Citrix Netscaler Gateway 11

Contents

Introduction

- 

  Netscaler TURing
- 

  Netscaler PINpad

This document shows the steps required to integrate Swivel with the Citrix NetScaler 11.0. Swivel can provide Two Factor authentication with SMS, Token, and Mobile Phone Client and strong Single Channel Authentication with TURing or Pinpad, or in the Taskbar using RADIUS.

It covers the following steps.

- Configuring Swivel to accept authentication requests from the CAGEE
- Modifying the CAGEE login pages
- Configuring the CAGEE to authenticate via PINsafe

To use the Single Channel Image such as the TURing Image, the Swivel server must be made accessible. The client requests the images from the Swivel server, and is usually configured using Network Address Translation, often with a proxy server. The Swivel virtual or hardware appliance is configured with a proxy port to allow an additional layer of protection. The Netscaler can be configured using its load balancing bridging feature to allow a Swivel Severs IP to provide Single Channel images, such as TURing and PINpad.

There is an alternative solution using Rewrite/Responder policies, which is recommended in preference to the solution outlined below. It is described in the Netscaler 12 article, but it applies to version 11 as well. Please check Citrix Netscaler Gateway 12.

Prerequisites

NetScaler version 11.0. The single channel customisation was created using build 62, and there may be minor cosmetic issues with other versions.

An administrative logon account for the Access Gateway

A Secure Shell (SSH) programme (eg putty) and an SSH-based file transfer application such as WinSCP

A Unicode-aware text file editor such as TextPad or WordPad

Swivel 3.x

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, this is usually implemented by a NAT to the Swivel server. Ensure that only the required ports are allowed access.

Netscaler pages to modify and/or Swivel files for version 11.0 default theme.

Netscaler pages to modify and/or Swivel files for version 11.0 Green Bubble theme.

If you would prefer to deploy ready-made themes, see the following:

- Default theme TURing image
- Default theme PINpad
- Green Bubble theme TURing image
- Green Bubble theme PINpad

See below for details on deploying these themes.

Note on upgrading the Netscaler

When upgrading see the note below if custom pages are used upgrading Netscalers with Custom Pages

Baseline

Tested with Swivel 3.10.4

Citrix Netscaler Gateway NS11.0 Build 62.0

Architecture

The Citrix NetScaler makes authentication requests against the Swivel server by RADIUS.

You can create different logon realms / pages called Virtual Servers, these can have different authentication servers/policies, SSL certificates and resources attached to them. However, the downside is they ALL use the same index.html/login.js/en.xml files, so you cannot have multiple landing pages with/without the Swivel modifications.

Swivel Configuration

Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

Enabling Session creation with username

To allow the TURing image, PINpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

Setting up Swivel Dual Channel Transports

See Transport Configuration

Citrix Netscaler Gateway Configuration

The Swivel integration uses RADIUS authentication, and where the login page is modified it uses the Netscaler custom web pages which are configured and then copied into an archive file which is deployed at boot time.

Citrix NetScaler RADIUS Configuration

The NetScaler needs to be configured to use the Swivel server as a RADIUS authentication server. Where several Swivel virtual or hardware appliances are used for resilience, configure the RADIUS request to be made against each of the Swivel servers together with the use of Session Sharing. **Note: for virtual or hardware appliances, the Swivel VIP should NOT be used as the RADIUS server IP address, see VIP on PINsafe Appliances**

Swivel can be configured as the only authentication server or as an additional authentication server, usually this would be together with AD. The required steps are pretty much the same for both scenarios.

Under System->Authentication->RADIUS, select the Servers Tab, click "Add" and enter the following information:

Name Swivel RADIUS

Server Name The name or IP address of the Swivel server

Port 1812

Secret Key The secret key configured on the Swivel NAS and also under **Confirm Secret Key**

Group Prefix CTXSUserGroups=

Group Separator ;

When complete click on Create.

If the Authentication option is not available check that the license allows authentication to be configured on the Netscaler licensing page.

Citrix NetScaler VPX - Con

https://192.168.12.100/menu/neo#noAnch

Apps | Google | Cinemas | Financial | G & S | Games | Home

NetScaler VPX (10)

Dashboard | Configuration | Reporting

Back

Create Authentication RADIUS Server

Name*

Swivel RADIUS

Server Name | Server IP

Server Name*

192.168.12.111

Port*

1812

Time-out (seconds)

