BLUECOAT PROXY

INTEGRATION GUIDE

SWIVEL SECURE
VICTORIA AVENUE
HARROGATE
HG1 1EL

BLUECOAT PROXY

INTEGRATION GUIDE

CONTENTS

INTRODUCTION

This document describes how to integrate a Bluecoat SG Reverse Proxy. It is based on the following product.

Model: 200-B

Software: SGOS 5.2.0.4 Proxy Edition, Release 29623

This focuses on the required integration steps rather than the general configuration required on both systems to meet the specific installation requirements.

PINSAFE CONFIGURATION

To configure PINsafe to work with the Blue Coat Proxy you need to:

- Enable the request for a TURing image by username
- Enable PINsafe to act as a RADIUS server and configure the SG Proxy as a NAS.

IMAGE REQUEST BY USERNAME

To support this integration, PINsafe needs to be configured to allow an image to be requested by an end-user's browser, but supplying the username.

To allow this, go to the Server->Single Channel screen and set "Allow session request by username" to Yes

Figure 1. Allow image request by username

PINSAFE RADIUS CONFIGURATION

The RADIUS server within PINsafe needs to be enabled and configured.

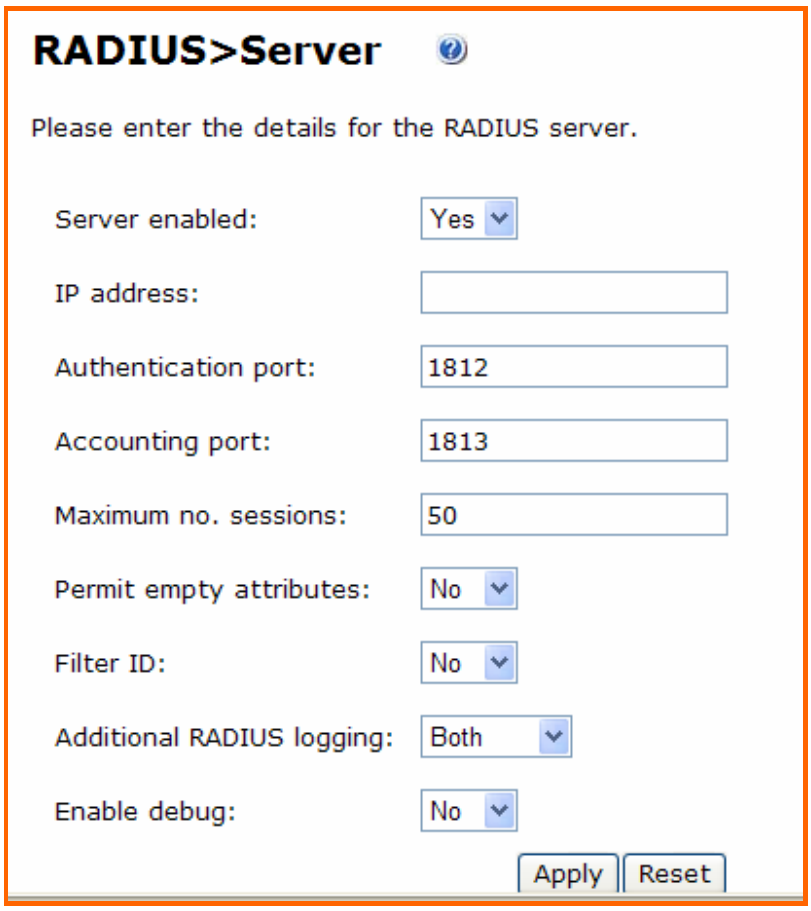

Figure 2. Configuring the RADIUS Server

The IP address is the IP address that the RADIUS server will bind to; if this is left blank the server will respond to all RADIUS requests received by the PINsafe server. The ports need to be set, generally the defaults as shown are fine, the key is that they match the ports used by device making authentication requests.

The next step is to create a NAS entry on PINsafe for the Bluecoat appliance.

