

F5 Firepass Integration

Contents

- 1 Introduction
- 2 Prerequisites
 - ◆ 2.1 Baseline
- 3 Architecture
- 4 Installation
 - ◆ 4.1 PINsafe Configuration
- 5 F5 Networks FirePass VPN Configuration
- 6 Test the RADIUS authentication
- 7 Modifying the FirePass login page for PINsafe TURING image
- 8 Verifying Installation
- 9 Troubleshooting
- 10 Additional Information

Introduction

This document outlines the steps required to integrate the F5 Networks FirePass SSL VPN with the Swivel PINsafe authentication server.

FirePass VPN appliances are able to use external RADIUS servers for providing authentication. The PINsafe server provides RADIUS authentication, thus the FirePass VPN can be configured to use the PINsafe server for authentication via RADIUS.

PINsafe users can use either PINsafe's Single Channel (**TURing**, **PATtern**) or Dual Channel (SMS, Swivlet applet) methods to retrieve Security Strings, which are applied against the user's PIN to extract a One-Time Code (OTC) which represents the password for an authentication request.

With Dual Channel methods, the user already holds one or more Security Strings on their mobile device (and can request more at any time) so with the FirePass VPN configured to use the matching PINsafe server for RADIUS authentication, no further integration is required.

However with Single Channel methods, the user must be presented with a TURing or PATtern image upon login (representing a single time-limited Security String), so they can extract their OTC. The Authentication configuration section below describes how to achieve the RADIUS configuration. Single Channel requires access to the PINsafe server by a Public IP address.

Prerequisites

Baseline

The FirePass VPN appliance tested was FirePass 600. (<http://www.f5.com/products/FirePass/FP600.html>)

The PINsafe server used was PINsafe v3.1. However, no changes have been made to PINsafe since then which would render the integration invalid.

The primary web browser used for testing was Internet Explorer 6.0.2900.2180.xpsp_sp2_gdr.050301-1519.

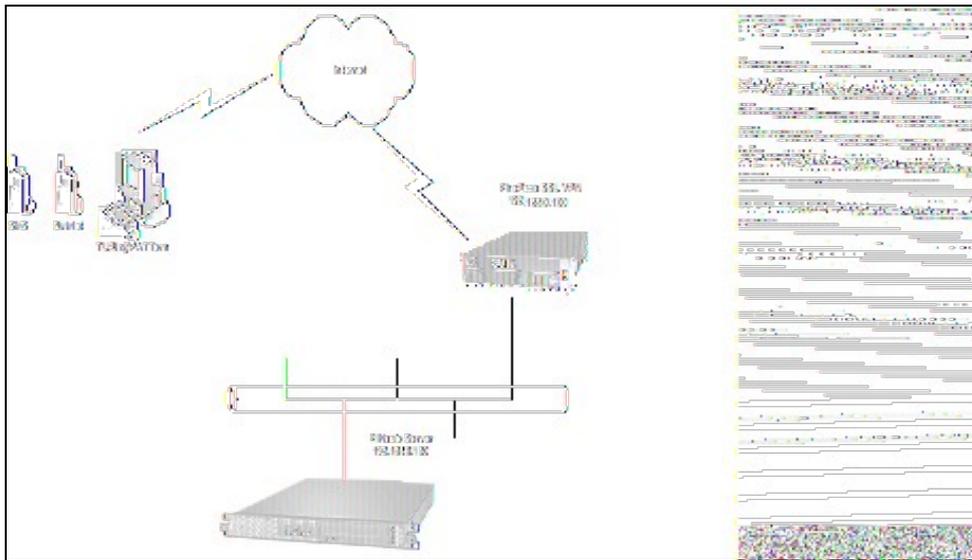
Architecture

The user connects to the FirePass VPN using a web browser, pointing to the appropriate login URL for the VPN in question.

The FirePass VPN is configured to use a PINsafe server for RADIUS authentication.

Users are stored and maintained in the PINsafe server.

Figure 1. The following diagram shows the configuration used and is typical. This example is used throughout this document:



Installation

PINsafe Configuration

Configuration of the PINsafe server for RADIUS authentication with the FirePass VPN consists of three steps:

1. Configure PINsafe RADIUS settings.
2. Set up the NAS (Network Access Server), which in this case is the FirePass VPN.
3. Configure the PINsafe server to allow TURing/PATtern session creation with a username.

NOTE ? This document assumes that the PINsafe server has been configured to use a specific user repository and populated with users. Please refer to the PINsafe Administration Guide for detailed instructions.

1. Configuring PINsafe RADIUS settings

Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In our example (see diagram above) the RADIUS Mode is set to ?RADIUS Server? and the HOST IP (the PINsafe server) is set to 192.168.0.150.

Figure 2. PINsafe RADIUS configuration page.

Radius > Server 

Please enter the details for the PINsafe RADIUS Server.

