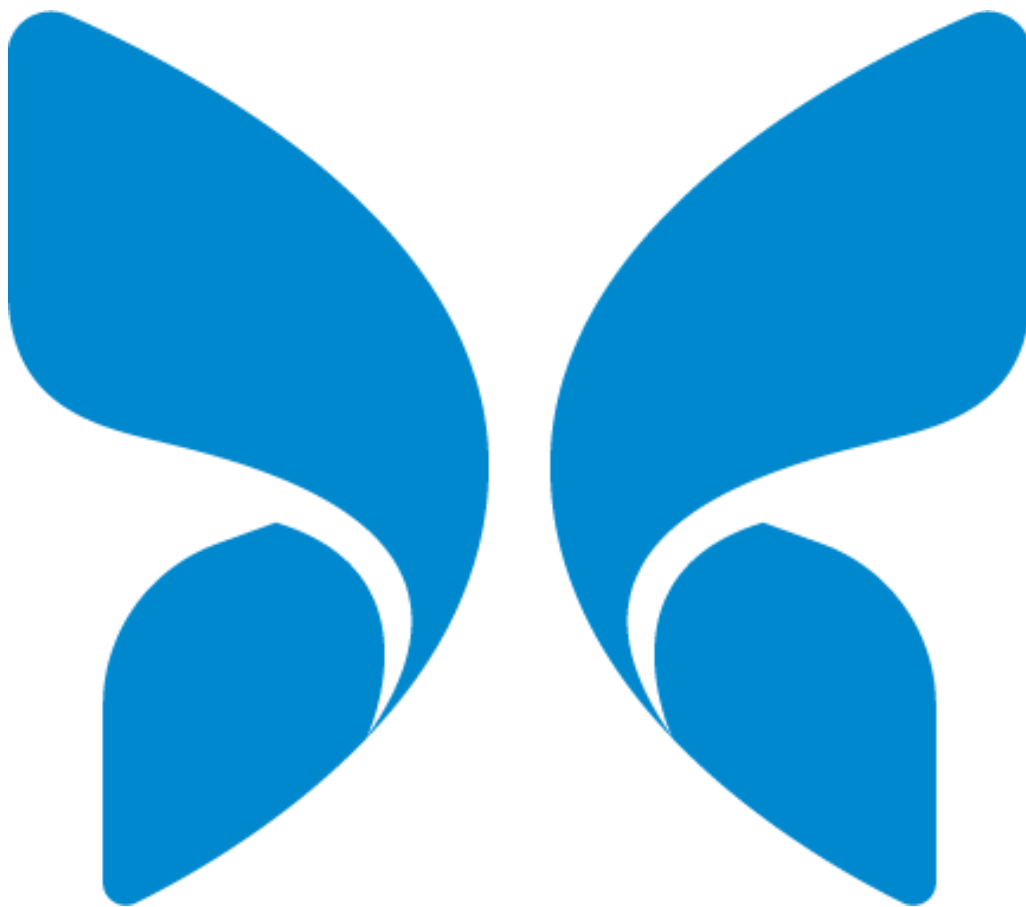


# **Butterfly Cloud DICOM Connector Implementation Guide**

(Intended for use by IT Professionals)



**Integrating the Butterfly Cloud with your existing PACS/VNA or Modality  
Worklist**

## Table of Contents

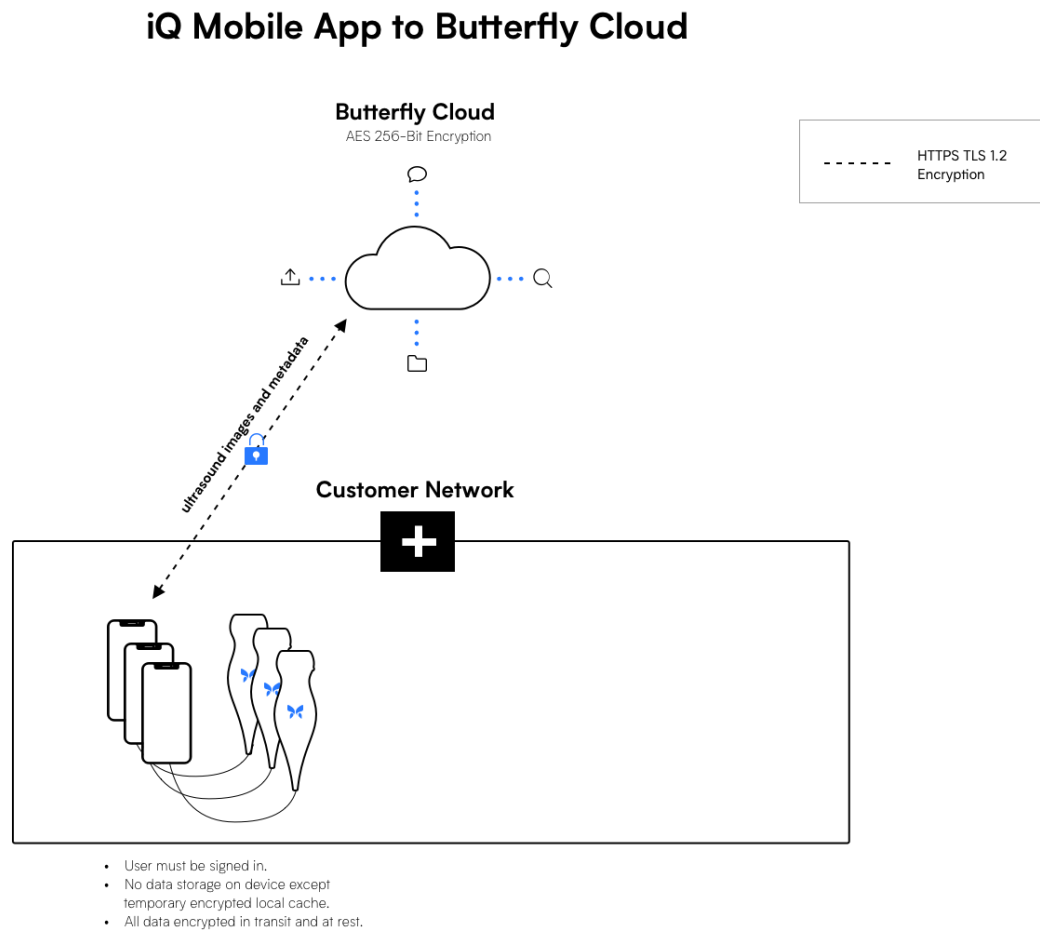
<b>1.0 - Introduction</b>	<b>3</b>
<b>2.0 - Integration Options for Your DICOM Endpoint</b>	<b>5</b>
2.1 - Direct integration via DICOM TLS	5
2.2 - TLS Integration intermediated by a perimeter network (aka DMZ)	6
<b>3.0 - Configuring the Butterfly Cloud to Connect to a DICOM Endpoint</b>	<b>8</b>
3.1 - Accessing DICOM Connections Settings in the Butterfly Cloud	8
3.2 - Adding a PACS/VNA or Modality Worklist	8
3.3 - Naming your PACS/MWL	8
3.4 - SCU - Service Class User	8
3.5 - SCP - Service Class Provider	8
3.6 - Security	9
3.7 - Compression	11
3.8 - Timeout	11
3.9 - Save Secure Configuration and Test	11
<b>4.0 - Associating a PACS to an Archive</b>	<b>11</b>
<b>Appendix A - Digital Certificate Generation Using OpenSSL</b>	<b>13</b>
1.0 - Certificate Generation	15
1.1 - Creating a Private Key	15
1.2 - Creating a Certificate Request file	15
1.3 - Creating a self-signed Certificate	15
1.4 - (optional) Export to .pfx file format for use with Qpath-E	15
<b>Appendix B - F5 Big-IP® TLS Termination Guide for DICOM-TLS Integration</b>	<b>16</b>
1.0 - Import or Generate the SSL Certificate and Key	17
1.1 - Import	17
1.2 - Generate	17
2.0 - Configure the SSL Profile	18
3.0 - Configure the Server Pool	19
4.0 - Configure the Virtual Server	20
5.0 - Setup Complete	21
<b>Appendix C - Configuration of the Citrix ADC (NetScaler) - TLS Termination Device</b>	<b>22</b>
1.0 - Configure a TCP Service	23
2.0 - Configure the SSL Cipher Group (optional)	24
3.0 - Import the SSL Certificate and Key	25
4.0 - Configure the Virtual Server	26
5.0 - Setup Complete	30
6.0 - Certificate Export for Butterfly Cloud (optional)	30

## 1.0 - Introduction

Butterfly Cloud can be connected to your organization's DICOM endpoints using a secure DICOM-TLS connection. Ultrasound studies acquired on any Butterfly iQ in your organization, can be transferred to the Butterfly Cloud, and then forwarded into one or more of your hospital's DICOM storage systems (e.g. Picture Archiving and Communication System (PACS) or Vendor Neutral Archive (VNA)). The Cloud can also connect to a DICOM Modality Worklist (MWL) to minimize the need for manual entry of patient data by users. When configured, members of your organization will be able to use the Worklist to populate the patient data fields prior to uploading studies from the Butterfly iQ App.

Figures 1 and 2 below represent the Butterfly ecosystem both with and without a DICOM endpoint enabled.

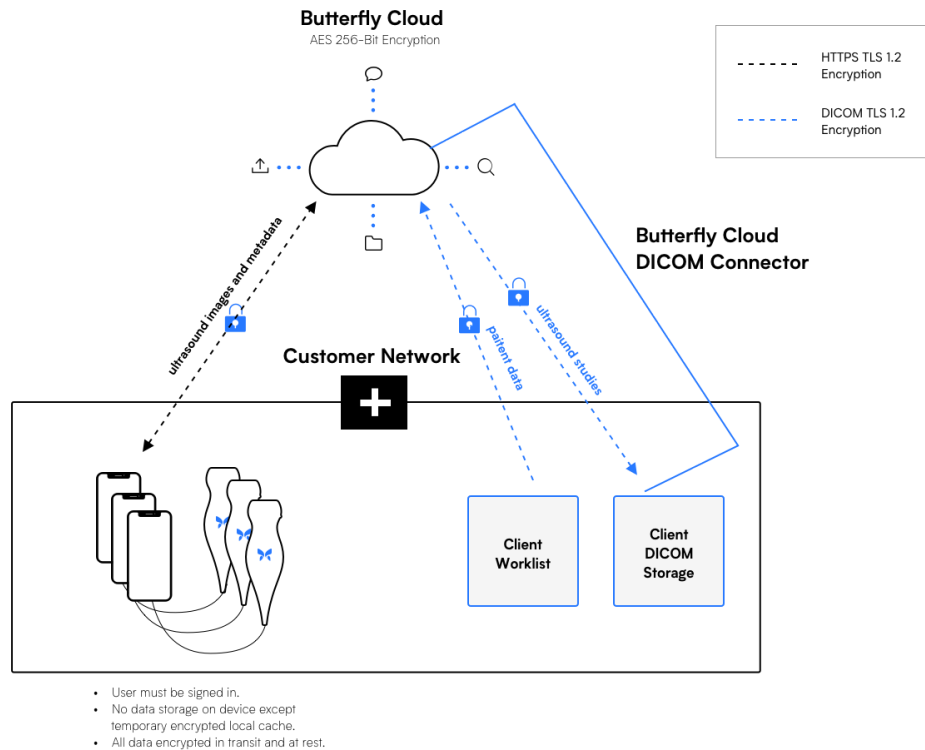
**Figure 1: iQ Mobile App to Butterfly Cloud - No DICOM**



**Figure 1:** The base Butterfly Cloud configuration is designed to support your image storage and collaboration needs without connection to a hospital network. No integration or installation is necessary.

