Fortigate SSL VPN 3.x With PINsafe Installation Notes

Table of Contents

Version: 2.1 Created: 02 2008 Updated: 28/01/2011

Author: Graham Field, Swivel Secure and Jon Addison, Fortinet

1. Introduction

PINsafe from Swivel Secure is an enhanced authentication system that utilizes both single and dual factor authentication. The essence of PINsafe is an ever changing one time password generated from an end user known PIN and a randomly generated string. The one time code is calculated by entering the letters or numbers of the random string according to the position they occur relative to the users PIN code. For example if the user's PIN code is 2468 and the random string is 0987654321 then the one time code will be the 2nd, 4th, 6th, then 8th character from the random string (9753 in this example).

The Pinsafe system can be integrated into the Fortigate login screens to display the random string as a "Turing" string. Whilst not achieving any dual factor authentication in this manner, the system helps to alleviate the problem of keyloggers capturing passwords as they are unique every time.

The PINsafe system has a dual channel option. In this mode the random string is sent to the user by a different channel. These channels include a request from a different web page, SMS message, email and others. The system can be setup to send a new random string after every login attempt, either successful or not, or the user may request a random string on demand which will have a validity period of 2 minutes.

The Swivelsecure PINsafe server acts as a radius server to the Fortigate and will provide authentication and accounting.

This document discusses the integration requirements, it does not go into detail regarding how to setup either Pinsafe, or The Fortigate SSL VPN as this information is available in other documents.

2. Overview

2.1. Prerequisites

PINsafe 3.x
Pinsafe admin guide
Fortigate SSL VPN 3.x
FortiGate SSL VPN User Guide

2.2. Baseline

The integration was tested with a Fortinet Fortigate SSL VPN version 3 MR6 and PINsafe 3.3
Note: Version 4 was tested August 2009 and has an update in the style sheet location (<link href="/sslvpn/css/login.css" rel="stylesheet" type="text/css">)

2.3. Architecture

The PINsafe server is usually situated with the DMZ and connects to various data sources. The Fortigate SSL VPN connects to the PINsafe server for authentication information by RADIUS.

