Checkpoint Connectra Integration

PINsafe to Checkpoint Connectra

Integration Notes

Contents

Overview

Swivel can provide strong and two factor authentication to the Checkpoint Connectra. This document outlines the details required to carry this out.

Baseline

Swivel 3.x

Checkpoint Connectra appliance version NGX R66. Also tested with R70.

Checkpoint R75 Mobile Access login page

Prerequisites

Working Connectra VPN

Swivel 3.x

Note that modifications to the Connectra login page will affect ALL users (but not the administration page).

Use of the TURing, Security String Index or SMS Confirmed message will require the use of a NAT.

When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

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

Connectra Configuration

Enabling RADIUS Authentication in Connectra

You need to configure Swivel as an authentication server on the Connectra appliance.

- Open Smart Dashboard and log in.
- Under Network and Resources -> Hosts, configure the Swivel server as a new host. You just need to give it a name and add the IP address.
- Under Users and Authentication -> Authentication -> RADIUS Servers, create a new RADIUS server. Select Swivel as the host, ?NEW-RADIUS? as the service, and enter the shared secret you previously set on the Swivel server. You can select RADIUS version 1 or 2, and PAP or MSChap as the protocol: Swivel will detect these protocols automatically. Note: When a Swivel appliance VIP is used, the real IP address should be used and not the VIP. For redundancy select Primary and Secondary RADIUS servers, see VIP on PINsafe Appliances.

You will also need to configure authentication for the relevant users. The simplest way to handle this is to create a new user group containing all users that will be using Swivel (if you do not already have one):

- Go to Users and Authentication -> Internal Users -> User Groups.
- Then under User Templates, create a new template, or modify an existing one, containing the relevant group, and set the authentication to RADIUS, using the Swivel server.

Don?t forget to save and install the policy once you have made all relevant changes.

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.

Customising the Connectra Login Page

NOTE: it is assumed here that you are familiar with Unix commands, in particular with the vi editor, as you will need to edit a file.

NOTE: There is an example LoginPage.php available which is the Login.php file with the modifications already included. This can be used for reference but may not be 100% suitable for specific installations and different Connectra versions.

Login to the Connectra

To modify the Connectra login page, you need to log into the console, either physically on the appliance, or using a SSH terminal server such as Putty see PuTTY How To Guide. Switch into expert mode.

Locate the file LoginPage.php

Change directory to /opt/CPcvpn-R66/phpincs (note: the exact directory name CPcvpn-R** will vary depending on the Connectra revision number). Backup the file LoginPage.php by making a copy of it.

Edit the LoginPage.php

After making a backup copy, edit the file LoginPage.php.

First of all, search for the end of the page header, ?</HEAD>?. There should be a ?</script>? tag just before that. Insert the following just before the </script>:

```
function showTuring() {
turing = document.getElementById("imgTuring");
username = document.getElementById("userName").value;
turing.src = "https://pinsafe_server:8443/proxy/SCImage?username=" +username + "&random=" + Math.floor(Math.random()*100000);
turingRow = turing.parentNode.parentNode;
turingRow.style.display = "";
}
```

NOTE: you should replace "pinsafe_server" in the value of turing.src above with the actual internet-visible address of the Swivel instance.

For a Swivel virtual or hardware appliance: "https://pinsafe_server:8443/proxy/SCImage?username="

For a software only install see Software Only Installation

Now locate the input field with ID ?userName?.

Add the following attribute to the field: onblur="showTuring();". The complete line should appear as follows:

```
<input type="text" id="userName" name="userName" class="inputText" autocomplete="off" <?=$User_Read_Only?> style="<?=$User_Style_Var?>" value
```

Look for the second <tr> tag after this field. Insert the following before this tag:

```
<tr style="display:none"><td colspan="2" align="center">
<input type="button" value="<?= TURING ?>" onclick="showTuring();"><br>
<img src="" id="imgTuring" alt="<?= TURING ?>">
</td></tr>
```

You can now save the file.

Editing the password prompt

If you want to change the prompt for the password (e.g to prompt for One-Time Code), or to change the text displayed on the button that requests a new TURing image, you will need to edit the file Strings.en_US.php, or the appropriate Strings file for your local language (type ls Strings* to see what files are available). Locate the string ?PASSWORD?, and change the text within the quotes to the right of the => symbol to ?OTC?, or whatever you prefer.