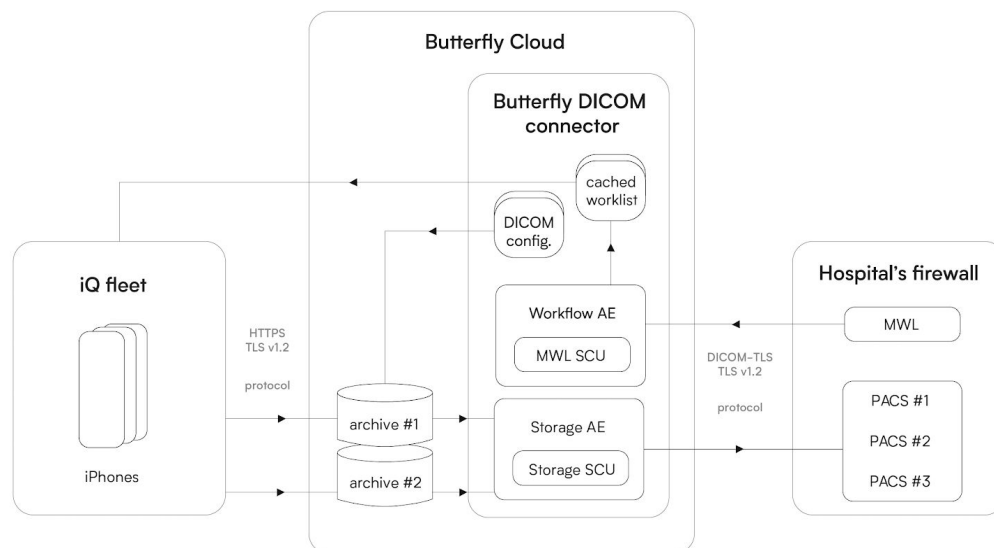
**Figure 2: Butterfly Cloud to PACS/WORKLIST via DICOM TLS**

## Butterfly Cloud to PACS/Worklist via DICOM TLS



**Figure 2:** The Butterfly Cloud can optionally be configured to securely push studies to a PACS and/or query a Modality Worklist (MWL) to Butterfly Cloud organization members through the Butterfly iQ mobile app. Communication is encrypted using TLS 1.2.

**Figure 3 - Butterfly Network Ecosystem (Detailed View)**



**Figure 3:** The Butterfly Cloud facilitates communication with DICOM storage endpoints on an archive by archive basis. This allows users to determine which studies are forwarded to a PACS, and which are not. The Butterfly Cloud supports integration with any number of DICOM storage endpoints, with each archive able to connect to up to three PACS. Only one Modality Worklist can be configured per organization.

## 2.0 - Integration Options for Your DICOM Endpoint

This step by step guide will enable your organization to configure a secure connection between the Butterfly Cloud and your hospital archiving systems and/or Worklist servers.

**IMPORTANT: Butterfly Network recommends that connections are first tested un-encrypted using a development environment with test data. Once connectivity is confirmed, the connection should be moved to a secured, TLS enabled production environment.**

There are two ways to integrate the cloud with your DICOM endpoints. Please proceed to the appropriate section depending on which connection your organization will use.

2.1 - Direct integration via DICOM TLS without DMZ

2.2 - TLS Integration intermediated by a perimeter network (aka DMZ)

**Note: This process is required for each DICOM endpoint that you connect with Butterfly Cloud.**

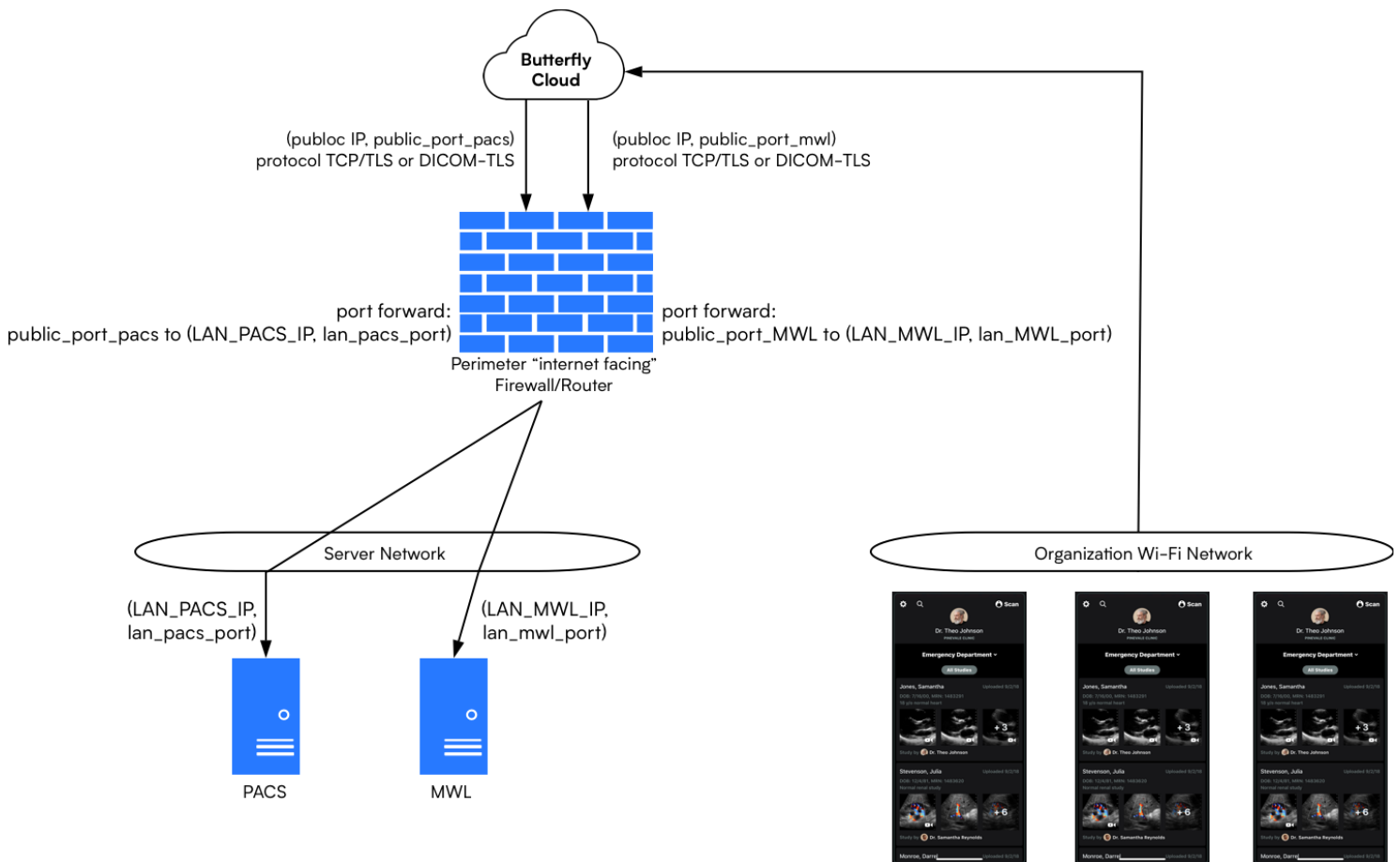
### 2.1 - Direct integration via DICOM TLS

In order to exchange information from the Butterfly Cloud to DICOM endpoints on your network, you will need to whitelist communication with the Butterfly Cloud on your organization's firewall.

**Note: If testing with a development environment perform steps 1-3 for your test DICOM endpoint and then again for your production DICOM endpoint. Each environment will require different ports.**

1. If connecting both a PACS and a Worklist, open two ports on your organization's internet facing firewall. The first port will allow traffic between the Butterfly Cloud storage Service Class User (SCU) and the Storage Service Class Provider (SCP), which is generally your organization's PACS. If connecting a Worklist, the second port will allow communication between the Butterfly Cloud Worklist SCU to the Worklist SCP provided by your organization's PACS.
  - a. The ports used can be selected by your organization. Common ports for secured DICOM communications are 2761 and 2762, but there is no requirement to use these. Please write down the ports opened. You will need this information later when using the Butterfly Cloud DICOM Connections panel.
  - b. Both ports should be authorized to allow inbound and outbound traffic from the Butterfly Cloud's IP address: **34.203.166.92.**
2. Configure your internet facing router to port forward incoming DICOM data from the previously opened ports to the IP and port of the DICOM SCPs (PACS and Worklist respectively).
  - a. Your PACS or Worklist will have a configured port and static IP address for you to use. This is typically managed by the radiology IT team supporting DICOM endpoints in your organization and is created during initial setup of those devices.

**Figure 4 - PACS and MWL Configuration without DMZ**



**Figure 4:** Connecting the Butterfly Cloud to your network's DICOM endpoints requires port forwarding data from the Butterfly Cloud to the PACS or Worklist installed in your organization.

3. Declare and authorize, on the storage SCP (PACS), MWL SCP, or both, a new Calling Application Entity Title (AET) for the Butterfly Cloud's SCU.
  - a. This value should be all uppercase, with no spaces and up to 16 characters. This name is the one that your DICOM endpoint will recognize the Butterfly Cloud with. For example, you may choose to identify the Butterfly Cloud as **BUTTERFLY**. Please write down the AETs declared. **Note: This information will be needed again, below, in step 7 of the section titled: Configuring the Butterfly Cloud to Connect to a DICOM Endpoint.**