Server Enabled:	<input type="text" value="Yes"/>
Enable Debug:	<input type="text" value="No"/>
Hostname:	<input type="text" value="pinsafeserver"/>
Host IP Address:	<input type="text" value="192.168.0.150"/>
Authorisation Port:	<input type="text" value="1812"/>
Accounting Port:	<input type="text" value="1813"/>
Maximum No. Session:	<input type="text" value="500"/>
Permit Empty Attributes:	<input type="text" value="No"/>
Additional RADIUS Logging:	<input type="text" value="Both"/>
Filter ID:	<input type="text" value="No"/>

2. Setting up the NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. In our example (see Figure 3), the meaningful name ?FirePass VPN? has been assigned so it can be identified if you have more than one NAS configured. The IP address has been set to the IP of the VPN appliance, and the NAS secret assigned that will be used on both the PINsafe server and VPN RADIUS configuration.

<center> Figure 3. Extract from PINsafe NAS setup page

Radius > NAS

Please enter the details for any RADIUS NAS.

NAS: Identifier: FirePass VPN

IP Address: 192.168.0.100

Secret: 000000

Apply Reset

3. Configure the PINsafe server to allow TURing/PATtern session creation with a username.

The PINsafe server must be configured to allow a Single Channel session to be created by accessing a specific URL on the PINsafe server. The following URL would create a start a session and return the image for the user ?test?:

For a Swivel hardware or virtual appliance http://Swivel_IP:8443/proxy/SCImage?username=test

For a software only install see [Software Only Installation](#)

</center>

F5 Networks FirePass VPN Configuration

The RADIUS FirePass configuration is found under Users, Groups, Master Groups, Radius_Users, and then the Authentication tab. The Primary RADIUS server was set to the IP address of the PINsafe server followed by the authorization port (see Figure 5). The shared secret entered was the same secret entered in the PINsafe NAS entry (see Figure 3).

If you want to configure a secondary PINsafe RADIUS server for failover you would add the details of the server in the ?Secondary RADIUS server? section on this page. If you are utilizing the High Availability PINsafe solution, failover/redundancy is managed by that solution, thus you would only enter the Primary RADIUS server address.

Figure 4. Extract from FirePass RADIUS Authentication setup page

RADIUS Authentication

[Convert authentication method >>](#)

RADIUS settings

Timeout:

Retries:

Service Type (optional): ▼

Primary RADIUS server

Server:

Port:

Change Shared Secret:

Shared Secret:

Confirm Shared Secret:

Retrieve Single Sign On Password from RADIUS attribute

Use a secondary RADIUS server

Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then [View Strings](#), and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

Modifying the FirePass login page for PINsafe TURING image

The PINsafe sends Security Strings to users via SMS, Swivlet applet (Dual Channel) or through a TURING image (Single Channel) accessed by public IP address from the PINsafe server. The user extracts their One Time Code (OTC) from the Security String and enters it into the VPN sign-in. If the user has been assigned a PINsafe server static password, they must enter the password plus their OTC. For example, if the user's PINsafe static password was ?foobar? and their OTC were 7452, they would enter ?foobar7452? at the login prompt.

If the PINsafe user were configured to use Dual Channel (SMS or applet), they should have a security string ready on their mobile device. No modification to the FirePass login page would be required. For Single Channel users, we need some way of presenting a TURING image on the FirePass VPN's login page. This can be achieved through configuration of the FirePass login screen via WebDAV.

To enable WebDAV based customization

1. Create an HTTP web service on the Device Management : Configuration : Network Configuration : Web Services screen.
2. Select the **Allow insecure access** option on the Device Management : Security : User Access Security screen.
3. Check **Allow WebDAV sandbox customization** on the Device Management : Customization screen and enter a WebDAV password in the text box that appears.

The WebDAV sandbox is accessed via HTTP at the URI **/sandbox** as the user **webdav**. So, for example, if the FirePass controller has been configured using the steps above with a HTTP web service at 192.168.0.99, you would use the URL <http://192.168.0.99/sandbox/>.

Any content can be placed in the sandbox directory. The FirePass controller uses specific files to override or supplement stock system behavior. To add the TURING image to the right of the logon prompt, the **right.inc** file was created and added to the sandbox, with the following content:

```
<script language="JavaScript">

</script>

<input name="btnTuring" type="button" value="OTC Image" class="submitbutton" onclick="ShowTuring()" />

<img id="imgTuring" style="visibility:hidden;" alt="Turing image" />
```

Edit the following line with the correct IP address

sUrl="http://192.168.0.150:8443/proxy/SCImage?UserName=";

For PINsafe 3.1.3a and later the following line needs to be edited:

```
sUrl="http://192.168.0.150:8443/proxy/SCImage?username=";
```

To upload the WebDAV pages browse to the sandbox with a web browser using http (not https) and enter the WebDAV username and password.

Once loaded into the sandbox, the login page should contain a new button and the ability to display the Turing image.

Figure 6. Example of a modified FirePass login page



Verifying Installation

Navigate to the F5 interface login page. The customisation is visible in the addition of a **One Time Code Image** button. Only when a correct PINsafe one time code is entered should the user be logged in. This can be done either by entering the OTC for a dual channel login, or selecting OTC Image and entering the OTC for a single channel login.

Troubleshooting

Check the PINsafe logs for any failure information.

Additional Information

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at support@swivelsecure.com