Sentry SSO with CiscoASA

Contents

Introduction

This article explains how to integrate a Cisco ASA with Sentry.

If focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Cisco ASA to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guide Cisco ASA Integration

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

Overview

The integration works by

1. configuring the Cisco ASA login page to redirect the user to Sentry to authenticate
2. user authenticates at Sentry
3. user is redirected back to the Cisco ASA login page with a claim
4. Cisco ASA login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access

Therefore the following steps are required

1. Configure Cisco ASA Login
2. Configure Sentry to work with Cisco ASA login page
3. Configure Sentry to accept RADIUS requests from Cisco ASA

Configure Cisco ASA Login

In order to make the Cisco ASA page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from Sentry or if the user have come directly.

If the user has come directly they need to be redirected to Sentry. If they have been directed from Sentry the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=CiscoVPN**. This is important as this application name must match the settings on Sentry

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
 window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
 + winndow.location.href + "&applicationNameNoSAML=CiscoVPN" );
}
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];
        // 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;
        // 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"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
   redirect();
  } else {
   $('[name=password]').val(claimPassedIn);
   $('[name=login]').val(usernamePassedIn);
   document.getElementsByName("unicorn_form")[0].submit();
 }
 });
 </script>
 </head>
```

Configuring Sentry Login

The Cisco ASA VPN needs to be added to Sentry as an Application.

The following entries are required.

- Name This must match the name in the redirect url, eg CiscoVPN
- Service Provider SwivelVPN. Indicates this is a VPN integration
- Points Number of points required to access the VPN, refer to Sentry User guide
- Endpoint URL This is the URL of the Cisco ASA login page configured to work with Sentry
- Entity ID Should match Name.

Configuring Sentry RADIUS

To complete the integration the Cisco ASA VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg CiscoVPN
- Hostname Must match IP of Cisco ASA VPN

Two stage auth, Check Password with repository should be set to NO

SSO

If the Sentry login has been configured with SSO enabled then the Cisco ASA login page will work in the same way as other Sentry applications. If a user has authenticated already with more points than the Cisco ASA requires then the user will gain access to the Cisco ASA without needing to authenticate again.

Testing

- Goto to Cisco ASA login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Cisco ASA VPN
- User should gain access

Logs should include

```
CiscoVPN:Processing user username as channel CLAIM
CiscoVPN:Login successful for user: username
```

Troubleshooting

The scripts on the login page work by injecting values into the login page and submitting this page. To work therefore the standard login page must have a form called unicorn_form that has an input field called login for the username and an input field called passwd for the password as shown in the javascript.

By "called" the html must have the name attribute set to this value