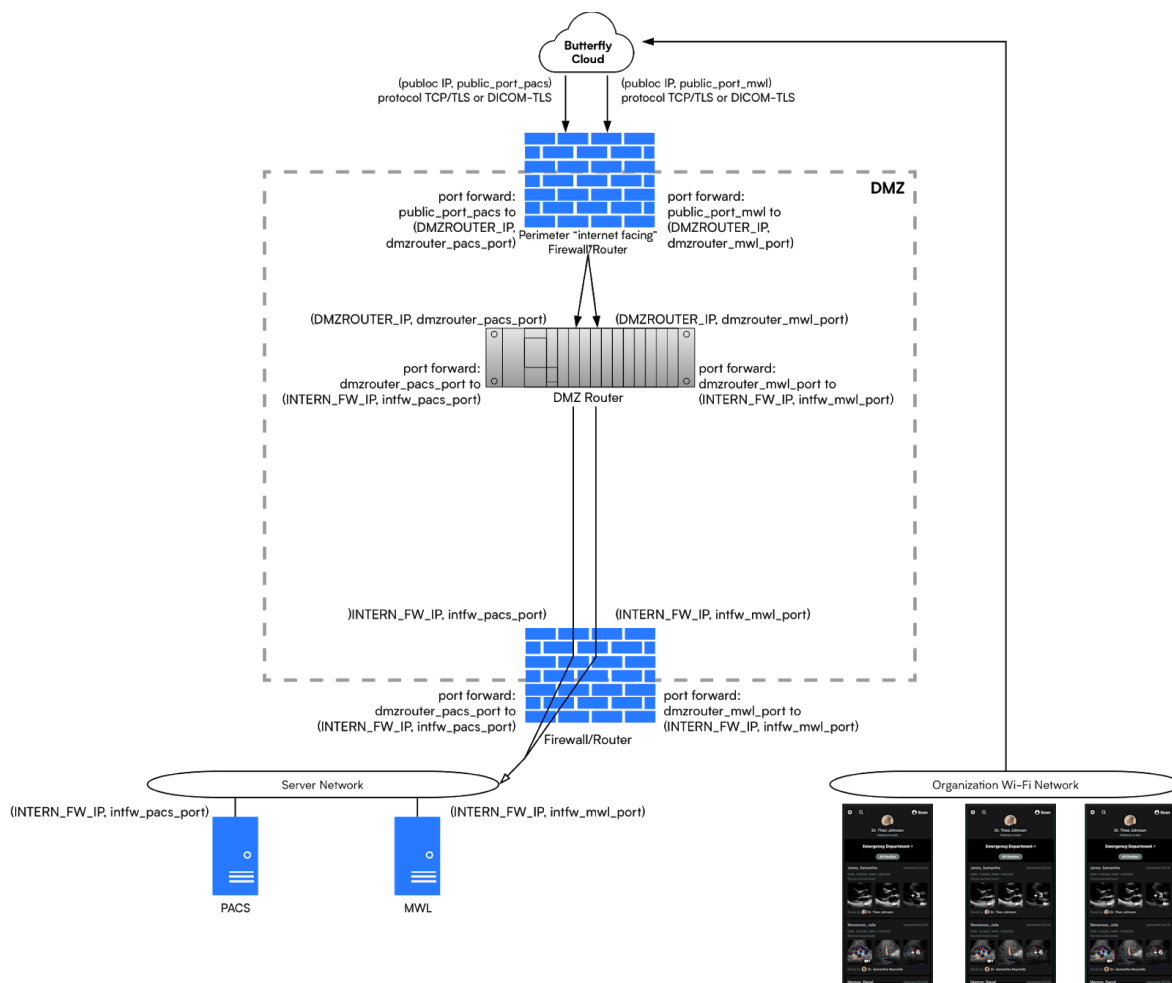
## 2.2 - TLS Integration intermediated by a perimeter network (aka DMZ)

If your organization prefers to route the traffic through a DMZ, then the internet-facing firewall/router must be configured to whitelist communication with the Butterfly Cloud. This externally facing router must then port forward data to a DMZ router. The DMZ router is a TLS termination or a DICOM router. A TLS termination (ie Citrix NetScaler) decrypts the TLS encrypted DICOM traffic and forwards the unencrypted, regular DICOM traffic to the DICOM endpoint via the internal network router. A DICOM router is a specific software component that also may decrypt TLS and forwards DICOM data in either DICOM or DICOM-TLS to your DICOM endpoint via the internal router. Your DMZ router must then port forward the data to your internal router. The internal router will then connect with the DICOM endpoints.

**Note: If testing with a development environment perform steps 1-4 for your test DICOM endpoint and then again for your production DICOM endpoint. Each environment will require different ports.**

1. If connecting both a PACS and a Worklist, open two ports on your organization's internet facing firewall. The first port will authorize traffic between the storage Service Class User (Butterfly Network) (SCU) and the Service Class Provider (SCP). If connecting a Worklist, the second port will allow communication between the Worklist SCU and the Worklist SCP.
  - a. The standard ports for secured DICOM communications are 2761 and 2762, but there is no requirement to use these. Please write down the ports opened. You will need this information later when using the Butterfly Cloud DICOM Connections panel.
  - b. Both ports should be authorized to allow inbound and outbound traffic from the Butterfly Cloud's IP address: **34.203.166.92**.
2. Configure your internet facing router to port forward from the previously opened ports to your DMZ router.
3. Configure your DMZ router to port forward these 2 ports to your internal firewall. Configure your internal facing router to direct incoming DICOM data (port forward) from the DMZ router to the IP address and port numbers of the DICOM SCPs (PACS and/or Worklist respectively). **Note: For additional information on configuring a Citrix NetScaler please see the Appendix of this document.**
  - a. Your PACS or Worklist will have a configured port and static IP address for you to use. This is typically managed by the radiology IT supporting DICOM endpoints and created during initial setup of those devices.

**Figure 5 - PACS and MWL Configuration through a DMZ**



**Figure 5:** When using a DMZ, the Butterfly Cloud connects with the internet facing router of the DMZ. The internet facing router of the DMZ will then transmit data to a DMZ router (ex: a Citrix NetScaler, or DICOM UltraRad Gateway), which is then configured to communicate with the DICOM endpoints inside the internal hospital network.

4. Declare and authorize, on the storage SCP (PACS), MWL SCP, or both, a new calling application entity title (AET) for the Butterfly's Cloud SCU.
  - a. This value should be all uppercase, with no spaces and up to 16 characters. This name is the one that your DICOM endpoint will recognize the Butterfly Cloud with. For example, you may choose to identify the Butterfly Cloud as **BUTTERFLY**. Please write down the AETs declared. **Note: This information will be needed again, below, in step 7 of the section titled: Configuring the Butterfly Cloud to Connect to a DICOM Endpoint.**

### 3.0 - Configuring the Butterfly Cloud to Connect to a DICOM Endpoint

*Note: In order to test your DICOM connections, a Butterfly iQ probe and mobile phone are required.*

*Note: If you are first testing your connection in a development environment, the steps in sections 3.1 to 3.6.3 should first be completed with the settings for your development environment and then revised to match the production settings once you have confirmed successful connectivity to your DICOM endpoint.*

#### 3.1 - Accessing DICOM Connections Settings in the Butterfly Cloud

1. Navigate to Butterfly Cloud (<https://cloud.butterflynetwork.com>) from a supported web browser. Butterfly Cloud always supports the most recent two versions of Chrome, Edge, Firefox, and Safari.
2. Log in to Butterfly Cloud using your Butterfly Network credentials.
3. From the landing page, navigate to the "DICOM" panel.
  - a. The link to the DICOM panel can be found in the top right menu of the screen after clicking on your name.
  - b. If you do not see "DICOM" please contact one of your organization's admins to request admin access. To determine who administers your Butterfly Cloud, review the members list in the dropdown menu revealed by clicking on your name at the top right of the screen.
  - c. Please contact [support@butterflynetwork.com](mailto:support@butterflynetwork.com) if you are already an admin and cannot access the DICOM Connections panel.

#### 3.2 - Adding a PACS/VNA or Modality Worklist

4. From inside the DICOM Connections panel, select whether you will be adding a PACS/VNA, or MWL. The information required to configure them is identical except for worklist filtering.
5. Click "Add" next to either PACS or MWL and the configuration settings screen will open.

#### 3.3 - Naming your PACS/MWL

6. Into the field "Name," enter the name of the PACS or MWL as it should be displayed within your Butterfly Cloud.
  - a. "Name" can be of any length, contain capital and lowercase letters, numbers and special characters and spaces.

#### 3.4 - SCU - Service Class User

7. Enter the Butterfly Cloud SCU AET which you declared above into the field "Calling AET."
  - a. This is the name under which the Butterfly Cloud will communicate with your internal DICOM systems (PACS and MWLs). **Note: You declared this field in step 3 of the previous sections of this manual.**
  - b. *Reminder: Your SCU Calling AET must contain all capital letters and contain no spaces.*

#### 3.5 - SCP - Service Class Provider

8. In the "AET" field, enter the AET of the PACS (or MWL) to which you would like the Butterfly Cloud to connect.
  - a. This information can be found within the settings menu of your PACS or Worklist server.
  - b. This value must be in capital letters and contain no spaces
9. Into the field "Host," enter the internet facing (public) IP address of your organization that will be used to connect the Butterfly Cloud to your hospital network.



- a. This value should be known by your IT Security or Network Administrator, or can be found within the settings of the router enabling your internet facing firewall.
10. Enter the port number of the PACS or MWL (previously configured) designated for connectivity with the Butterfly Cloud into the field "Port."
  - a. This is one of the ports opened in step 1 of the section titled: Preparing your Organization for a DICOM connection.
11. Select the timezone of the location of your SCP into the field timezone.
12. For USA-based PACS or MWL use the default encoding option (ISO IR100). Please contact your PACS/MWL service provider for encoding information for non USA-based PACS.

### 3.6 - Security

**Note: For connecting QPath Classic to the Butterfly Cloud, set the "TLS" field to "Secured Mode for QPath Classic" and SCU authentication to "Anonymous." Then proceed to section 3.7, Compression.**

**Note: For QPath E, an SCP certificate is required, but SCU authentication is not needed. Follow the steps below for SCP, set SCU authentication to "Anonymous".**

#### 3.6.1 - Confirming Connectivity without TLS Enabled

**Note: Only use the TLS Secure connection when you are testing your DICOM endpoint in a production environment. If you have confirmed connectivity in your development environment, and are ready for patient data in production, skip these steps and proceed to step 51 below.**

The Butterfly Cloud enables customers to test DICOM connectivity without TLS authentication activated. All functions of a DICOM connection can be performed such as pushing images, or reading Modality Worklists, however, only test patient data should be used during non-TLS testing. Once functionality is confirmed, TLS should be turned on.

13. Set TLS to "Inactive." An acknowledgement of an unsecured connection will appear to notify users that no PHI should be sent over the connection until TLS is enabled.
14. Settings for Compression (section 3.7) and Timeout (section 3.8) can be left in their default states
15. Click "Save Configuration."
16. Click the back arrow just below the search bar to return to the DICOM connections panel. You should see the word "Unsecured" next to your connection. **Note: This will change to "Secured" once you have enabled TLS.**
17. To test the connection, click "Echo" for the PACS or MWL that was just added.
18. Upon completion, the results will show automatically. If you would like to echo again click "Echo" in the modal. All tests will show "Accepted" and the "Errors" section of the report will be blank.

**Please use steps 19-40 to test PACS functionality and steps 40-50 for Worklist functionality prior to securing your connection.**

#### 3.6.2 - Testing End to End PACS/VNA Send Functionality without TLS

The following steps will be used to test actual DICOM image transfer if you are configuring a PACS/VNA system.

19. To ensure that no data from existing archives are uploaded to an unsecured PACS system, create a test archive by clicking the word "Create" in the top left quadrant of the Butterfly Cloud.
  - a. Create a unique title for the test archive and click "Create." You will be brought to the empty archive.
20. Click "Archive Settings" in the top right quadrant of the screen showing your newly created, empty archive.
21. Select your newly configured PACS system from the dropdown menu.
22. Return to the empty archive by clicking the left arrow next to the word "Archive Settings."
23. Download the Butterfly iQ application from the Apple App Store using your iPhone.
24. Log in to the app with your Butterfly Cloud credentials that were previously used to access the cloud from your desktop browser.
  - a. If this is your first time accessing the application, you may be asked to walk through a tutorial on how to use the application. Enable push notifications.