3. Installation

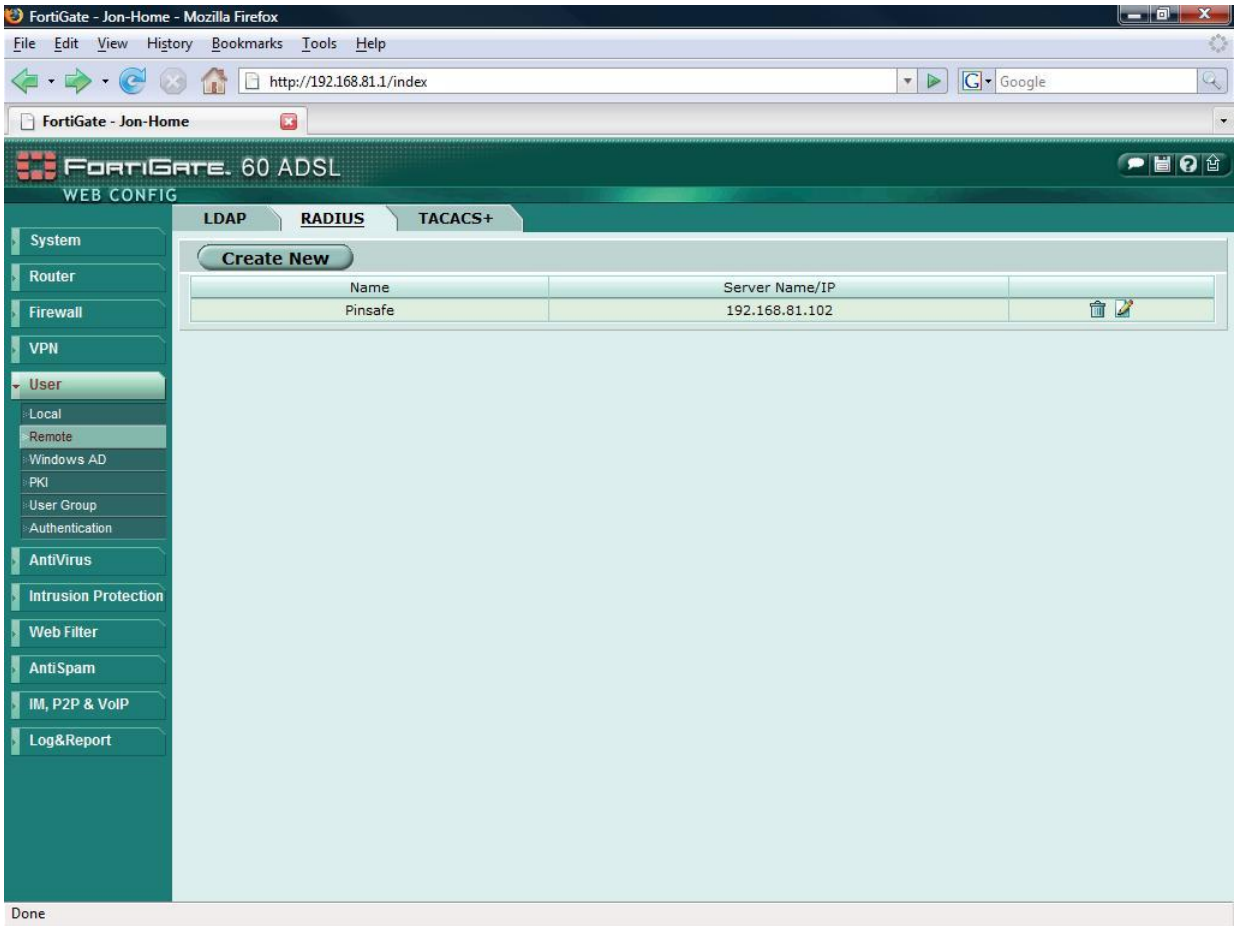
3.1. Configuring the PINsafe server

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 Fortigate device and its IP address and a shared secret key.

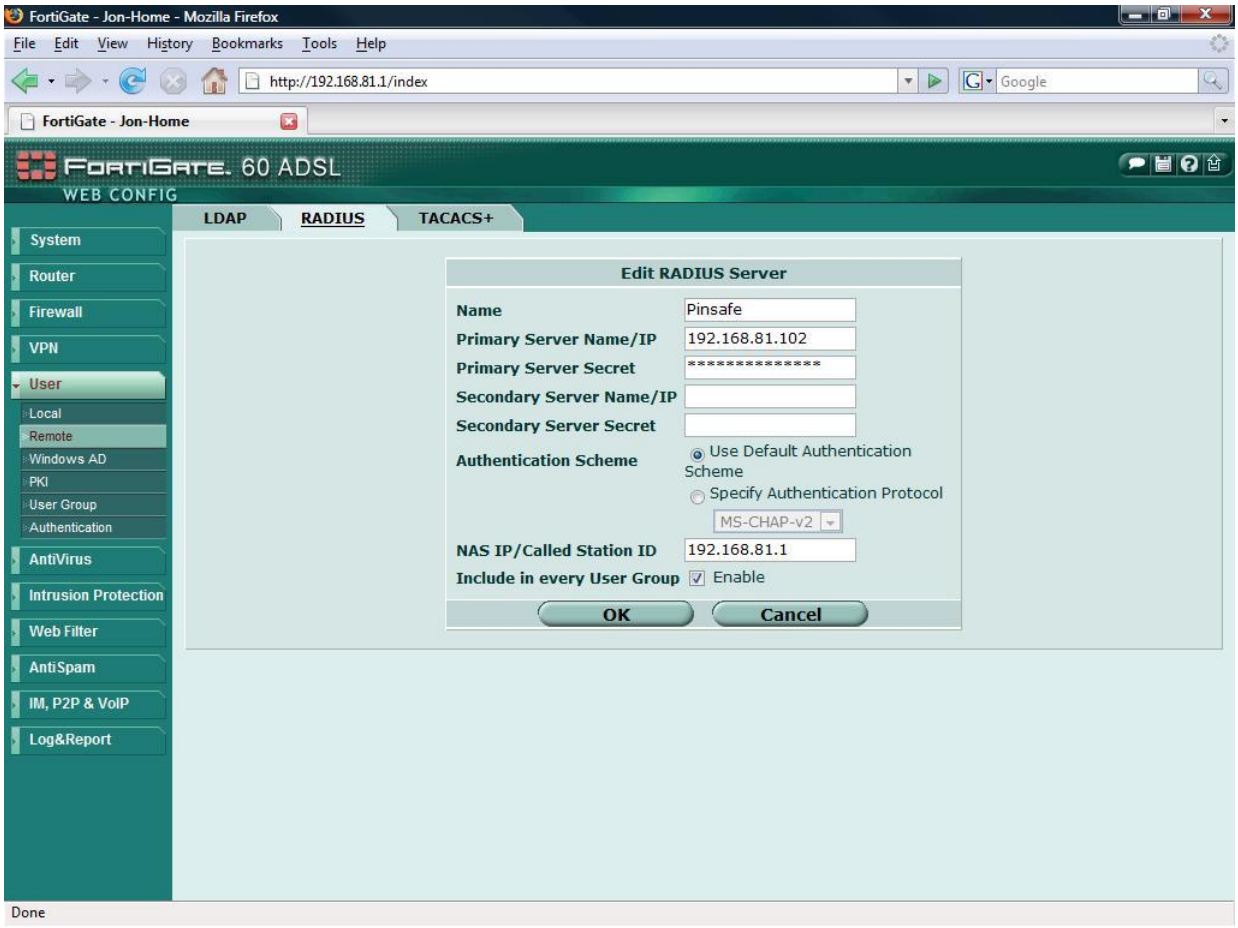
If using Single Channel, select Server/Single Channel and set session request by user name to YES.

