Citrix Netscaler Gateway 12

Contents

Introduction

This article covers how to adjust an integration between pinsafe protocol and Citrix Netscaler Gateway 12.

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. For all the methods which do not require an image at the article Citrix_Netscaler_Gateway_11 covers them.

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. Both the authentication methods need an image for which there are a set of rules to be applied. This document covers the application of those rules through the NS command line.

Integration Architecture

Swivel Secure ? Radius ? Nas ? Netscaler ? login page ? AD ? login customised page

Turing Image Integration

This solution uses the NetScaler Rewrite and Responder features: please make sure these features are enabled before proceeding. The custom actions and policies can be added through the web administration console, but we provide them below as NetScaler shell commands.

This solution will work with NetScaler 11 as well, and is recommended in preference to the previous article.

You can customise the labels from the web console. Under NetScaler Gateway, select Portal Themes, then the theme you are using, and Edit. On the right, click Logon Page, and the text can be edited there.

There is need to have a valid certificate for the turing image to appear. As a trial you can try a self signed certificate that is trusted by the host: cd /usr/local/share/ca-certificates/swivel.crt

It has been reported that the rewrite and responder actions used for version 11 do not work with the latest release of version 12. Below is an updated set of actions & policies that need to be installed. Before you install them, edit the responder action and change the URL following pinsafeUrl to the correct URL for your TURing. You don't need the "SCImage" part - that will be added automatically.

To install the rules, you need to open a command prompt on the NetScaler. You can just paste the entire file contents to the shell window. Once you have installed them, they have to be bound to a virtual server. There isn?t a script for that as it will be different for each installation. It's easiest to do this right at the netscaler?s web admin console.

Rewrite Rules

Copy the lines from the text below to a text editor: note that each action should be on a single line. Edit the URL as described above, then copy and paste the result into your NetScaler?s command line. Be sure to have complete lines without additional spaces or line breaks.

The action Act_Sentry_Username_Blur and the associated policy is optional, and shows the TURing image as soon as you tab away from the username. If you prefer users to click a button to get the image, then do not include this action/policy.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri

add rewrite action Act_Sentry_Mod insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=$('<div></div>').addClass('field').add

add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_

add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search

add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho

add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js

add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Mod

add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_Append

add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA

add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur

add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox

add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

Binding the applied rules

This is done at the netscaler GUI.

Select the virtual server you are going to use, and edit it. Scroll down to the Policies section and click "+". Select Responder policy, then click Continue. Click "Add Binding" and select the policy "ResPol_pinsafe.js". Click Bind. Click Close, then click + again. This time, select "Rewrite" as the policy, and "Response" as the type. Click "Add Binding" and then select the rewrite policies just added, one at a time. After each one, make sure the GOTO expression is "NEXT", to ensure that all policies are executed. This doesn?t apply to the responder policy. In the end there should be 5 rewrite policies in total (4 if you don't want automatic TURing), and one responder policy. It doesn't matter which order you add them.

The last thing you will need to do is to persuade NetScaler not to use the cached version of its JavaScript. Go back to the command prompt, and open a shell. The following have been tested successfully for Netscaler?s web files, and we recommend trying both to ensure the result:

cd /netscaler/ns_gui/vpn/js

cd /var/netscaler/gui/vpn/js

After getting to those locations apply touch as Netscaler seems to cache JavaScript files.

```
touch gateway_login_form_view.js
```

You should now get the TURing image embedded into the login page.

Green Bubble Theme

Use the following rules for the Green Bubble theme.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri
add rewrite action Act_Sentry_ModGB insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_image=$(\"<div></div>\").attr({'id':'divTur
add rewrite action Act_Sentry_AppendEULAGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_image)\"" -se
add rewrite action Act_Sentry_AppendGB replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_image)\"" -search "text(\"form
add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho
add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js
add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModGB
add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_AppendGB
add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULAGB
add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur
add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox
add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

The action names have been changed, so that you can have actions for multiple themes in the configuration and simply change the policies to point to the appropriate actions.

RfWebUI theme

Unfortunately, the RfWebUI theme doesn't support responder actions. Instead, you have to replace the file script.js with the one below, or if it is already modified, add the attached scripts to the existing file.

