FortiNAC

Analytics SSL Certificates

Version: 5.x

Date: 8/28/2018

Rev: D

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINETTRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Tuesday, August 28, 2018

Contents

Overview

What it Does

SSL Certificates secure communications between the FortiNAC/Analytics Server and FortiNAC. Additionally, the Analytics web server (wildfly or jboss) will not start if a certificate is not installed.

How it Works

In order to secure communications with FortiNAC, trusted SSL certificates need to be installed.

There are four components involved:

- Certificate Signing Request (CSR)
- Private Key
- Leaf Certificate
- Certificate bundle (contains Intermediate and Root certificates)

SSL Certificate Basic Installation Steps:

1. **Obtain a Valid SSL Certificate from a Certificate Authority (CA)**. A certificate signing request (CSR) is issued and submitted to the Certificate Authority. The CSR may be generated in FortiNAC/Analytics Server, or from another source. The CA then issues the certificates based on the CSR.

2. **Install Certificates Received from the CA**. Once the certificates are received from the CA, these files must be installed in FortiNAC/Analytics Server.

3. **Renew or Install New Certificates:** SSL Certificates must be renewed periodically or they expire.

Note: For centOS 5 systems: replace all instances of **wildfly** with **jboss** in these instructions.

Configuration Options

SSL Certificates can be issued from the following Certificate Authorities (CA):

- **Third party public** - certificates issued from Certificate Authorities like GoDaddy, DigiCert, GlobalSign, etc.
- **Corporate Owned Internal CA** - certificates issued from within the organization.
- **Self-Signed** - FortiNAC/Analytics Server issues its own certificate. This option is not as secure, but is an option in situations where a new certificate is not yet available.

Configuration

Third Party Public and Corporate Owned Internal CA Certificates

Generate Certificate Signing Request (CSR)

1. Log into the CLI of the FortiNAC/Analytics Server as root and type
   `cd /bsc/services/wildfly`

2. Request a certificate. Type
   `openssl req -new -newkey rsa:2048 -sha256 -keyout server.key -out server.csr`

   Note: RSA Private key can also be set to 1024 bit.

   If prompted for a PEM passphrase, enter **cchaos**.

   Hit **<Enter>** to skip the 'extra' attributes (challenge password, optional company name).

   Resulting files:
   server.key (Private Key)
   server.csr (Certificate Signing Request)

3. Send the Certificate Signing Request file server.csr to the Certificate Authority (CA). When submitting request, specify the files be in PEM format.

   The key (server.key) will be used when importing certificates.

   Note: Depending upon the Certificate Authority, the time it takes for certificate files to be returned after submitting the request will vary.

Import Certificates

When importing certificates, the Certificate Authority will generally return:

- Certificate
- CA bundle containing the private key and any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle containing only the intermediate and root certificates must be in separate files. This document uses the following filenames:
server.key = private key
server.crt = leaf certificate
Bundle.crt = certificate bundle (intermediate and root certificates)

1. In the Analytics Server CLI type
   cd /bsc/services/wildfly

2. Copy the files from the CA to the **/bsc/services/wildfly** directory.

3. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix A before proceeding.

4. Verify Private Key is in RSA format. Review the private key file using a text editor. Alternatively, if in Linux, the file can be viewed by running the command:
   cat <filename>

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   This is an indication the Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):
   openssl rsa -in <old_file_name> -out <new_file>

   Complete SSL Certificate installation using the newly converted Private Key file.

5. Create the keystore and associate it to the leaf certificate. Type
   keytool -noprompt -import -keystore keystore.jks -file <filename> -storepass cchaos

   Example using certificate (server.crt):
   keytool -noprompt -import -keystore /bsc/services/wildfly/keystore.jks -file server.crt -storepass cchaos

   The "Certificate was added to keystore" message appears when the certificate is successfully added.

6. Import the private key, leaf certificate and intermediate file or bundle into the keystore:
   ImportCertificateWithKey -import -keystore keystore.jks -key <key filename> -cert <certificate filename> -cas <CA bundle filename> -storepass cchaos -alias root

   Example using private key (PrivateKey.txt), certificate (server.crt), and CA bundle (DigiCertCA.crt):
   ImportCertificateWithKey -import -keystore /bsc/services/wildfly/keystore.jks -key server.key -cert server.crt -cas DigiCertCA.crt -storepass cchaos -alias root

   "Successfully imported key and certificate chain" appears when the certificate and intermediate files are successfully imported.

7. Restart the wildfly server.
   service bsc-wildfly restart

8. Proceed to Validate SSL Certificate Installation.

Renew Public or Internal CA Certificates (Same Key)

These steps assume the new set of certificate files were generated using the same private key.