3.2. Configuring the Fortigate SSL VPN

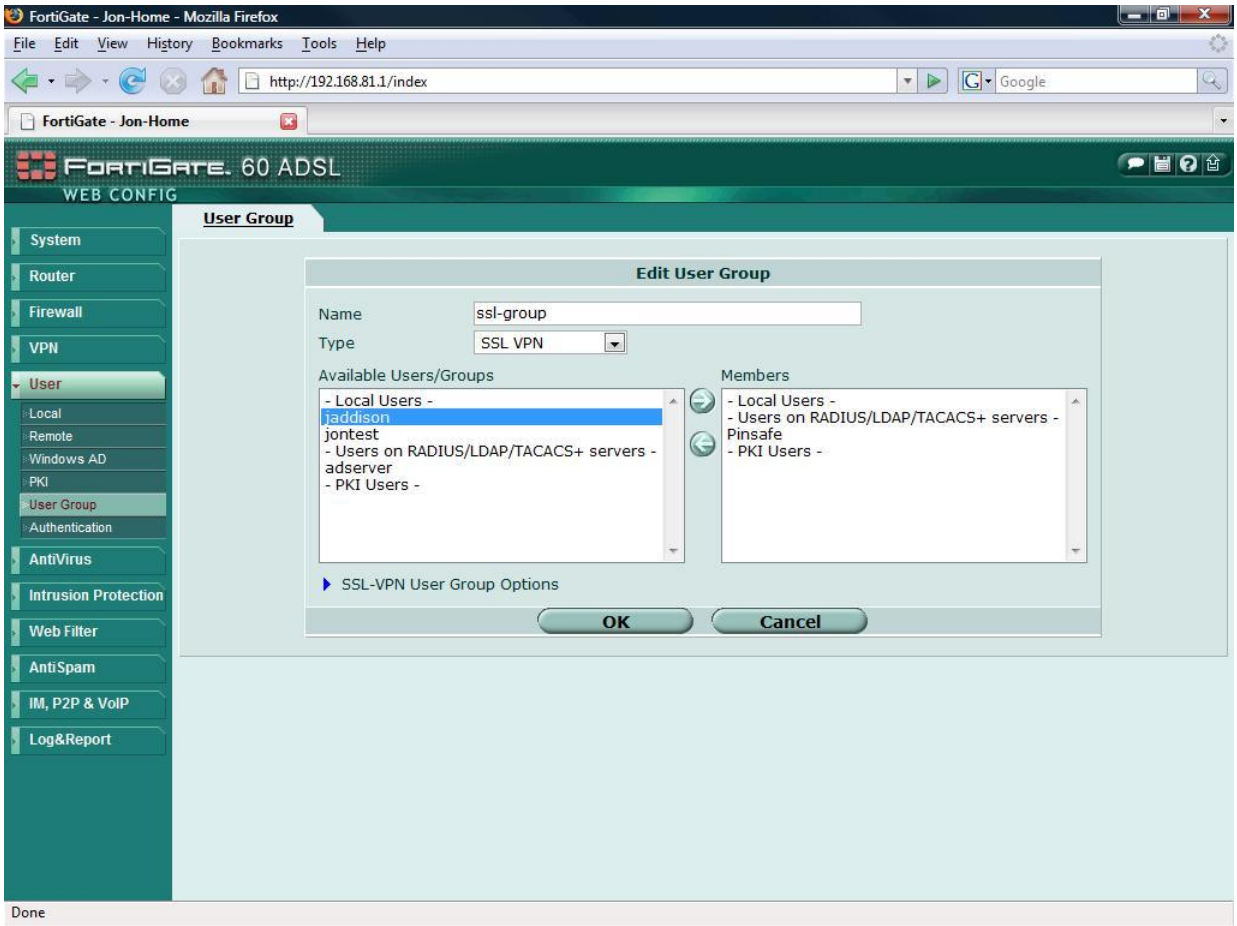
Set the PINsafe server as a RADIUS server. Select User=>Remote in the left hand navigation pane, the select the Radius tab. Press create new to bring up the new Radius server option.