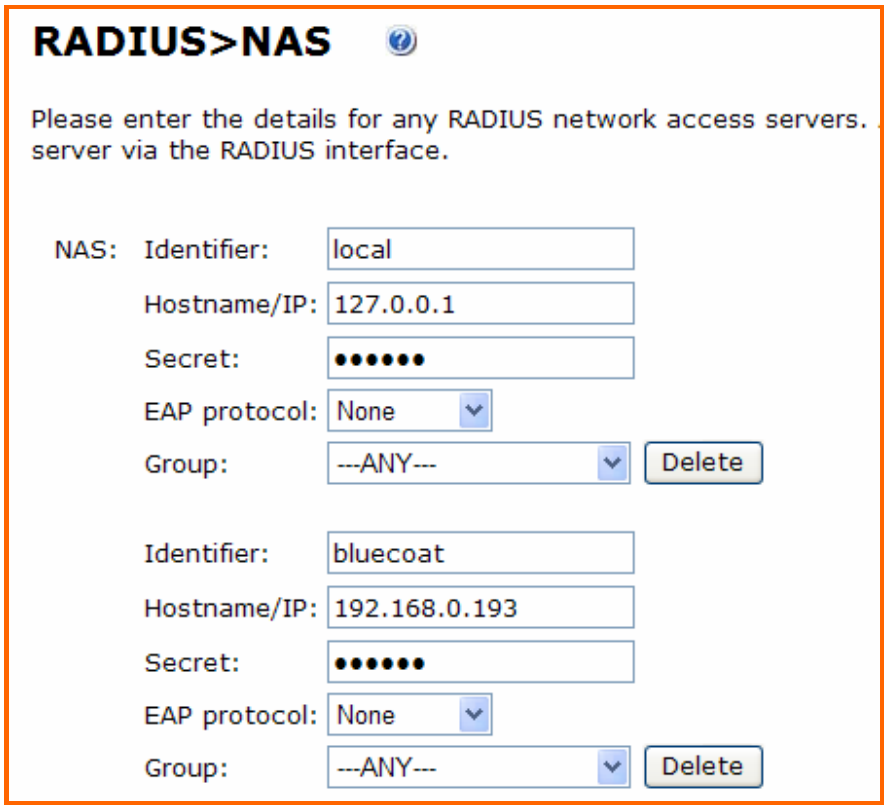

Figure 3. NAS Configuration

The NAS entry consists of an Identifier, the hostname or IP address of the Bluecoat server and shared secret, which will need to be matched within the Bluecoat configuration.

The EAP protocol should be left as None.

PINsafe can restrict authentication to members of a specific PINsafe user group, it can also pass back group information as part of the RADIUS response, for more details consult the PINsafe documentation.

BLUECOAT CONFIGURATION

To complete the integration, you need to.

- Create and upload a PINsafe specific authentication form, for displaying the TURing image.
- Create a PINsafe realm
- Create an authentication rule that uses the authentication form and realm

MODIFIED LOGIN PAGE

The required modifications to the standard login page are:

- Add a button to allow the user to request a TURing Image

```
<input type=button id=btnTuring name=btnTuring value=Turing
onclick=ShowTuring()>
```

- Add an image tag to display the image

```
<img id=imgTuring name=imgTuring style='visibility:hidden'>
```

Note that the image is initially hidden.

- Add the required Javascript to retrieve the image when it is requested.

```
var sUrl = "http://sandbox.swivel.local:8080/pinsafe/SCImage?username=";
```

Note that the sUrl variable needs configuring to point to the PINsafe server IP address. If you are using a PINsafe appliance then this may need to request the TURing image via the proxy.

```
var sUrl = "http://sandbox.swivel.local:8443/proxy/SCImage?username=";
```

The required changes to the standard page are shown in blue in the screen below.

Once the required modified form has been created, it needs to be uploaded onto the server. To do this, go to the Authentication ->Forms option.

Select New, selecting Authentication Form and giving it a suitable name.

Then select the form you have created, select Edit. Then select Local File and Install. Browse to the file you have created and upload it.

Click apply to apply the changes made.

