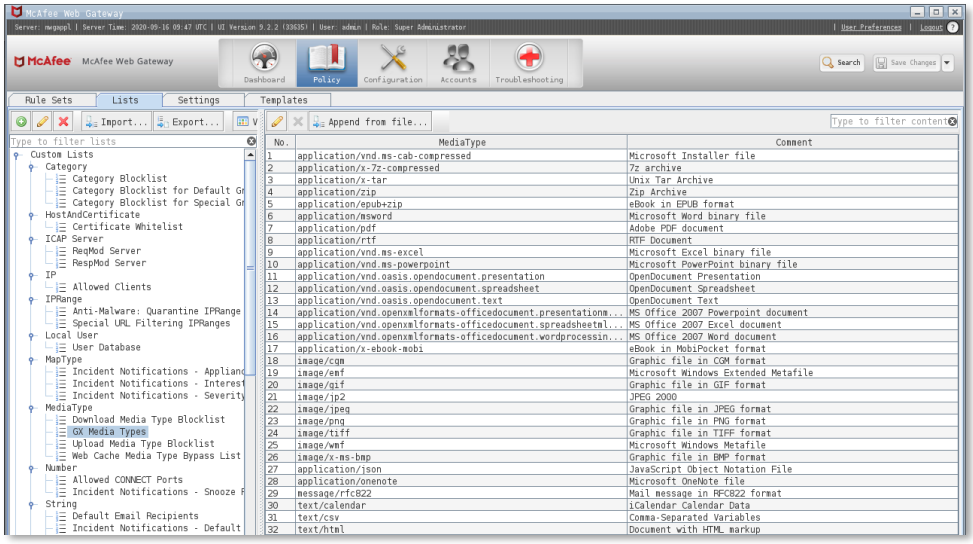
Deep Secure Gateway eXtension uses ICAP to receive data from McAfee Web Gateway. This means a on premises McAfee Web Gateway will be required to push the ICAP configuration to MVISION.

1. Download the `Deep_Secure_GX_ICAP_Client.zip`
2. Unzip the `Deep_Secure_GX_ICAP_Client.zip` to extract the `Deep_Secure_GX_ICAP_Client.xml`

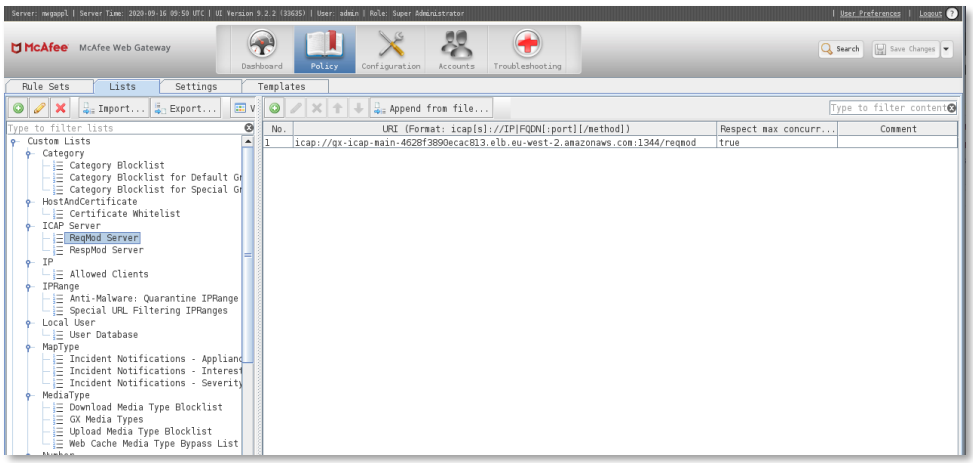
3. Connect to the **McAfee Web Management** page and import the `Deep_Secure_GX_ICAP_Client` file. To do this navigate to `Policy -> Rule Set -> Media Type Filtering` and click `Add -> Rule Sets from Library`, click `Import from File` and select the `Deep_Secure_GX_ICAP_Client.xml` file.