Enter a name for the Radius server
Enter the Radius Server primary IP address
Enter the shared secret chosen between the Fortigate and the Pinsafe server
Enter the IP address of the Interface that will be used to send information to the PINsafe Server
Check the Include in every User Group check box


FortiGate - Jon-Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.81.1/index
FortiGate - Jon-Home
FortiGate 60 ADSL
WEB CONFIG
LDAP
RADIUS
TACACS+
System
Router
Firewall
VPN
User
Local
Remote
Windows AD
PKI
User Group
Authentication
AntiVirus
Intrusion Protection
Web Filter
AntiSpam
IM, P2P & VoIP
Log&Report
Edit RADIUS Server
Name
Pinsafe
Primary Server Name/IP
192.168.81.102
Primary Server Secret
****
Secondary Server Name/IP
Secondary Server Secret
Authentication Scheme
Use Default Authentication Scheme
Specify Authentication Protocol
MS-CHAP-v2
NAS IP/Called Station ID
192.168.81.1
Include in every User Group
Enable
OK
Cancel
Done

Add the Radius server to the SSL VPN Group. Under User=>User Group slect an existing, or create a new SSL VPN User group. Add the newly created Radius server to the Member list by selecting it from the left hand panel and pressingthe right facing arrow.



3.3. Integrating PINsafe into login screens

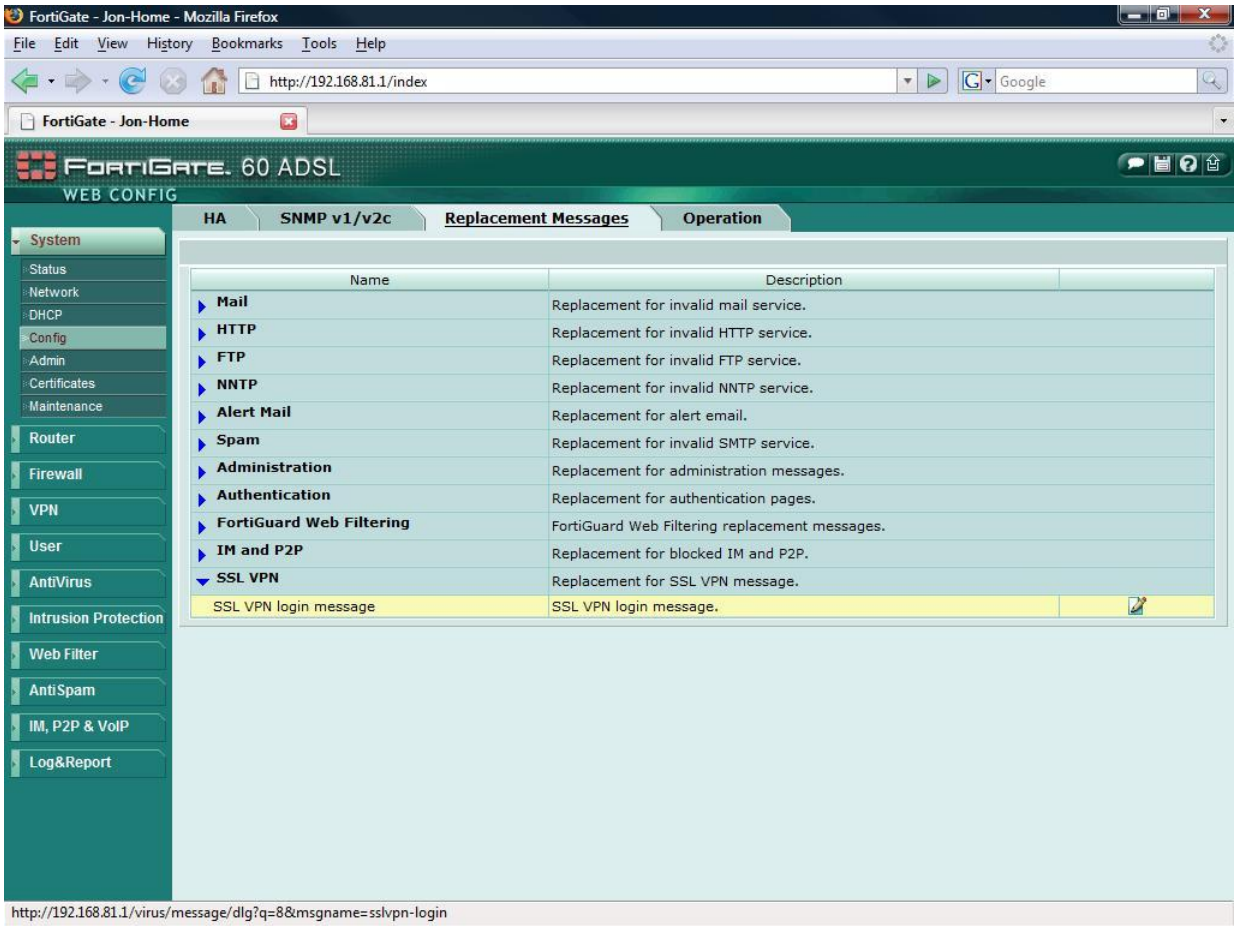
If you are using a standard dual channel authentication then no further action is required on the Fortigate. The PINsafe server will send the security strings and PIN information to the user on first setup of the account and after every subsequent login attempt.