25. The first screen that you will land on is the scanning screen.
26. Connect a Butterfly iQ probe and ensure that an image can be seen, or if you do not have a probe handy go to the settings menu and click “DICOM Connections” and “Create Test Images.” This will generate real images for testing and automatically drop them in the camera roll. If you use the test option feature please skip to 29 after backing out of the settings menu.
27. Swipe your finger from left to right on the screen to increase the gain. (This will just make the image very noisy, which will be ideal for testing purposes.
28. Click the snow flake at the bottom of the screen to freeze the image.
29. Click the camera icon to add the frozen photo to the “exam reel.” A “1” will be now be seen at the top right of the screen.
30. Click on the “exam reel” by selecting the box at the top right around the “1”.
31. Tap “Associate a Patient.”
32. Manually enter test patient information.
33. Tap “Save” in the top right-hand corner of the screen.
34. Click “Add Notes”
35. Add a test note if you desire.
36. Tap “Save” in the top right-hand corner of the screen.
37. Tap “Save” in the top right-hand corner of the screen again to be presented with available archives for upload.
38. Select the new archive that you created and associated with the PACS in steps 18 to 20. You should see the word DICOM next to that archive in the list.
39. Tap “Confirm” in the top right-hand corner of the screen.
40. In a few moments (up to 5 minutes, but likely much faster) confirm that the image and associated metadata can be found on the PACS.

### 3.6.3 - Testing Worklist Functionality Without TLS

**Note: It is critical to test Worklists with a development system, so that no patient data is shared over an unsecured network.**

41. Download the Butterfly iQ application from the Apple App Store using your iPhone.
42. Log in to the app with your Butterfly Cloud credentials that were previously used to access the cloud from your desktop browser.
  - a. If this is your first time accessing the application, you may be asked to walk through a tutorial on how to use the application. If prompted, choose to enable or disable push notifications.
43. The first screen that you will land on is the scanning screen.
44. Connect a Butterfly iQ probe and ensure that an image can be seen.
45. Swipe your finger from left to right on the screen to increase the gain, so that a bright image can be seen.
46. Click the snow flake at the bottom of the screen to freeze the image.
47. Click the camera icon to add the frozen photo to the “exam reel.” A number “1” will be now be seen at the top right of the screen.
48. Click on the “exam reel” by selecting the box at the top right under the number “1”.
49. Tap “Associate a Patient.”
50. Tap “Add from Worklist.” **Note: If the Worklist is not configured properly you will not see items on the Worklist and will receive an error message when “Add from Worklist” is tapped. If no Worklist is set up “Add from Worklist” will not be visible.**
51. Select the fake patient from the Worklist to populate the patient info on your test study with.

### 3.6.4 - Securing Your TLS Secure Connection on the Butterfly Cloud

**Note: Only use the TLS Secure connection when you are ready to connect to your production DICOM endpoint. If you are testing in your development environment, please skip to section 3.7 below.**

Non-TLS connections should only be used for testing purposes. Prior to sending patient data between the Butterfly Cloud and your organization’s DICOM systems, please enable TLS. Secure DICOM-TLS connections require the generation and upload of a public digital certificate from your organization to the Butterfly Cloud. In some instances, your DICOM systems may also require an authenticated SCU certificate. This requires that you download a certificate from the Butterfly Cloud which you’ll need to upload to your organization’s

DICOM endpoint. The configuration of the system which terminates the TLS connection will determine whether or not this additional certificate exchange is required.

52. From the DICOM Connections panel click “Edit” next to the PACS or MWL that is being configured and was previously tested with an unsecured connection in a development environment.
53. Update the configuration settings previously entered in steps 7 to 10 for the production environment.
54. Set TLS to “Active.”
55. In the SCP field, upload your public certificate generated by your hospital’s IT Security team by pressing the “Upload” button. The private certificate will stay with your DICOM endpoint. **Note: Butterfly Cloud supports .pem and .cer (Base64 encoded ASCII files, but not DER files) file types. If the certificate is opened in a text editor, the first line will read ---Begin Certificate---**. For information on generating private and public keys please see this document’s appendix.
56. If your configuration requires an authenticated SCU connection, please set the SCU Security field to “Authenticated.” If not, set SCU to “Anonymous.” Note: **A connection will be fully encrypted with just the exchange of TLS certificates and SCU configuration is an added level of security.**
  - a. If you have selected “Authenticated,” click “Download Certificate” and upload the certificate from the Butterfly Cloud to the administration panel of the system where the TLS connection terminates. **Note: If you do not see Download Certificate you may need to save your settings and then scroll back up in order to enable downloading of the certificate.**

### 3.7 - Compression

57. For the most common image compression please use the settings of “JPEG Lossless” or “JPEG Lossy” for both the “Image” and “Loop” fields. If your organization chooses to use different compression settings, please modify these as appropriate.
58. To save storage you may use the Monochrome Mode option. If your Review WorkStations supports the display of Grayscale JPEG images, you can use the option “B-Mode Only” to encode Grayscale images into Grayscale files, and images containing Color Doppler into color. If you are not sure, you may leave the default value “Never”.

### 3.8 - Timeout

59. Butterfly Network recommends using the default timeout settings pre-populated in the Butterfly Cloud for the “ACSE,” “DIMSE” and “Connection” fields. This value is 300 seconds for each. If your organization or DICOM endpoints use other settings, please enter these in the appropriate fields.
  - a. ACSE: timeout in seconds of the association negotiation.
  - b. DIMSE: timeout in seconds for receiving data.
  - c. Connection: timeout in seconds when connecting to SCPs.

### 3.9 - Save Secure Configuration and Test

60. After completing all of the fields in the list please click “Save Configuration.”
61. Click the back arrow just below the search bar to return to the DICOM Connections panel.
62. “Secured” should now be displayed next to your PACS or Worklist signifying that TLS is enabled.
63. Click “Echo” to test your newly secured DICOM system.
64. Click “View Results” and make sure that “Accepted” and no errors are still shown.

## 4.0 - Associating a PACS to an Archive

As performed above in the Butterfly Cloud, organizations can select which archives upload to a PACS and even which PACS to upload if there are multiple configured. With a PACS successfully added, perform the following steps: **Note: The PACS associated with the test archive will still be present. Skip steps 65-67 if you would like to continue using that archive as your main PACS forwarding archive. If you wish to use a different archive from the one configured and assigned during the test please follow the steps below.**

65. Select, an archive from the left-hand side of the screen that you would like to associate with a PACS.

- a. If you do not want to associate any of your existing archives with a PACS please create a new archive by clicking “Create” and then naming your Archive.
  - b. You will be brought into your new Archive.
66. Click “Archive Settings” in the top right quadrant of the screen. **Note: PACS forwarding configurations can be changed at any time, but the user must be an organization admin to do so.**
67. Select the newly configured PACS system from the dropdown menu for “PACS 1.”
68. Repeat this process for multiple PACS and archives.
69. Begin using your Butterfly Cloud with PACS integration.

**Note: If you have any questions regarding configuring the Butterfly Cloud to work with your organization's DICOM endpoints please reach out to [support@butterflynetwork.com](mailto:support@butterflynetwork.com).**

## Appendix A - Digital Certificate Generation Using OpenSSL

### How to use these Instructions:

These instructions will guide the user in the use of OpenSSL to create a self-signed digital certificate. This will create a private and public key pair. The digital certificates are used as keys for encrypting DICOM communications using TLS 1.2, with the private key being stored on the DICOM SCP-side of the connection.

- Instructions assume that OpenSSL will be installed on a current generation Windows-based OS.
- This is the most typical deployment model.
- The public and private digital certificates are kept on the TLS termination point (e.g. F5 Big-IP or Netscaler).
- The public certificate (only) is uploaded to the Butterfly Cloud for creating the TLS connection.

### Introduction - What is a Digital Certificate?

When a computer connects to a server, communication begins between the computer and the server. Typically, this communication is unsecured, meaning any third party could potentially see what data is being exchanged. In some instances, such as with personal health information (PHI), allowing data to be transmitted unsecured is not safe.

An SSL/TLS certificate serves two main functions. The first is that it grants permissions to use encrypted communication. The second is that it also authenticates the identity of the certificate's holder.

A certificate for a TLS encryption is generated by a software (ie KeyChain on MacOS, Certificate Services MMC Snap-in on Windows and OpenSSL on all platforms). Certificate generation is required to setup the connection between the Butterfly Cloud and an organization's PACS and MWL servers.

The following steps will guide you through certificate generation using a tool called OpenSSL if your organization does not already have a method for producing digital certificates.

### Prerequisites

- Download and extract OpenSSL binaries: [https://indy.fulgan.com/SSL/openssl-1.0.2r-x64\\_86-win64.zip](https://indy.fulgan.com/SSL/openssl-1.0.2r-x64_86-win64.zip)
- Extract zip file to path **C:\openssl**
- Create text file **openssl.cnf** in **C:\openssl**
- Paste all content below into openssl.cnf and save the file.
  - Note - You can update the **highlighted** values now to match your information; otherwise you will be prompted to input this information when generating the Certificate Request.

```

[ req ]
default_bits = 2048
default_keyfile = key.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
x509_extensions = v3_ca

dirstring_type = nobmp

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US
countryName_min = 2
countryName_max = 2

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Connecticut

localityName = Locality Name (eg, city)
localityName_default = Guilford

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Butterfly Network Inc.

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Medical Informatics

commonName = Common Name (eg, YOUR name)
commonName_default = John Smith
commonName_max = 64

emailAddress = Email Address
emailAddress_default = support@butterflynetwork.com
emailAddress_max = 40

[ req_attributes ]
#challengePassword = A challenge password
#challengePassword_min = 4
#challengePassword_max = 20

[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints = CA:true

```

## 1.0 - Certificate Generation

### 1.1 - Creating a Private Key

This will set the path to the Openssl config file and create the 2048 bit private key of the digital certificate in a file called SCP\_key.pem

- A. Open windows [Administrator] command prompt to the OpenSSL folder (C:\openssl).
- B. Run command:
  - **set OPENSSL\_CONF=C:\openssl\openssl.cnf**
  - **openssl genrsa -out SCP\_key.pem 2048**

### 1.2 - Creating a Certificate Request file

This will create the certificate request and output it to a file called SCP\_req.pem

- A. Open windows command prompt to the OpenSSL folder (C:\openssl).
- B. Run command: **openssl req -new -key SCP\_key.pem -out SCP\_req.pem**
- C. Confirm or update default values for the certificate request.

### 1.3 - Creating a self-signed Certificate

This will create the public key of the digital certificate and output it to a file called SCP\_cert.pem

The certificate will be valid for 3650 days - you may edit this value as needed.

- A. Open windows command prompt to the OpenSSL folder (C:\openssl).
- B. Run command: **openssl x509 -req -in SCP\_req.pem -days 3650 -signkey SCP\_key.pem -out SCP\_cert.pem**

### 1.4 - (optional) Export to .pfx file format for use with Qpath-E

This will create a binary file that combines the private key and certificate. This file format is required for use with Telexy Qpath-E.

- A. Open windows command prompt to the OpenSSL folder (C:\openssl).
- B. Run command: **openssl pkcs12 -export -out Qpath-certificate.pfx -inkey SCP\_key.pem -in SCP\_cert.pem**
- C. Provide password. This will be needed when importing the certificate by Telexy for use with Qpath-E.

To implement TLS, follow the instructions for TLS termination for your specific situation.

- Import the key pair (**SCP\_key.pem, and SCP\_cert.pem**) to your TLS termination solution (e.g. PACS, F5 Big-IP or Netscaler).
- Upload the Public key (**SCP\_cert.pem**) to the Butterfly Cloud DICOM Configuration for your connection.