3

Secret Key*

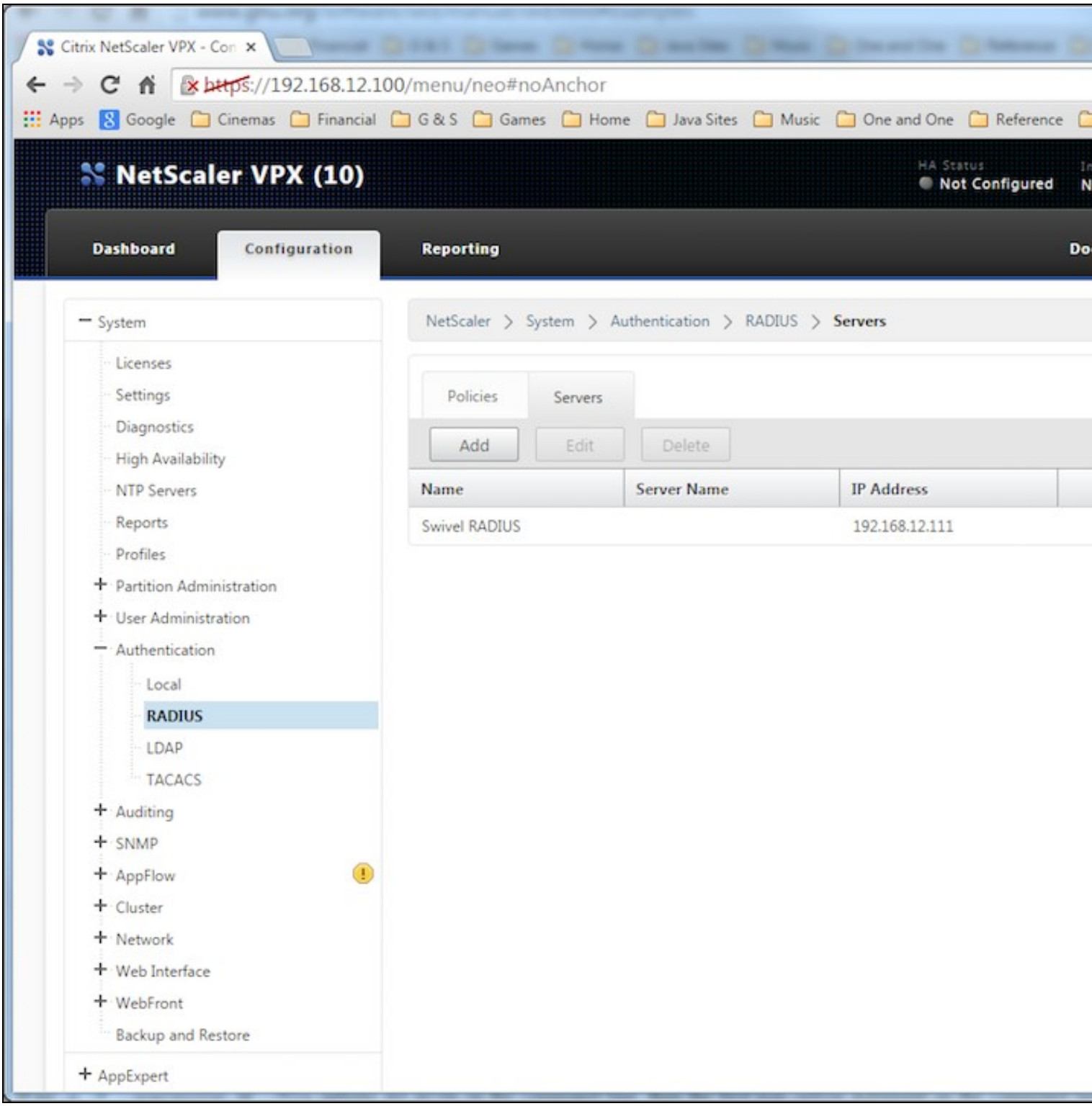
••••••

Confirm Secret Key*

••••••

More

Create | Close

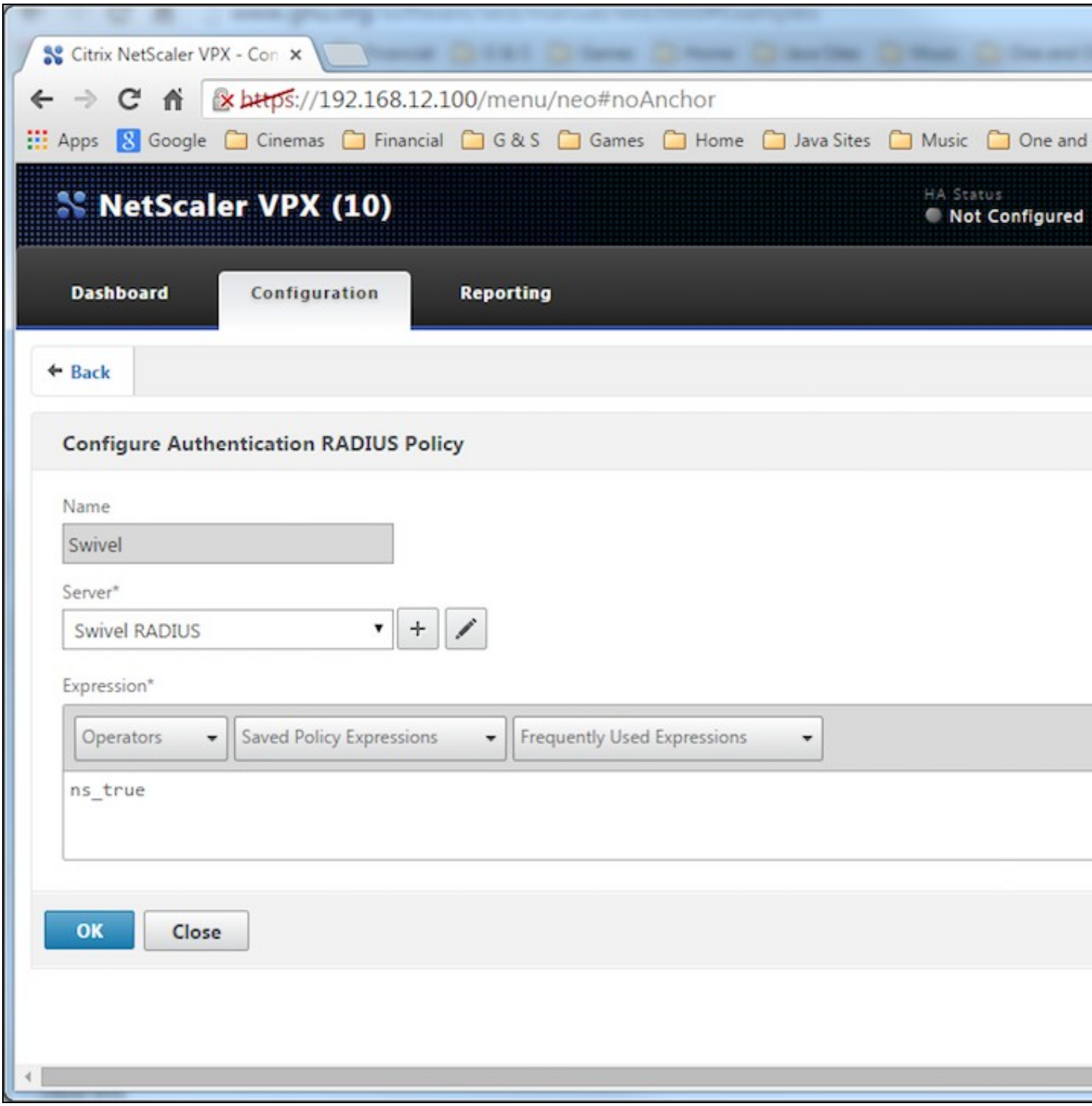


Now select the Policies Tab, click "Add" and enter the following information:

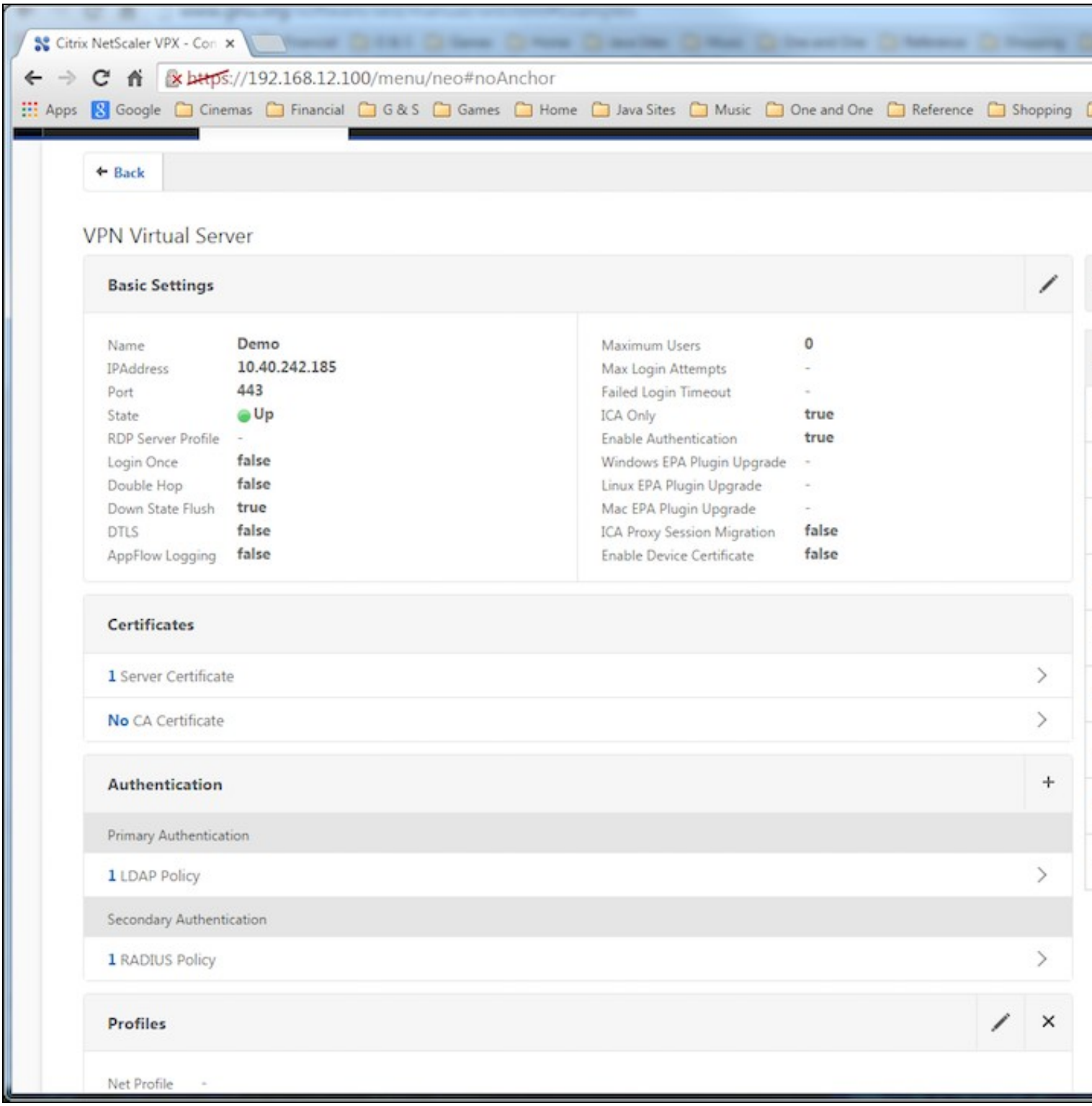
Name Swivel RADIUS Policy

Server Swivel RADIUS

Expression select "ns_true" under Saved Policy Expressions



The authentication must be then added such as the Access Gateway/Virtual Servers menu. If just Swivel authentication is required then ensure that only the Swivel policy is active for the Primary. If you require AD and Swivel authentication then you need to make active the Swivel policy as the secondary. Save the settings.



Citrix Receiver with Netscaler configuration

See Citrix Netscaler configuration for Receiver

Additional Configuration Options

Netscaler RADIUS Monitor and RADIUS Load Balancer

See Citrix Netscaler RADIUS Monitor and RADIUS Load Balancer

Netscaler SSL Bridge

The Netscaler allows a SSL Bridge to be created that allows a Network Address Translation to allow access to the Swivel instance to provide single channel images or Mobile App security strings. On the Netscaler Gateway Administration Console Configuration tab select Traffic Management -> Load Balancing -> Virtual Servers, then click on Add, to open a Create Virtual Server (Load Balancing) window.

Name Name of the SSL Bridge

Protocol select SSL_Bridge

Select IP Adress Based

IP address Enter the public IP Address

Port Enter the internet-facing port number, usually 443

Citrix NetScaler VPX - Con

https://192.168.12.100/menu/neo#noAnchor

Apps | Google | Cinemas | Financial | G & S | Games | Home | Java Sites | Music

NetScaler VPX (10)

HA Status: Not Configured

Dashboard | Configuration | Reporting | Docu

Back

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.
You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Swivel-SSL-Bridge

