Understanding Traffic Decryption

By default, the system cannot inspect traffic encrypted with the Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. As part of access control, the *SSL inspection* feature allows you to either block encrypted traffic without inspecting it, or inspect encrypted or decrypted traffic with access control. As the system handles encrypted sessions, it logs details about the traffic. The combination of inspecting encrypted traffic and analyzing encrypted session data allows greater awareness and control of the encrypted applications and traffic in your network.

If the system detects an SSL or TLS handshake over a TCP connection, it determines whether it can decrypt the detected traffic. If it cannot, it applies a configured action:

- block the encrypted traffic, and optionally reset the TCP connection
- not decrypt the encrypted traffic

Note that access control rules handle encrypted traffic when your SSL inspection configuration allows it to pass, or if you do not configure SSL inspection. However, some access control rule conditions require unencrypted traffic, so encrypted traffic may match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured. For more information, see Creating and Editing Access Control Rules, page 14-2 and Using the SSL Preprocessor, page 27-69.

If the system can decrypt the traffic, it blocks the traffic without further inspection, evaluates undecrypted traffic with access control, or decrypts it using one of the following methods:

- Decrypt with a known private key. When an external host initiates an SSL handshake with a server on your network, the system matches the exchanged server certificate with a server certificate previously uploaded to the appliance. It then uses the uploaded private key to decrypt the traffic.
- Decrypt by re-signing the server certificate. When a host on your network initiates an SSL handshake with an external server, the system re-signs the exchanged server certificate with a previously uploaded certificate authority (CA) certificate. It then uses the uploaded private key to decrypt the traffic.

Decrypted traffic is subject to the same traffic handling and analysis as originally unencrypted traffic: network, reputation, and user-based access control; intrusion detection and prevention; advanced malware protection; and discovery. If the system does not block the decrypted traffic post-analysis, it reencrypts the traffic before passing it to the destination host.

Note Certain SSL inspection actions, such as blocking traffic and decrypting outgoing traffic, modify the flow of traffic. Devices deployed inline can perform these actions. Devices deployed passively or in tap mode cannot affect the flow of traffic. However, these devices can still decrypt incoming traffic; see Example: Decrypting Traffic in a Passive Deployment, page 19-5 for more information.

For more information, see the following sections:

- SSL Inspection Requirements, page 19-2
- Analyzing SSL Inspection Appliance Deployments, page 19-5

SSL Inspection Requirements

License: feature dependent

Supported Devices: Series 3

Only certain appliance models support SSL inspection. How you deploy the appliances on your network, in addition to your configuration settings and licenses, influences the actions you can take to control and decrypt encrypted traffic.

Available features and actions to configure SSL inspection depend on your user role. The system includes predefined user roles designed for a variety of administrators and analysts, and you can create custom user roles with specialized access privileges.

SSL inspection requires public key certificates and paired private keys for certain features. You must upload certificates and paired private keys to the Defense Center to decrypt and control traffic based on encryption session characteristics.

For more information, see the following sections:

- Deploying Appliances that Support SSL Inspection, page 19-2
- Determining Necessary Licenses for SSL Inspection, page 19-2
- Managing Your SSL Inspection Deployment with Custom User Roles, page 19-3
- Collecting Prerequisite Information to Configure SSL Rules, page 19-4

Deploying Appliances that Support SSL Inspection

License: Any

Supported Devices: Series 3

SSL inspection requires a Series 3 device.

Devices configured and deployed with inline, routed, switched, or hybrid interfaces can modify the flow of traffic. These devices can monitor, block, allow, and decrypt incoming and outgoing traffic.

Devices configured and deployed with passive or inline (tap mode) interfaces cannot affect the flow of traffic. They can only monitor, allow, and decrypt incoming traffic. Note that passive deployments do not support decrypting traffic encrypted with the ephemeral Diffie-Hellman (DHE) or the elliptic curve Diffie-Hellman (ECDHE) cipher suites.

Review your list of mapped actions, existing network deployment, and overall requirements to determine whether one or the other type of deployment better suits your organization. See Analyzing SSL Inspection Appliance Deployments, page 19-5 for more information.

Determining Necessary Licenses for SSL Inspection

License: feature dependent

Depending on your licenses, you can use a combination of criteria to determine how to handle encrypted traffic. Although you can create SSL policies regardless of the licenses on your Defense Center, certain aspects of SSL inspection require that you enable specific licensed capabilities on target devices before you can apply the policy. The Defense Center uses warning icons ( ) and confirmation dialog boxes to designate unsupported features for your deployment. For details, hover your pointer over a warning icon.

You apply an SSL policy to a managed device as part of an access control policy, and the access control policy inspects traffic decrypted by the SSL policy. See Access Control License and Role Requirements, page 12-2 for more information on access control licensing.

The following table explains the license requirements to apply an SSL policy as part of an access control policy.