Once the modified page has been installed the page can be previewed by selecting View

You can test the image retrieval by clicking on the Turing button.

```
<HTML>
<HEAD>
<TITLE>Enter Proxy Credentials for Realm $(cs-realm)</TITLE>
</HEAD>
<BODY>
<H1>Enter Proxy Credentials for Realm $(cs-realm)</H1>
<P>Reason for challenge: $(exception.last_error)
<P>$(x-auth-challenge-string)
<FORM METHOD="POST" ACTION=$(x-cs-auth-form-action-url)>
$(x-cs-auth-form-domain-field)
<P>Username: <INPUT NAME="PROXY_SG_USERNAME" MAXLENGTH="64" VALUE="$(cs-
username)"></P>
<P>Password: <INPUT TYPE=PASSWORD NAME="PROXY_SG_PASSWORD" MAXLENGTH="64"></P>
<INPUT TYPE=HIDDEN NAME="PROXY_SG_REQUEST_ID" VALUE="$(x-cs-auth-request-id)">
<INPUT TYPE=HIDDEN NAME="PROXY_SG_PRIVATE_CHALLENGE_STATE" VALUE="$(x-auth-
private-challenge-state)">
<P><INPUT TYPE=SUBMIT VALUE="Submit"> <INPUT TYPE=RESET></P>
</FORM>

<input type=button id=btnTuring name=btnTuring value=Turing
onclick=ShowTuring()>
</br>
<img id=imgTuring name=imgTuring style='visibility:hidden'>
<P>$(exception.contact)
<script language="javascript">
var sName ="PROXY_SG_USERNAME";
var sUrl = "http://sandbox.swivel.local:8080/pinsafe/SCImage?username=";

function ShowTuring() {
   sUser=document.getElementsByName(sName)[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>
</BODY>
</HTML>
```

Figure 4. Modified Log-in Page

CREATING A PINSAFER REALM

On the Authentication – RADIUS option on the Blue Coat configuration tool, select new.

Enter the details for the RADIUS server to match the PINsafe configuration.

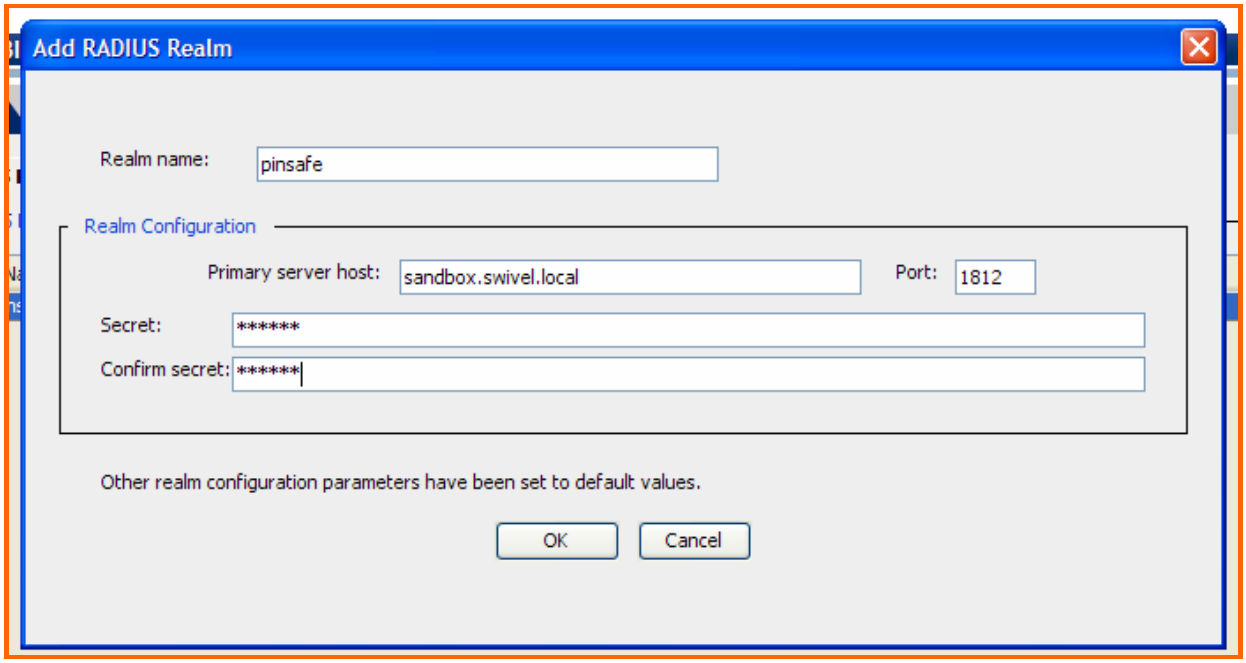

Figure 5. Realm configuration Screen

Then apply the changes. Then select the RADIUS server tab and ensure that the one-time passwords option is ticked. In addition you can add secondary RADIUS servers, on the RADIUS servers tab. This is appropriate when integrating with PINsafe High-Availability installations.