The following section discusses how to modify the Fortigate authentication screens to integrate with PINsafe Turing image and on demand features. For this example we discuss only the SSL VPN login screen, but the theory can be applied to any of the Fortigate's Web Authentication methods.

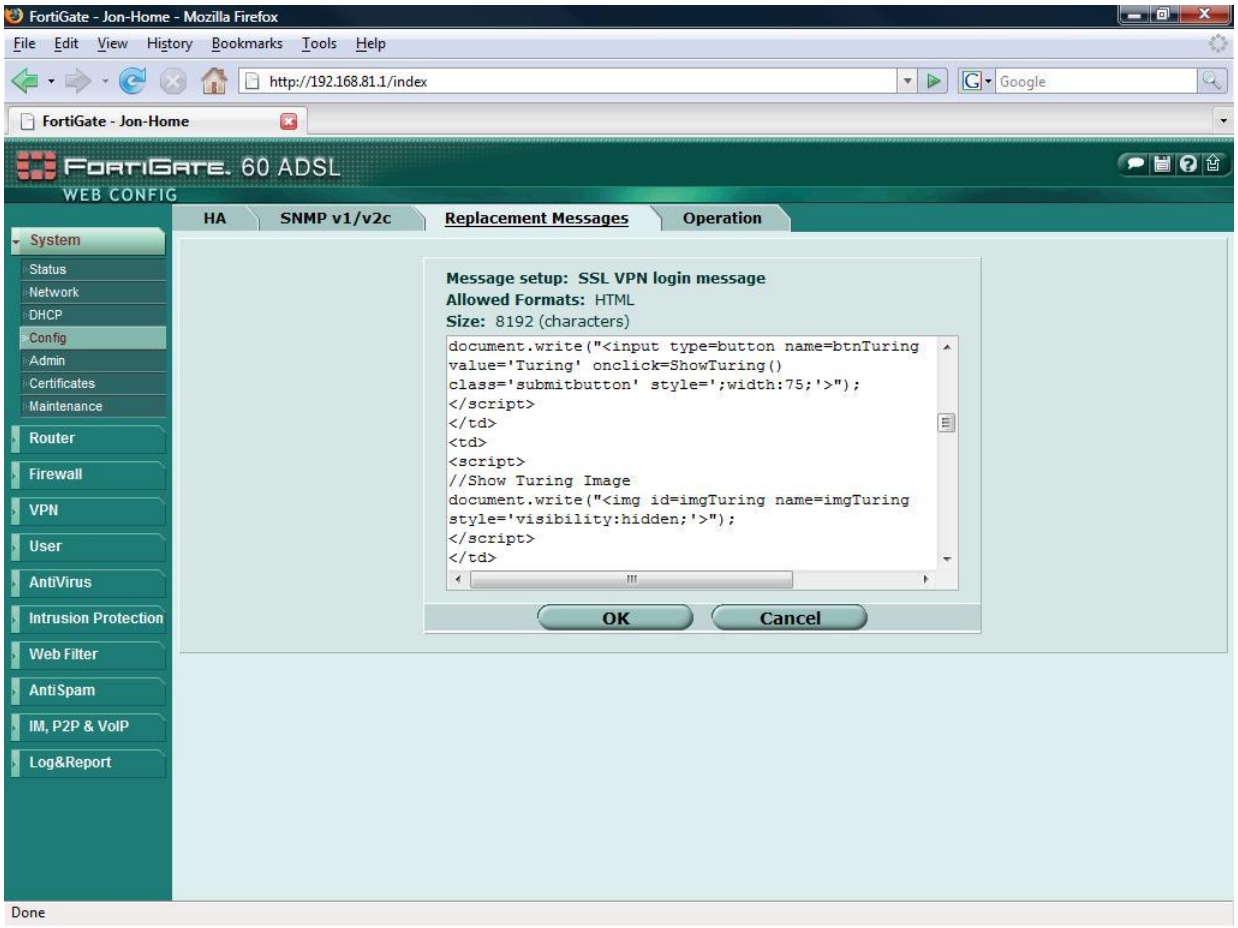
3.4. Modifying the SSL login screen to integrate with the PINsafe Server.

In this scenario we will add some simple client side java script to the default SSL login page, to allow the user to directly request information from the Pinsafe server.

