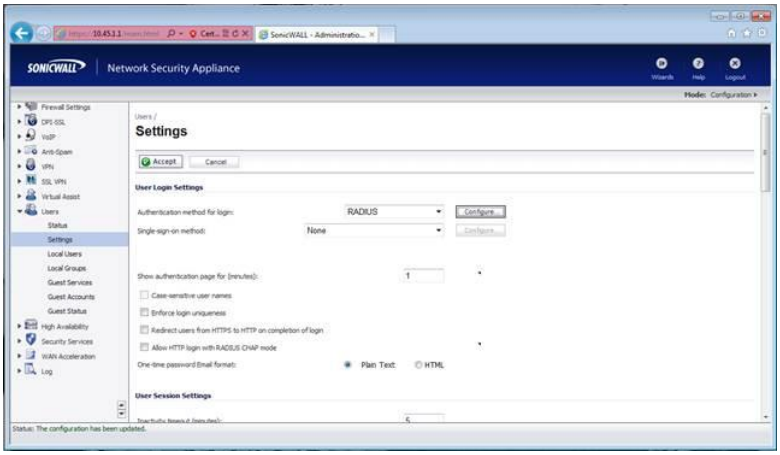
Securenvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the SonicWall SSL VPN appliance, additional open ports will be required.
NOTE: *SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the SonicWall SSL VPN appliance®.*

NOTE: *Add radius profiles for each SonicWall SSL VPN appliance® that requires Two-Factor Authentication.*

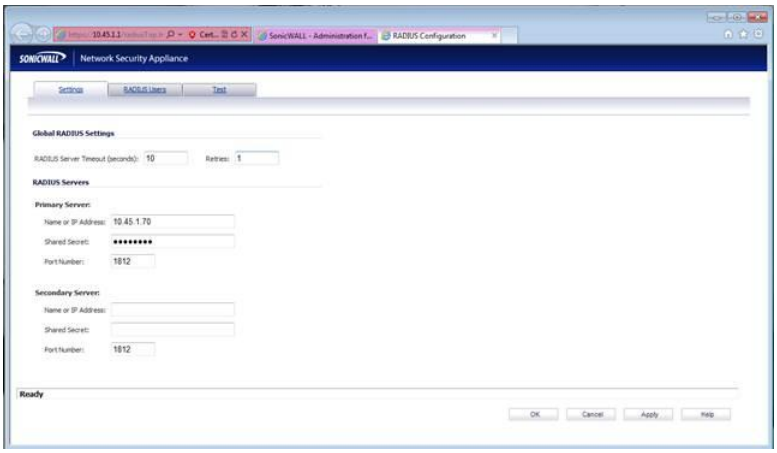
© 2012 SecurEnvoy Ltd. All rights reserved

2.0 Configuration of SonicWall SSL VPN

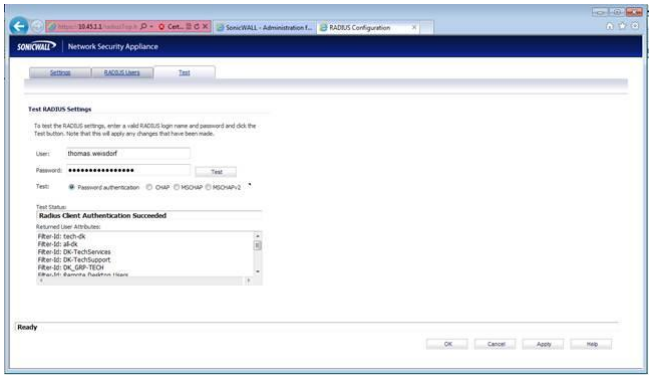
2.1 Launch the SonicWall Admin GUI
2.2 Navigate to the Users-Settings area
2.3 Select RADIUS for "Authentication method for logon"
2.4 Then select "Configure"



2.5 Set "Global RADIUS settings" to 10 seconds timeout and 1 retry
2.6 Set IP address, shared secret and port used to communicate to SecurEnvoy Server
2.7 A secondary (SecurEnvoy) server can be added for resilience



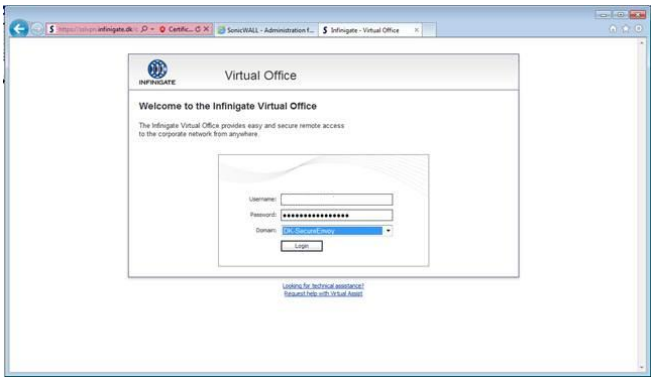
2.8 A test logon can be accomplished, go to "Test" tab
2.9 Enter UserID in User filed and Domain Password plus Passcode in password field. Click the "Test" button to complete the sequence



© 2012 SecurEnvoy Ltd. All rights reserved

3.0 Test Logon (Using Pre Load Passcodes or Soft Token)

3.1 Navigate to logon page
3.2 Enter UserID into Username filed (This is your Microsoft AD account)
3.3 Enter Domain password and passcode into password field
3.4 Select Authentication Domain (If required)



3.5 Click "Logon

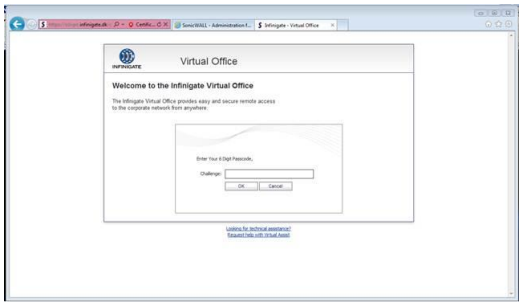
3.6 Once complete, applications will be shown in the portal



4.0 Configuration of Real Time passcodes

There is no other configuration required upon the SonicWall SSL VPN to support the use of "Real Time" passcodes.

4.1 To use Real Time Passcodes – Enable real time passcodes in the SecurEnvoy Admin GUI navigate to – Config- Real Time passcodes and select enable
4.2 Set desired user(s) to use Real time.
4.3 When a user logs on, they will enter UserID in Username field and press logon, the SonicWall SSL VPN will the present the following screen



4.4 User then enters passcode that is delivered to the phone and completes the logon sequence

© 2012 SecurEnvoy Ltd. All rights reserved

4.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to only authenticate the passcode component as both authentication servers that are required to authenticate a remote user.

SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone, via SMS, email or generated by the Soft Token.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

1. Click the **"Radius"** Button
2. Enter IP address and Shared secret for each SonicWall SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



3. Press Update
4. Now Logout

NOTE: If you require Group to application mapping:

4.5 Set Pass back data to RADIUS Client to value 11 (FilterID)
4.6 Check the radial button LDAP group membership are passed back (Default is short group name, or the Full DN path can be selected)
4.7 Click update
4.8 Refer to SonicWall configuration guide to setup using Microsoft Groups