Protocol*

SSL_BRIDGE

IP Address Type*

IP Address

IP Address*

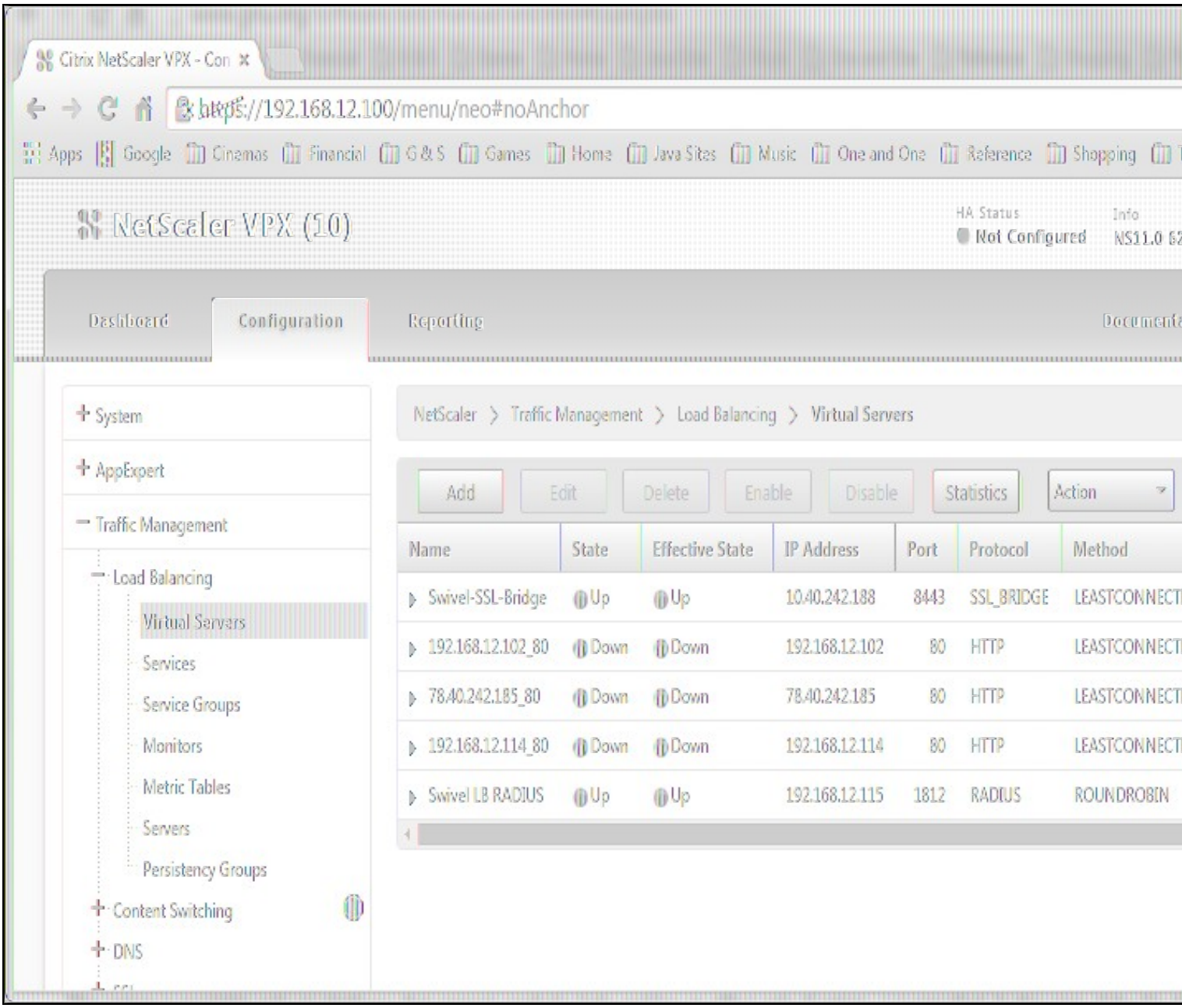
10 . 40 . 242 . 188 IPv6

Port*

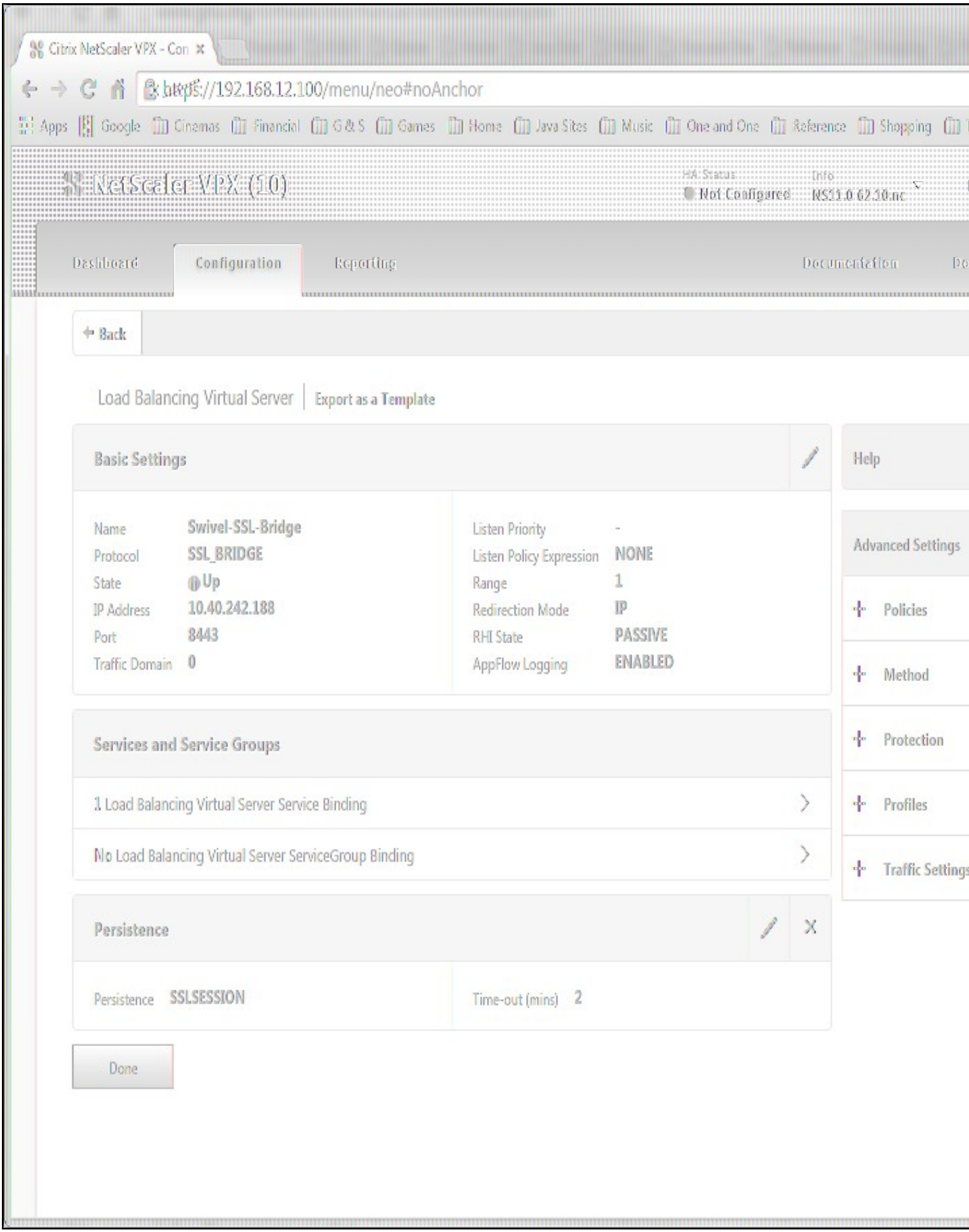
443

More

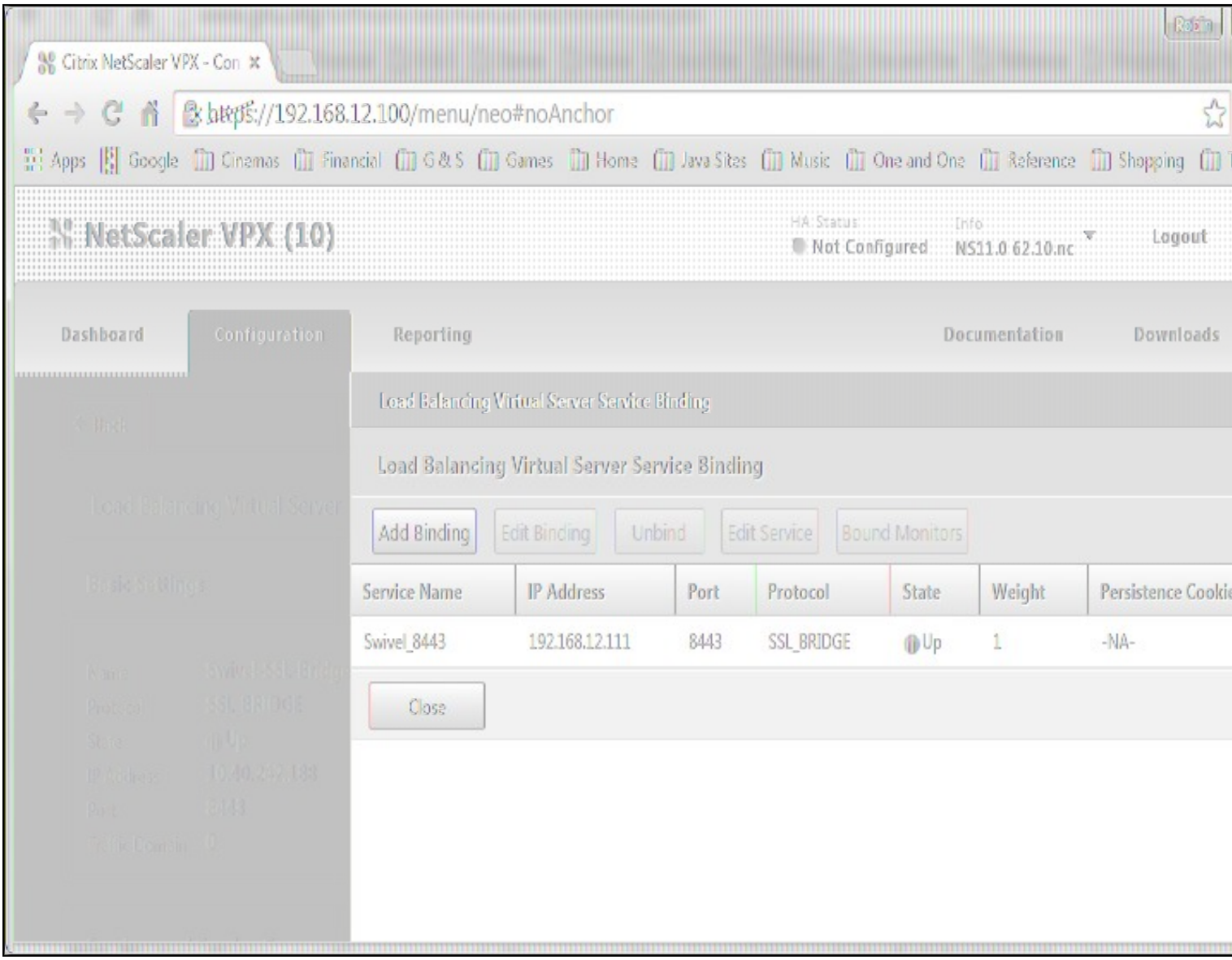
OK Cancel



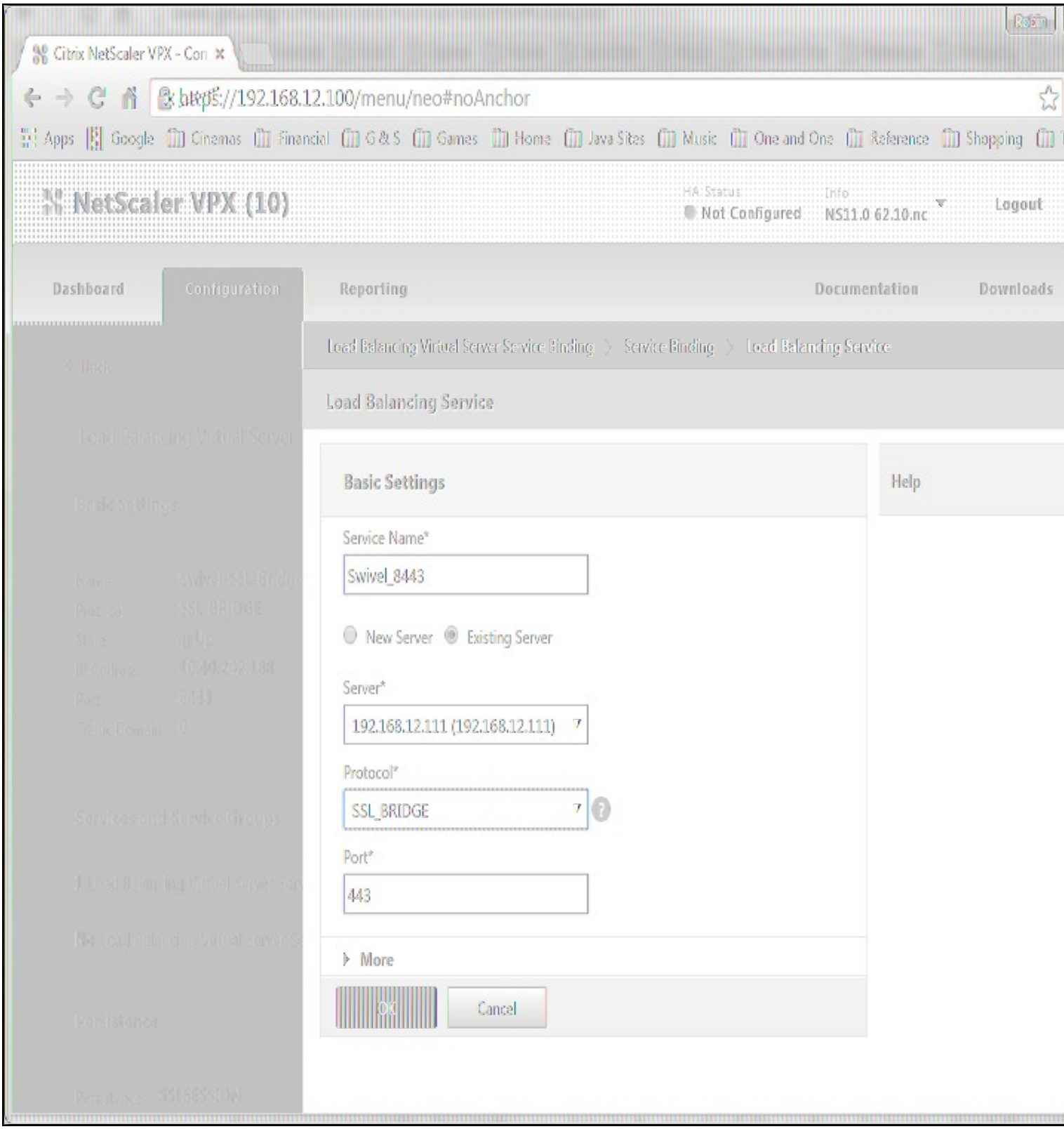
After creating the virtual server, select it and then Edit



Select "Load Balancing Virtual Server Service Binding"



Now click "Add Binding", then under "Select Service", click "+"



Service Name Name of the SSL Bridge

Select "New Server" and enter the IP address of the Swivel server.

Protocol select SSL_Bridge from the drop down menu

port select the port used to connect to Swivel server, usually 8443 for the proxy application.

From the Monitors tab select TCP then Add it to the list of Configured so that it appears on the right hand side with the State box checked., then click on Create.

Login Page Customisation

This step only needs to be followed if login page customisation is required. Many of the steps described below are derived from the following articles:

This article describes creating a custom theme on NetScaler 10.x:

http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-connect-users-wrapper-con/ng-connect-users-cr-integration-con/ng-connect-custom-theme-page-tsk.html

This article describes the additional steps required for NetScaler 11:

http://discussions.citrix.com/topic/367268-netscaler-11-custom-theme/ - item #13.

Thanks to the originators of these articles.