> **Tip** If the Media Type rule has not been unlocked, unlock this and import the Deep Secure GX ICAP Client Rule

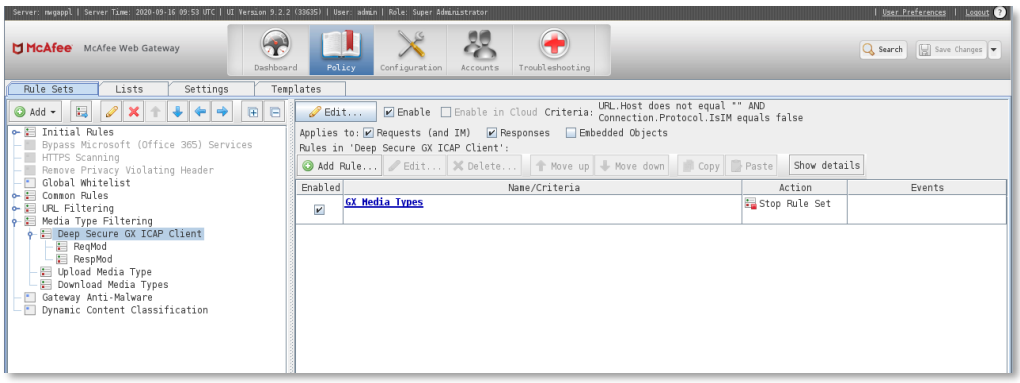
4. Verify the import was successful by navigating to:
   a. `Policy -> Media Type -> GX Media Types`



   b. `Policy -> ICAP Server -> ReqMod Server & RespMod Server`



c. Policy -> Rule Sets -> Media Type Filtering -> Deep Secure GX ICAP Client.

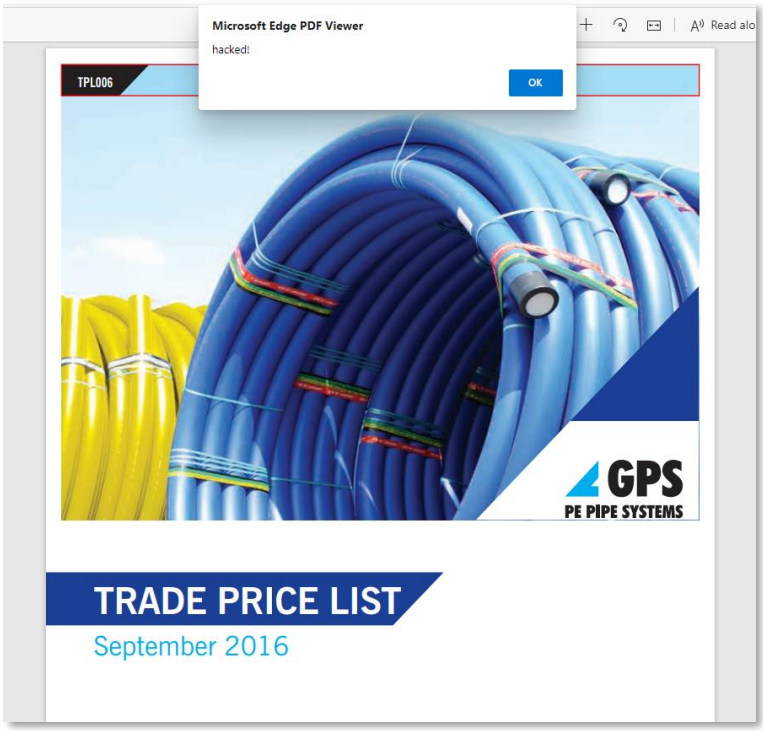


To test the before and after Deep Secure Policy change:

1. Navigate to http://demo.deep-secure.com/poc/Restricted/index.html and sign in with the Username and Password provided by Deep Secure.

2. Using a browser that is not being protected by Deep Secure navigate to Scripted Malware → Trade Price List.

3. Download and open the PDF hover over the top left corner of the document. A pop up will appear saying hacked!



Using a browser that is being protected by McAfee and Deep Secure navigate to the same URL as shown in *step 1* and download the same PDF (Trade Price List). This time when the PDF is view it will look the same as the original, however the hacked pop up will no longer appear.