SonicWall SSL VPN Integration

Contents

Introduction

Swivel can provide Two Factor authentication such as SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

If Strong authentication is required using Single Channel such as TURing, Pinpad then the image can be displayed in the login page or in the Taskbar. The image is served from the PINsafe server to the client.

This document will use the following steps:

- Configuring the PINsafe server
- Configuring the SonicWall login page
- Configuring the SonicWall authentication

To use the Single Channel Image such as the Turing Image, the PINsafe server must be made accessible. The client requests the images from the PINsafe server, and is usually configured using Network Address Translation, often with a proxy server. The PINsafe virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection.

Prerequisites

Swivel 3.x configured with users and SMS gateway

SonicWALL SSL VPN

Swivel login script for the SonicWall SSL VPN

The customisation script can be downloaded from here

A customisation script that also includes refresh for the TURing is [1] here

Swivel server must be accessible by client when using Single Channel Images, such as the TURing Image.

Baseline

SonicWALL SMA

SonicWALL SRA

SonicWALL SSL VPN 200 and 4200 and Firmware 3.5 onwards

SonicOS SSL-VPN 7.5.0.6-23sv

Architecture

The SSL VPN appliance and the Swivel server are usually located within the DMZ. Authentication requests are made from the SonicWall SSL VPN using RADIUS.

Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the Swivel server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for virtual or hardware appliances, the Swivel appliance VIP should not be used as the server IP address, see VIP on PINsafe Appliances

RADIUS>Server ❓

Please enter the details for the RADIUS server.

Server enabled:	Yes ▾
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No ▾
Filter ID:	No ▾
Additional RADIUS logging:	Both ▾
Enable debug:	Yes ▾
Radius Groups:	Yes ▾
Radius Group Keyword:	POLICY

Apply   Reset

Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the Swivel Administration console. Enter a name for the SonicWall SSL VPN server. The IP address has been set to the IP of the VPN virtual or hardware appliance, and the secret that will be used on both the Swivel appliance and VPN RADIUS configuration.

RADIUS>NAS ⓘ

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: Identifier: `Device Name`

Hostname/IP: `192.168.0.1`

Secret: `••••••`

EAP protocol: `None ▼`

Group: `---ANY--- ▼`

Authentication Mode: `All ▼`

Change PIN warning: `No ▼`

[Apply] [Reset]

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless
authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel appliance can be configured so that it returns an image stream containing a TURing image by presenting the username via the XML API or
the SCImage servlet. It is this mechanism that is used to return the TURing image to the VPN sign in page.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance

https://PINsafe_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see Software Only Installation

