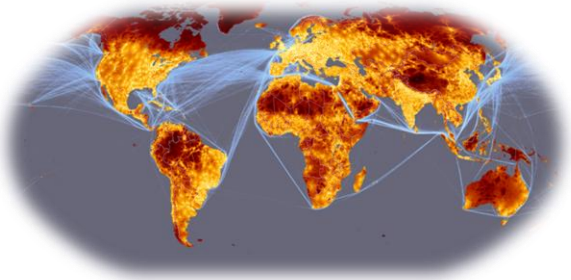
SSL/TLS Traffic Management User Manual

Supported Product Line
FlowMagic-400
FlowMagic-3200
FlowMagic-3200-12
FlowMagic-3240

RELEASE 1.2.0.81
Doc. No. UM115
February 13, 2017
INFINICORE INCOPORATED



Publishing Information:

Document Number	UM115
Doc. Release Number	1.2.0.81
Date	Feb. 13, 2017

Contact Information:

Infinicore Incorporated
Information: info@infinicoreinc.com Web Site: http://www.infinicoreinc.com

Table of Contents

Welcome to InfiniCORE Operating System User Manual.

In this manual, you will find detailed information to operate FlowMagic SSL/TLS Traffic Management Feature that are presented in FlowMagic Firmware Release 1.6.0 or later.

SSL/TLS Traffic Management described in this manual is designed to help operators to view, analyze, track and decrypt SSL/TLS traffic.

 Due to the critical importance and the nature of server private key involved in the operation, it is highly recommended that operator uses HTTPS based connection to FlowMagic UI for all the activities including configuration, maintenance and diagnosis of all the SSL/TLS Traffic Management function. Please also refer to Section 2.3.3.4.2 Security of Server Private Key file for more considerations.

This manual contains the following three chapters:

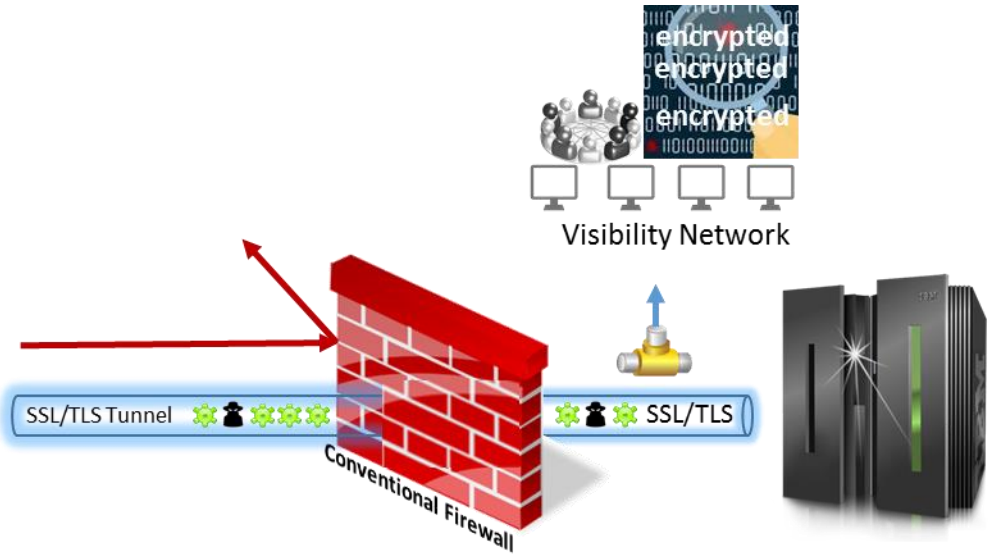
- Chapter 1 Overview of SSL/TLS Traffic Management Capabilities
- Chapter 2 Configuration of SSL/TLS Traffic Management
- Chapter 3 Monitoring and Trouble Shooting SSL/TLS Traffic Management

Should you have any question, suggestion or feature request, please do not hesitate to contact Infinicore support team at Email: support@infinicoreinc.com. We are more than happy to assist you.

Chapter 1 Overview of SSL and TLS Traffic Management Capabilities

Secure Socket Layer (SSL)/Transport Layer Security (TLS) protocols are widely used in the computer communication systems to ensure communications' Confidentiality, Integrity and Authentication.

Due to its nature of confidentiality, SSL/TLS have increasingly become a communication channel for variety of enterprise threats as well such as information leakage, phishing, worms and malwares. The encrypted traffic can avoid inspection from the regular firewall or IPS/IDS devices. Upon server decrypts the traffic, the true nature of traffic gets revealed and creates damage. Additionally SSL/TLS protocols render the conventional visibility and forensic network less useful since the traffic acquired is encrypted and appeared as if random noise.



The SSL/TLS Traffic Management feature provided by InfiniCORE's FlowMagic product family is designed to help network administrator to solve the SSL/TLS dilemma.

FlowMagic SSL/TLS management provides the following main functions:

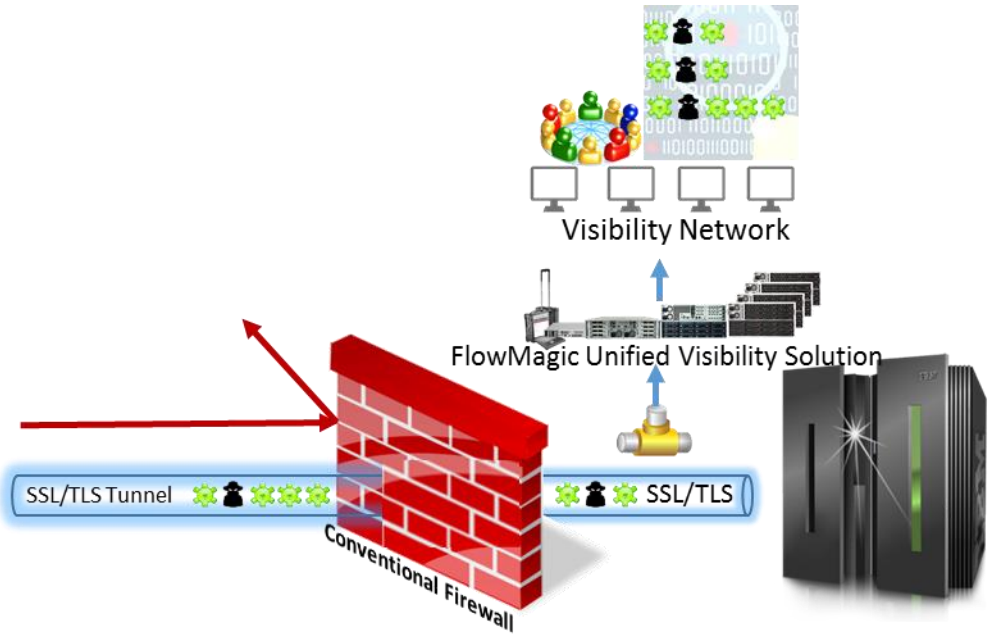
- Discover, Detect And Capture SSL/TLS Based Traffic
  FlowMagic appliance can be configured to capture SSL/TLS traffic in encrypted form. Further operations such as certification extraction, end point and geolocation analysis can be invoked over the captured traffic through regular FlowMagic analytic flow.