## Appendix B - F5 Big-IP® TLS Termination Guide for DICOM-TLS Integration

### How to use these Instructions:

The purpose of this Guide is to assist an Administrator of an F5 Networks Big-IP Load Balancer to configure SSL/TLS termination and assumes prior experience with management of the device. The SSL/TLS termination is to be used with the Butterfly Network DICOM-TLS feature that allows for encrypted DICOM communications between the Butterfly Cloud and the Customers' DICOM archive.

#### Trademark:

F5 Big-IP® is a registered trademark of F5 Networks Inc.

#### Version Information:

This Guide refers to configuration procedures as per F5 Networks BIG-IP 13.1.1 Build 0.0.4 Final. The process will be similar on F5 Big-IP 11.0.0 and later.

### Introduction

SSL/TLS termination (offloading) relieves an Application Server or Web Server of the processing that is normally required to encrypt and/or decrypt traffic sent via TLS or SSL. Note that the SSL standard has been replaced by TLS as the encryption mechanism for most web-based communications. Any use of "SSL" in this guide is strictly for convenience and is, in fact, referring to TLS.

The processing is offloaded to a separate device designed specifically to perform TLS termination. When a DICOM server system is not capable of receiving TLS-encrypted DICOM data, the TLS termination capability of an F5 Networks BIG-IP load balancer device can be used to decrypt/encrypt the data.

The F5 Big-IP provides 2 ways in which SSL/TLS is processed. These are:

- Client SSL – F5 decrypts the encrypted traffic inbound from the client.
- Server SSL – Traffic is re-encrypted by the F5 then routed onto the backend servers.

This guide will focus on Client SSL exclusively.

### Prerequisites

In most environments, the F5 Load Balancer is located in the Demilitarized Zone (DMZ) portion of the network. In order for the device to be able to process the DICOM-TLS traffic; the Internet-facing firewall must be configured to permit traffic on the port(s) that the F5 Big-IP has been configured to listen on.

- Note external (Internet-facing) IP address of the firewall or F5 Big-IP.
- For the purposes of this document, we will be creating a TLS termination, Virtual Server on the F5 Big-IP.
  - A DICOM Store virtual server will be configured to use port 2762.
  - A DICOM Worklist virtual server will be configured to use port 2761.
- Ensure that the external firewall permits TCP traffic from the Internet to the above ports used by the Virtual Servers.
- If you will not be using the F5 Big-IP to generate a self-signed digital certificate, then ensure you have the Key and Certificate files in .pem format generated by OpenSSL or a certificate authority.
  - A public certificate is not required for the DICOM-TLS encryption. We are only using the certificate for encryption/decryption, not for end-point trust and validation.
  - For instructions on certificate generation using OpenSSL please refer to the document Using OpenSSL to generate a self-signed Digital Certificate for TLS Encryption
- Login to F5 Networks Big-IP GUI.



### Configuring Client SSL consists of 4 steps:

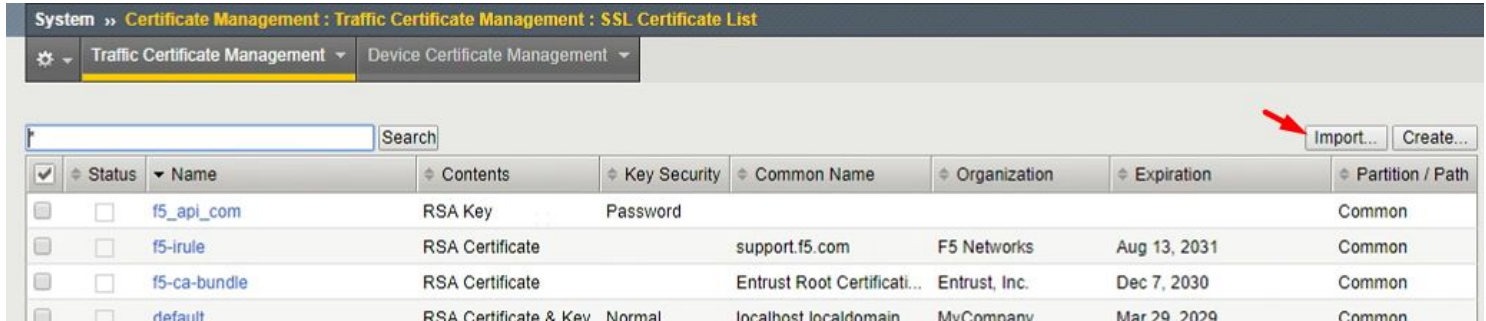
1. Import or generate the SSL Certificate and Key.
2. Configure the client SSL-client profile.
3. Configure the Server Pool.
4. Configure the Virtual Server.

## 1.0 - Import or Generate the SSL Certificate and Key

### 1.1 - Import

1.1.1 - Go to 'System » Certificate Management: Traffic Certificate Management: SSL Certificate List'.

1.1.2 - Select Import.



The screenshot shows the 'System » Certificate Management : Traffic Certificate Management : SSL Certificate List' page. The 'Traffic Certificate Management' tab is selected. A search bar is at the top left. On the top right, there are 'Import...' and 'Create...' buttons. A red arrow points to the 'Import...' button. Below the buttons is a table with columns: Status, Name, Contents, Key Security, Common Name, Organization, Expiration, and Partition / Path.

✓	⚙	Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>	<input type="checkbox"/>		f5_api_com	RSA Key	Password				Common
<input type="checkbox"/>	<input type="checkbox"/>		f5-irule	RSA Certificate		support.f5.com	F5 Networks	Aug 13, 2031	Common
<input type="checkbox"/>	<input type="checkbox"/>		f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust, Inc.	Dec 7, 2030	Common
<input type="checkbox"/>	<input type="checkbox"/>		default	RSA Certificate & Key	Normal	localhost.localdomain	MvCompanv	Mar 29, 2029	Common

1.1.3 - Select 'Certificate' Import Type.

1.1.4 - Enter the Certificate Name (e.g. Butterfly-Network-Cert).

1.1.5 - Upload the certificate within the Certificate Source section\*.

\* Note: Certificates should be either Base-64 encoded or PEM format.

1.1.6 - Click Import.

1.1.7 - Repeat the process (above) to import the Key.

1.1.8 - Select 'Key' Import Type.

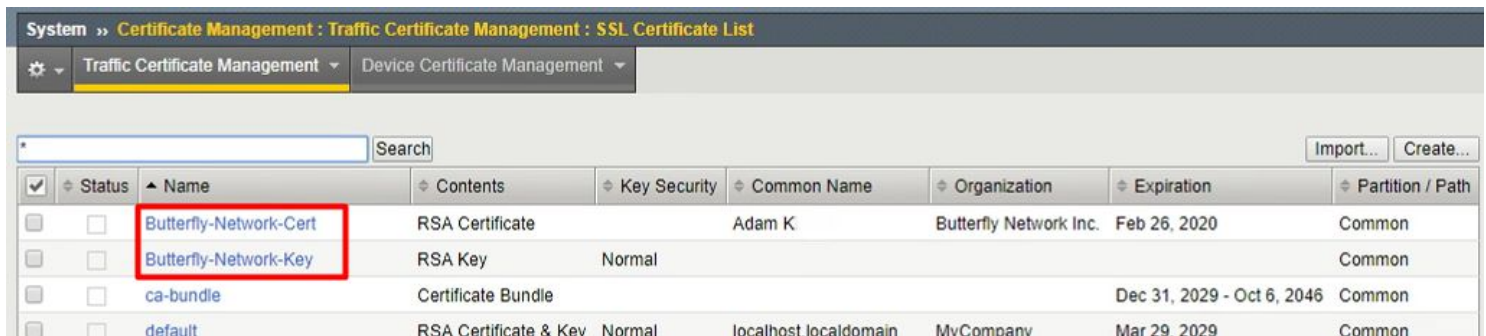
1.1.9 - Enter the Key Name (e.g. Butterfly-Network-Key).

1.1.10 - Security Type should be defaulted to 'Normal'.

1.1.11 - Upload the key within the Key Source section.

1.1.12 - Click Import.

1.1.13 - SSL Certificate List should appear similar to below, when complete.



The screenshot shows the same 'SSL Certificate List' page as before, but now with two new entries at the top: 'Butterfly-Network-Cert' and 'Butterfly-Network-Key'. These two entries are highlighted with a red box. The 'Butterfly-Network-Cert' entry has a status of 'Certificate' and a common name of 'Adam K'. The 'Butterfly-Network-Key' entry has a status of 'Key' and a security type of 'Normal'.

✓	⚙	Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>	<input type="checkbox"/>		Butterfly-Network-Cert	RSA Certificate		Adam K	Butterfly Network Inc.	Feb 26, 2020	Common
<input type="checkbox"/>	<input type="checkbox"/>		Butterfly-Network-Key	RSA Key	Normal				Common
<input type="checkbox"/>	<input type="checkbox"/>		ca-bundle	Certificate Bundle				Dec 31, 2029 - Oct 6, 2046	Common
<input type="checkbox"/>	<input type="checkbox"/>		default	RSA Certificate & Key	Normal	localhost.localdomain	MvCompanv	Mar 29, 2029	Common

### 1.2 - Generate

**Note - if you have already imported a Certificate then generating one is not needed - skip to section 2 - Configure the SSL Profile.**

1.2.1 - Go to 'System » Certificate Management: Traffic Certificate Management: SSL Certificate List'.

1.2.2 - Select Create.

1.2.3 - In the General Properties section enter the Name (e.g. Butterfly-Network-Cert-2) and then complete the Certificate Properties fields.

1.2.3.1 - Issuer → Self.

1.2.3.2 - Common Name → (e.g. Butterfly-Network-Cert-2)

1.2.3.3 - Replace values with those specific to your organization.

1.2.3.4 - Increase Certificate Lifetime to **3650 days** or a value based on your Organization's policies.

1.2.3.5 - Key Properties → RSA and 2048 bits.

**System » Certificate Management : Traffic Certificate Management : SSL Certificate List » New SSL Certificate...**

**General Properties**

Name

**Certificate Properties**

Issuer

Common Name

Division

Organization

Locality

State Or Province

Country

E-mail Address

Lifetime  days

Subject Alternative Name

**Key Properties**

Key Type

Size  bits

1.2.4 - Click Finished

## 2.0 - Configure the SSL Profile

Next, we will need to configure the SSL Client profile.

2.1 - Go to 'Local Traffic » Profiles: SSL: Client'

2.2 - Select Create.

Local Traffic » Profiles : SSL : Client

Services Content Persistence Protocol SSL Authentication Message Routing Other

Search Create...

Name	Application	Parent Profile	Partition / Path
<input type="checkbox"/> wom-default-clientssl		clientssl	Common
<input type="checkbox"/> splitsession-default-clientssl		clientssl	Common
<input type="checkbox"/> crypto-server-default-clientssl		clientssl	Common
<input type="checkbox"/> clientssl-secure		clientssl	Common

2.3 - Within the General Properties enter the Name (e.g. Butterfly-TLS) and select the Parent Profile as **clientssl** and check mark **Custom**.

2.4 - Within the Configuration section select the Certificate and Key.

2.5 - Click Finished.

### 3.0 - Configure the Server Pool

This step defines the server(s) to which the Big-IP Virtual Server (Step 4) will send traffic after it has terminated TLS. In situations where you have one (1) DICOM destination (most customer sites) then you will have a Pool with 1 member server only.