From System=>Config in the left hand navigation pane select the replacement messages tab.
Open the SSL VPN section by pressing on the blue arrow to the left of it.
Press the edit icon to the right of the SSL VPN login message



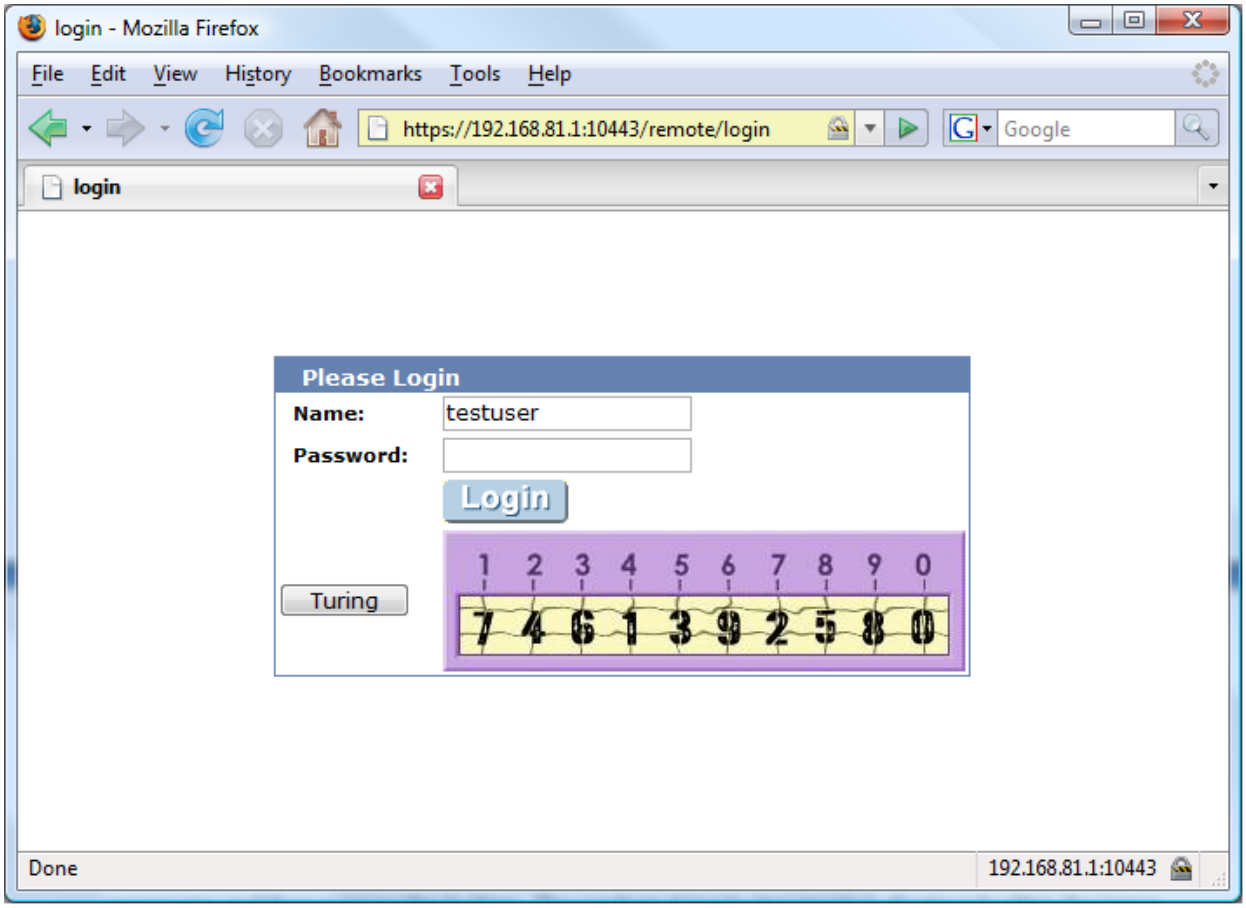
You can directly add to the default page, or simply copy and paste from a HTML/text editor a complete new login page
The example below shows a modified login page already applied.


FortiGate - Jon-Home - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.81.1/index
FortiGate - Jon-Home
FortiGate 60 ADSL
WEB CONFIG
HA
SNMP v1/v2c
Replacement Messages
Operation
System
Status
Network
DHCP
Config
Admin
Certificates
Maintenance
Router
Firewall
VPN
User
AntiVirus
Intrusion Protection
Web Filter
AntiSpam
IM, P2P & VoIP
Log&Report
Message setup: SSL VPN login message
Allowed Formats: HTML
Size: 8192 (characters)
document.write("<input type=button name=btnTuring
value='Turing' onclick=ShowTuring()
class='submitbutton' style=';width:75;'>");
</script>
</td>
<td>
<script>
//Show Turing Image
document.write("<img id=imgTuring name=imgTuring
style='visibility:hidden;'>");
</script>
</td>
OK
Cancel
Done

3.5. Example SSL VPN login pages.

Display Turing request button and Turing image

In this page a script is included that will display a button called “Turing”. When a user enters his username and then presses the button. The random string Turing image is displayed within the logon box.