- Store and log detailed SSL/TLS record
  Alternate to full SSL/TLS traffic recording, FlowMagic can store the SSL/TLS record that represents the key aspects of the conversation including the source, destination, certification etc. The record is useful to trace the origin and route of the traffic.

- Decrypt Traffic with Session Master Key
  Under forensic cases when server's private certificate is not available, session master key can be calculated in a separate location and input into FlowMagic for decryption a particular session.

- Decrypt and Forward Traffic with Server Private Certification
  To automate the decryption process, a server private certificate can be imported into FlowMagic and be used to decrypt all SSL/TLS traffic from/to the server. The decrypted traffic can be forwarded out to downstream device for further processing. Post processing is available for the decrypted traffic to have a different destination port etc.

  The decryption can be applied to selected portion of the traffic through decryption descriptor. FlowMagic supports using the following fields in the packet:
  - Server IP Address
  - Client IP Address
  - Connection's Destination Port Number, a.k.a application port

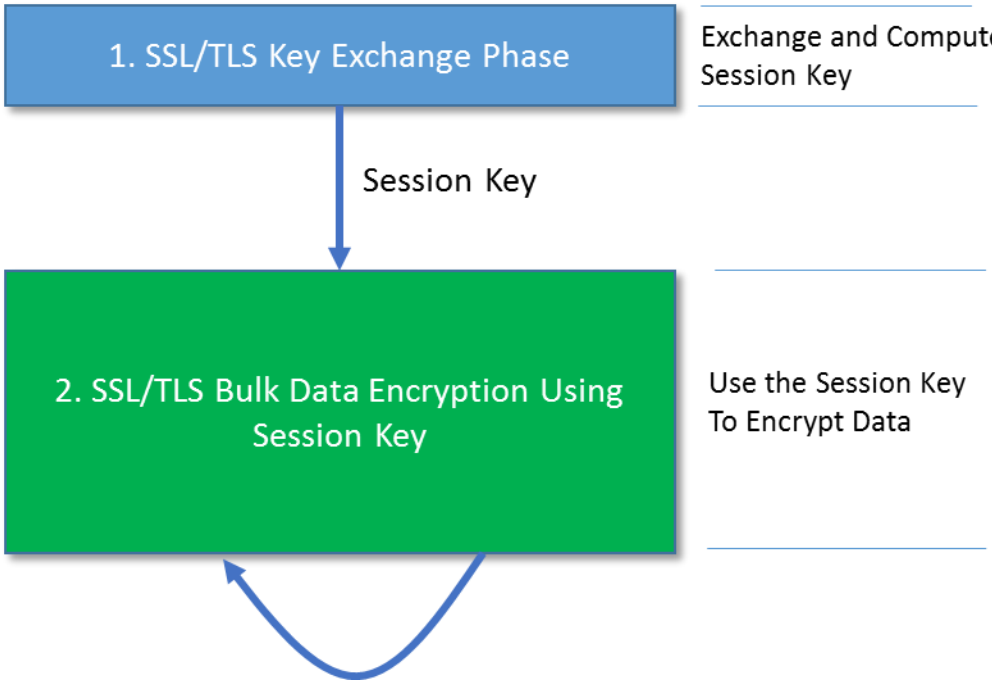


1.1 Overview of SSL/TLS through the Lens of Decryption

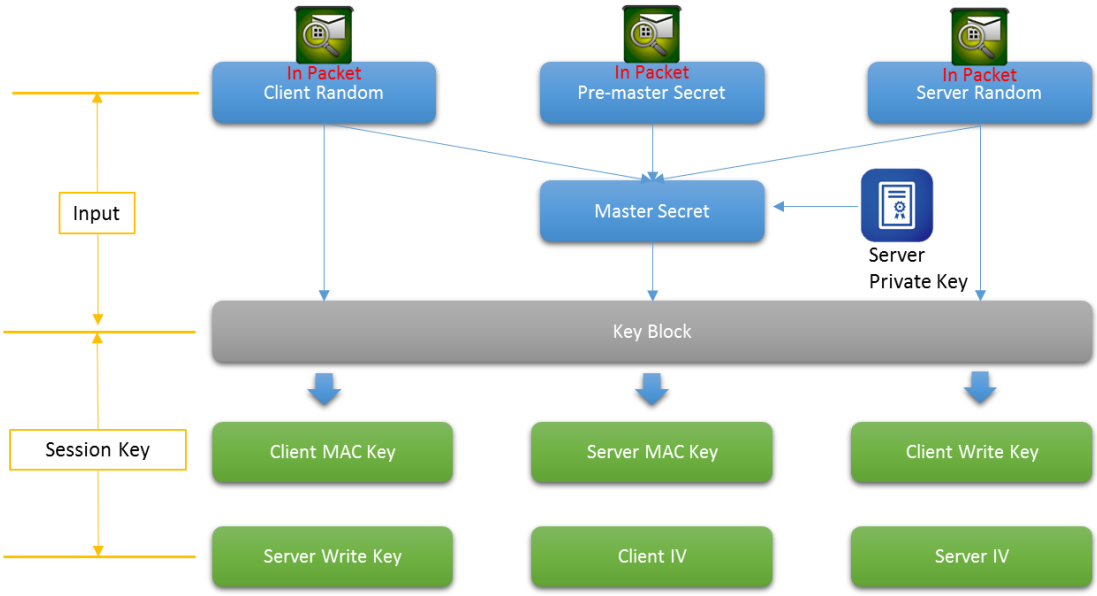
There will be many details involved to completely understand SSL and TLS protocols. However the whole process can be simplified if the purpose is just to understand how decryption can work in the context of FlowMagic.