Table 19-1 License and Model Requirements for SSL Inspection

To apply an SSL policy that...	Licenses	Supported Defense Centers	Supported Devices
handles encrypted traffic on the basis of zone, network, VLAN, port, or SSL-related criteria	Any	Any	Series 3
handles encrypted traffic using geolocation data	FireSIGHT	Any except DC500	Series 3
handles encrypted traffic using application or user criteria	Control	Any, except the DC500 cannot perform user control	Series 3
filters encrypted traffic using URL category and reputation data	URL Filtering	Any except DC500	Series 3

Managing Your SSL Inspection Deployment with Custom User Roles

License: Any

As described in Managing Custom User Roles, page 61-53, you can create custom user roles with specialized access privileges. Custom user roles can have any set of menu-based and system permissions, and may be completely original or based on a predefined user role. The following table describes the role permissions that determine the user's privileges to configure and deploy SSL inspection:

Table 19-2 SSL Inspection-Related User Role Permissions

User Permission	Description
Object Manager	allows you to create, modify, and delete objects related to SSL inspection
SSL	allows you to generate reports for SSL policies and compare SSL policies or policy revisions
Modify SSL Policy	allows you to view, create, modify, and delete an SSL policy, and create, modify, and delete SSL rules not in the Administrator Rules or Root Rules categories
Modify Administrator Rules	allows you to create, modify, and delete SSL rules in the Administrator Rules category
Modify Root Rules	allows you to create, modify, and delete SSL rules in the Root Rules category

Table 19-2 SSL Inspection-Related User Role Permissions (continued)

User Permission	Description
Apply SSL Policy	allows you to apply an SSL policy if you apply the access control policy with which it is associated
Access Control List	allows you to view the list of access control policies
Modify Access Control Policy	allows you to associate an SSL policy with an access control policy
Apply Access Control Policies	allows you to apply the access control policy associated with the SSL policy

For more information, see Access Control License and Role Requirements, page 12-2.

Collecting Prerequisite Information to Configure SSL Rules

License: feature-dependent

SSL inspection relies on a significant amount of supporting public key infrastructure (PKI) information. Consider your organization's traffic patterns to determine the matching rule conditions you can configure. Collect the information listed in the following table:

Table 19-3 SSL Rule Condition Prerequisites

To match on...	Collect the...
detected server certificates, including self-signed server certificates	server certificate
trusted server certificates	CA certificate
detected server certificate subject or issuer	server certificate subject DN or issuer DN

For more information, see Tuning Traffic Decryption Using SSL Rules, page 22-1.

Decide whether you want to not decrypt, block, monitor, or decrypt the encrypted traffic you match your rules against. Map these decisions to SSL rule actions, undecryptable traffic actions, and the SSL policy default action. If you want to decrypt traffic, see the following table:

Table 19-4 SSL Decryption Prerequisites

To decrypt...	Collect...
incoming traffic to a server you control	the server's certificate file and paired private key file
outgoing traffic to an external server	a CA certificate file and paired private key file You can also generate a CA certificate and private key.

For more information, see Using Rule Actions to Determine Encrypted Traffic Handling and Inspection, page 21-8.

After you have collected this information, upload it to the system and configure reusable objects. See Managing Reusable Objects, page 3-1 for more information.

Analyzing SSL Inspection Appliance Deployments

License: feature-dependent

Supported Devices: Series 3

This section presents several scenarios in which the Life Insurance Example, Inc. life insurance company (LifeIns) uses SSL inspection on encrypted traffic to help audit their processes. Based on their business processes, LifeIns plans to deploy:

- one Series 3 managed device in a passive deployment for the Customer Service department
- one Series 3 managed device in an inline deployment for the Underwriting Department
- one Defense Center to manage both devices

Customer Service Business Processes

LifeIns created a customer-facing website for their customers. LifeIns receives encrypted questions and requests regarding policies from prospective customers through their website and through e-mail. LifeIns's Customer Service department processes them and returns the requested information within 24 hours. Customer Service wants to expand its incoming contact metrics collection. LifeIns has an established internal audit review for Customer Service.

LifeIns also receives encrypted applications online. The Customer Service department processes the applications within 24 hours before sending the case file to the Underwriting department. Customer Service filters out any obvious false applications sent through the online form, which consumes a fair portion of their time.

Underwriting Business Processes

LifeIns's underwriters submit encrypted medical information requests online to the Medical Repository Example, LLC medical data repository (MedRepo). MedRepo reviews the requests and transmits the encrypted records to LifeIns within 72 hours. The underwriters subsequently underwrite an application and submit policy and rate decisions. Underwriting wants to expand its metrics collection.

Lately, an unknown source has been sending spoofed responses to LifeIns. Though LifeIns's underwriters receive training on proper Internet use, LifeIns's IT department first wants to analyze all encrypted traffic that takes the form of medical responses, then wants to block all spoof attempts.