Import New Certificates

When importing certificates, the Certificate Authority will generally return:

- Certificate
- CA bundle containing the private key and any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle containing only the intermediate and root certificates must be in separate files. This document uses the following filenames:
server.key = private key
server.crt = leaf certificate
bundle.crt = certificate bundle (intermediate and root certificates)

1. In the Analytics Server CLI type
   `cd /bsc/services/wildfly`

2. Copy the files from the CA to the **/bsc/services/wildfly** directory.

3. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix A before proceeding.

4. Delete the existing keystore. Type
   `rm keystore.jks`

5. Re-create the keystore and associate it to the new leaf certificate. Type
   `keytool -noprompt -import -keystore keystore.jks -file server.crt -storepass cchaos`

   The "Certificate was added to keystore" message appears when the keystore is successfully created.

6. Import the existing private key, new leaf certificate and intermediate file or bundle into the keystore:
   `ImportCertificateWithKey -import -keystore keystore.jks -key server.key -cert server.crt -cas bundle.crt -storepass cchaos -alias root`

   “Successfully imported key and certificate chain” appears when the files are successfully imported.

7. Restart the wildfly server.
   `service bsc-wildfly restart`

8. Verify that wildfly is running. Type
   `service bsc-wildfly status`

"Active: active (running)" is returned.

9. Proceed to Validate SSL Certificate Installation.

Renew Public or Internal CA Certificates (New Key)

Generate Certificate Signing Request (CSR)

If using an existing set of certificates, proceed to Import Certificates.

1. Log into the CLI of the FortiNAC/Analytics Server as root and type
   `cd /bsc/services/wildfly`

2. Request a certificate. Type
   `openssl req -new -newkey rsa:2048 -sha256 -keyout server.key -out server.csr`

   If prompted for a PEM passphrase, enter **cchaos**

   Note: RSA Private key can also be set to 1024 bit.

3. Send the Certificate Signing Request file server.csr to the Certificate Authority (CA). When submitting request, specify the files be in PEM format.

   The key (server.key) will be used when importing certificates.

   Note: Depending upon the Certificate Authority, the time it takes for certificate files to be returned after submitting the request will vary.

Backup Existing Certificate Files

If the current certificates installed are still valid, copy the key, leaf certificate and bundle to another directory in case they need to be re-installed due to an issue with the new certificates.

Import Certificates

When importing certificates, the Certificate Authority will generally return:

- Leaf certificate
- CA bundle containing the private key and any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle containing only the intermediate and root certificates must be in separate files. This document uses the following filenames:
server.key = private key
server.crt = leaf certificate
bundle.crt = certificate bundle (intermediate and root certificates)

1. In the Analytics Server CLI type
   `cd /bsc/services/wildfly`

2. Copy the new files to the **/bsc/services/wildfly** directory.

3. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. Complete the steps in Appendix A before proceeding.

4. Delete the keystore file. Type
   `rm keystore.jks`

5. Delete the alias associated with the keystore. Type
   `keytool -delete -alias root`

6. Re-create the keystore and associate it to the new leaf certificate. Type
   `keytool -noprompt -import -keystore keystore.jks -file server.crt -storepass cchaos`

   The "Certificate was added to keystore" message appears when the keystore is successfully created.

7. Import the new private key, leaf certificate and intermediate file or bundle into the keystore:
   `ImportCertificateWithKey -import -keystore keystore.jks -key server.key -cert server.crt -cas bundle.crt -storepass cchaos -alias root`

   “Successfully imported key and certificate chain” appears when the files are successfully imported.

8. Restart the wildfly server.
   `service bsc-wildfly restart`

9. Proceed to Validate SSL Certificate Installation.

Create and Import Self-Signed Certificate

If a public or internal certificate is not available, a self-signed certificate can be used.

1. In the Analytics Server CLI type
   `cd /bsc/services/wildfly`

2. Create the keystore file. Type
   `keytool -genkey -alias root -keyalg RSA -validity xxx -keystore ./keystore.jks`

   Where **xxx** is the number of days the certificate will remain valid. By default, self-signed certificates are only valid for 90 days.

3. Respond to the questions with the appropriate information. Use the password **cchaos** (including password for root).

4. Create the certificate. Type
   `keytool -export -alias root -storepass cchaos -file ./server.cer -keystore ./keystore.jks`

   "Certificate stored in file…" is returned.

5. Import the certificate to the keystore. Type
   `keytool -import -v -trustcacerts -alias root -file ./server.cer -keystore ./cacerts.jks -keypass cchaos -storepass cchaos`

6. Type **yes** to trust the certificate when prompted.

   "Certificate was added to the keystore" is returned.