In all the SSL/TLS variants, the protocol employs a combination of public-key and symmetric-key encryption. Public-key encryption, among other purposes, is used for client and server to establish a common known key, a session key to encrypt the rest of the traffic. Once the session key is negotiated, symmetric-key encryption is used for the bulk data encryption. The benefit of using a symmetric-key is that symmetric-key encryption algorithm such AES can yield significant performance gain over public-key encryption.

The whole SSL/TLS process can be broken down into the following two stages.



To decrypt a particular SSL/TLS session, it becomes obvious that one needs to know the session key. The session key is calculated with the following overly simplified process.



In summary, to decrypt SSL/TLS traffic, other than packet trace, either the session key or server's private key information is necessary for the decryption to be carry out properly.

1.2 Supported SSL/TLS Versions and Ciphers

FlowMagic software defined data path supports a wide range of SSL/TLS versions and ciphers. The following two sections list the major supported version and cipher suites.

1.2.1 Supported SSL/TLS Protocol Versions

The following table lists the support status of SSL/TLS protocol versions. InfiniCORE Networks Inc. commits to support the latest version when the specification becomes available and mature.

Protocol Variant	Specification	Release Status
SSL v2.0	N/A	Not Supported Due to Prohibiting Status (RFC6176)
SSL v3.0	RFC 6101	Supported
TLS v1.0	RFC 2246	Supported
TLS v1.1	RFC 4346	Supported
TLS v1.2	RFC 5246	Supported

1.2.2 Supported Cipher Suites

The following table lists the support status of cipher suites. InfiniCORE Networks Inc. commits to support new ciphers when the specification becomes available.

Cipher Suites	Release Status
RSA-WITH-NULL-NULL	Supported
RSA-WITH-NULL-MD5	Supported
RSA-WITH-NULL-SHA	Supported
RSA-WITH-NULL-SHA256	Supported
RSA-WITH-RC4-128-MD5	Supported
RSA-WITH-RC4-128-SHA	Supported
RSA-WITH-DES-CBC-SHA	Supported
RSA-WITH-3DES-CBC-SHA	Supported
RSA-WITH-AES128-SHA	Supported
RSA-WITH-AES128-SHA256	Supported
RSA-WITH-AES256-SHA256	Supported
RSA-WITH-AES128-GCM-SHA256	Supported
RSA-WITH-AES256-GCM-SHA384	Supported

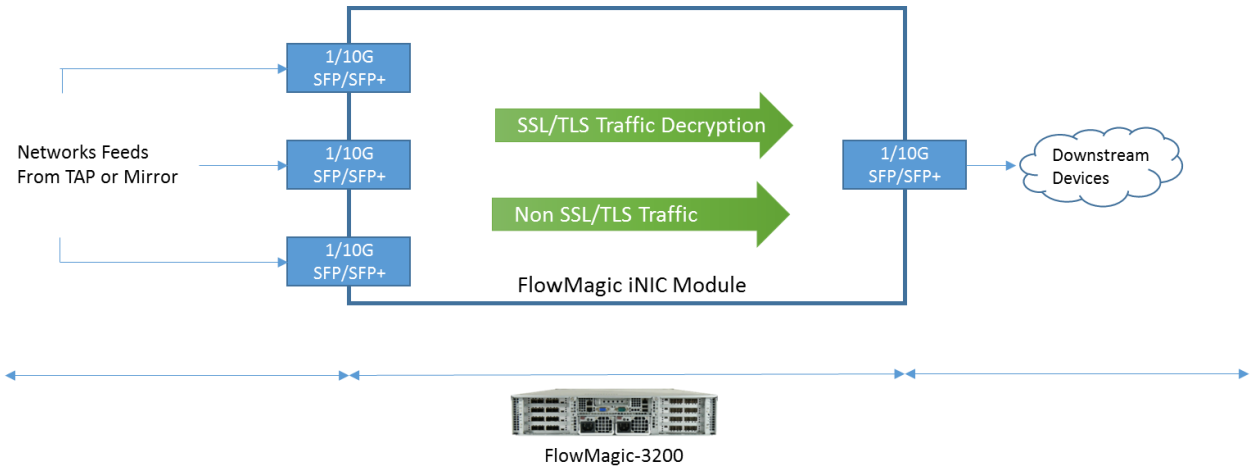
1.3 Deploy SSL/TLS Decryption with FlowMagic

To enable SSL/TLS decryption, at least two FlowMagic ports are needed. More ports can be used as the ingress ports.

- Ingress Ports
  Ingress ports are used to receive SSL/TLS traffic. Multiple ports can be defined as ingress ports. Traffic are internally aggregated from multiple ingress ports. FlowMagic does not transmit traffic over ingress ports.

- Egress Port
  Egress port are used to transmit the decrypted traffic. Optionally if enabled by configuration, non SSL/TLS traffic can be passed through egress ports transparently without modification.

The following simplified diagram displays the deployment view of FlowMagic Appliance with SSL/TLS decryption enabled.



In this diagram, FlowMagic is deployed to process network feeds from customer's network TAP or Mirror points. The FlowMagic ports that receive traffic are called ingress ports. The decrypted traffic is sent out to downstream network or devices through egress ports.

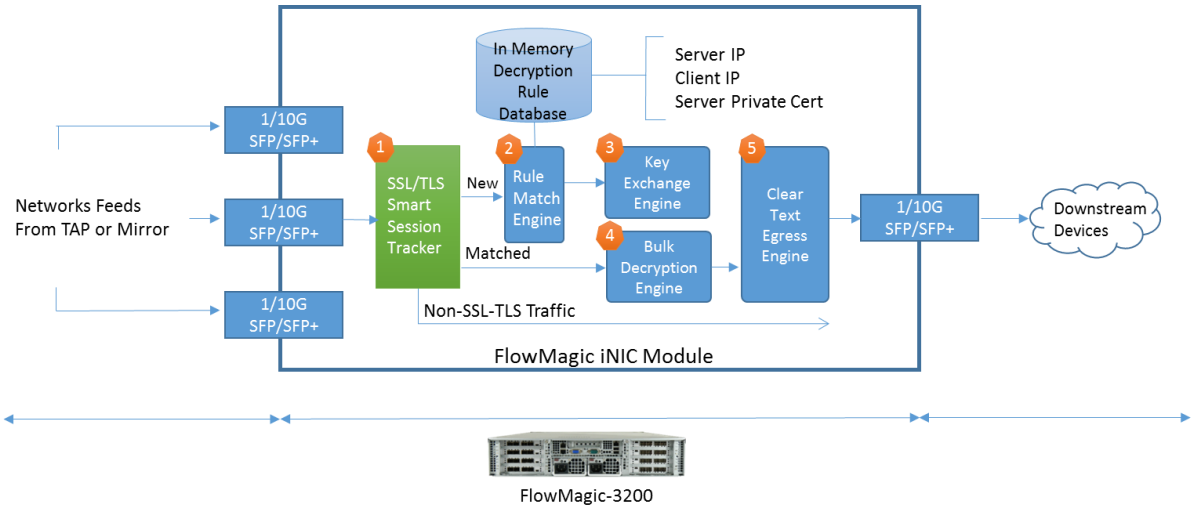
FlowMagic supports up to 8 (Eight) InfiniCORE's intelligent traffic processing modules. Each module provides 4 (four) 1/10G SFP/SFP+ dual mode network interfaces to connect to customer's IEEE 802.3 (Ethernet) compliant network.