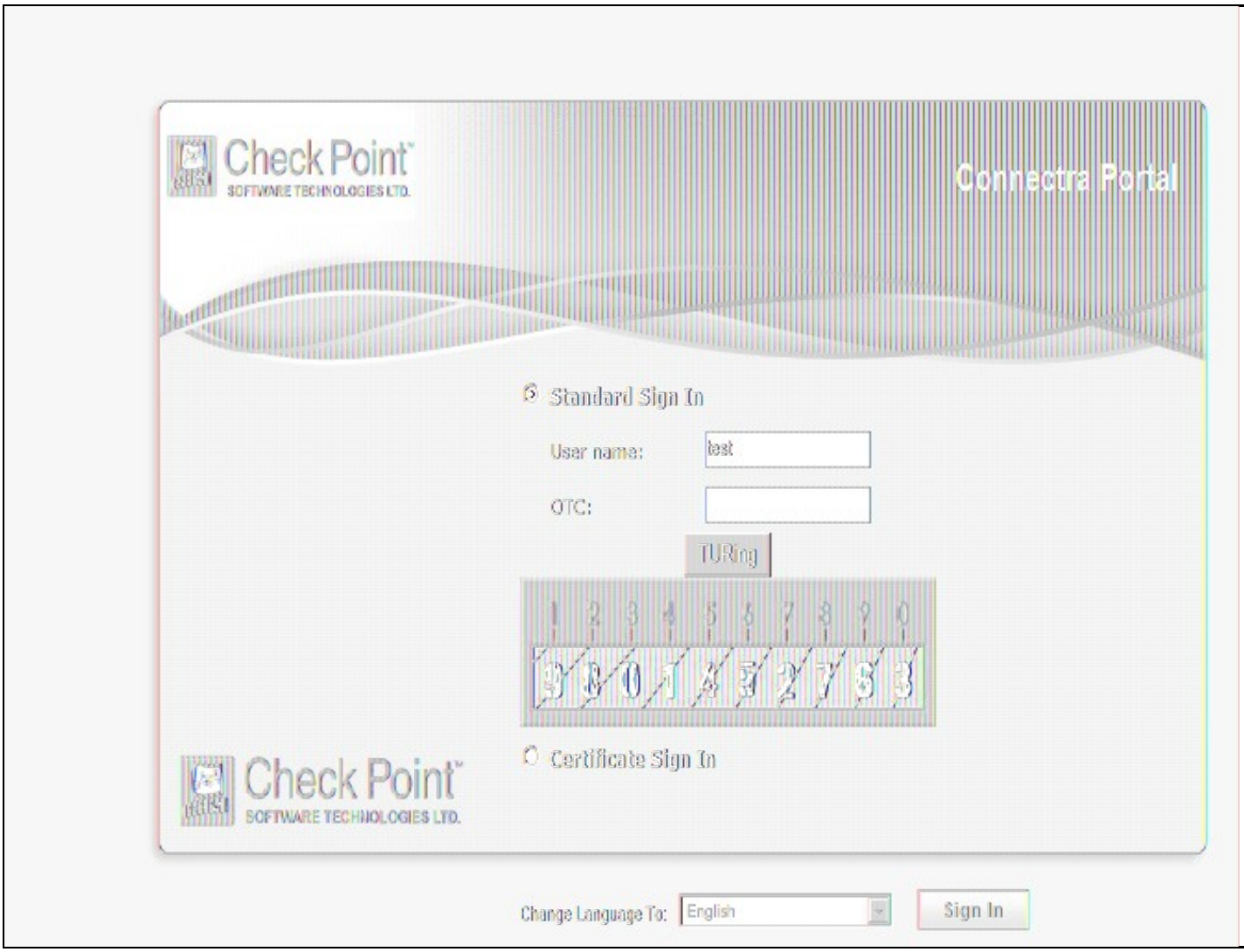
To set the text displayed on the TURing image button, insert a new line after this line, with the following content:

"TURING" => "TURing",

You can replace the right-hand text with anything you prefer. Don?t forget the comma at the end of the line.

Testing

With the changes in place, when a user accesses the Connectra portal the will see the modified login page.



After entering their username and either tabbing away from the username field of clicking the TURing button they will be presented with a TURing image. The PINsafe log should record a session start for that user.

The user can then use their PIN to extract their one-time code and enter this to authenticate. The PINsafe log show record the RADIUS dialogue associated with this authentication.

Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Image from PINsafe server absent

Known Issues and Limitations