LifeIns places junior underwriters on six-month training periods. Lately, these underwriters have been incorrectly submitting encrypted medical regulation requests to MedRepo's customer service department. MedRepo has submitted multiple complaints to LifeIns in response. LifeIns plans on extending their new underwriter training period to also audit underwriter requests to MedRepo.

For more information, see the following sections:

- Example: Decrypting Traffic in a Passive Deployment, page 19-5
- Example: Decrypting Traffic in an Inline Deployment, page 19-10

Example: Decrypting Traffic in a Passive Deployment

License: feature-dependent

Supported Devices: Series 3

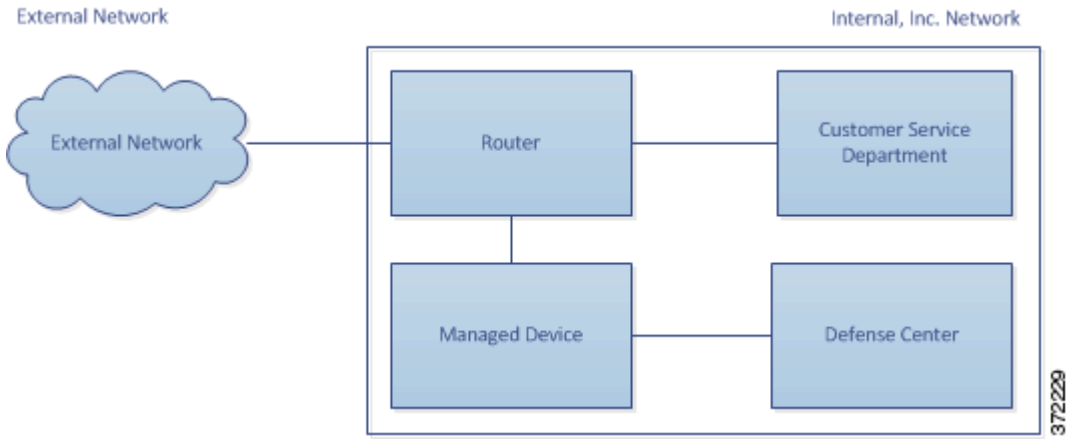
LifeIns's business requirements state that Customer Service must:

- process all requests and applications within 24 hours

- improve its incoming contact metrics collection process
- identify and discard incoming false applications

Customer Service does not require additional audit review.

LifeIns plans to passively deploy a Customer Service managed device. The following diagram illustrates LifeIns's passive deployment.



Traffic from an external network goes to LifeIns's router. The router routes traffic to the Customer Service department, and mirrors a copy of the traffic to the managed device for inspection.

On the managing Defense Center, a user in the Access Control and SSL Editor custom role configures SSL inspection to:

- log all encrypted traffic sent to the Customer Service department
- decrypt encrypted traffic sent using the online application form to Customer Service
- not decrypt all other encrypted traffic sent to Customer service, including traffic sent using the online request form

The user also configures access control to inspect the decrypted application form traffic for fake application data and log when fake data is detected.

In the following scenarios, the user submits an online form to Customer Service. The user's browser establishes a TCP connection with the server, then initiates an SSL handshake. The managed device receives a copy of this traffic. The client and server complete the SSL handshake, establishing the encrypted session. Based on handshake and connection details, the system logs the connection and acts upon the copy of the encrypted traffic.

For more information, see the following:

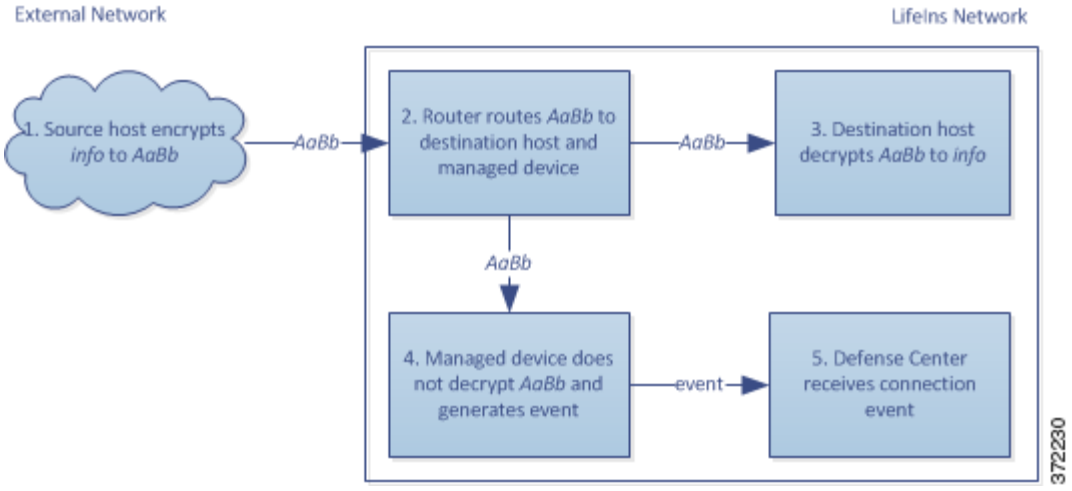
- Monitoring Encrypted Traffic in a Passive Deployment, page 19-6
- Not Decrypting Encrypted Traffic in a Passive Deployment, page 19-7
- Inspecting Encrypted Traffic with a Private Key in a Passive Deployment, page 19-8