The supported interface standard is listed in the following table.

Interface Standard	SFP Plug or Cable
1000M-BaseT	SGMII Based SFP
1000M-SFP	Optical SFP Plug
10G-Base SFP+	Optical SFP+ Plug
10G-Base Direct Attached Copper	Up to 5 meter DAC cable

1.4 FlowMagic SSL/TLS Traffic Decryption Data Flow

The following diagram shows the main traffic processing flow that are used to support SSL/TLS Traffic Decryption.



There are five stages in SSL/TLS traffic decryption data path.

1.4.1 SSL/TLS Smart Session Tracker

The session tracker is used to screening ingress traffic into three categories.

- Non SSL/TLS Traffic

  The non SSL/TLS is identified by predefined and user configurable destination port. Multiple ports can be defined.
  The packets that do not have defined destination port are considered non-SSL/TLS traffic. For non-SSL/TLS traffic, default behavior can be defined for packets to be passed through to egress port or dropped.

- Traffic that is part of New SSL/TLS Connection

  Traffic that is part of new SSL/TLS Connection will be identified and pass to the rule match engine, where the packet will be matched against rule data base defined by the operator. When a match is found, the packets will be redirected to Key Exchange Engine.

- Traffic with Existing SSL/TLS Connection

  Traffic within known SSL/TLS connection that have session key ready will be passed directly to Bulk Decryption Engine.

1.4.2 Rule Match Engine

Rule match Engine is to make a real time decision if a potential SSL/TLS connection is required to be decrypted. The matching criteria can be the following:

- Server IP Address
- Client IP Address

The Server IP is mandatory while the Client IP is optional.
Depend on the matching result, the packet can be either sent to Key Exchange Engine to trace the progress of key exchange or directly pass through or drop without further action.

1.4.3 Key Exchange Engine

Key exchange engine will keep track of the progress of SSL/TLS process. It will queue and store the selected content of the following messages:

- Client Hello Message
- Server Hello Message
- Pre-Master Secret Message
- Client Finished Message
- Server Finished Message

Together with user supplied Server Private Certificate File and the recorded messages, FlowMagic is able to compute the same session key that has been used to encrypt messages between client and server.
Upon finish, the Key Exchange Engine will update the state of the connection so that the subsequent message will be sent to bulk decryption engine with the session key and the correct cipher suite.

1.4.4 Bulk Decryption Engine

Once a connection has session key successfully decrypted, the bulk decryption engine handles the rest of the packet decryption.

For every successfully decrypted and authenticated packet, Bulk Decryption Engine sends the clear text packet to Clear Text Egress Engine so that the packet can be encapsulated with proper header information.

1.4.5 Clear Text Egress Engine

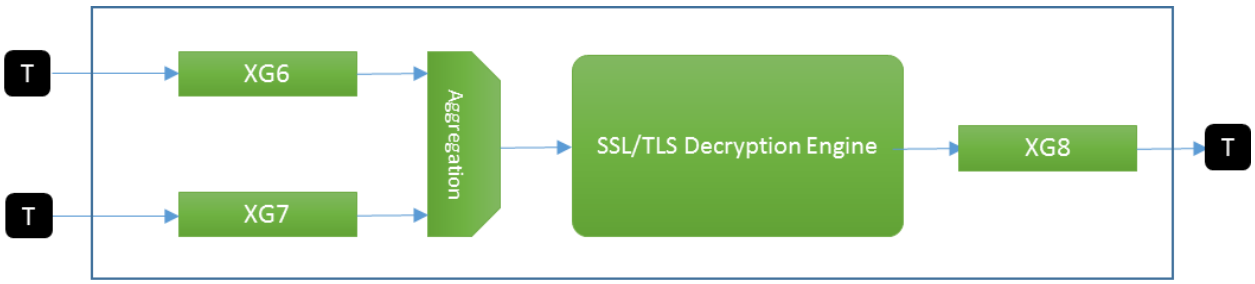
Clear text egress engine is designed to encapsulate the output of Bulk Decryption Engine so that clear text packet appears to be from normal unencrypted connection when it is received by the downstream device.

Currently the destination port number found in the TCP header can be reassigned to new value in the egress stage.

Chapter 2 Configuration of SSL/TLS Traffic Management

This chapter provides detailed description on how to configure the SSL/TLS Traffic Management feature. Following the steps described in this chapter, operators can create a SSL/TLS Traffic Decryption Flow Domain as shown below.

This configuration uses XG6 and XG7 as ingress port for the encrypted SSL/TLS traffic. XG8 is the egress port for the decrypted clear text packet.



FlowMagic iNIC Module

2.1 Prerequisites

Please check make sure the following prerequisites are met before proceed to configuration:

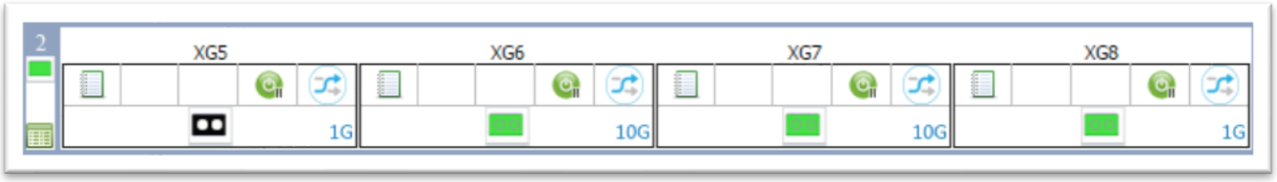
- The Management IP address of FlowMagic Appliance and a standard based browser

  FlowMagic Web Based UI is compatible with all major browsers such as Chrome, Firefox, Safari for MacOS or IE10 and 11.