The file can be found under /var/netscaler/logon/themes/RFWebUI/. If you have copied the original RFWebUI theme, the last part of the path will be whatever the new theme is named as.

As with other customisations, you will need to modify the first line to set swivelUrl to the correct public URL for your system.

Customised script.js

X1

Here are the actions and policies for the X1 theme. Only one action needs to be changed here.

```
add rewrite action Act_pinsafe.js insert_before_all "HTTP.RES.BODY(12000)" q{"<script type=\"text/javascript\" src=\"/vpn/pinsafe.js\"></scri
add rewrite action Act_Sentry_ModX1 insert_after_all "HTTP.RES.BODY(1000000)" q| "\n\tvar pinsafe_button=$(\"<div></div>\").addClass('field')
add rewrite action Act_Sentry_AppendEULA replace_all "HTTP.RES.BODY(1000000)" "\"form.append(eula_section,field_login,pinsafe_button,pinsafe_
add rewrite action Act_Sentry_Append replace_all "HTTP.RES.BODY(1000000)" "\"form.append(field_login,pinsafe_button,pinsafe_image)\"" -search
add rewrite action Act_Sentry_Username_Blur replace_all "HTTP.RES.BODY(100000)" q|".focus(function(){loginFieldCheck();}).blur(function(){sho
add rewrite policy Pol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/index.html\")" Act_pinsafe.js
add rewrite policy Pol_Sentry_Mod "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_ModX1
add rewrite policy Pol_Sentry_Append "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")"  Act_Sentry_Append
add rewrite policy Pol_Sentry_AppendEULA "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_AppendEULA
add rewrite policy Pol_Sentry_Username_Blur "HTTP.REQ.URL.STARTSWITH(\"/vpn/js/gateway_login_form_view.js\")" Act_Sentry_Username_Blur
add responder action ResAct_pinsafe.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinsafeUrl = \\\"https://sentry.swiveldev.com:8443/prox
add responder policy ResPol_pinsafe.js "HTTP.REQ.URL.STARTSWITH(\"/vpn/pinsafe.js\")" ResAct_pinsafe.js
```

Pinpad Integration

The following document provides the rules which need to be applied for Pinpad integration. Before applying the responder action you'll need to edit the url for the swivel server to match yours: swivel.mycompany.com:8443/proxy/SCPinPad.

Be sure you have 2 rewrite actions (one of which is big), 2 rewrite policies, 2 responder actions and 2 responder policies. Avoid adding extra spaces when copying the rules onto the netscaler's shell.

```
add rewrite action ReAct_pinpad_js insert_before_all "HTTP.RES.BODY(12000)" q{"\r\n<script type=\"text/javascript\" src=\"/vpn/pinpad.js\"></

add rewrite action ReAct_Insert_Pinpad replace_all "HTTP.RES.BODY(1000000)" q|"form.append(field_errormsg);\r\n\tvar refresh_button=$(\"<inpu

add rewrite policy RePol_pinpad_js "HTTP.REQ.URL.EQ(\"/vpn/index.html\")" ReAct_pinpad_js

add rewrite policy RePol_Insert_Pinpad "HTTP.REQ.URL.EQ(\"/vpn/js/gateway_login_form_view.js\")" ReAct_Insert_Pinpad

add responder action ResAct_pinpad.js respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"var pinpadUrl=\\\"https://swivel.mycompany.com:8443/proxy/SC

add responder action ResAct_pinpad.css respondwith "\"HTTP/1.1 200 OK\r\n\r\n\"+\"div.pinpadHidden { display : none; }\r\n\"+\"div.pinpadVisi

add responder policy ResPol_pinpad.js "HTTP.REQ.URL.EQ(\"/vpn/pinpad.js\")" ResAct_pinpad.js

add responder policy ResPol_pinpad.css "HTTP.REQ.URL.EQ(\"/vpn/pinpad.css\")" ResAct_pinpad.css
```

Delete previous rules

The optimal option is to unbound all the rules through the NS GUI and after delete them. Also bear in mind the need to touch the .js files mentioned throughout the article as NS caches the previous versions - so changes might not be visible or immediately available.

Adjust Buttons at the login page

For further adjustments of the login page read the following section. Bear in mind X1 theme allows a quick editing of some features so the following might not apply. Normally the login page can be slightly edited, we are not going onto details regarding aesthetics and branding but only renaming of some sections which report to this integration.