Monitoring Encrypted Traffic in a Passive Deployment

License: Any

Supported Devices: Series 3

For all SSL-encrypted traffic sent to Customer Service, the system logs the connection. The following diagram illustrates the system monitoring encrypted traffic.



The following steps occur:

1. The user submits the plain text request (`info`). The client encrypts this (`AaBb`) and sends the encrypted traffic to Customer Service.
2. LifeIns's router receives the encrypted traffic and routes it to the Customer Service department server. It also mirrors a copy to the managed device.
3. The Customer Service department server receives the encrypted information request (`AaBb`) and decrypts it to plain text (`info`).
4. The managed device does not decrypt the traffic.

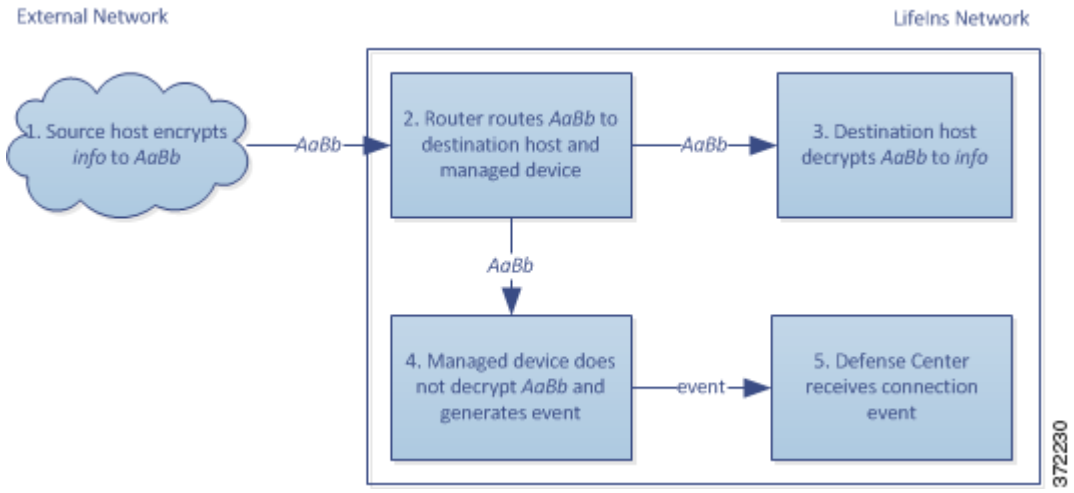
   The access control policy continues to process the encrypted traffic and allows it. The device generates a connection event after the session ends.
5. The Defense Center receives the connection event.

Not Decrypting Encrypted Traffic in a Passive Deployment

License: Any

Supported Devices: Series 3

For all SSL-encrypted traffic that contains requests about policies, the system allows the traffic without decrypting it and logs the connection. The following diagram illustrates the system allowing encrypted traffic without further inspection.



The following steps occur:

1. The user submits the plain text request (`info`). The client encrypts this (`AaBb`) and sends the encrypted traffic to Customer Service.
2. LifeIns's router receives the encrypted traffic and routes it to the Customer Service department server. It also mirrors a copy to the managed device.
3. The Customer Service department server receives the encrypted information request (`AaBb`) and decrypts it to plain text (`info`).
4. The managed device does not decrypt the traffic.

   The access control policy continues to process the encrypted traffic and allows it. The device generates a connection event after the session ends.
5. The Defense Center receives the connection event.