- Login Credentials
- The ports used as ingress port(s) and their link configuration, whether it is 1G or 10G
- The ports used as egress port and their link configuration, whether it is 1G or 10G

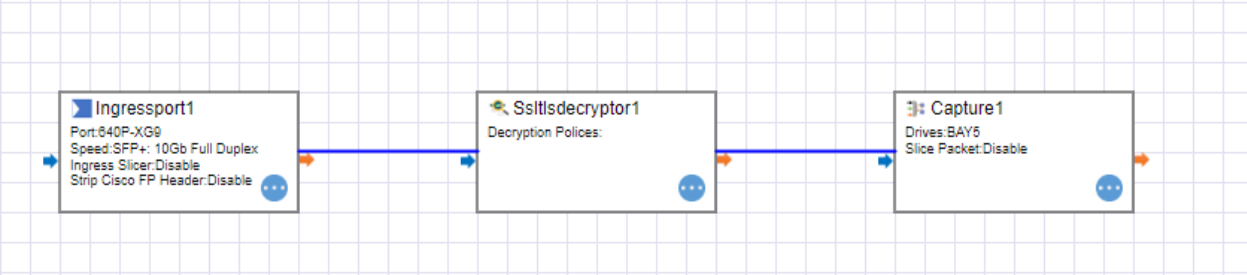
TIP:
It is always a good practice to login to FlowMagic UI and make sure all the ingress ports and egress ports have link, which will be shown in green color.

In the following example, XG5 does NOT have link while XG6, XG7 and XG8 all have established link with peer device.

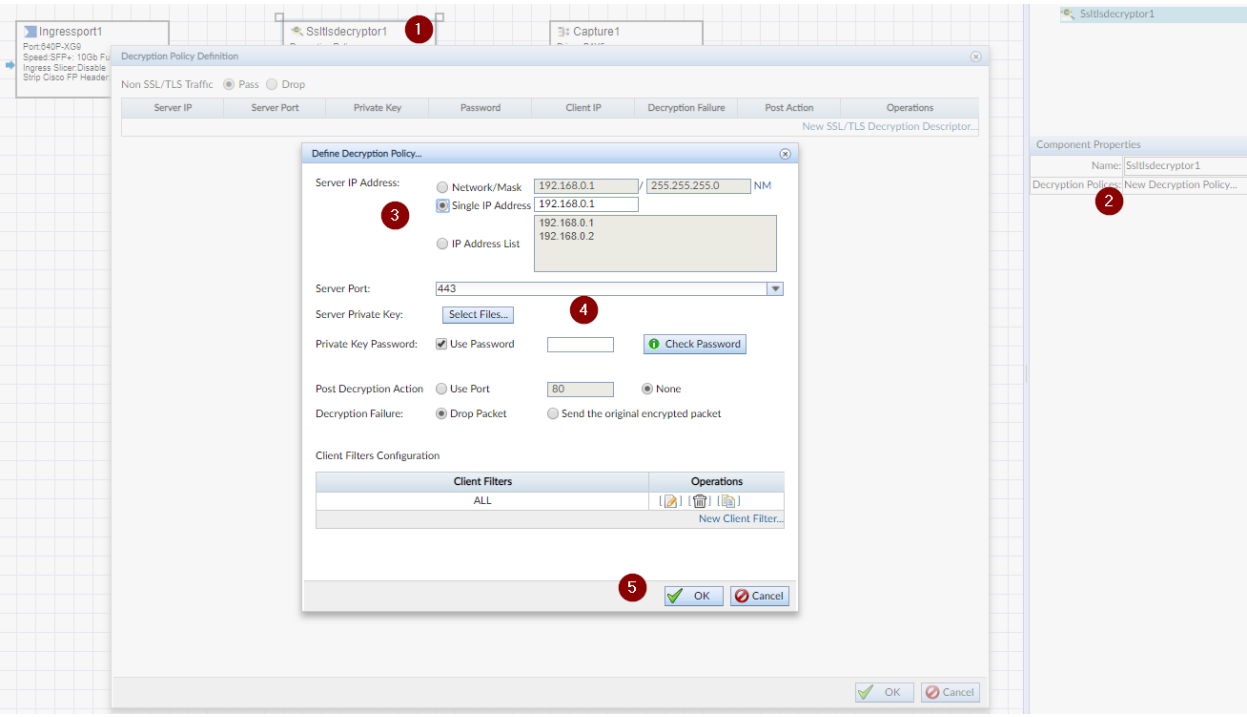


2.2 Creation of SSL/TLS Traffic Decryption Domain

To create a SSL/TLS Traffic Decryption Domain, use the topology similar to what's shown below.



Configure the decryptor as shown below.



2.3 Configuration of SSL/TLS Traffic Management Domain

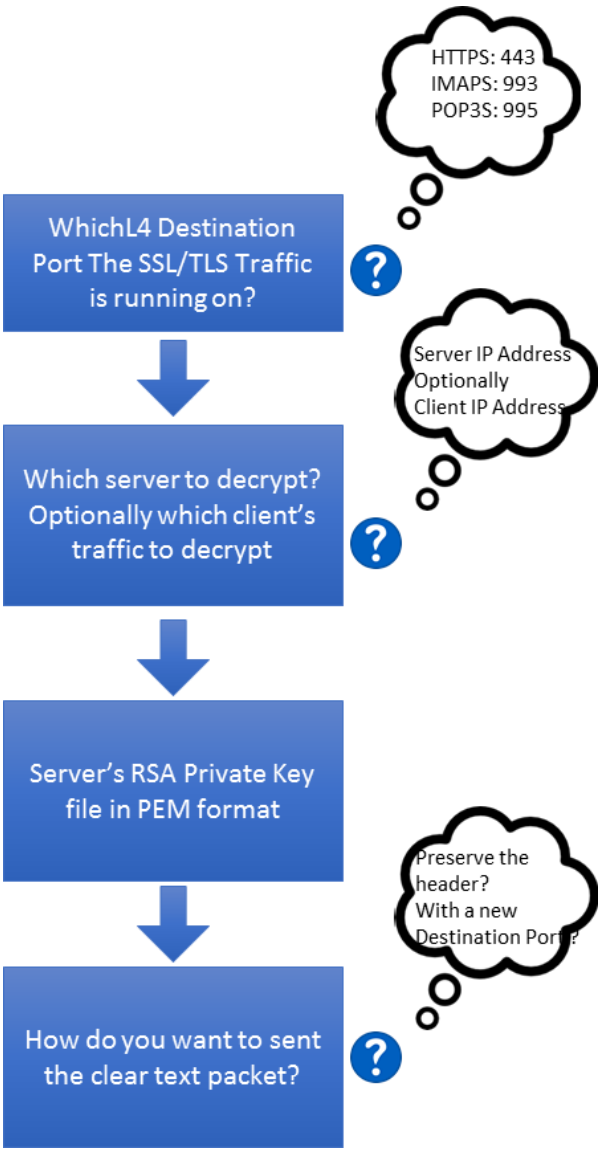
Once SSL/TLS Traffic Management domain is created, the following dialog will appear to allow further configuration of the operation.

