Verification of Authentication Object on FireSIGHT System for Microsoft AD Authentication Over SSL/TLS

Contents

Introduction

You can configure a FireSIGHT Management Center to allow external Active Directory LDAP users to authenticate access to the web user interface and CLI. This article discuss how to configure, test, troubleshoot Authentication Object for Microsoft AD Authentication Over SSL/TLS.

Prerequisite

Cisco recommends that you have knowledge on user management and external authentication system on FireSIGHT Management Center.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Procedure

Step 1. Configure Authentication Object without SSL/TLS encryption.

1. Configure the Authentication Object as you normally would. The basic configuration steps for encrypted and unencrypted authentication are the same.
2. Confirm that Authentication Object is working and AD LDAP users can authenticate unencrypted.

Step 2. Test the Authentication Object over SSL and TLS without CA Certificate.

Test the authentication object over SSL and TLS without CA cert. If you encounter an issue, please consult with your System Admin to resolve this issue on the AD LDS Server. If a certificate have previously been uploaded to the authentication object, please select "**Certificate has been loaded (Select to clear loaded certificate)**" to clear the cert and test AO again.

If the Authentication Object fails, please consult your System Admin to verify the AD LDS SSL/TLS configuration before you move on to the next step. However, please feel free to continue to the following steps to test the Authentication Object further with CA Certificate.

Step 3. Download **Base64** CA Cert.

1. Login to the AD LDS.
2. Open a Web browser and connect to `http://localhost/certsrv`
3. Click on "**Download a CA certificate, certificate chain, or CRL**"
4. Choose the CA cert from "**CA Certificate**" list and "**Base64**" from "**Encoding Method**"
5. Click on "**Download CA certificate**" link to download the `certnew.cer` file.

Step 4. Verify the **Subject** value in the cert.

1. Right Click on the `certnew.cer` and select **open**.
2. Click on **Details** tab and select **<All>** from the **Show** drop-down options
3. Verify the value for each field. In particular, verify that the **Subject** value matches the **Primary Server Host** name of the Authentication Object.

Step 5. Test the Cert on a Microsoft Windows machine. You can perform this test on a Workgroup or Domain joined Windows machine.

> **Tip**: This step can be used to test CA Certificate on a Windows system before creating Authentication Object on a FireSIGHT Management Center.

1. Copy the CA cert to `C:\Certficate` or any preferred directory.
2. Run Windows command line, `cmd.exe. as an administrator`
3. Test the CA certificate with Certutil command

```
cd c:\Certificate

certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

If the Windows machine is already joined the domain, the CA certificate should be in the certificate store and there should be no error in `cacert.test.txt. However, if the Windows machine is on a workgroup, you may see one of the two messages depending on the existence of CA cert in the trusted CA list.`

a. The CA is trusted but no CRL found for the CA:

```
ERROR: Verifying leaf certificate revocation status returned The revocation function
was unable to check revocation because the revocation server was offline. 0x80092013
(-2146885613)

CertUtil: The revocation function was unable to check revocation because the
revocation server was offline.
```

b. The CA is not trusted:

```
Verifies against UNTRUSTED root
Cert is a CA certificate
Cannot check leaf certificate revocation status
CertUtil: -verify command completed successfully.
```

If you get any other ERROR messages like below, please consult with your System Admin to resolve the issue on the AD LDS and Intermediate CA. These error messages are an indicative of incorrect Cert, subject in the CA cert, missing certificate chain, etc.

```
Failed "AIA" Time: 0
Failed "CDP" Time: 0
Error retrieving URL: The specified network resource or d evice is no longer available
```

Step 6. Once you confirm the CA cert is valid and have passed the test in Step 5, upload the cert to the Authentication Object and run the test.

Step 7. Save the Authentication Object and reapply the system policy.