Inspecting Encrypted Traffic with a Private Key in a Passive Deployment

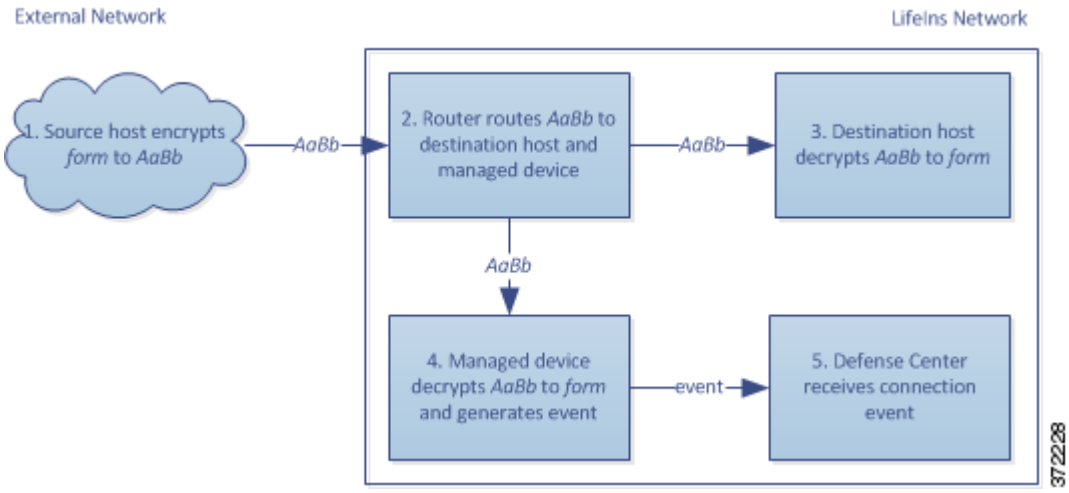
License: Any

Supported Devices: Series 3

For all SSL-encrypted traffic that contains application form data, the system decrypts the traffic and logs the connection.

Note In a passive deployment, if traffic is encrypted with either the DHE or ECDHE cipher suite, you cannot decrypt it with a known private key.

For traffic with legitimate application form information, the system logs the connection. The following diagram illustrates traffic decryption using a known private key.

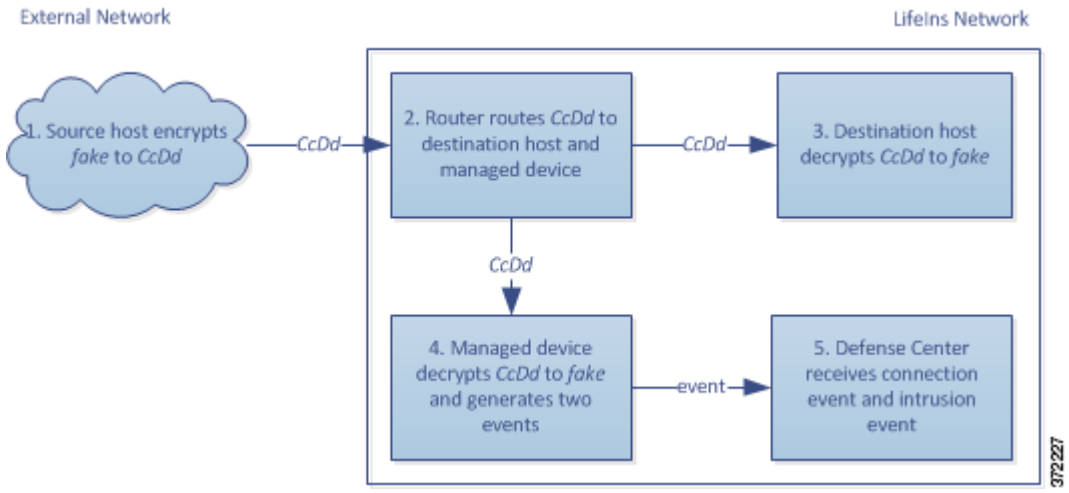


The following steps occur:

1. The user submits the plain text request (`form`). The client encrypts this (`AaBb`) and sends the encrypted traffic to Customer Service.
2. LifeIns's router receives the encrypted traffic and routes it to the Customer Service department server. It also mirrors a copy to the managed device.
3. The Customer Service department server receives the encrypted information request (`AaBb`) and decrypts it to plain text (`form`).
4. The managed device uses the session key obtained with the uploaded known private key to decrypt the encrypted traffic to plain text (`form`).

   The access control policy continues to process the decrypted traffic and does not find fake application information. The device generates a connection event after the session ends.
5. The Defense Center receives a connection event with information about the encrypted and decrypted traffic.

In contrast, if the decrypted traffic contains fake application data, the system logs the connection and the fake data. The following diagram illustrates the system decrypting incoming traffic containing fake application data using a known private key.



The following steps occur:

1. The user submits the plain text request (`fake`). The client encrypts this (`CcDd`) and sends the encrypted traffic to Customer Service.
2. LifeIns's router receives the encrypted traffic and routes it to the Customer Service department server. It also mirrors a copy to the managed device.
3. The Customer Service department server receives the encrypted information request (`CcDd`) and decrypts it to plain text (`fake`).
4. The managed device uses the session key obtained with the uploaded known private key to decrypt the encrypted traffic to plain text (`fake`).

   The access control policy continues to process the decrypted traffic and finds fake application information. The device generates an intrusion event. After the session ends, it generates a connection event.
5. The Defense Center receives a connection event with information about the encrypted and decrypted traffic, and an intrusion event for the fake application data.