There are three main sections this dialog.

- Configuration of Ingress Ports

  More than one ingress port can be assigned.

- Configuration of Egress Port
- Configuration of SSL/TLS Decryption



- Application Port Number
- Server IP Address
- Client IP Address (Optional)
- Server's RSA Private Key in PEM format
- Post processing options

In the above five parameter sets, client IP address and port processing operations are optional.

Without client IP address, all the packets towards the server are subject for SSL/TLS traffic processing.

Without the post processing options, the existing TCP headers will be preserved with only the modification on the sequence number so that it will appear as a valid stream to downstream devices.

2.3.3.1 Application Ports

Application ports defines a port number to filter out the non-SSL/TLS packets at earlier stage. Multiple ports can be defined.

2.3.3.2 Server IP Address

Server IP address defines the destination address in the packets that should subject to decryption processing. FlowMagic tracks the session so bi-directional traffic will be examined and server IP address will become source address when the traffic is from server to client.

2.3.3.3 Client IP Address

Optionally, operator can supply a client IP address so that only the portion of traffic between client IP and server IP address is decrypted.

2.3.3.4 Server Private Key

To successfully decrypt SSL/TLS connection, a server private key is needed. There are two ways to supply a server private key.

- Import private key in a PEM file.

  A PEM file often has the following format:

```
"-----BEGIN RSA PRIVATE KEY-----"
Description
Numbers
"-----END RSA PRIVATE KEY-----"
```

- Supply the private key's exponent and modulus

  When the certificate uses other formats different from PEM, since the essential information carried in certificate regarding to decryption is the exponent and modulus, one can directly input the numbers for the decryption operation.

2.3.3.4.1 Server Private Key file in PEM format

The following shows a server private key file in PEM format.

```
FlowMagic-3200:/tmp/cert$ openssl rsa -in server_private_key
Enter pass phrase for server_private_key:
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAwcqN9w7InSr/Z4GugSt++IOl7xRnbMCW3zJS7FW8vST3yfSI
spHn1cQqakSNgUBPiSCgu2cHTzTnufbgUa+ImtynLIch38lk8jZccoLGxGv9Fwk1
ijrUF6Sot6hvALT5LvofkavtEp/btdA7jQkNFuFYoGJuTlSVMlPXntQLyXgtPJ0v
VGWgtCt7HeyNYPacbUA7kEedkZTwd9xQ+eSZEfGwhfxROVolKsfZi6+qesjm8IGF
z8bl4zC2Oiur8wYVZkzWVUBJ9N9Zbh38JY5C5/8quVXOIFbaEk/2fT7sBF6WDoR3
FbYCxhBMhcy0/YpSOOxZiG3Xn/VHRAqAosthCQIDAQABAoIBAQCpI5EkwNJ32r9w
J8+XDc+UN9LsCHL8iFsmE1Ysz+gbbdiXe8aTlKUz/jLG7W5UET1aAhBHgHTwvMxD
```

```
kyXWJc6k21FNm+QE3lIs1SV7DIlPhrEvGeqQ6yeSOzTGl0vK4ilaxxQmoFgamUu6
NDTFs9Co16Xy1fZQh6Jwep0HEyv2elbOW8qUNFW9b28i9jEq1X1AxVL2wNTlpv8u
cXMFaDPMe3TGaI3naIOzFNVaWST80gL8k/Z1SWIB7GEwLdcgYEGdorYYnRbr9M0V
oi0dCoLPPKBczlkQXOAz5JYd8dKl197obLrdbQaX55jVxvzIle0cv2qZaTqo5sTX
krWOKEnBAoGBAPXSg95I8CVWCuzD5nPrD3LLqhDh1Pc5sHpxbW8oSxVNFV1ky3/S
kRrm+e4J+cm7U4kNSjcpRYu3XsE4F0g/sVtMpJM49FvDY5GVLkw/xjng8FOj7lvu
lQse7T1zZBJAdpLi7JHGMzb+1I8NAlIDB+5jeQxPpytBWjvWT23QgCZ7AoGBAMnQ
jxKH2Pkaph79aQs0taUgrhE01v4bL9fRXlWB2Wt5B9tkXw7FIu42zhjWpQ2MTHqu
Mdn1fXPmS61qRjI6IvNAzsVQxXOz1HaGclww3U26Xi8epbgXBULPRgje2rRsSDuY
rCVtHxlhMxJ7lYc23PL3jTDlnyCUl4vCH42N6uFLAoGAVd2OylpX5/LCJinXma4F
22dgpDz+Es1H470zKJy+fVZLnC/VFXUL0oXTz14Urm6Mo1bNEa+M51zJ8FwTZd05
qlZ/Nh2y3UrGwNeHMIMmTplP2Sdt3xbbYOMQo2JnFikGQhCZ6eF9ijxBKya0JMmC
P7bnVXGNRwKw7i3R2N33pXkCgYEAuXHQlkmIQdaQAXgAV1C2/SZbbOouCE95FgqI
cXAhFlWft6SyiILzhwuLNF3ASwO5nx2EJ3EiNybOMWqvWCX9yaKqnbuLxLbhK4x9
d2NbZ7oyI4A47UESD4MhKrOFKjc55LF0tetgoVSktn4jN51dSFHbRqwpHaoM21qk
3dEjnKMCgYEAyNxQD2J0Nst5/4q2lLhrFEG2gBXOjgTMNOZvT4f+jm9xKYW9dQBS
xOG3L2OPEt5iDpBIL8M8n4AhrIoDH013xgDg48ZLrSxFFFWsdRxjNO/wRgC4BTYD
eM1X69ixCTGzs4I4SjvakYyq5lLp+44GYNPso/Xx8rYGi9MI7PH7an4=
-----END RSA PRIVATE KEY-----
```