For further information see Single Channel How To Guide

Setting up Swivel Dual Channel Transports

See Transport Configuration

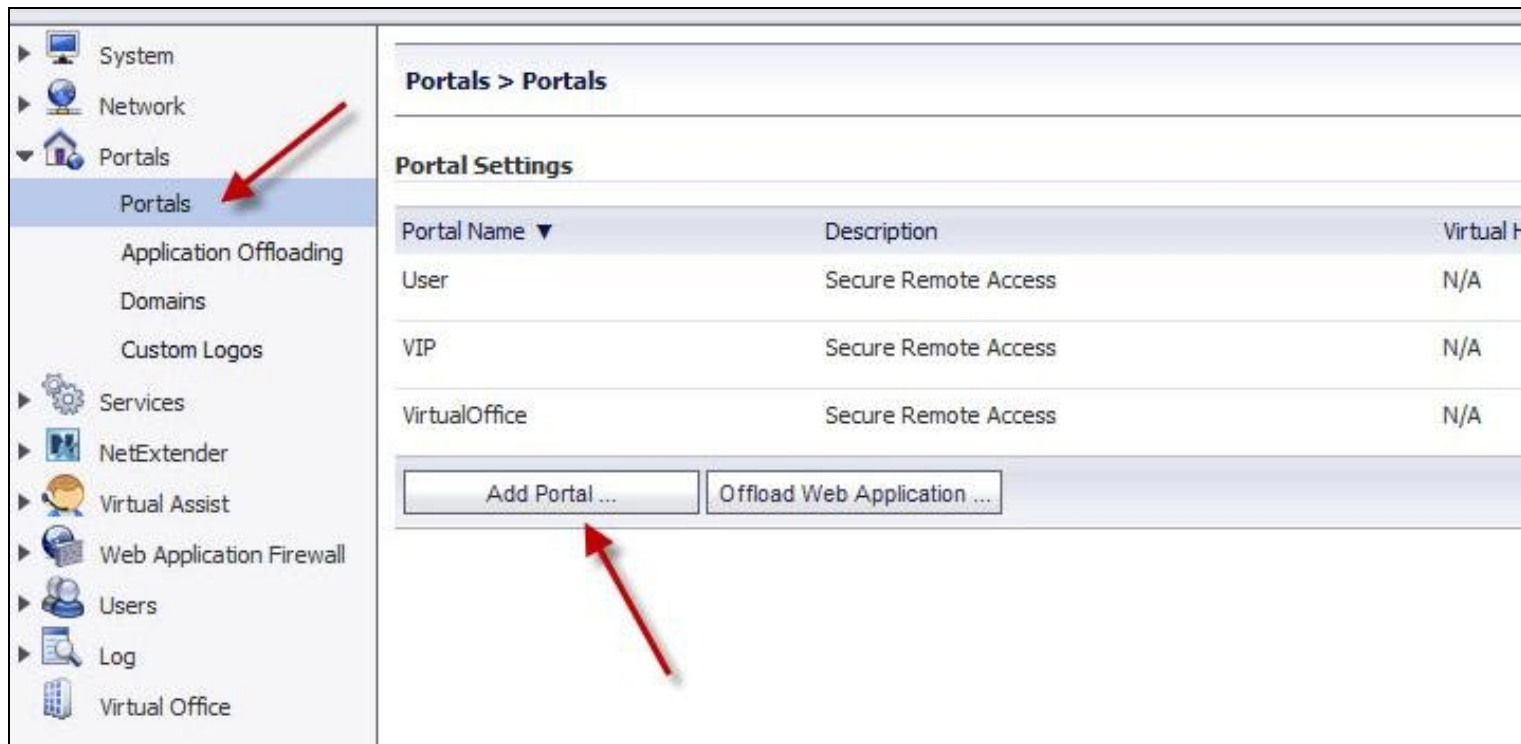### Using AD Password Authentication

This is an option to enter the AD password of users for authentication

See Check Password With Repository

SonicWall SSL VPN Configuration

Login Page Customisation

On the SonicWall SSL VPN select Portals, then click on Add Portal to open the add portal page.

Enter the following information:

Portal Name: Name for the Portal, Example, PINsafe

Portal Site Title: Name for Portal Site, Example Virtual Office

Portal Banner Title: Name for Page, Example Virtual Office

Login Message: optional login message. If the Single channel TURing image is to be used then the login script needs to be pasted into this section. Ensure the relevant scripts are modified with the External IP NAT address of the PINsafe server:

```
$('#psImage').attr('src', 'https://192.168.0.35:8443/proxy/SCImage?username=' + encodeURIComponent(username));
```

For a PINsafe virtual or hardware appliances this would need to be:

https://192.168.0.35:8443/proxy/SCImage?username=

For a software only install see Software Only Installation

Portal URL: The name of the login portal

Display custom login page: Ensure this is ticked

Display login message on custom login page: Ensure this is ticked

Enable HTTP meta tags for cache control (recommended): Usually selected

Enable ActiveX web cache cleaner: Optional

Enforce login uniqueness: Ensure this is ticked

Click OK to save the settings.
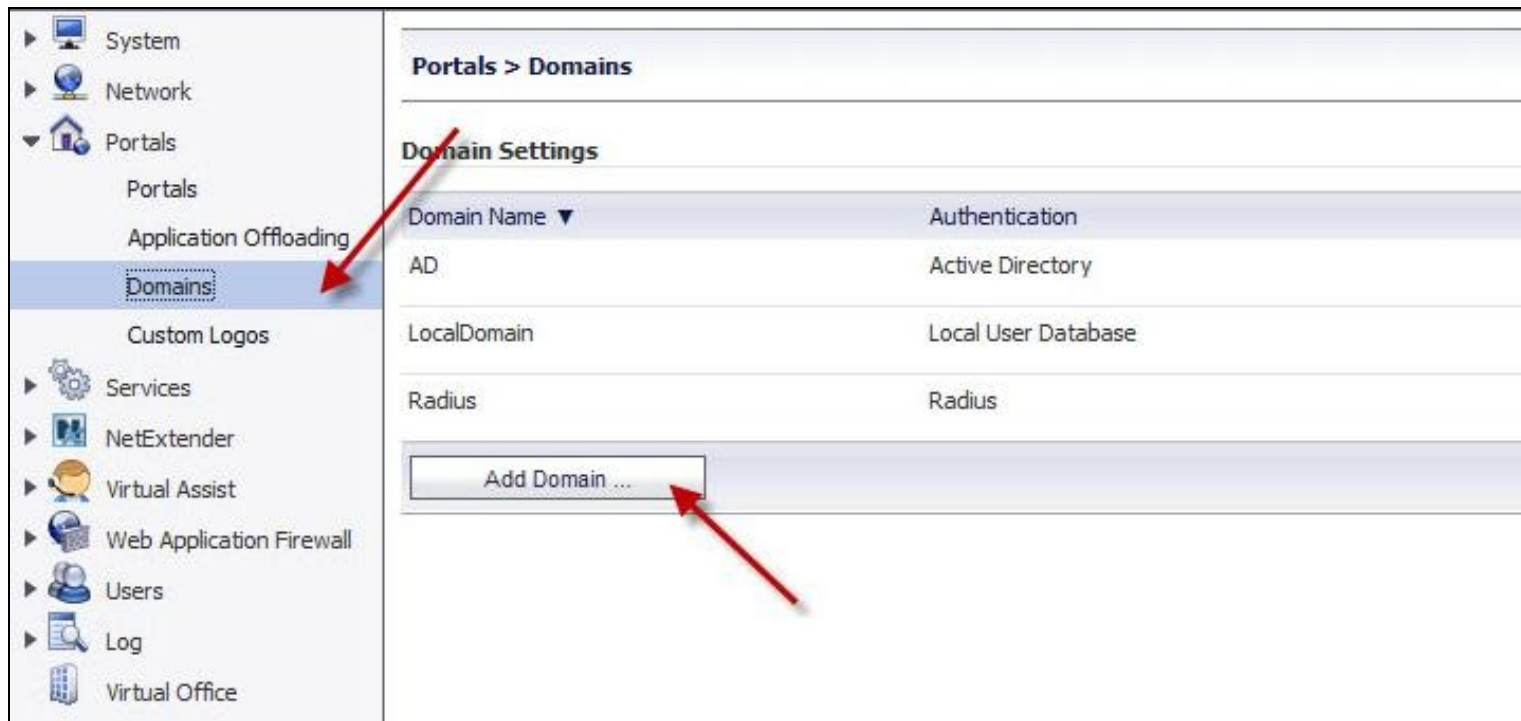
Configuring SonicWall SSL VPN Domain Settings

On the SonicWall SSL VPN select Portals then domains and click on Add Domain.

On the Add Domain page configure the Authentication server

Authentication type: select RADIUS

Domain name: Name for the domain

Authentication Type: Select the required authentication

RADIUS server address: Hostname or IP address of the PINsafe server

RADIUS server port: Usually 1812

Secret password: Enter a shared secret that needs to be also entered on the PINsafe server NAS entry

Portal Name: Select the Portal Name created above.

Click OK to save the settings.

Add Domain

Authentication type:	Radius ▾
Domain name:	pin
Authentication Protocol:	MSCHAP ▾

Primary Radius server

Radius server address:	192.168.168.3
Radius server port:	1812
Secret password:	•••••••••
Radius Timeout (Seconds):	5
Max Retries:	2

Backup Radius server

Radius server address:	
Radius server port:	1812
Secret password:	