7. Restart the wildfly service.
   `service bsc-wildfly restart`

8. Proceed to Validate SSL Certificate Installation.

Renew Self-Signed Certificate

1. In the Analytics Server CLI type
   `cd /bsc/services/wildfly`

2. Delete the certificate and keystore files. Type
   `rm server.cer`
   `rm keystore.jks`

3. Delete the alias associated with these files. Type
   `keytool -delete -alias root`

4. Proceed to Create and Import Self-Signed Certificate.

Validate SSL Certificate Installation

1. Verify that wildfly is running. Type
   service bsc-wildfly status

   "Active: active (running)" is returned.

2. Display keystore.jks contents (expiration, owner, issuer, etc) and verify expiration dates. Type
   keytool -list -v -keystore keystore.jks -storepass cchaos | grep -i valid

```
keytool -list -v -keystore keystore.jks  -storepass cchaos | grep -i valid
Owner: CN=*.Fortinetnetworks.com, OU=Domain Control Validated
Valid from: Thu Mar 06 17:09:03 EST 2014 until: Fri Mar 10 13:42:25 EST 2017
Valid from: Tue May 03 03:00:00 EDT 2011 until: Sat May 03 03:00:00 EDT 2031
Valid from: Wed Jan 01 02:00:00 EST 2014 until: Fri May 30 03:00:00 EDT 2031
Valid from: Tue Jun 29 13:06:20 EDT 2004 until: Thu Jun 29 13:06:20 EDT 2034
Owner: CN=*.Fortinetnetworks.com, OU=Domain Control Validated
Valid from: Thu Mar 06 17:09:03 EST 2014 until: Fri Mar 10 13:42:25 EST 2017
```

3. Connect to Analytics Server URL and login.
   https://<name defined in SSL certificate>:8543/Fortinet-reporting/

4. Once at the Dashboard, verify the web browser indicates a secure connection.

Appendix

Create SSL Certificate Bundle

If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle.

1. Confirm the files are in PEM format. When opened in a text editor, the content should look similar to the format:
   -----BEGIN CERTIFICATE1-----
   sajaisjkajfsdvjJV;kjvd;Kjv;Js;FDJVKjv
   -----END CERTIFICTATE1-----

   If the content does not have these types of headers, convert to PEM format first.

   Convert **DER/Binary** to **PEM** Format:
   `openssl x509 -inform der -in <filename> -out <newfilename>`

   Example converting certificate.cer:
   openssl x509 -inform der -in certificate.cer -out certificate.pem

   Convert **P7B/PKCS#7** to **PEM** Format:
   `openssl pkcs7 -print_certs -in <filename> -out <newfilename>`

   Example converting certificate.p7b:
   openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer

   Convert **PFX/PKCS#12** to **PEM** Format:
   `openssl pkcs12 -in <filename> -out <newfilename> -nodes`

   Example converting certificate.pfx:
   openssl pkcs12 -in certificate.pfx -out certificate.cer –nodes

2. Append all intermediate files into a single text file (bundle.crt).

   a. Determine the order in which the certificates will be listed in the bundle (order is important). This is done by using keytool to review each certificate.

      Use the following command to decode and view the content of each certificate:
      `keytool -v -printcert -file <certificate filename>`

   b. Start with the leaf certificate. Look at the Issuer to determine the certificate to be listed first in the bundle.

      keytool -v -printcert -file server.crt
      Owner: CN=bcm.mydomain.edu, OU=ITS Servers & Apps, O=My Organization,L=Somewhere, ST=NY, C=US
      Issuer: CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US

c. The first Intermediate Certificate's Owner should match the leaf certificate's Issuer.

keytool -v -printcert -file InCommonServerCA.pem
Owner: CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US
Issuer: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE

d. The next Intermediate Certificate's Owner should match the first Intermediate certificate's Issuer. In this case it is the Root certificate (which will always be listed last).

keytool -v -printcert -file AddTrustUTNSGCCA.pem
Owner: CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
Issuer: CN=UTN - DATACorp SGC, OU=http://www.usertrust.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US

e. Create a new text file (bundle.crt) and append the certificate files in order.

Example of importing the text content of each intermediate and root certificate (in the appropriate order) into a new bundle called bundle.crt:
cat InCommonServerCA.pem >> bundle.crt
cat AddTrustUTNSGCCA.pem >> bundle.crt

f. View the bundle and ensure there are no spaces between the start and end of each file.
cat bundle.crt
Example Bundle content:
-----BEGIN CERTIFICATE1-----
sajaisjkajfsdvjJV;kjvd;Kjv;Js;FDJVKjv
-----END CERTIFICTATE1-----
-----BEGIN CERTIFICATE2----
sajdjsaskdjfkjdskvjsadvkjBDSVKBkdjv
-----END CERTIFCATE2-----

3. Proceed to step 4 in the section Import Certificates.