To understand the content, one can use the following command if available on the server to display all the fields. The `modulus` and `privateExponent` are used during the decryption operation.

```
FlowMagic-3200:/tmp/cert$ openssl rsa -in server_private_key -noout -text
Enter pass phrase for server_private_key:
Private-Key: (2048 bit)
modulus:
    00:c1:ca:8d:f7:0e:c8:9d:2a:ff:67:81:ae:81:2b:
    7e:f8:83:a5:ef:14:67:6c:c0:96:df:32:52:ec:55:
    bc:bd:24:f7:c9:f4:88:b2:91:e7:d5:c4:2a:6a:44:
    8d:81:40:4f:89:20:a0:bb:67:07:4f:34:e7:b9:f6:
    e0:51:af:88:9a:dc:a7:2c:87:21:df:c9:64:f2:36:
    5c:72:82:c6:c4:6b:fd:17:09:35:8a:3a:d4:17:a4:
    a8:b7:a8:6f:00:b4:f9:2e:fa:1f:91:ab:ed:12:9f:
    db:b5:d0:3b:8d:09:0d:16:e1:58:a0:62:6e:4e:54:
    95:32:53:d7:9e:d4:0b:c9:78:2d:3c:9d:2f:54:65:
    a0:b4:2b:7b:1d:ec:8d:60:f6:9c:6d:40:3b:90:47:
    9d:91:94:f0:77:dc:50:f9:e4:99:11:f1:b0:85:fc:
    51:39:5a:25:2a:c7:d9:8b:af:aa:7a:c8:e6:f0:81:
    85:cf:c6:e5:e3:30:b6:3a:2b:ab:f3:06:15:66:4c:
    d6:55:40:49:f4:df:59:6e:1d:fc:25:8e:42:e7:ff:
    2a:b9:55:ce:20:56:da:12:4f:f6:7d:3e:ec:04:5e:
    96:0e:84:77:15:b6:02:c6:10:4c:85:cc:b4:fd:8a:
    52:38:ec:59:88:6d:d7:9f:f5:47:44:0a:80:a2:cb:
    61:09
publicExponent: 65537 (0x10001)
privateExponent:
    00:a9:23:91:24:c0:d2:77:da:bf:70:27:cf:97:0d:
    cf:94:37:d2:ec:08:72:fc:88:5b:26:13:56:2c:cf:
    e8:1b:6d:d8:97:7b:c6:93:94:a5:33:fe:32:c6:ed:
    6e:54:11:3d:5a:02:10:47:80:74:f0:bc:cc:43:93:
    25:d6:25:ce:a4:db:51:4d:9b:e4:04:de:52:2c:d5:
    25:7b:0c:89:4f:86:b1:2f:19:ea:90:eb:27:92:3b:
    34:c6:97:4b:ca:e2:29:5a:c7:14:26:a0:58:1a:99:
```

```
        4b:ba:34:34:c5:b3:d0:a8:d7:a5:f2:d5:f6:50:87:
        a2:70:7a:9d:07:13:2b:f6:7a:56:ce:5b:ca:94:34:
        55:bd:6f:6f:22:f6:31:2a:d5:7d:40:c5:52:f6:c0:
        d4:e5:a6:ff:2e:71:73:05:68:33:cc:7b:74:c6:68:
        8d:e7:68:83:b3:14:d5:5a:59:24:fc:d2:02:fc:93:
        f6:75:49:62:01:ec:61:30:2d:d7:20:60:41:9d:a2:
        b6:18:9d:16:eb:f4:cd:15:a2:2d:1d:0a:82:cf:3c:
        a0:5c:ce:59:10:5c:e0:33:e4:96:1d:f1:d2:a5:d7:
        de:e8:6c:ba:dd:6d:06:97:e7:98:d5:c6:fc:c8:95:
        ed:1c:bf:6a:99:69:3a:a8:e6:c4:d7:92:b5:8e:28:
        49:c1
    prime1:
        00:f5:d2:83:de:48:f0:25:56:0a:ec:c3:e6:73:eb:
        0f:72:cb:aa:10:e1:d4:f7:39:b0:7a:71:6d:6f:28:
        4b:15:4d:15:5d:64:cb:7f:d2:91:1a:e6:f9:ee:09:
        f9:c9:bb:53:89:0d:4a:37:29:45:8b:b7:5e:c1:38:
        17:48:3f:b1:5b:4c:a4:93:38:f4:5b:c3:63:91:95:
        2e:4c:3f:c6:39:e0:f0:53:a3:ee:5b:ee:95:0b:1e:
        ed:3d:73:64:12:40:76:92:e2:ec:91:c6:33:36:fe:
        d4:8f:0d:02:52:03:07:ee:63:79:0c:4f:a7:2b:41:
        5a:3b:d6:4f:6d:d0:80:26:7b
    prime2:
        00:c9:d0:8f:12:87:d8:f9:1a:a6:1e:fd:69:0b:34:
        b5:a5:20:ae:11:34:d6:fe:1b:2f:d7:d1:5e:55:81:
        d9:6b:79:07:db:64:5f:0e:c5:22:ee:36:ce:18:d6:
        a5:0d:8c:4c:7a:ae:31:d9:f5:7d:73:e6:4b:ad:6a:
        46:32:3a:22:f3:40:ce:c5:50:c5:73:b3:d4:76:86:
        72:5c:30:dd:4d:ba:5e:2f:1e:a5:b8:17:05:42:cf:
        46:08:de:da:b4:6c:48:3b:98:ac:25:6d:1f:19:61:
        33:12:7b:95:87:36:dc:f2:f7:8d:30:e5:9f:20:94:
        97:8b:c2:1f:8d:8d:ea:e1:4b
    exponent1:
        55:dd:8e:ca:5a:57:e7:f2:c2:26:29:d7:99:ae:05:
        db:67:60:a4:3c:fe:12:cd:47:e3:bd:33:28:9c:be:
        7d:56:4b:9c:2f:d5:15:75:0b:d2:85:d3:cf:5e:14:
        ae:6e:8c:a3:56:cd:11:af:8c:e7:5c:c9:f0:5c:13:
        65:dd:39:aa:56:7f:36:1d:b2:dd:4a:c6:c0:d7:87:
        30:83:26:4e:99:4f:d9:27:6d:df:16:db:60:e3:10:
        a3:62:67:16:29:06:42:10:99:e9:e1:7d:8a:3c:41:
        2b:26:b4:24:c9:82:3f:b6:e7:55:71:8d:47:02:b0:
        ee:2d:d1:d8:dd:f7:a5:79
    exponent2:
        00:b9:71:d0:96:49:88:41:d6:90:01:78:00:57:50:
        b6:fd:26:5b:6c:ea:2e:08:4f:79:16:0a:88:71:70:
        21:16:55:9f:b7:a4:b2:88:82:f3:87:0b:8b:34:5d:
        c0:4b:03:b9:9f:1d:84:27:71:22:37:26:ce:31:6a:
        af:58:25:fd:c9:a2:aa:9d:bb:8b:c4:b6:e1:2b:8c:
        7d:77:63:5b:67:ba:32:23:80:38:ed:41:12:0f:83:
        21:2a:b3:85:2a:37:39:e4:b1:74:b5:eb:60:a1:54:
        a4:b6:7e:23:37:9d:5d:48:51:db:46:ac:29:1d:aa:
        0c:db:5a:a4:dd:d1:23:9c:a3
    coefficient:
        00:c8:dc:50:0f:62:74:36:cb:79:ff:8a:b6:94:b8:
        6b:14:41:b6:80:15:ce:8e:04:cc:34:e6:6f:4f:87:
        fe:8e:6f:71:29:85:bd:75:00:52:c4:e1:b7:2f:63:
```

```
8f:12:de:62:0e:90:48:2f:c3:3c:9f:80:21:ac:8a:
03:1f:4d:77:c6:00:e0:e3:c6:4b:ad:2c:45:14:55:
ac:75:1c:63:34:ef:f0:46:00:b8:05:36:03:78:cd:
57:eb:d8:b1:09:31:b3:b3:82:38:4a:3b:da:91:8c:
aa:e6:52:e9:fb:8e:06:60:d3:ec:a3:f5:f1:f2:b6:
06:8b:d3:08:ec:f1:fb:6a:7e
```

