Microsoft TMG RADIUS Integration

Contents

Microsoft Threat Management Gateway Integration

This guide describes how to integrate Swivel with Microsoft Forefront Threat Management Gateway using RADIUS authentication. No additional software is required.

If you want more control over authentication, with support for restricting Swivel to certain hostnames and allowing non-Swivel users to authenticate, see the TMG filter documentation for more information.

Configuring Swivel

- Log on to the Swivel Admin Console
- Under RADIUS -> Server, make sure that the server is enabled. All the other settings can be left as default.
- Under RADIUS -> NAS, enter a name in the blank identifier box (e.g. ?TMG?). Enter the name or IP address of the TMG server, and a chosen secret. Remember what you enter in the Secret box, as you will need it later.
- Click Apply.

Configuring Firewall Rules

It is assumed that you already have a firewall rule set up to support the website you need to protect. If not, use the appropriate wizard under Firewall Policy Tasks to set up the rule.

Modifying the Website Access Rule

To support Swivel authentication, all you need to do is to right-click on the Listener for the rule and select Properties. On the Authentication tab, select HTML Form Authentication, if it is not already selected.

Under most circumstances, you will need to authenticate to Windows Active Directory as well as to Swivel. Configure both AD and Swivel as authentication servers. To use Windows and Swivel authentication, check the box marked ?Collect additional delegation credentials in the form?. Make sure ?RADIUS OTP? is selected in the lower box, then click on ?Configure Validation Servers?. On the RADIUS Servers tab, click Add. Enter the IP or name of the Swivel server and the shared secret that you entered earlier for the Swivel NAS.

If you only want to use Swivel to authenticate, and no other method, then leave the option for additional delegation credentials unchecked and select either RADIUS or RADIUS OTP. You can only select RADIUS OTP if the Authentication Delegation option on the main rule is No Delegation.

NOTE: As described below, you may choose to create a new set of custom login pages, rather than replacing the existing ones. If you do, you will need to check the option to use custom HTML forms (on the Forms tab), and enter the name of the custom forms set.

Proxying the TURing Image

In order to allow Swivel to deliver a TURing image to the end user without exposing the Swivel server to the internet, it is necessary to create a firewall rule to proxy it. If you are using dual channel only, except for dual channel on demand, you can skip this step.

- Click on Publish Web Sites.
- Call the rule Swivel Image, or as required.
- Accept the defaults for the first few steps.
- Under internal site name, enter the name of the Swivel server. Note that this name must match the name of the SSL certificate on the Swivel server, since SSL requests through this rule must not generate any errors. Alternatively, you can configure Swivel not to use HTTPS.
- For Path, enter /proxy/SCImage (assuming this is an appliance, or /pinsafe/SCImage if not). For dual channel on demand, change SCImage to DCMessage.
- Select Any domain name.
- Create a new Listener. Call it TURing, or whatever you like.
- Require SSL (if you don't have an SSL certificate installed, select non-SSL)
- Select External networks only
- Select an SSL certificate if required
- Select No Authentication
- The remaining Listener options do not require configuration
- Back on the publishing wizard, accept the defaults for the remaining options.
- Once the rule is complete, right-click and select Properties
- On the Bridging tab, choose to redirect to port 8443 for context /proxy, or 8080 for context /pinsafe.

Customising Login Pages

If you are using dual channel authentication in Swivel, and do not require an embedded TURing image in your login page, you do not need to customise the login pages. This does not apply to dual-channel on-demand, for which the customisation IS required.

You can choose either to customise the default login pages, or to create a custom set of pages. If you are not using Swivel for all authentication rules on this TMG, you must create a custom set.

To create a custom set of rules:

- In Explorer, go to the TMG root folder: under a default installation, this is C:\Program Files\Microsoft Forefront Threat Management Gateway.
- Select the Templates sub-folder
- Select the CookieAuthTemplates sub-folder.
- Make a copy of one of the folders you find underneath here: for an Exchange firewall rule, select Exchange, and for other rules select ISA.
- Give the folder an appropriate name. NOTE: remember to change the custom forms option on the listener to specify the name of this folder.

If you choose to replace the existing login pages, select the CookieAuthTemplates folder as described above, then select either the ISA sub-folder, or the Exchange sub-folder, depending on whether or not you are customising Exchange access. If you have created a custom set, select that. Select the HTML sub-folder.

NOTE: if you are replacing existing standard login pages, make sure you take backup copies of any files you replace.

There are 3 files you might need to replace, depending on which authentication option you selected:

- For RADIUS authentication only, replace usr_pwd.htm
- For RADIUS OTP authentication only, replace usr_pcode.htm
- For dual Windows and RADIUS OTP authentication, replace usr_pwd_pcode.htm

The custom pages can be found here.

You will need to edit the file(s), and change the value of imageUrl to the appropriate external URL for the TURing image, as determined by the firewall rule you created earlier.

Changing the OTC button text

To change the OTC label, edit the following file:

C:\Program Files\Microsoft Forefront Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm.

Search for OTC as a whole word. You should find the following line:

```
<td class="nowrap"><label for="otc">OTC</label></td>
```

Change the prompt as required, and restart the firewall service.

Automatic sending of SMS

The login page can be configured to automatically send the user an SMS message when they have entered the username and proceed to the next field. On a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

locate the following

function setUserExists(attribute)

Approximately 20 lines below this, you should find the following section:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
} else {
btnMessage.style.display = "none";
}
}
```

Insert a new line, as follows:

```
if (btnMessage) {
if (showMessage) {
btnMessage.style.display = "";
ShowMessage();
} else {
btnMessage.style.display = "none";
}
}
```

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

Removing the OTC button

If you don't want the button to appear at all, on a default installation, edit the file "C:\Program Files\Microsoft Threat Management Gateway\Templates\CookieAuthTemplates\PINsafeExchange\HTML\usr_pwd.htm".locate the following lines:

<input class="btn" id="btnImage" type="button" value="@@L_StartSession_Text" onclick="ShowTuring();" />

<input class="btn" id="btnMessage" type="button" value="@@L_SendMessage_Text" onclick="ShowMessage();" />

and delete them.

Once you have made this change and saved the file, you have to restart the Microsoft Gateway service for the change to take effect. Also, be aware that you need to make the same change on all TMG servers in the farm.

These instructions assume you have the latest version of the TMG filter.

Troubleshooting

The thing you are most likely to have problems with in this integration is SSL certificates. When linking to a server that requires SSL, the TMG will fail if there are any errors in SSL handshaking. The guidelines here should help.

NOTE: to import a certificate from a Swivel appliance into a TMG to use as a proxy for the Swivel server, you must generate the private key with the argument -keyalg RSA. This is NOT the default when using the CMI options, so the certificate must be generated from the command line.

If you create SSL certificates using an internal Windows certificate authority, and generate the certificate request from the web interface, be aware that certificates generated using the Web Server template are not exportable. You need to create a new template for exportable web server certificates, as detailed here. Also, TMG does not support CNG / Windows 2008 certificates, so when creating the new template, make sure you select Windows 2003 compatibility. For the same reason, if you generate a new certificate request using the certificates MMC plug-in (details not given here), make sure you select Legacy rather than CNG. Our recommendation, however, is to use Keystore Explorer (see SSL Solutions) and to generate the certificate request with that.

As a last resort, particularly if the Swivel Appliance is not to be visible on the internet, you can simply disable HTTPS on the Swivel server. See the appliance documentation for details on this. Note that if you do disable https, you must alter the TURing Listener to match the settings.

If users are allowed to authenticate without Swivel authentication ensure 'Require all users to authenticate' option is checked.