With the image displayed the user then enters the one time code according to his PIN number and logs in as usual. The login request is sent to the PINsafe RADIUS server for authentication. NB. PINsafe also allows for the one time code to be appended to a static password for increased security.

3.6. Turing Display Script

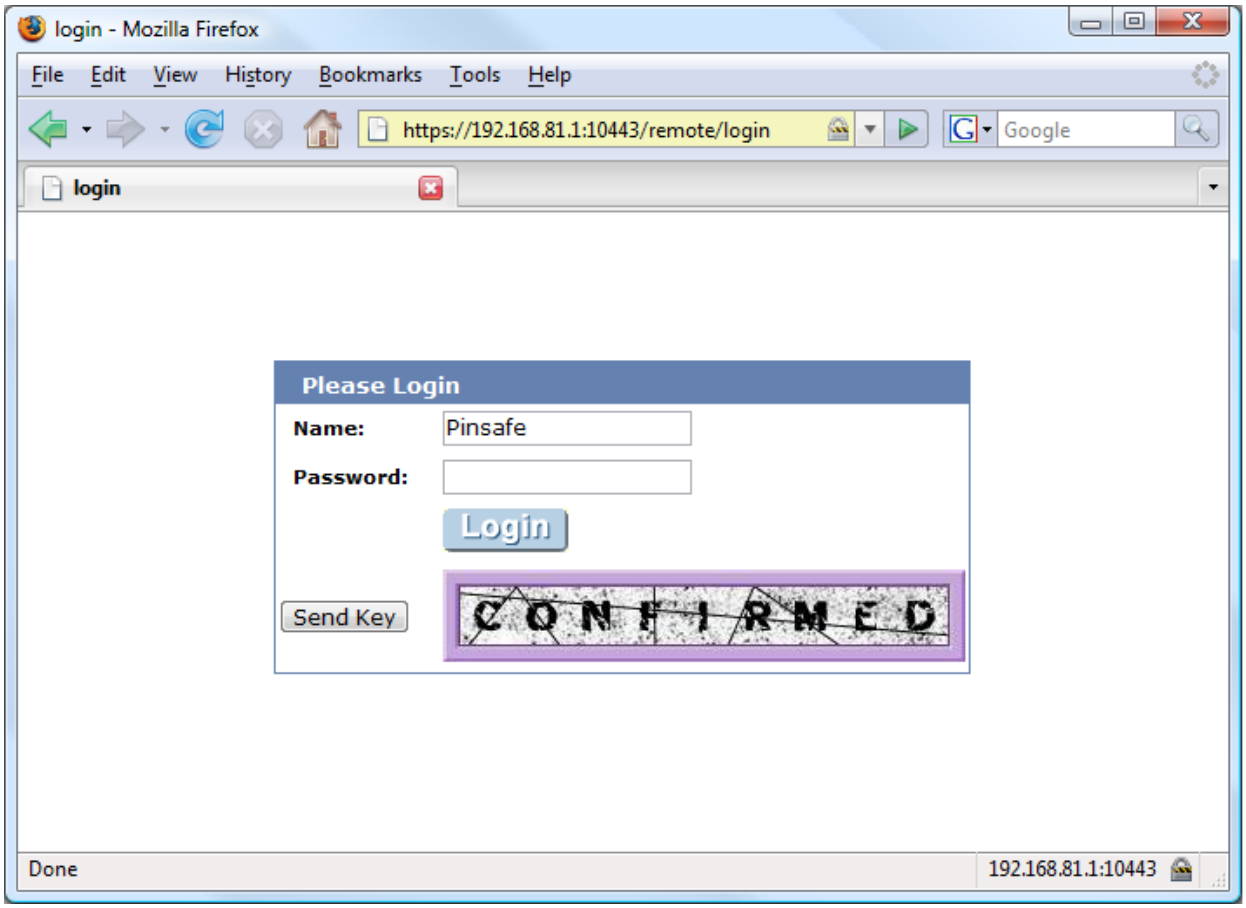
The bold sections indicate additions to the default page

```
<html><head><title>login</title>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
<link href="/ssl_style.css" rel="stylesheet" type="text/css">
<script language="JavaScript"><!--if (top && top.location != window.location) top.location
= top.location;if (window.opener && window.opener.top) { window.opener.top.location =
window.opener.top.location; self.close(); }//--></script>
</head>
<body class="main">
<center><table width="100%" height="100%" align="center" class="container"
valign="middle" cellpadding="0" cellspacing="0">
<tr valign=middle>
<td>
<form action="%%SSL_ACT%%" method="%%SSL_METHOD%%" name="f">
<table class="list" cellpadding=10 cellspacing=0 align=center width=400
height=180>%%SSL_LOGIN%%
<td>
<script>
//Print Turing Buttom
document.write("<input type=button name=btnTuring value='Turing'
onclick=ShowTuring() class='submitbutton' style=';width:75;'>");
</script>
</td>
<td>
<script>
//Show Turing Image
document.write("<img id=imgTuring name=imgTuring style='visibility:hidden;'>");
</script>
</td>
</table>
%%SSL_HIDDEN%%
</td>
</tr>
</table>
</form>
</center>
</body>
<script>document.forms[0].username.focus();
</script>
<script>
{
//~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
//
```

```
//Configuration section.....

//URL of radiusTuring page on the PINsafe server....
//var sUrl="http://pinsafe.server.com:8080/pinsafe/SCImage?username=";
var sUrl="https://pinsafe.server.com:8443/proxy/SCImage?username=";

//Names of the username and password texboxes in the page that's calling this script...
//(On Fortinet these are username and credential)
var sNameOfUsernameText = "username";
var sNameOfPasswordText = "credential";

//End configuration section.....
//
//~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

function ShowTuring() {
sUser=document.getElementsByName(sNameOfUsernameText)[0].value;
    if (sUser=="") {
        alert ("Please enter your username first!");
document.getElementsByName(sNameOfUsernameText)[0].focus()
    }else{
        //Find the image using Mozilla compatible pproach...
        varImg = document.getElementById("imgTuring");

        //Set the image SRC and make it visible
        varImg.src = sUrl + sUser;
        varImg.style.visibility = "visible";

        //Set focus to the OTC input
        document.getElementsByName(sNameOfPasswordText)[0].focus()
    }
}
}
</script>
</html>
```