Example: Decrypting Traffic in an Inline Deployment

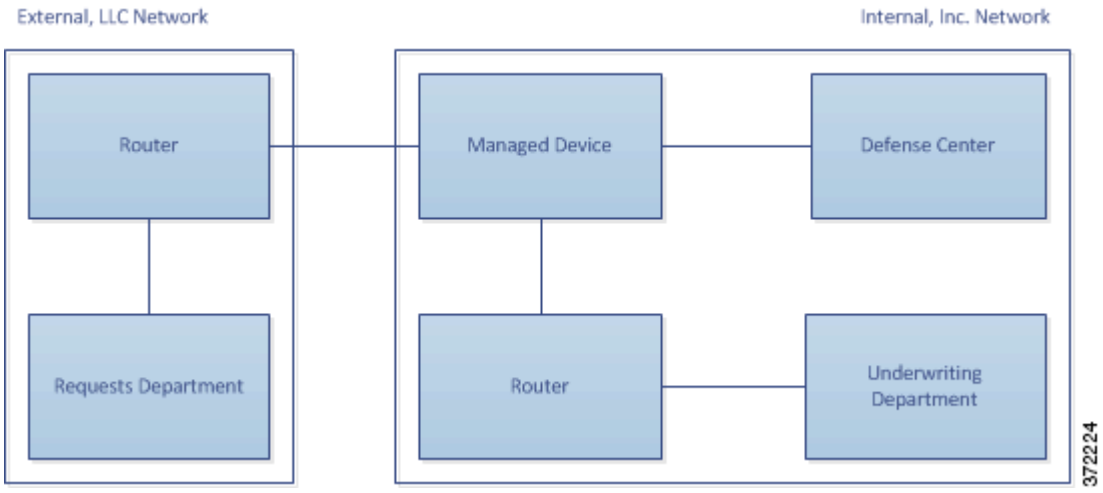
License: feature-dependent

Supported Devices: Series 3

LifeIns's business requirements state that Underwriting must:

- audit new and junior underwriters, verifying that their information requests to MedRepo comply with all applicable regulations
- improve its underwriting metrics collection process
- examine all requests that appear to come from MedRepo, then drop any spoofing attempts
- drop all improper regulatory requests to MedRepo's Customer Service department from the Underwriting department
- not audit senior underwriters

LifeIns plans to deploy a device in an inline deployment for the Underwriting department. The following diagram illustrates LifeIns's inline deployment.



Traffic from MedRepo's network goes to MedRepo's router. It routes traffic to LifeIns's network. The managed device receives the traffic, passes allowed traffic to LifeIns's router, and sends events to the managing Defense Center. LifeIns's router routes traffic to the destination host.

On the managing Defense Center, a user in the Access Control and SSL Editor custom role configures SSL inspection to:

- log all encrypted traffic sent to the Underwriting department
- block all encrypted traffic incorrectly sent from LifeIns's underwriting department to MedRepo's customer service department
- decrypt all encrypted traffic sent from MedRepo to LifeIns's underwriting department, and from LifeIns's junior underwriters to MedRepo's requests department
- not decrypt encrypted traffic sent from the senior underwriters

The user also configures access control to inspect decrypted traffic with a custom intrusion policy and:

- block decrypted traffic if it contains a spoof attempt, and log the spoof attempt
- block decrypted traffic that contains information not compliant with regulations, and log the improper information
- allow all other encrypted and decrypted traffic

The system reencrypts allowed decrypted traffic before sending it to the destination host.

In the following scenarios, the user submits information online to a remote server. The user's browser establishes a TCP connection with the server, then initiates an SSL handshake. The managed device receives this traffic; based on handshake and connection details, the system logs the connection and acts on the traffic. If the system blocks the traffic, it also closes the TCP connection. Otherwise, the client and server complete the SSL handshake, establishing the encrypted session.

For more information, see the following:

- Monitoring Encrypted Traffic in an Inline Deployment, page 19-12
- Allowing Specific Users' Encrypted Traffic in an Inline Deployment, page 19-12
- Blocking Encrypted Traffic in an Inline Deployment, page 19-13