3.1 - Go to 'Local Traffic » Pools: Pool List'.

3.2 - Select Create.

Local Traffic » Pools : Pool List » New Pool...

Configuration: Basic

Name: DICOM-Store-Server-Pool

Description:

Health Monitors:

Active: /Common tcp

Available: https\_443, https\_head\_f5, inband, tcp\_half\_open, udp

Resources:

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members:

Node Name: PACS\_INFINITT (Optional)

Address: 192.168.2.30

Service Port: 104

Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
PACS_INFINITT	192.168.2.30	104		0

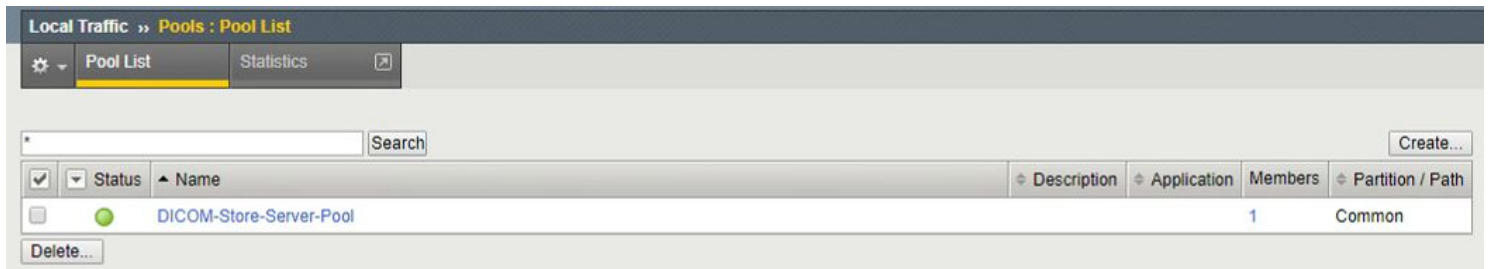
Edit Delete

Cancel Repeat Finished

3.3 - Within the Configuration enter the Name (e.g. DICOM-Store-Server-Pool) and select the Health Monitors (e.g. TCP).

3.4 - In Resources - Add member servers to the Pool as required (repeat steps 2-3 as indicated).

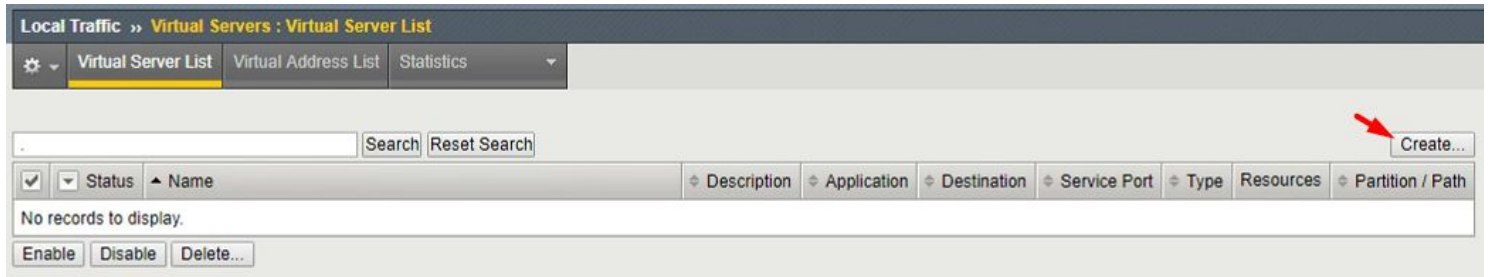
3.5 - Click Finished.



## 4.0 - Configure the Virtual Server

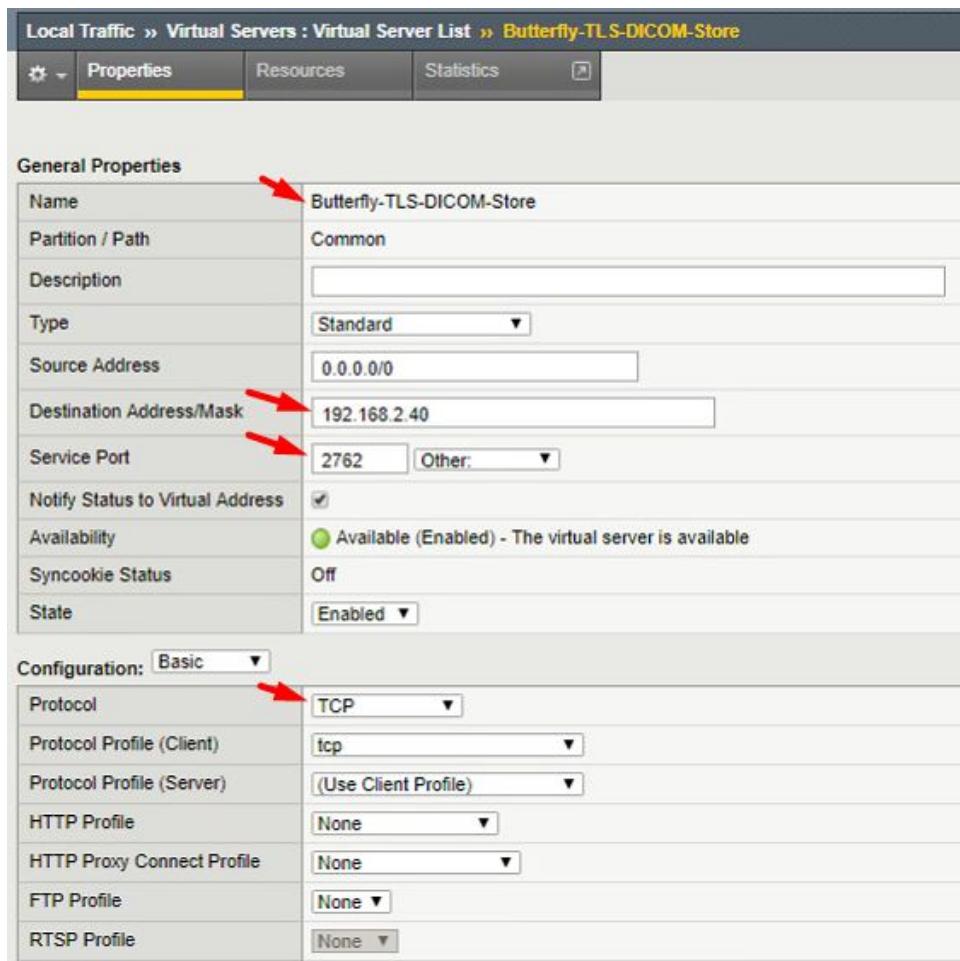
4.1 - Go to 'Local Traffic >> Virtual Servers: Virtual Server List'.

4.2 - Select Create.



4.3 - Within the General Properties enter the Name (e.g. Butterfly-TLS-DICOM-Store) and Destination Address and Service Port.

4.3.1 - This is the (virtual) IP address and port that you are defining for this Virtual Server. Your firewall will need to permit traffic to this IP/port.



4.4 - Within the Configuration section → SSL Profile (Client), select the previously created profile (Butterfly-TLS).

Configuration: Basic ▼

Protocol	TCP ▼
Protocol Profile (Client)	tcp ▼
Protocol Profile (Server)	(Use Client Profile) ▼
HTTP Profile	None ▼
HTTP Proxy Connect Profile	None ▼
FTP Profile	None ▼
RTSP Profile	None ▼
SSL Profile (Client)	<div> <div>Selected</div> <div> / Common Butterfly-TLS </div> </div> <div> <div>Available</div> <div> / Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl </div> </div>
SSL Profile (Server)	<div> <div>Selected</div> <div> </div> </div> <div> <div>Available</div> <div> / Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl </div> </div>
SMTPS Profile	None ▼
Client LDAP Profile	None ▼
Server LDAP Profile	None ▼
SMTP Profile	None ▼
VLAN and Tunnel Traffic	All VLANs and Tunnels ▼
Source Address Translation	Auto Map ▼

4.5 - SSL Profile (Server) should be blank.

4.6 - In a one-armed Big-IP configuration (single interface), ensure that Source Address Translation is set to Auto Map.

4.7 - Under Resources → Default Pool, select the previously created Server Pool (DICOM-STore-Server-Pool).

4.8 - Click Finished.

Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List Virtual Address List Statistics

Search Create...

✓	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
	●	Butterfly-TLS-DICOM-Store			192.168.2.40	2762	Standard	Edit...	Common

Enable Disable Delete...

## 5.0 - Setup Complete

5.1 - Repeat Steps 3.0-4.0 if you need to set up another TLS Termination - Virtual Server for your DICOM Modality Worklist.



## Appendix C - Configuration of the Citrix ADC (NetScaler) - TLS Termination Device

### How to use these Instructions:

The purpose of this Guide is to assist an Administrator of a Citrix Application Delivery Controller (ADC), formerly known as Netscaler, to configure SSL/TLS termination and assumes prior experience with management of the device. The SSL/TLS termination is to be used with the Butterfly Network DICOM-TLS feature that allows for encrypted DICOM communications between the Butterfly Cloud and the Customers' DICOM archive.

#### Trademark:

Citrix ADC and Netscaler are registered trademarks of Citrix Systems, Inc.

#### Version Information:

This Guide refers to configuration procedures as per Citrix ADC version 12.0 . The process will be similar on prior versions of Citrix ADC (Netscaler).

### Introduction

SSL/TLS termination (offloading) relieves an Application or Web server of the processing burden of encrypting and/or decrypting traffic sent via TLS or SSL. Note that the SSL standard has been replaced by TLS as the encryption mechanism for most web-based communications. Any use of "SSL" in this guide is strictly for convenience and is, in fact, referring to TLS.

When a DICOM server system is not capable of receiving TLS-encrypted DICOM data, the TLS termination capability of a Citrix ADC device can be used to decrypt/encrypt the data. In this scenario, the TLS termination function of a Citrix ADC (Netscaler) device will be used to decrypt/encrypt the data between itself and Butterfly Cloud. Once the connection is terminated at the ADC, the unencrypted DICOM data is forwarded to the designated DICOM server.

The Citrix ADC provides multiple modes for SSL/TLS processing. This guide will focus on SSL/TLS termination with a Virtual Server configured for the SSL\_TCP protocol. Note that the Citrix ADC must have the following Basic Features enabled:

- SSL Offloading (required).
- Load Balancing (optional, if you use Service Groups).

### Prerequisites

In most environments, the Citrix ADC is located in the DMZ portion of the network. In order for the device to be able to process the DICOM-TLS traffic; the Internet-facing firewall must be configured to permit traffic on the port(s) that the ADC has been configured to listen on.

- Note the external (Internet-facing) IP address of the firewall or Citrix ADC.
- For the purposes of this document, we will be creating an SSL\_TCP, Virtual Server on the ADC.
  - A DICOM Store virtual server will be configured to use port 2762.
  - A DICOM Worklist virtual server will be configured to use port 2761.
- Ensure that the external firewall permits TCP traffic from the Internet to the above ports used by the Virtual Servers.
- Butterfly Network has had varied success with using the ADC to generate a self-signed digital certificate - this Guide will require that you generate a self-signed certificate using OpenSSL (see Appendix A).
  - Ensure you have the Key and Certificate files in .pem format generated by OpenSSL or a certificate authority.
  - A public certificate is not required for the DICOM-TLS encryption. We are only using the certificate for encryption/decryption, not for end-point trust and validation.
- Login to Citrix ADC GUI.

