IDENTIFY MISSING CERTIFICATES VIA THE ADMINISTRATION UI

02/19/2019

Rev: B

Contents

Overview

SSL Certificate validation cannot be successful if there are certificates missing in the chain. This document provides steps to validate the completion of the certificate chain installed in FortiNAC via the Administration UI.

Procedure

Access the Certificate Details

1. Login to the Administrative UI and navigate to **System > Settings > Security > Certificate Management**. Click to highlight the Certificate Target and click the **Details** button.

2. The Certificate Hierarchy contains a list of certificates installed for the selected target. They can be viewed by clicking the drill down.

Example of Certificate Hierarchy using a wildcard certificate:

```
-- *.bradfordnetworks.com
 -- Go Daddy Secure Certificate Authority - G2
  -- Go Daddy Root Certificate Authority - G2
   -- Go Daddy Class 2 Certification Authority
```

Each certificate has a **Details** section below. The three fields of interest are:
Subject
Issuer
Issuer Certificate

For each Issuer Certificate, its Issuer must be listed in the Certificate Hierarchy. If not, at least one intermediate certificate is missing (the number of Intermediate Certificates used will differ per installation).

Follow the Certificate Chain

1. Review details for the certificate listed at the top of the hierarchy.

   Details using above example (*.bradfordnetworks.com):
   Subject: CN=*.bradfordnetworks.com ...
   Issuer: CN=Go Daddy Secure Certificate Authority - G2 ...
   Issuer Certificate: http://certificates.godaddy.com/repository/gdig2.crt

2. Drill down and locate the Issuer in the hierarchy (Go Daddy Secure Certificate Authority - G2). It should be listed.

   -- *.bradfordnetworks.com
   -- Go Daddy Secure Certificate Authority - G2
   -- Go Daddy Root Certificate Authority - G2
   -- Go Daddy Class 2 Certification Authority

3. Click on the Issuer (Go Daddy Secure Certificate Authority - G2) and view its details.
   Subject: CN=Go Daddy Secure Certificate Authority - G2 ...
   Issuer: CN=Go Daddy Root Certificate Authority - G2 ...
   Issuer Certificate: (none listed)

4. Drill down and locate the Issuer in the hierarchy (Go Daddy Root Certificate Authority - G2). It should be listed. If the Issuer is not listed, an Intermediate Certificate is missing.

   -- *.bradfordnetworks.com
   -- Go Daddy Secure Certificate Authority - G2
   -- Go Daddy Root Certificate Authority - G2
   -- Go Daddy Class 2 Certification Authority

The Root Certificate is the last certificate in the chain. Once this certificate has been reached, verification is complete.

Retrieve Missing Intermediate Certificates

1. Download the Issuer Certificate whose Issuer is missing from the Hierarchy. This can be done from any workstation. If using a Linux station type
   wget <Issuer Certificate URL>

   Example:
   ```
   wget “http://certificates.godaddy.com/repository/gdig2.crt”
   ```

2. View the certificate details searching for "CA Issuers" for additional Issuer certificates (.crt files). If Linux type
   openssl x509 -noout -text -in <certificatefilename> | grep "CA Issuers"

   Example:
   ```
   openssl x509 -noout -text -in gdig2.crt | grep "CA Issuers"

   CA Issuers - URI:http://crt.usertrust.com/AddTrustUTNSGCCA.crt
   ```

If an error occurs, the certificate may be in the wrong format. Convert the file from DER to PEM format.

```
openssl x509 -inform der -in gdig2.crt -out gdig2.pem
openssl x509 -noout -text -in gdig2.pem | grep "CA Issuers"
```

3. Download the certificate using the wget command (as in step 1). Repeat this process until no further certificates are found.

Install Intermediate Certificates Missing in Hierarchy

1. Save the certificates to the computer used to access the Administrative UI. This can be done via SCP, FTP or saving content to a text file on the computer.

2. cat the certificate file or browse to the URL. The format should look similar to below:

```
------BEGIN CERTIFICATE---------
MIIC1zCCAb8CAQAwgZExCzAJBgNVBAYTAlVTMRUwEwYDVQQIEwxO
ZXcgSGFtc2hpcmUxEDAOBgNVBAcTB0NvbmNvcmQxGjAYBgNVBAoTEU
JyYWRmb3JkIE5ldHdvcmtz3D3uBgc2pLw98Rqg/e5BCZPmXu0V19kyuRxn3p
DMuvTSq+NU0aTRg7dI6NJa76smzbYUBe5ti8QpyRGNmOf8kkSsPlzuIwOQZ
8qSUDsr6WEp9oThCl8gyt/PysTDNxMO41fmRtDv79YL3w65FOMpjtTIXqwD
9Om9PjddmyElQ9hIVxKjhIZLtTZe3BA7f50SbTA2X3iEwfwrG8LJbIfnc9zAX
K7S7kzTITIlGVWqgVZlYe9Hr5Wfjjj5ExCNq7wZ98gZ7S73Tx44+Xj5c3xnvwI
------END CERTIFICATE---------
```

3. Save content to a text file using a basic text editor (such a notepad). **Important:** There must not be any extra spaces or characters.

4. Once the missing certificate(s) has been saved to the computer, re-upload the entire certificate package (leaf certificate, previously present certificate as well as the missing certificates) to the target through the Administrative UI.

    a. Navigate to **System > Settings > Security > Certificate Management**.
    b. Click to highlight the Certificate Target.
    c. Click **Upload Certificate.**
    d. Select the target where the certificate will be uploaded (should already be listed).
    e. Select "**Reuse Private Key from Existing Certificate**"
    f. Click the **Choose File** button to find and select the certificate to be uploaded.
    g. Click the **Add Certificate** button to enter each additional certificate file.
    h. Click **OK.**

Validate

Once completed, right click on the target and select **Details**. Go through the instructions under "Follow the Certificate Chain" and verify that each Issuer Certificate listed now has its Issuer listed in the Hierarchy.

Contact Support if assistance is needed.