Array Networks SPX Integration

Contents

Introduction

This configuration document outlines how to integrate Swivel with the Array Networks SPX using password authentication in addition to the Swivel authentication.

Additional Contributors

Swivel Secure would like to thank Wender Putters from Connect Data Solutions

Prerequisites

Array Network SPX 8.2, 8.3, 8.4

Swivel 3.x

If the TURing is required to be used a NAT is required to the Swivel virtual or hardware appliance

Website to host custom login page, this can be the Swivel virtual or hardware appliance.

Custom login page, this can be downloaded from here: here

Baseline

Array Networks SPX 8.2.2.0 and also 8.4.4.2 Build 9

Swivel 3.5 and Swivel 3.7

Architecture

The Array Networks SPX makes authentication requests against the Swivel virtual or hardware appliance by RADIUS. The login page is redirected from the Array Networks SPX onto another web server. The Swivel virtual or hardware appliance can be used to host this page. The hosted page must be accessible from the internet.

If the AD password is required to be used then these are added together into the RADIUS request, and Swivel has to have the *require password* and *check password with repository set to yes*. Remember that in Swivel 3.7 and earlier this is a global setting. In Swivel 3.8 it is possible to set password checks by NAS devic rather than being a global setting.

Installation

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.

Configure Password

Swivel 3.7 and earlier

If the AD Password is required to be used, on the Swivel Administration Console select Policy/Password, enable *Require Password* and *check password with repository*

Swivel 3.8 and later

If the AD Password is required to be used, on the Swivel Administration Console select RADIUS NAS, enable *check password with repository*

Configure the custom login page

Editing the Login Page

Edit the file login.html with the required values

The externally accessible IP address of the Swivel virtual or hardware appliance needs to be set for the following lines:

_AN_base_host = "http://192.168.100.100:8080";

_AN_base_path = "http://192.168.100.100:8080/login";

sUrl = "https://192.168.100.100:8443/proxy/SCImage?username=";

Change the IP address for that of the public URL. For a Swivel virtual or hardware appliance the sURL also needs to be changed as follows:

For a Virtual or hardware appliance:

sUrl = "https://IP:8443/proxy/SCImage?username=";

For a software only install see Software Only Installation

Copy the login page files

The login page can be hosted on a web server. Note that this page needs to be accessible from the internet by the client.

To use Swivel as a to host the login page:

Copy login.html to one of the following locations:

Swivel Virtual or hardware Appliance: create the folder ROOT in /usr/local/tomcat/webapps2 using a program such as WinSCP, see the WinSCP How To Guide, then ensure that the ownership/group of the folder and file are *swivel* and permissions for the ROOT folder are rwxrwxr-x. Copy in the file login.html and ensure the permissions are rw-rw-r--, and it is owned by the swivel user.

Software only install: <path to Tomcat>/webapps/ROOT

Test that the web page is accessible

Virtual or hardware appliance: http://IP of Swivel server:8443/login.html

For a software only install see Software Only Installation

Create a Failed Login Page

When a login fails, the page redirects, to ensure that this is a Swivel login page either redirect the login failure back to the Swivel login.html, or make a copy of that file and edit it as required, such as to indicate that a login has failed.

Configure the Array Networks SPX

Configure RADIUS authentication

On the Array Networks SPX Select under Site Configuration AAA, then method. Configure the RADIUS server on the authentication menu. Set the authentication method to RADIUS

File   Edit   View   Favorites   Tools   Help

Back ▾ ◯ ▾ ⚊ 🖹 🏠 | 🔎 Search ⭐ Favorites 🥚 | 🖂 ▾ 🖶 📄

Address 🖉 https://192.168.200.240:8888/

Array
NETWORKS

Username: array

SPX Host Name: UK01-IPH-SPX

Mode: ◯ Enable ◉ Config

Portal2 ▾

Virtual Site Home

SITE CONFIGURATION
SSL Certificates

AAA

Portal
Security Settings
Networking

LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization

ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN

ACCESS POLICIES
ACLs
URL Filtering

ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password

| General | Method | Authentication | Authorization | Accounting |

AAA METHOD RANKING

Method Ranking	Authentication Method	Autho
Rank 1:	RADIUS ▾	L
Rank 2:	LocalDB ▾	
Rank 3:	▾	
Rank 4:	▾	

*Note: If Authorization method is not specified, Authentication servers will be

** Note: When "Authorize" is selected as the authentication method, the SPX
screen will be presented.

Done

On the Authentication tab, Swivel needs to be configured as the RADIUS server for the VPN, ensuring that the shared secret matches that set on the RADIUS->NAS screen on Swivel.