## Citrix ADC TLS Termination Setup

Configuring SSL-TCP termination consists of 4 steps:

- 1. Configure a TCP Service or Service Group.**

This will define the information for your internal DICOM system (PACS/VNA/etc.) that is to receive the studies from Butterfly.

- 2. Verify or Configure SSL Cipher Group.**

This step configures a secure SSL Cipher Group for use with the TLS 1.2 connection. It is an optional step and may be skipped if you already have preferred cipher group that supports TLS 1.2.

- 3. Import the SSL Certificate and Key.**

It is preferable to use OpenSSL to generate the self-signed SSL Certificate-key pair, however, the Citrix ADC has a built-in Certificate creation feature that may also be used. The Certificate and Key will be associated with the Virtual Server.

- 4. Configure the Virtual Server.**

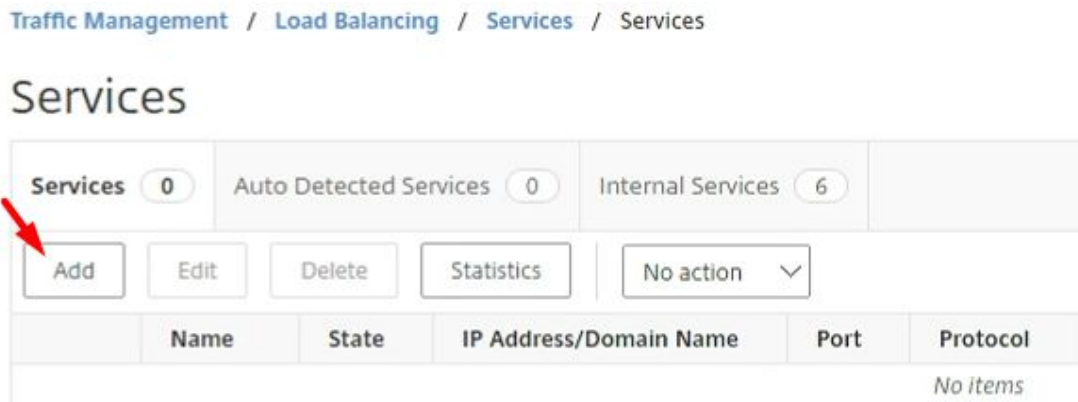
This is the final step to create the Virtual Server that will terminate the TLS connection, using the bound Certificate-key pair, and will forward the decrypted data to the TCP Service.

### 1.0 - Configure a TCP Service

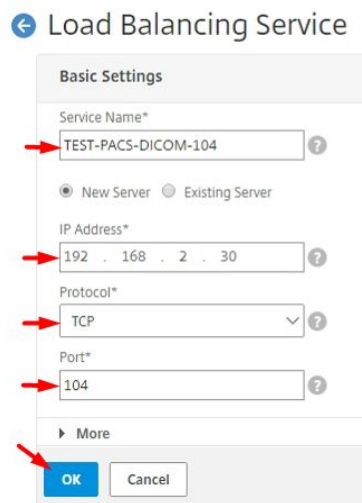
1.1 - Navigate to the Configuration tab.

1.2 - Go to 'Traffic Management >> Load Balancing >> Services'

1.3 - Select Add to create a new Service.



1.4 - Within the Service configuration screen enter the Service Name (e.g. Qlink-DICOM), correct IP, and Port information for your DICOM end-point. Ensure that you select TCP as the protocol.



1.5 - Click **OK** to confirm the settings, and **Done** on the following details screen to accept all defaults and complete the setup.

1.6 - Once complete, the Service list should resemble the image below. Ensure that the Service State is Up (green) before proceeding.

### Services

Services	1	Auto Detected Services	0	Internal Services	6
Add	Edit	Delete	Statistics	Select Action	▼
<input checked="" type="checkbox"/>	Name	State	IP Address/Domain Name	Port	Protocol
<input checked="" type="checkbox"/>	TEST-PACS-DICOM-104	UP	192.168.2.30	104	TCP

## 2.0 - Configure the SSL Cipher Group (optional)

2.1 - Butterfly Cloud uses TLS 1.2 to encrypt data - the encryption process uses Cipher Groups to securely encode the data. For maximum security, it is recommended to configure a Cipher Group which contains the strongest available ciphers for TLS 3.5.2 - This step is optional if you already have an existing preferred Cipher Group for use with SSL termination.

2.2 - Navigate to the Configuration tab.

2.3 - Go to **'Traffic Management >> SSL >> Cipher Groups'**

2.4 - Select **Add** to create a new Cipher Group.

Traffic Management / SSL / Cipher Groups

### Cipher Groups

Add	Edit	Delete
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ALL	All ciphers supported by NetScaler, excluding NULL ciphers
<input type="checkbox"/>	DEFAULT	Default cipher list with encryption strength >= 128bit
<input type="checkbox"/>	kRSA	Ciphers with Key-ex algo as RSA

2.5 - Within the Cipher Group configuration screen, enter the Cipher Group Name (e.g. TLS-1.2-Only) and click **Add**. Filter the Available cipher groups by entering **'TLS1.2'** into the **Search Ciphers** field. Select and move the TLS 1.2 ciphers only to the Configured box by using the right-arrow.

Cipher Group Name\*  
TLS-1.2-Only

Available (16)

Search Ciphers: TLS1.2

- ☐ DEFAULT
- ☐ TLS1.2-AES-256-SHA256
- ☐ TLS1.2-AES-128-SHA256
- ☐ TLS1.2-AES256-GCM-SHA384
- ☐ TLS1.2-AES128-GCM-SHA256
- ☐ TLS1.2-ECDHE-RSA-AES-256-SHA384
- ☐ TLS1.2-ECDHE-RSA-AES-128-SHA256
- ☐ TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- ☐ TLS1.2-ECDHE-RSA-AES128-GCM-SHA256
- ☐ TLS1.2-ECDHE-ECDSA-AES256-SHA384
- ☐ TLS1.2-ECDHE-ECDSA-AES128-SHA256

Configured (0)

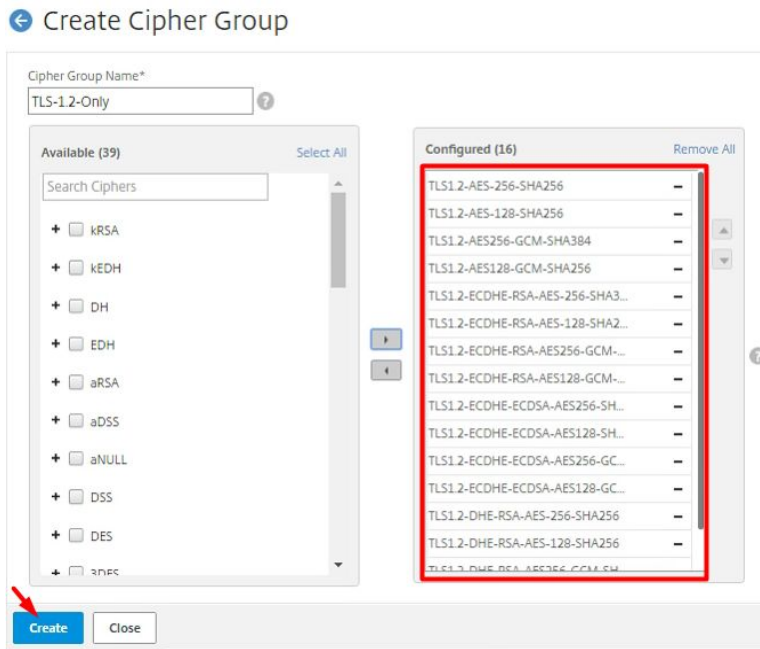
No items

➡

⬅



2.6 - The Cipher Group should resemble the image below, click **Create** when finished.



### 3.0 - Import the SSL Certificate and Key

The SSL Certificate-Key pair should be imported into the ADC; the certificate chain can be issued by a public certificate authority, an organizational certificate authority, or self-signed. Please reference the **Appendix A - Digital Certificate Generation Using OpenSSL** for detailed instructions on the use of OpenSSL for this purpose.

An alternative approach is to generate the Certificate-Key pair using the Server Certificate Wizard in ADC - however, this method has resulted in variable success for termination of the DICOM-TLS data from Butterfly Cloud and will not be covered in this Guide.

3.1 - Ensure that you have both the Certificate file (e.g. SCP\_Cert.pem) and Key file (e.g. SCP\_Key.pem) that form the Digital Certificate-Key pair.

3.2 - Go to '**Traffic Management >> SSL >> SSL Certificate >> Server Certificate**'.

3.3 - Click **Install**.

Traffic Management / SSL / SSL Certificate / Server Certificates

#### Server Certificates

<input type="checkbox"/>	<b>Install</b>	<input type="checkbox"/>	<b>Update</b>	<input type="checkbox"/>	<b>Delete</b>	<input type="button" value="No action"/>	<input type="button" value="v"/>
<input type="checkbox"/>	Name	Common Name	Issuer Name				
<input type="checkbox"/>	ns-sftrust-certificate	SFTrust default JPHHLI	SFTrust default JPHHLI				
<input type="checkbox"/>	ns-server-certificate	default ICVWSX	default ICVWSX				

3.4 - Enter the Certificate-Key Pair Name (e.g. Butterfly-Cert-Key-Pair). Select **Local** under Certificate File Name and find the Certificate file on your local computer (e.g. SCP\_Cert.pem).

## ← Install Server Certificate

Certificate-Key Pair Name\*

Butterfly-Cert-Key-Pair

Certificate File Name\*

Choose File ▾

Local ☒ Expires

Appliance

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period

30

Install Close

3.5 - Again select **Local** under Key File Name and find the Key file on your local computer (e.g SCP\_Key.pem). Click **Install**.

## ← Install Server Certificate

Certificate-Key Pair Name\*

Butterfly-Cert-Key-Pair

Certificate File Name\*

Choose File ▾ SCP\_cert.pem

Key File Name\*

Choose File ▾ SCP\_key.pem

☒ Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period

30

Install Close

3.6 -The newly imported Certificate-Key pair will appear in the list of Server Certificates.

Traffic Management / SSL / SSL Certificate / Server Certificates

## Server Certificates

Install	Update	Delete	No action ▾
<input type="checkbox"/>	Name	Common Name	Issuer Name
<input type="checkbox"/>	ns-sftrust-certificate	SFTrust default JPHHLI	SFTrust default JPHHLI
<input type="checkbox"/>	ns-server-certificate	default ICVWSX	default ICVWSX
<input checked="" type="checkbox"/>	Butterfly-Cert-Key-Pair	Support/emailAddress=support@butterflynetwork.com	Support/emailAddress=

## 4.0 - Configure the Virtual Server

4.1 - Navigate to the Configuration tab.

4.2 - Go to 'Traffic Management >> Load Balancing >> Virtual Servers'.

4.3 - Click **Add**.

Traffic Management / Load Balancing / Virtual Servers

## Virtual Servers

Add Edit Delete Enable Disable Statistics Select Action ▾

Name	State	Effective State
------	-------	-----------------

4.4 - Enter the Name of the Virtual Server (e.g. Butterfly-DICOM-TLS), select the protocol as **SSL\_TCP**, enter the IP address that you wish to use for the Virtual Server (*this can be any available IP address on the subnet/VLAN that the Citrix ADC has access to, you may also re-use an IP address of another Virtual Server, as long as the Port is different*). Enter the Port (e.g. 2762). Click **OK**.