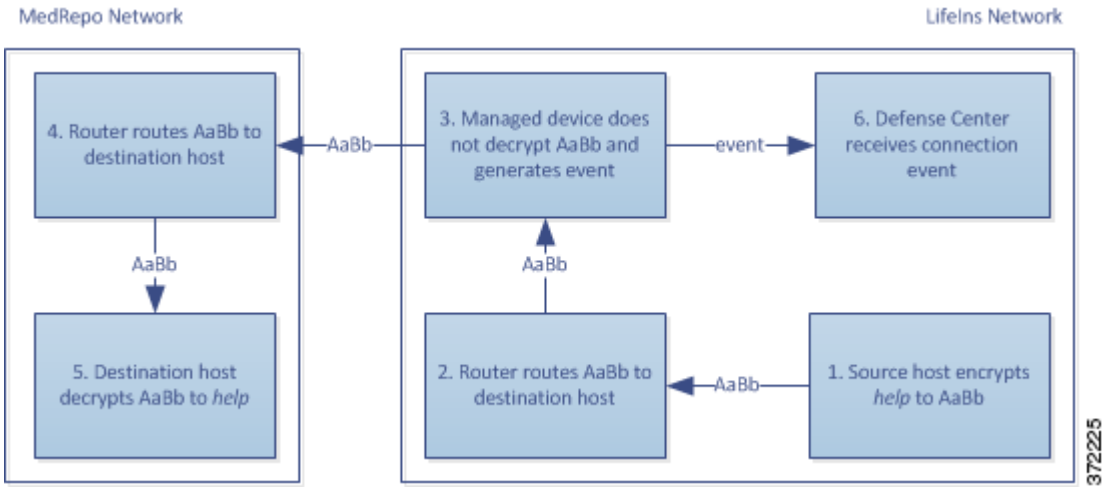
- Inspecting Encrypted Traffic with a Private Key in an Inline Deployment, page 19-14
- Inspecting Specific Users' Encrypted Traffic with a Re-signed Certificate in an Inline Deployment, page 19-16

Monitoring Encrypted Traffic in an Inline Deployment

License: Any

Supported Devices: Series 3

For all SSL-encrypted traffic sent to and from the Underwriting department, the system logs the connection. The following diagram illustrates the system monitoring encrypted traffic.



The following steps occur:

1. The user submits the plain text request (`help`). The client encrypts this (`AaBb`) and sends the encrypted traffic to MedRepo's Requests department server.
2. LifeIns's router receives the encrypted traffic and routes it to the Requests department server.
3. The managed device does not decrypt the traffic.

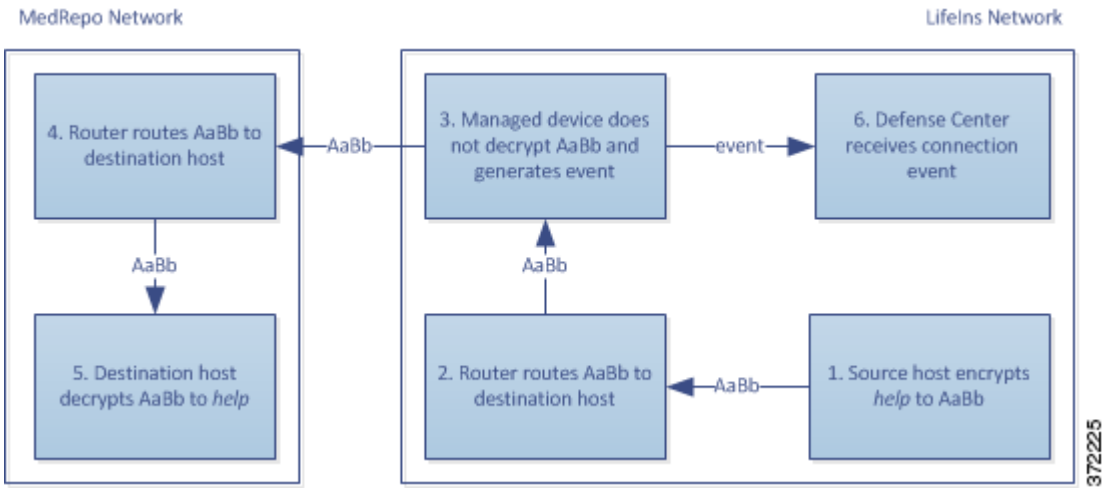
   The access control policy continues to process the encrypted traffic and allows it, then generates a connection event after the session ends.
4. The external router receives the traffic and routes it to the Requests department server.
5. The Underwriting department server receives the encrypted information request (`AaBb`) and decrypts it to plain text (`help`).
6. The Defense Center receives the connection event.

Allowing Specific Users' Encrypted Traffic in an Inline Deployment

License: Control

Supported Devices: Series 3

For all SSL-encrypted traffic originating from the senior underwriters, the system allows the traffic without decrypting it and logs the connection. The following diagram illustrates the system allowing encrypted traffic.



The following steps occur:

1. The user submits the plain text request (`help`). The client encrypts this (`AaBb`) and sends the encrypted traffic to MedRepo's Requests department server.
2. LifeIns's router receives the encrypted traffic and routes it to the Requests department server.
3. The managed device does not decrypt this traffic.