Update: we recommend using rewrite / responder actions to customise the login page, as suggested by Stuart Carroll in the Additional Information section. We have adapted and updated his original solution, which is now available in the NetScaler 12 article. Despite the name, it will also work with NetScaler 11.

Using Existing Customisations

If you already have a customisation including Swivel TURing or PINpad, from version 10.x, it may still work with version 11. Results are mixed on this. However, the customisations described on these articles are based on the assumption that you are starting from the default or green bubble theme for version 11. They will not work if you are starting from a 10.x theme. In this case, you should start from one of the built-in themes for version 11 and customise those.

First Steps

Follow these steps whether you plan to use a pre-built theme or to customise your own theme.

Citrix recommend when upgrading a Netscaler with custom pages, the custom pages should be set back to use default pages, upgrade and then the custom pages reapplied. When upgrading it is recommended to make a backup or snapshot of the existing system.

When upgrading a Netscaler 10.1 or 10.5 with custom pages to 11.0, backup the modified pages and scripts, then set the login page back to default. Upgrade, test the Administration console, then upload the modified pages as if carrying out a new Swivel install as given below, then recreate the custom tar file as below as this will then include the updated GUI.

Similarly, we recommend that you select the Default theme initially, before starting the customisation.

Ensure that the folder for the custom theme exists:

- Log on to the NetScaler Gateway command line and enter the following commands:

```
shell
mkdir /var/ns_gui_custom
```

You may get the response "File exists".

Copy the theme files for either the Default or Green Bubble theme using the following commands:

```
cd /var/netscaler/logon/themes
cp -r Default Custom
```

or for the Green Bubble theme

```
cp -r Greenbubble Custom
```

If you are using one of the ready-made themes linked above, skip to the section Deploying a Ready-Made Theme. If you are customising an existing theme, continue to the next section.

Customising an Existing Theme

Preparing the Custom Theme

Assuming that you have copied the appropriate theme as described in First Steps, select the Custom theme in order to ensure it is deployed. The files you need to modify will now be in /var/netscaler/logon/themes/Custom. Prepare the new custom theme as follows:

```
tar -cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/*
```

Now use the NetScaler administration console to select the custom theme: select NetScaler Gateway -> Global Settings, then click on Change Global Settings, select the Client Experience tab, and at the bottom of the tab, switch the UI Theme to Custom.

Login to Netscaler Command Line

Use WINscp to use a web file tool or SSH onto the virtual or hardware appliance using an admin account. Once onto the box you need to type shell to get access to the command line.

```
>Last login: Wed Sep 10 19:12:45 2008
Done
> shell
Last login: Wed Sep 10 21:13:35 2008
```

Backup Netscaler files

Navigate to the location of the pages to be modified, and make a local backup copy of them.

```
cd /var/ns_gui_custom/ns_gui/vpn
cp index.html index.html.bak
cd js
cp gateway_login_form_view.js gateway_login_form_view.js.bak
```

Customise the login script

See under **prerequisites** for the modified files that need to be uploaded to the Netscaler.

Note on editing files: If the files are edited in Windows-based systems it may be possible that control code ^M are added to the end of the line. These can be viewed and removed by using vi.

It is assumed that your custom theme has already been deployed under /var/ns_gui_custom/ns_gui. As noted above, it is also assumed that the theme is based on one of the built-in version 11 themes. If you have a version 10.x customisation that you cannot get to work with version 11, please contact support@swivelsecure.com for further advice.

Download the customised files from the pre-requisites above. This contains 5 files, in the appropriate folders:

- /vpn/index.html - a replacement for the existing file, containing additional lines to insert the swivel files below
- /vpn/js/gateway_login_form_view.js - a replacement for the existing file, containing a single additional line, which calls a script from swivel.js to insert the customisation.
- /vpn/js/swivel.js - a new file, containing the JavaScript to insert the customisation
- /vpn/images/swivel.css - a new file, containing the stylesheet for the Swivel customisation
- /vpn/images/pinpadBlank.png - an optional blank image for the PINpad buttons.

Before you copy these files across, you will need to modify the first part of swivel.js as shown here:

```
// Set this to be the correct URL for the required image.
var swivelUrl = "https://citriximage.swivelsecure.com/proxy/";
// Set this to "turing" or "pinpad". Anything else will result in no image.
var swivelImageType = "pinpad";
// Set this to the ID of the password field to populate: "passwd" or "passwd1"
var pinpadField = "passwd1";
```

- swivelUrl should contain the public URL for your image. Do not add "SCImage" or "SCPinPad" - this will be done for you.
- swivelImageType should be "turing" or "pinpad" as described
- pinpadField defines which password field should be filled by the PINpad buttons. If Swivel is the primary authentication, use "passwd", or for secondary authentication use "passwd1".

Customise the OTC field and TURing image button text

This is an optional step.

Modify the language resource files in /netscaler/logon/themes/Default/resources. If you are only using the English language, then edit en.xml and search for

```
<Partition id="logon">
```

Just below this, look for

```
<String id="Password2">Password 2</String>
```

Replace "Password 2" with "OTC".

If you want to change the label on the TURing button, insert a new line just below this:

```
  <Property id="New_Turing" property="value">New Image</Property>
```

Replace "New Image" with the appropriate text.

If you want to change the label on the PINpad refresh button, insert the following line:

```
  <Property id="Refresh_Pinpad" property="value">Refresh</Property>
```

Replace "Refresh" with the appropriate text.

Additional Languages file modifications

If you will be using languages other than English, you will also need to edit any other language files you use, following the pattern above.

Upload files to Netscaler

Download the files under the prerequisites and modify as described above, then copy them to the appropriate locations under /var/ns_gui_custom/ns_gui.

Create the boot archive file

```
cd /var/ns_gui_custom
tar -zcvf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*
```

This should create the customtheme.tar.gz file used at boot time, and list all the files used.

Select the custom theme

- Log on to the NetScaler Administration Console and select the "Custom" theme.
- Save customisation changes.

Create Backup and Script to Deploy Files

Once you have a working configuration, you should back up the modified files to a suitable location off the NetScaler. It is recommended that the backup directory structure reflects the deployed structure - e.g. put the .js files in a js subdirectory, and the .css file(s) in a images subdirectory. This makes it easier to carry out the next step.

As NetScaler often replaces files after a reboot, you also need to take precautions to ensure the custom files are restored after a reboot. To do this, you need to copy the backups you just created into a folder on the NetScaler: the recommended location is to create a folder "custom" under /var/mods. As described above, the directory structure under custom should reflect the directory structure under vpn.

To restore these files on reboot, you need to edit the file /nsconfig/rc.netscaler. Insert the following line at the beginning of the file:

```
cp -r /var/mods/custom/* /var/netscaler/ns_gui/vpn/*
```

This assumes that your web directory is /var/netscaler/ns_gui - modify accordingly.

Reboot Netscaler to verify files are copied across

Reboot the Netscaler to ensure that the files are copied across at boot time and that the login page has been modified as required.