CREATING AN AUTHENTICATION POLICY

This aspect of the configuration is dependent on how you are deploying the SG Proxy and what elements you wish to secure with PINsafe authentication. This example illustrates using PINsafe authentication to protect access to certain urls with the Blue Coat server acting as a forward web proxy.

The first stage is to set the default policy, in this example this will be to allow access. Therefore from the Policy->Policy Options screen, ensure that the default proxy policy is set to Allow.

The remainder of the policy configuration is achieved from the Visual Policy Manager (VPM). This is launched by selecting Launch from the Visual Policy Manager screen.

CREATING THE AUTHENTICATION LAYER

The first stage is to create a Web Authentication layer, by selecting Policy->Add Web Authentication Layer. This will create the layer with a single blank rule.

DEFINING THE AUTHENTICATION

On the action column within the rule, right click the mouse and choose set.

Then select new->authenticate

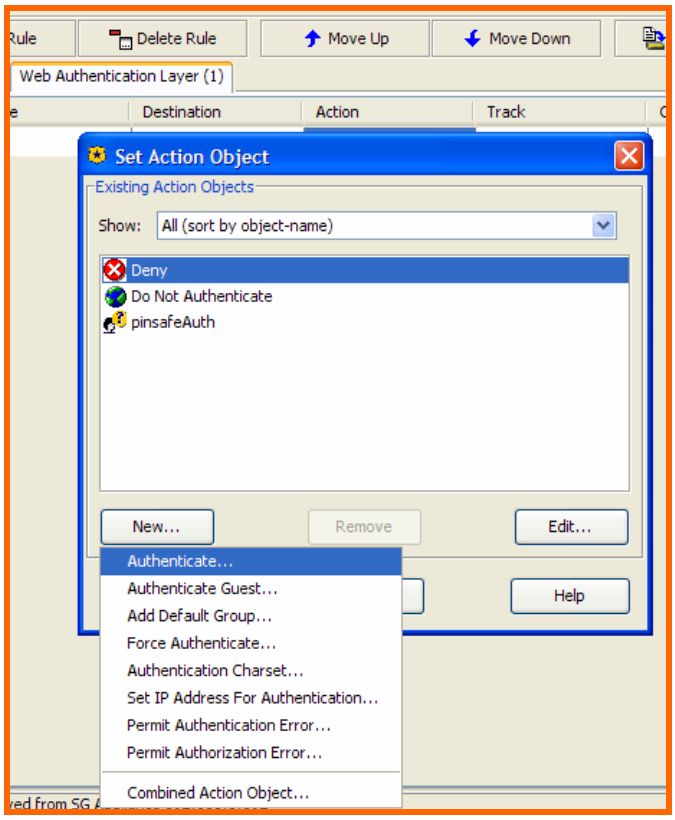

Figure 6. Adding an authentication action object

You then specify the authentication object by specifying the Authentication form and PINsafe RADIUS realms previously created.