☐ Use Filter-ID For RADIUS Groups

Portal name:	VirtualOffice User VIP **Pinsafe**

☐ Enable client certificate enforcement

☐ Delete external user accounts on logout

☐ One-time passwords

Add	Cancel

Additional Configuration Options
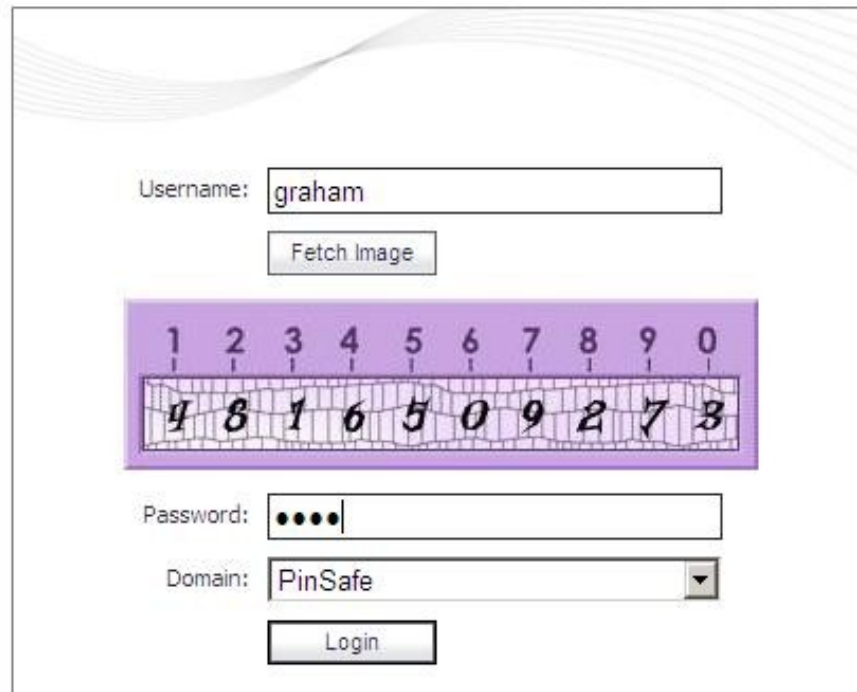
Testing

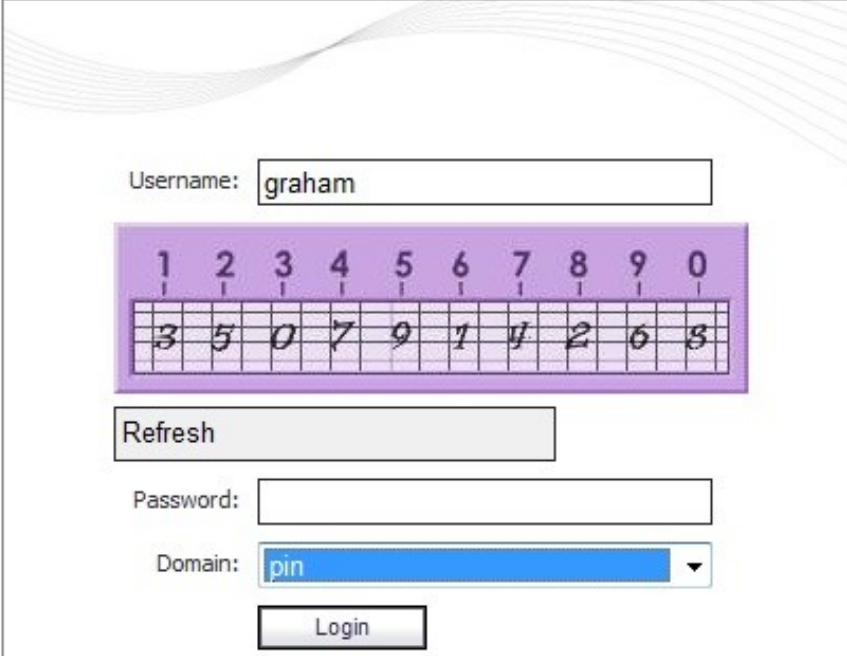Browse to the login page and verify the login

Login page showing the TURing image where OTC is entered as the Password

Login page showing the TURing image with where OTC is entered as Passsword and a *Refresh* Image button

Troubleshooting

Check the PINsafe logs for Turing images and RADIUS requests.

Users can bypass Swivel authentication

When a user authenticates using RADIUS, a local account may be created on the SonicWall. With some SSO policies the user may then not be required to sign in using RADIUS authentication. Verify the SSO policy and adjust as required.

Known Issues and Limitations

None

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