The following section can be skipped if you are customising an existing theme.

Deploying a Ready-Made Theme

These instructions assume you are using one of the pre-built themes listed above.

- Copy the chosen theme to /var/ns_gui_custom. We recommend WinSCP to copy the files, but any suitable file transfer file will do.
- Go to /var/netscaler/logon/themes/Custom/resources and edit en.xml (again, you can use WinSCP for this):
  - Search for "Password2"
  - If required, change the text for <String id="Password2"> to "OTC":

```
<String id="Password2">OTC</String>
```

  - Insert a new line below this:

```
<String id="SwivelUrl">https://swivel.mycompany.com/proxy/</String>
(Substitute the public URL for your Swivel images (TURing or Pinpad) in the above.)
```

  - Save the file.
  - If you need to support multiple languages, repeat this process for all supported language files.
- Log on to the NetScaler Administration Console and select the "Custom" theme.
- Save customisation changes.

If you prefer, as an alternative to inserting the Swivel URL in the resources file(s), you can manually modify swivel.js, as described below. However, if you do this, you will also need to rebuild the custom theme, again as described above.

Additional Login Customisation options

Requesting the String Index

See also Multiple Security Strings How To Guide

To request the string index, use the "turing" option.

Modify swivel.js. Search for the following line:

```
swivelUrl += "/SCImage?username=";
```

Replace "SCImage" with "DCIndexImage".

Requesting an SMS

See also Challenge and Response below

To request an SMS on demand, use the "turing" option.

Modify swivel.js. Search for the following line:

```
swivelUrl += "/SCImage?username=";
```

Replace "SCImage" with "DCMessage".

One Touch

DISCLAIMER: the following One Touch solution is based on NetScaler 10.5, and has not yet been tested on version 11.

One touch is a different approach as the user is redirected to a separate page to authenticate and therefore does not actually see the Netscaler login page.

Refer to VPN_OneTouch_Integration

To customise the page for one touch you need to include the following in the header section of index.html where <swivelappliance> is the hostname of the associated Swivel Appliance

```
//-->
//-> Swivel elements
function redirect(){
window.location.replace("https://<swivelappliance>:8443/onetouch/onetouch?returnurl=" + window.location.href );
}

var QueryString = function () {
 // This function is anonymous, is executed immediately and
 // the return value is assigned to QueryString!
 var query_string = {};
 var query = window.location.search.substring(1);
 var vars = query.split("&");
 for (var i=0;i<vars.length;i++) {
   var pair = vars[i].split("=");
        // If first entry with this name
   if (typeof query_string[pair[0]] === "undefined") {
     query_string[pair[0]] = pair[1];
      //  alert(pair[0] + "," + pair[1]);
        // If second entry with this name
   } else if (typeof query_string[pair[0]] === "string") {
     var arr = [ query_string[pair[0]], pair[1] ];
     query_string[pair[0]] = arr;
       //alert(pair[0] + "," + arr);
        // If third or later entry with this name
   } else {
     query_string[pair[0]].push(pair[1]);
   }
 }
```

```
   return query_string;
} ();

$(document).ready(function(){
 usernamePassedIn = QueryString["username"];
 passwordPassedIn = QueryString["password"];

if(typeof passwordPassedIn == 'undefined') {
 redirect();
} else {
$('[name=passwd]').val(passwordPassedIn);
$('[name=login]').val(usernamePassedIn);
 //alert("GO " + usernamePassedIn);
 document.getElementsByName("vpnForm")[0].submit();

 }
});
```

Before the closing </SCRIPT> tag

Challenge and Response

To use two-stage authentication - also known as challenge and response - you will need these custom files. These files are for the Green Bubble theme: for different themes, see the detailed customisation section below. Also note that these files only support TURing in the second stage: for other options, see below.

See Challenge and Response How to Guide for details on setting up challenge/response on the Swivel server. In particular, note that the option "Send username with challenge" must be set to "Yes" to use single-channel challenge-response, so if your version of the Swivel software is too old to have that option, you will need to upgrade in order to use challenge-response with TURing.

Customisation

See above for details on where the custom files need to be put. Always take backups of the original files before making any changes. If you are using dual channel, you may not need to make any of these changes: see comments below.

You should always download the custom files linked above, even if you are not using the Green Bubble theme with TURing, as you will need the file swivel.js at least. This should be put in the js folder. The other files that need to be changed are index.html, nsshare.js and js/gateway_login_form_view.js.

The only change to index.html is to insert a single line:

```
<script type="text/javascript" src="/vpn/js/swivel.js"></script>
```

somewhere in the <head> section.

The only change required to gateway_login_form_view.js is as follows:

Locate the following line:

```
 changePage();           // Prefill names if cert auth
```

Insert before it the following line:

```
 customLoginPage(form);
```

This calls a function from swivel.js to add the Swivel customisation to the first login page. This hides the Swivel password field, and copies the first password field to it before submitting the page. This assumes that you are using the "Check repository password" option. If you don't want to use that, don't make this change.

The second login page is rendered by nsshare.js, so you need to make the following changes to it, only if you want to show TURing in the second page. In the custom files, these are inserted before the DialogInclude function, but they can go anywhere in the file:

```
 // Alter this URL as appropriate.
 var swivelUrl = "https://citrixiimage.swivelsecure.com/proxy/SCImage?username=";

 function showTuring(sUser) {
   if (sUser!="") {

     // Find the image field.
     var varImg = document.getElementById("imgTuring");

     // Set the image SRC and make it visible
     varImg.src = swivelUrl + sUser + "&random=" + Math.round(Math.random()*100000);
     varImg.style.display = "";

   }

 }

 function showTuringImageChallenge() {
   var challengeDiv = document.getElementById("dialogueStr");
   if (challengeDiv) {
     var challenge = challengeDiv.innerHTML;
     var colonPos = challenge.lastIndexOf(":");
     if (colonPos > 0) {
       var username = challenge.substr(0, colonPos).trim();
       challenge = challenge.substr(colonPos+1);
       challengeDiv.innerHTML = challenge;
       showTuring(username);
     }
   }
 }
```

Then, in the function DialogueBodyII, look for

```
   ln += '<tr><td class="dialogueSubmitCell" style="float:left">';
```

and insert the following line before it:

```
ln += '<tr><td><img id="imgTuring" style="display:none" /></td></tr>';
```

Then, at the end of DialogueBodyII, insert the following line:

```
showTuringImageChallenge();
```

If you are unclear about any of these changes, they are clearly labelled in the custom files provided.