Edit Password to OTC

The example below describes the use of the english language at the login interface.

> shell root@VLABSRV0# cd /var/netscaler/logon/themes/Default/resources root@VLABSRV0# chmod +w en.xml root@VLABSRV0# vi en.xml

```
   [change word directly ? beginning of the word - cw ? write ? escape - :wq!]
```

ng> <String id="User_name">User name</String> <Property id="Enter user name" property="title">Enter user name</Property> <String id="Password">OTC</String> <String id="Password2">Password 2</String> <String id="Enter password">Enter password</String> <Property id="Log_On" property="value">Log On</Property> <String id="You need to enter login name">You need to enter login name</Stri ng> <String id="You need to enter passwd">You need to enter a password</String> * <String id="Enter_password2_Alert">You need to enter the second password </String> <String id="domain">Domain</String> <String id="eula_title">End User License Agreement</String> <String id="eula_agreement">I accept the </String> <String id="terms">Terms & Conditions</String> <String id="errorMessageLabelBase">errorMessageLabel</String> <String id="eulaback">Back</String> <String id="errorMessageLabel4001">Incorrect credentials. Try again.</String > <String id="errorMessageLabel4002">You do not have permission to log on at t his time.</String> <String id="errorMessageLabel4003">Cannot connect to server. Try connecting en.xml: 597 lines, 51853 characters. root@VLABSRV015# exit shell

- You can also change ?You need to enter a password? to ?You need to enter an OTC?. We recommend avoiding obvious naming, mainly as a security measure.

Troubleshooting

If the logging in is not working please check the certificate and if the netscaler as the same valid certificate. Also if there as been made any change to the ip?s check if there is a firewall blocking the content.

It has been reported that sometimes the JavaScript file gets cached. To resolved this you should touch gateway_login_form_view.js and try to log after. NetScaler tends to cache JavaScript files, and doesn't detect changes made by rewrite rules. You have to force it to refresh its cache.

If the pinsafe.js file is coming through OK it means that some of the rules are working.

For further assistance please write to supportdesk@swivelsecure.com

Netscaler Upgrade from 11 to 12

As recommended by CITRIX, for previous versions the upgrade should be made gradually, eg from NS 11.0 to NS 11.1 prior to get to NS 12. The upgrade should be easily done through the NS GUI but if you bump into trouble the CLI upgrade version is also easy.

Download the build file from Citrix page, Netscaler Gateway 12, upload it to /flash through Filezilla/WinSCP. Example below:

soc@support ~ $ ssh nsroot@10.10.10.21 > save config > shell root@VLABSRV0# cd /nsconfig root@VLABSRV0# cp ns.conf ns.conf11.ns root@VLABSRV0# cd /var/nsinstall

root@VLABSRV0# mkdir nsinstall12 root@VLABSRV0# cd nsinstall12 root@VLABSRV0# mv /flash/build-12.0-53.13_nc_32.tgz . root@VLABSRV0# tar -xvzf build-12.0-53.13_nc_32.tgz (...) root@VLABSRV0# ./installns installns: [36026]: VERSION ns-12.0-53.13.gz (...) installns: [36026]: installns version (12.0-53.13) kernel (ns-12.0-53.13.gz)

The Netscaler version 12.0-53.13 checksum file is located on http://www.mycitrix.com under Support > Downloads > Citrix NetScaler. Select the Release 12.0-53.13 link and expand the "Show Documentation" link to view the SHA2 checksum file for build 12.0-53.13.

There may be a pause of up to 3 minutes while data is written to the flash. Do not interrupt the installation process once it has begun.

Installation will proceed in 5 seconds, CTRL-C to abort Installation is starting ... installns: [36026]: Installation is starting ... installns: [36026]: detected Version >= NS6.0 installns: [36026]: Installation path for kernel is /flash (...) installns: [36026]: Installing Linux EPA and Linux EPA version file... (...) Installation has completed. Reboot NOW? [Y/N] Y Rebooting ? installns: [36026]: Rebooting ...

nFactor ? Customizing UI to Display Images

Please also check the following article at the Citrix website: https://support.citrix.com/article/CTX225938

Backup Configuration

We'd also recommend backing up the configuration in case after a reboot the configuration gets messed up:
https://ogris.de/howtos/netscaler-restore.html