**Basic Settings**

Create a virtual server by specifying a name, an IP address, a port, and a protocol. A virtual IP (VIP) is usually a private (RFC1918 non-routable) IP address. You can configure multiple virtual servers to receive client requests.

Name\*

Protocol\*

IP Address Type\*

IP Address\*

Port\*

More

**OK**

4.5 - Click **NO** next to Load Balancing Virtual Server Service Binding.

**Load Balancing Virtual Server** | [Export as a Template](#)

**Basic Settings**

Name	Butterfly-DICOM-TLS
Protocol	SSL_TCP
State	● DOWN
IP Address	192.168.2.31
Port	2762
Traffic Domain	0

**Services and Service Groups**

A service is a logical representation of an application running on a server. A service group enables you to manage a group of services as though it were a single service. **Note:** Bind at least one service or service group to the virtual server.

Click **Continue** to display the advanced settings and select the method, protocol, and port.

☒ **No** Load Balancing Virtual Server Service Binding

☐ Load Balancing Virtual Server ServiceGroup Binding

**Continue**

4.6 - Click the right arrow to select the previously configured TCP Service (e.g. Qlink-DICOM). Click **Select**. Click **Bind** to complete.

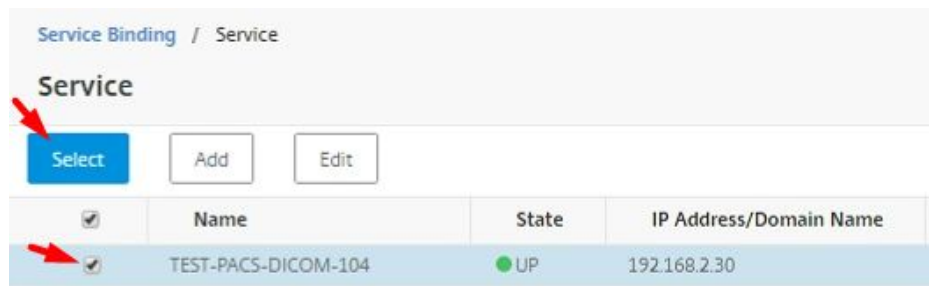
**Service Binding**

Select Service\*

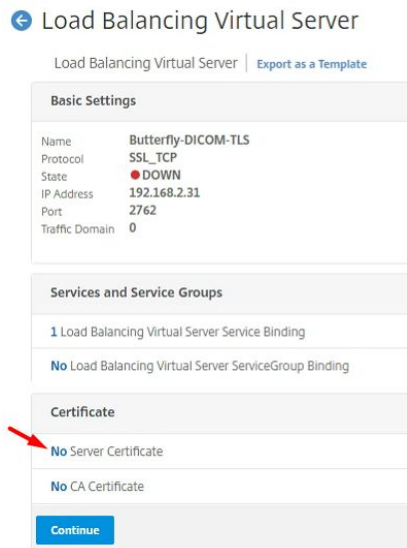
**Binding Details**

Weight

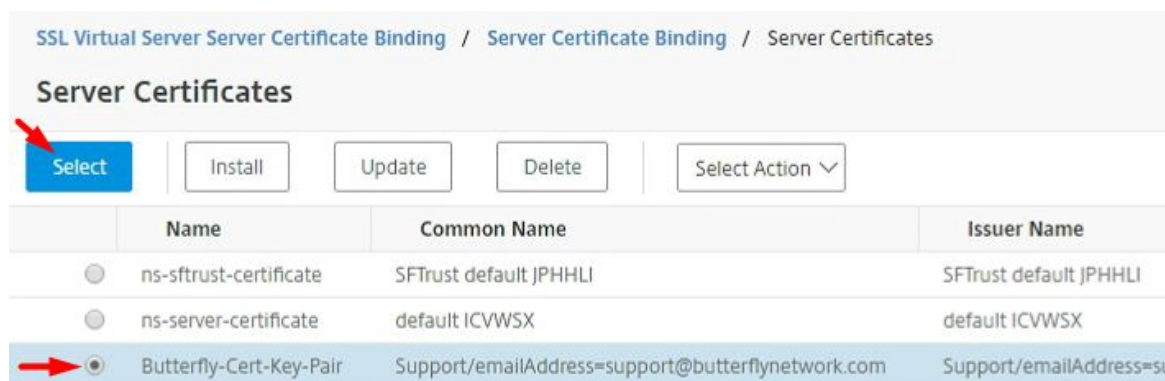
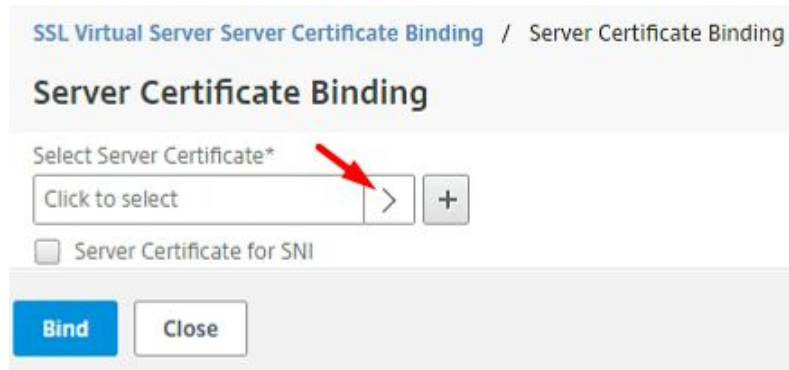
**Bind**



4.7 - Click **Continue** on the final confirmation screen. This will expand the Certificate section. Click **NO** next to Server Certificate.



4.8 - Click the right arrow to select the previously imported Server Certificate-Key pair (e.g. Butterfly-Cert-Key-Pair). Click **Select**. Click **Bind** to complete.



4.9 - Click **Continue** on the final confirmation screen. This will expand the various SSL configuration parameters.

4.10 - In the SSL Ciphers section click the Edit icon.

The screenshot shows the SSL configuration interface. The 'Certificate' section has two items: '1 Server Certificate' and 'No CA Certificate', each with a right arrow. The 'SSL Ciphers' section has a header bar with an edit icon (pencil) and a close icon (X). A red arrow points to the edit icon. Below the header bar, there is a 'Configured (1)' button and a 'Remove All' button.

4.11 - Select **Cipher Groups** and select the previously created Cipher Group (e.g. TLS 1.2 Only). Click **OK**. Follow the same process to remove the 'Default' Cipher Group.

The screenshot shows the 'SSL Ciphers' dialog box. The 'Cipher Groups' radio button is selected, and 'TLS-1.2-Only' is selected in the dropdown menu. The 'OK' button is highlighted with a red arrow.

4.12 - Scroll down to the SSL Parameters section, click the Edit icon.

The screenshot shows the 'SSL Parameters' section. The 'Edit' icon (pencil) is highlighted with a red arrow. The parameters are listed in a table:

Parameter	Value	Parameter	Value	Parameter	Value
Enable DH Param	DISABLED	Clear Text Port	0	OCSP Stapling	DISABLED
Enable DH Key Expire Size Limit	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Client Authentication	DISABLED	SSLv2	DISABLED
Refresh Count	0	Send Close-Notify	YES	SSLv3	DISABLED
Enable Session Reuse	ENABLED	PUSH Encryption Trigger	Always	TLSv1	DISABLED
Time-out	120	SNI Enable	DISABLED	TLSv11	DISABLED
SSL Redirect	DISABLED	HSTS	DISABLED	TLSv12	ENABLED
Strict Signature Digest Check	DISABLED	Max Age	0		
		Include Subdomains	NO		

4.13 - Ensure that in the Protocol list, only TLS 1.2 is selected, uncheck all other protocols. Click **OK**.

The screenshot shows the 'SSL Parameters' dialog box. The 'Protocol' section shows 'TLSv12' selected, and the 'OK' button is highlighted with a red arrow.

4.14 - Scroll to the bottom of the configuration screen and click **Done**, to confirm completion of the Virtual Server setup.

4.15 - The following screen will contain the list of your Virtual Servers. Ensure that the newly created Virtual Server (e.g. Butterfly-DICOM-TLS) has a green indicator.

[Traffic Management](#) / [Load Balancing](#) / Virtual Servers

## Virtual Servers

<a href="#">Add</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Enable</a>	<a href="#">Disable</a>	<a href="#">Statistics</a>	<a href="#">Select Action</a> ▼	
<input type="checkbox"/>	Name	State	Effective State	IP Address	Port	Protocol	Method
<input type="checkbox"/>	Butterfly-DICOM-TLS	UP	UP	192.168.2.31	2762	SSL_TCP	LEASTCONNECTION

## 5.0 - Setup Complete

Repeat Steps in sections **1.0** and **4.0** if you need to set up another TLS Termination - Virtual Server for your DICOM Modality Worklist.

## 6.0 - Certificate Export for Butterfly Cloud (optional)

If the certificate was generated using OpenSSL, then the public certificate will need to be uploaded to the PACS Configuration screen of Butterfly Cloud. If the Certificate was generated on the Citrix ADC (as per this Guide), then follow the steps below to export the Certificate to a file for upload to the Butterfly Cloud.

6.1 - Navigate to the Configuration tab.

6.2 - Go to **'Traffic Management >> SSL'**.

6.3 - Select Manage Certificates / Keys / CSRs.

[Traffic Management](#) / [SSL](#)

## SSL

**Getting Started**  
[Server Certificate Wizard](#)  
[Client Certificate Wizard](#)  
[Intermediate-CA Certificate Wizard](#)  
[Root-CA Certificate Wizard](#)  
[Create and Install a Server Test Certificate](#)  
[Install Certificate \(HSM\)](#)  
[CRL Management](#)

**Tools**  
[Create Diffie-Hellman \(DH\) key](#)  
[Import PKCS#12](#)  
[Export PKCS#12](#)  
[Manage Certificates / Keys / CSRs](#)  
[Start SSL certificate, key file synchronization for HA](#)  
[Start SSL certificate, key file synchronization for Cluster](#)  
[OpenSSL interface](#)

**Policy Manager**  
[SSL Policy Manager](#)

**Settings**  
[Change advanced SSL settings](#)

**Configuration Summary**  
5 Certificate-key pairs  
41 Cipher Groups  
No CRL  
No SSL Policy  
No SSL Policy Label  
No OCSP Responder

6.4 - Select the certificate file that is associated with the Certificate-Key pair that is bound to your Virtual Server (e.g. SCP-Cert), and select **Download**.

## ← Manage Certificates

Current Directory: /nsconfig/ssl/

[Download](#)
[Upload](#)
[View](#)
[Delete](#)
[Open Directory](#)
[Select Action](#) ▼

<input type="checkbox"/>	Name	Type	Date Modified
<input type="checkbox"/>	SCP_Key.pem	File	Wed Jun 5 00:47:47 2019
<input checked="" type="checkbox"/>	SCP_Cert.pem	File	Wed Jun 5 00:47:41 2019
<input type="checkbox"/>	ns-sftrust.sig	File	Tue May 28 12:56:21 2019

6.5 - The downloaded file will already be in the correct format for use with Butterfly Cloud.