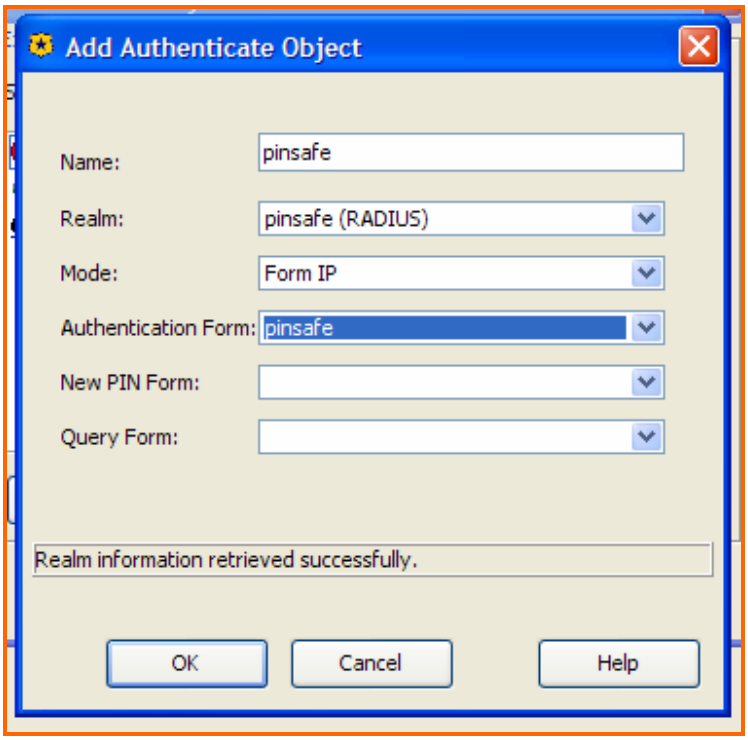

Figure 7. Configuring Authentication Object

Once the authentication object has been created , rules can be created that call this authentication object.

3	Any	google	pinsafeAuth	None

For example a rule that requires users to authenticate before accessing google.

TESTING

You need to configure a browser to use the SG Proxy.

(For example, in IE7, tools->internet options->connections->LAN settings enter the IPaddress/hostname in the proxy section, port 8080)

The proxy needs to be accessible from the client computer.

If you attempt to access a url protected by the proxy, you will be redirected to the login page.

Enter a valid username and click the TURing button.

Enter the correct One-Time code in the password

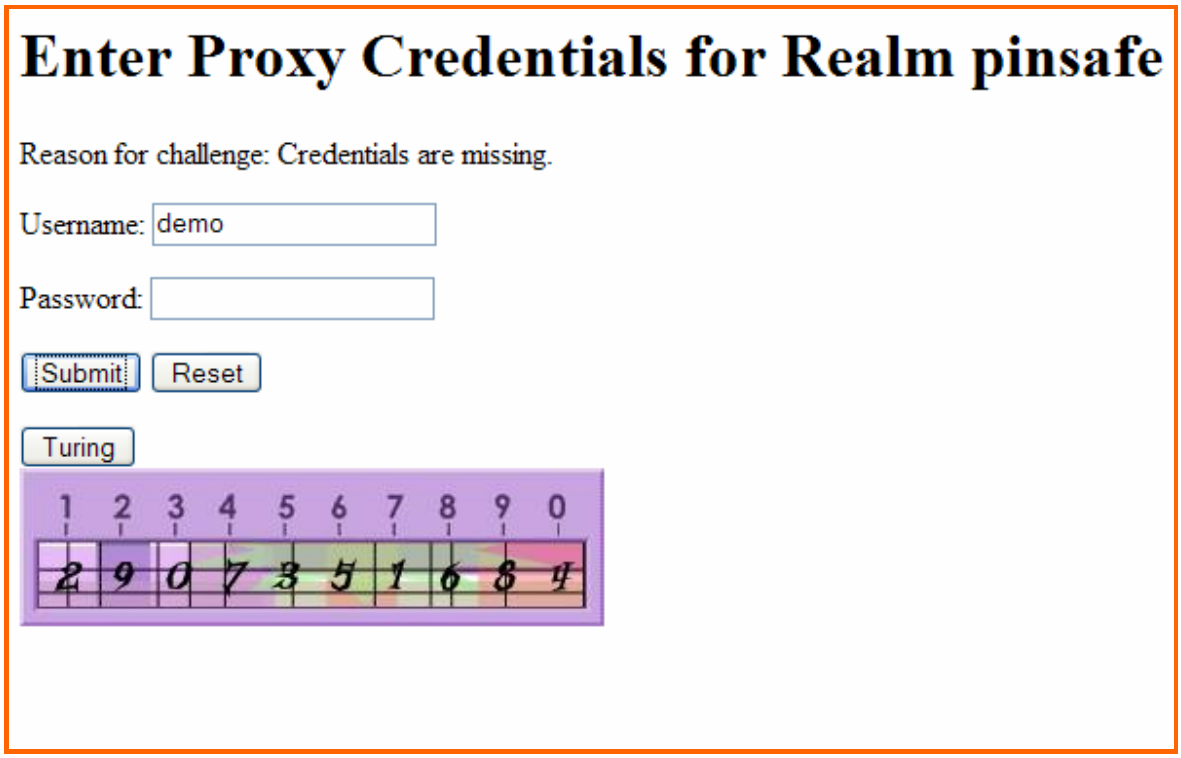

Figure 8. Authentication Page