2.3.3.4.2 Security of Server Private Key file

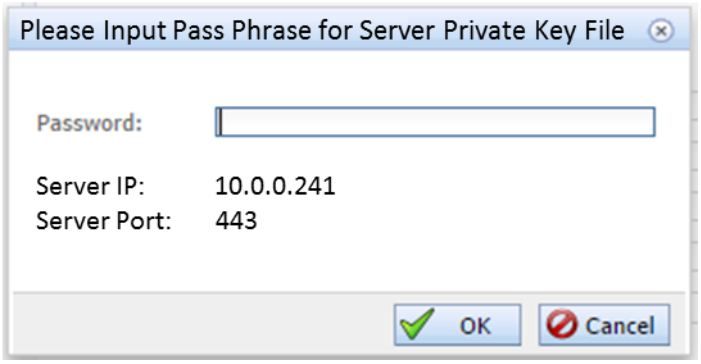
It is recommended to use a PEM file as a vehicle to upload server private key. The PEM file, if configured properly and often by default will have a passphrase to protect the server private key information.

When FlowMagic stores the PEM file to hard drive, the PEM file is stored in original encrypted form within the domain configuration. This essentially gives the private key file the same level of security as if it is stored on server.

Once the domain is configured and activated by the operator, a dialog will be displayed to ask for pass phrase for each and every PEM file. The pass phrase is used only once and is not stored on FlowMagic.

FlowMagic will use the pass phrase to read out the private exponent and modulus in the PEM file and pass the data to decryption module. The decryption module keeps data in the RAM and the rest copy will be erased with 0.

When operator disables the domain, the key data stored in decryption module's RAM will be erased with 0 before the domain is disabled.



Optionally, FlowMagic decryption module has the ability to interop with the Enterprise Key Management Solution from SafeNet Inc. through KMIP protocol. Please contact InfiniCORE for detailed agreement.

2.3.3.5 Traffic Post Processing

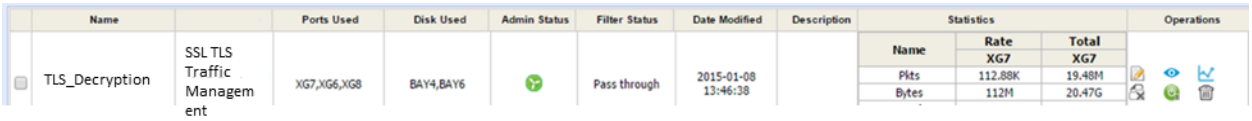
After packet is decrypted, the original TCP layer can be kept intact or the destination port within the original TCP layer can be updated with a new port.

For example, by specifying the new destination port be 80, the original HTTPS traffic with destination port 443 will be sent to downstream device as HTTP traffic on port 80.

Chapter 3 Monitoring SSL/TLS Traffic Management Domain

One the configuration is completed and downloaded to hardware, the domain will be activated and start to process the traffic.

Once the domain is active, the real time statistics will be collected and displayed in the “Flow OPS” tab.



Name		Ports Used	Disk Used	Admin Status	Filter Status	Date Modified	Description	Statistics			Operations
								Name	Rate XG7	Total XG7	
TLS_Decryption	SSL TLS Traffic Management	XG7,XG6,XG8	BAY4,BAY6		Pass through	2015-01-08 13:46:38		Pkts	112.88K	19.48M	
								Bytes	112M	20.47G	

The following real time statistics are also collected for diagnosis purpose.

- Packet Rate
  Indicate the packet rate of each interface
- Bit Rate
  Indicate the throughput of each interface
- Dropped Packet Rate
  Indicates the number of packets are dropped before decryption engine
- SSL/TLS Connections
  Indicate the number of SSL/TLS connections processed by SSL/TLS decryption engine
- Decrypted Packet
  Indicate the number of successfully decrypted packets

Chapter 4 Recommended Reading Material

The following list provides further reading materials when users find the need to gain in-depth knowledge in specific area.

- UM101- FlowMagic Operating System Dashboard User Manual
- UM102- FlowMagic Operating System Interfaces User Manual
- UM103- FlowMagic Operating System Storages User Manual
- UM104- FlowMagic Operating System Capture Operations User Manual
- UM106- FlowMagic Operating System Traffic Recreation User Manual
- UM107- FlowMagic Operating System Data Navigation User Manual
- UM108- FlowMagic Operating System PCAP Management User Manual
- UM109- FlowMagic Operating System SysLog User Manual
- UM110- FlowMagic Operating System Capture and NFS Share PCAP User Manual
- UM111- FlowMagic Operating System HTTP Header Rewrite Engine User Manual
- UM112- FlowMagic Operating System Traffic Micro Burst Analysis User Manual
- UM113- FlowMagic Operating System Traffic Geo Fence User Manual
- UM114- FlowMagic Operating System Traffic Normalization User Manual