If you want to configure more RADIUS servers for failover, add more servers.

Link custom page to URL for login

The custom log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, enter the path to the Swivel virtual or hardware appliance. Note that this page needs to be accessible from the internet by the client.

The required settings are:

URL: Full address of where the login page can be reached

Username: default: uname, the username attribute used in the login page

Password: default: pwd, the password attribute used in the login page

Token: default: token, the token attribute used in the login page

Password: default: pwd2, the secondary password attribute

Other options

Change Password Page Full address of the ChangePIN page

File   Edit   View   Favorites   Tools   Help

Back ▾   ▾   ✕   ⟳   🏠   🔍 Search   ⭐ Favorites   ✉ ▾ 🖶 📄

Address 🔗 https://192.168.200.240:8888/

Array NETWORKS

Username: array

SPX Host Name: UK01-IPH-SPX

Mode: ○ Enable ⦿ Config

Portal ▾

Virtual Site Home

SITE CONFIGURATION
SSL Certificates
AAA

Portal

Security Settings
Networking

LOCAL USERS & GROUPS
Local Users
Local Groups
Login Authorization

ACCESS METHODS
Web Access
File Access
TCP Applications
L3VPN

ACCESS POLICIES
ACLs
URL Filtering

ADMIN TOOLS
Session Management
Config Management
Monitoring
Troubleshooting
Change Password

General Settings **Themes** **External Pages**

Portal Pages   **Error Pages**

LOGIN PAGE

URL: http://192.168.200.30/login/default.html

Username: uname

Password: pwd

Token: token

Password: pwd2

WELCOME PAGE

URL:

CHANGE PASSWORD PAGE

URL: http://192.168.200.30:8080/changepin/changepin.jsp

LOGOUT PAGE

URL:

Link custom page to URL for failed login

The custom failed log-in page created then needs to be associated with the url of the log-in page. On the Array Networks SPX Select under Site Configuration Portal then External pages, select Error Pages, and for error type select failed login, enter either the path to the Swivel page or to a custom failed login page. Note that this page needs to be accessible from the internet by the client. Click save and the login page will now be listed.

Custom page for failed login:

The custom login page should be listed under Error Pages

Link custom page to URL for generic login error

It is also recommended to create another error page (as above) using the same custom login page URL (as above) but for a **generic login error**, which is a selectable Error Type. This prevents the default localhost login page of the Array being presented in the event of a generic login error.

Configure URL Policy

This page allows certain attributes to be used in the login page. On the Array Networks SPX Select under access methods/Web Access then URL Policies. Create the following policies:

Priority: 1 Type Public: keyword: SCImage

Priority: 2 Type Public: keyword: .gif

Priority: 3 Type Public: keyword: .jpg

Priority: 4 Type Public: keyword: .jsp
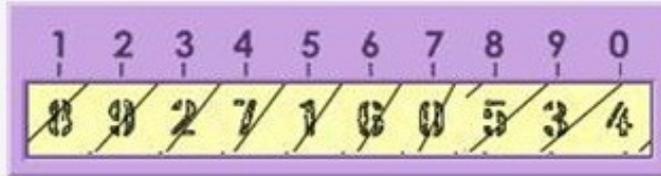
Verifying the Installation

Browse to the login page, enter a username, click on the Request Turing button and the Turing image should appear. Check for Session requests with that username on Swivel, and RADIUS requests.

Test using the SMS option without clicking on the Turing button. Note: If the Single Channel Turing image is clicked it will expect a Single Channel login for the length of the session request (usually 2 minutes). Check for RADIUS requests on Swivel.

Ensure that the failed login redirects to a Swivel login page.

Your attempt to sign in failed. Please make sure that your username and password are correct, and try again.

Username: graham

Password:

Get Security Image

OTC:

Sign In

Troubleshooting

Check the Swivel logs and system event logs for any errors or lack of communication as well as the Array Networks SPX logs.

Known Issues and Limitations

Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com