3.7. On Demand Request for one time Security String

The on demand script causes the PINsafe server to simply send the one time security string to the user via the chosen transport (SMTP, SMS etc.) The script is almost identical, with just the button name and URL requested changed. (changes are highlighted in red in the following script)



In this configuration, the server simply displays confirmed to tell the user that the one time security string has been sent via his/her preferred method. The user then has two minutes <default> to login before this one time pad expires.
NB: If this "on demand" mode is chosen, then the automatic sending of a one time security strings after failed or successful login is disabled

3.8. On demand script

```
<html><head><title>login</title>
<meta http-equiv="Pragma" content="no-cache">
<meta http-equiv="cache-control" content="no-cache">
<meta http-equiv="cache-control" content="must-revalidate">
<link href="/ssl_style.css" rel="stylesheet" type="text/css">
<script language="JavaScript"><!--if (top && top.location != window.location) top.location =
top.location;if (window.opener && window.opener.top) { window.opener.top.location =
window.opener.top.location; self.close(); }//--></script>
</head>
<body class="main">
<center><table width="100%" height="100%" align="center" class="container"
valign="middle" cellpadding="0" cellspacing="0">
<tr valign=middle>
<td>
<form action="%%SSL_ACT%%" method="%%SSL_METHOD%%" name="f">
<table class="list" cellpadding=10 cellspacing=0 align=center width=400
height=180>%%SSL_LOGIN%%
<td>
<script>
//Print Turing Buttom
document.write("<input type=button name=btnTuring value='Send Key'
onclick=ShowTuring() class='submitbutton' style=';width:75;'>");
</script>
</td>
<td>
<script>
//Show Turing Image
document.write("<img id=imgTuring name=imgTuring style='visibility:hidden;'>");
</script>
</td>
</table>
%%SSL_HIDDEN%%
</td>
</tr>
</table>
</form>
</center>
</body>
<script>document.forms[0].username.focus();
</script>
<script>
{
//~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
//
//Configuration section.....
```

```
//URL of confirmation page on the PINsafe server....
var sUrl="http://pinsafe.server.com:8080/pinsafe/DCMessage?username=";

//Names of the username and password textboxes in the page that's calling this script...
//(On Fortinet these are username and credential; on Netscreen they are username and
password)
var sNameOfUsernameText = "username";
var sNameOfPasswordText = "credential";

//End configuration section.....
//
//~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

function ShowTuring() {
sUser=document.getElementsByName(sNameOfUsernameText)[0].value;
    if (sUser=="") {
        alert ("Please enter your username first!");
document.getElementsByName(sNameOfUsernameText)[0].focus()
    }else{
        //Find the image using Mozilla compatible pproach...
        varImg = document.getElementById("imgTuring");

        //Set the image SRC and make it visible
               varImg.src = sUrl + sUser + "&Random=" + Math.random();
        varImg.style.visibility = "visible";

        //Set focus to the OTC input
        document.getElementsByName(sNameOfPasswordText)[0].focus()
    }
}
}
</script>
</html>
```

4. Verifying the Installation

Connect to the SSL VPN login page and check that the correct authentication methods are available.

5. Troubleshooting

Check the PINsafe and Fortigate logs.

6. Known Issues and Limitations

None

7. 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