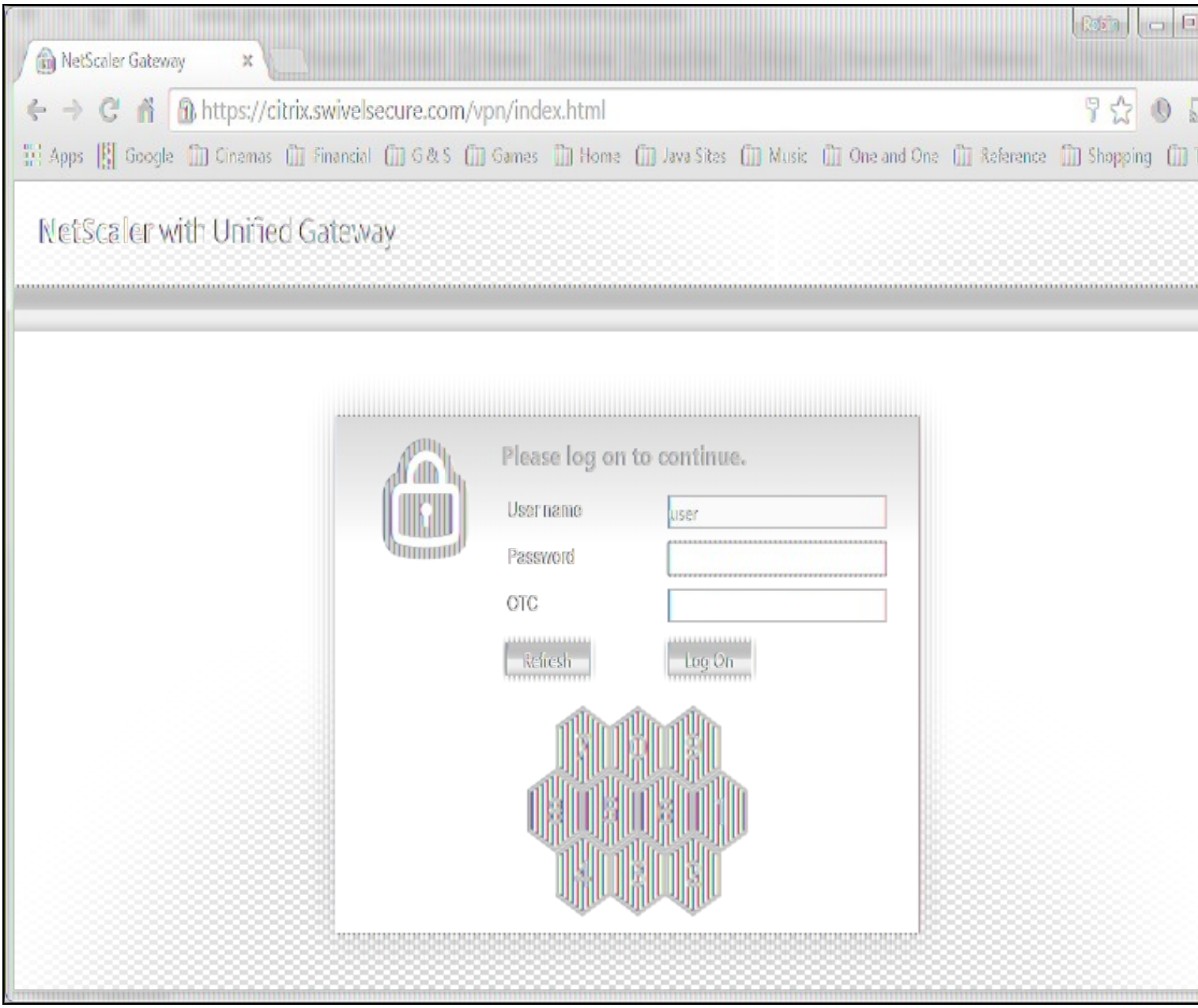
Image Request button displayed when needed

The following code allows the Single Channel Image request button to be only shown when required. This is useful for refreshing an image or when SMS/Mobile client authentication is used, since when a Single Channel image is generated, either automatically or manually, it then expects a single channel login (within 2 minutes by default).

```
function ns_showpinsafe()
{
  var pspwc = ns_getcookie("pwcount");
  if ( pspwc == 2 )
  {
    document.write('<td>');
    document.write('<img src="/vpn/images/LoginButtonRolloverGlow.gif"/>');
    document.write('');
    document.write('<input type="button" id="btnTuring" value="Get Image" ');
    document.write('onclick="showTuring();" class="CTX_CaxtonButton" ');
    document.write('onmouseover="this.className=');
    document.write("'CTX_CaxtonButton_Hover';");
    document.write('" onmouseout="this.className=');
    document.write("'CTX_CaxtonButton';");
    document.write('" />');
    document.write('</td>');
  }
}
```

Testing

Browse to the login page and check that a TURing or PINpad image appears and the One time Code can be entered to login.



Uninstall/Removing the integration

If the login pages have been modified restore the default login page and remove the added files.

Remove Swivel as the authentication server.

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

The CAGEE Netscaler checks each password/OTC in turn, so if the AD password is checked first and is incorrect then the secondary authentication will not be tested.

Error Messages

Files moved but have a ? appended to the end

If the script to move the files on login contains the control code ^M at the end of each line (usually introduced by Windows based text editors), then the files may appear with a ? at the end of the filename. Use vi to remove the ^M

Username field length incorrect

If the username field is too short it can be increased. Edit the index.html file and locate the below section setting the size="40"

<td align="right" style="padding-right:10px;white-space:nowrap;"></td> <td colspan=2 style="padding-right:8px;"><input id="Enter user name" class="CTXMSAM_ContentFont" style="font-size: 8pt" type="text" title="" name="login" size="40" maxlength="127" onFocus="loginFieldCheck()" style="width:100%;" /></td>

login command failed over API. Reason: Response not of type text/xml: text:html

This error can be seen on the Netscaler Administration console when upgrading with a custom theme. This will preventy login to the Netscaler Administration, although the user login pages should continue to work. To enable login to the Administration console, login to the Netscaler through the command line, backup and then and edit the /nsconfig/ns.config file and set the CUSTOM page to DEFAULT.

Look for the line containing -UITHEME CUSTOM and change it to DEFAULT as below:

```
set vpn parameter -localLanAccess ON -defaultAuthorizationAction ALLOW -proxy BROWSER -clientCleanupPrompt OFF -forceCleanup none -clientOp
```

After making the changes, reboot the system to login.

Known Issues and Limitations

The CAGEE caches the javascript so when you make modifications on the CAGEE they are not reflected on the log-in page as rendered. A way round this is to change the name of the .js file and edit the index.html file to use this new .js file. see [1]

Potential File Locations:

/netscaler/ns_gui/vpn

/var/ns_gui/vpn

/var/ns_gui_custom/vpn

/var/netscaler/gui/vpn

Additional Information

NOTE: there is an alternative solution to this that uses the NetScaler rewrite feature, and so doesn't require you to make changes to any files. It also has the advantage that it can be applied selectively. Many thanks to Stuart Carroll for finding this approach:

http://www.stuartc.net/blog/tech/netscaler-11-0-swivel-integration-using-netscaler-rewrite/

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