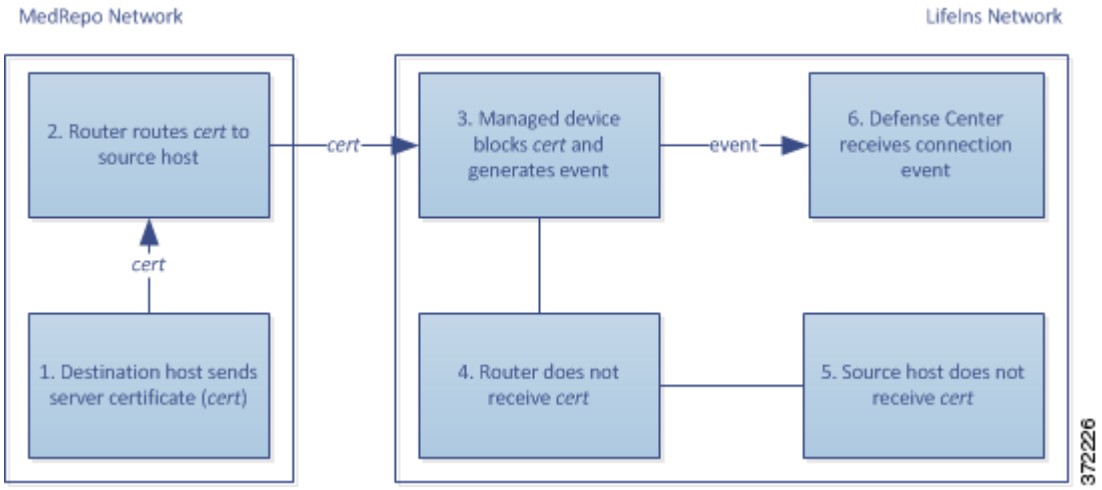
   The access control policy continues to process the encrypted traffic and allows it, then generates a connection event after the session ends.
4. The external router receives the traffic and routes it to the Requests department server.
5. The Requests department server receives the encrypted information request (`AaBb`) and decrypts it to plain text (`help`).
6. The Defense Center receives the connection event.

Blocking Encrypted Traffic in an Inline Deployment

License: Any

Supported Devices: Series 3

For all SMTPS email traffic improperly sent from LifeIns's underwriting department to MedRepo's Customer Service department, the system blocks the traffic during the SSL handshake without further inspection and logs the connection. The following diagram illustrates the system blocking encrypted traffic.



The following steps occur:

1. Having received the request to establish an SSL handshake from a client's browser, the Customer Service department server sends the server certificate (`cert`) as the next step in the SSL handshake to the LifeIns underwriter.
2. MedRepo's router receives the certificate and routes it to the LifeIns underwriter.
3. The managed device blocks the traffic without further inspection and ends the TCP connection. It generates a connection event.
4. The internal router does not receive the blocked traffic.
5. The underwriter does not receive the blocked traffic.
6. The Defense Center receives the connection event.

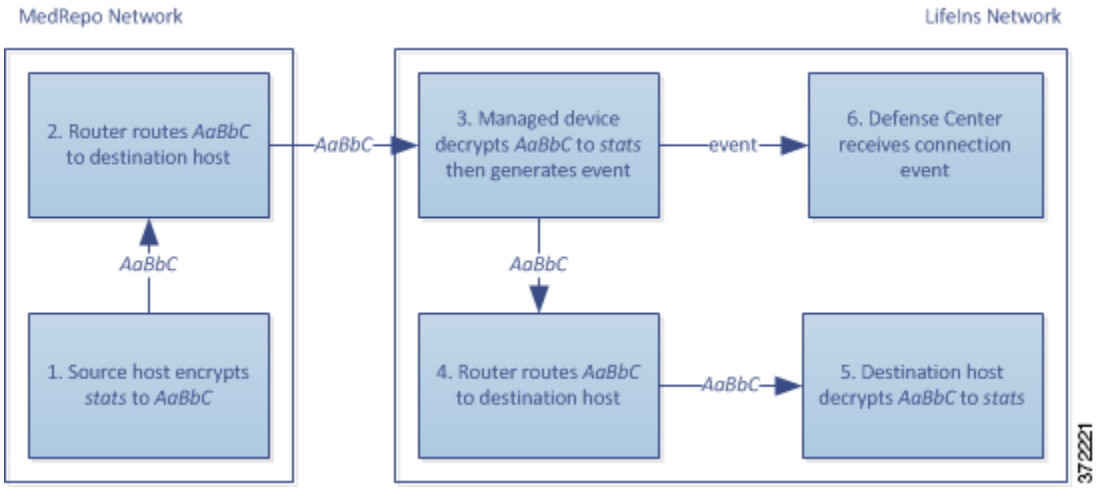
Inspecting Encrypted Traffic with a Private Key in an Inline Deployment

License: Any

Supported Devices: Series 3

For all SSL-encrypted traffic sent from MedRepo to LifeIns's underwriting department, the system uses an uploaded server private key to obtain session keys, then decrypts the traffic and logs the connection. Legitimate traffic is allowed and reencrypted before being sent to the Underwriting department.

The following diagram illustrates the system decrypting encrypted traffic with a known private key, then inspecting the traffic using access control and allowing the decrypted traffic.

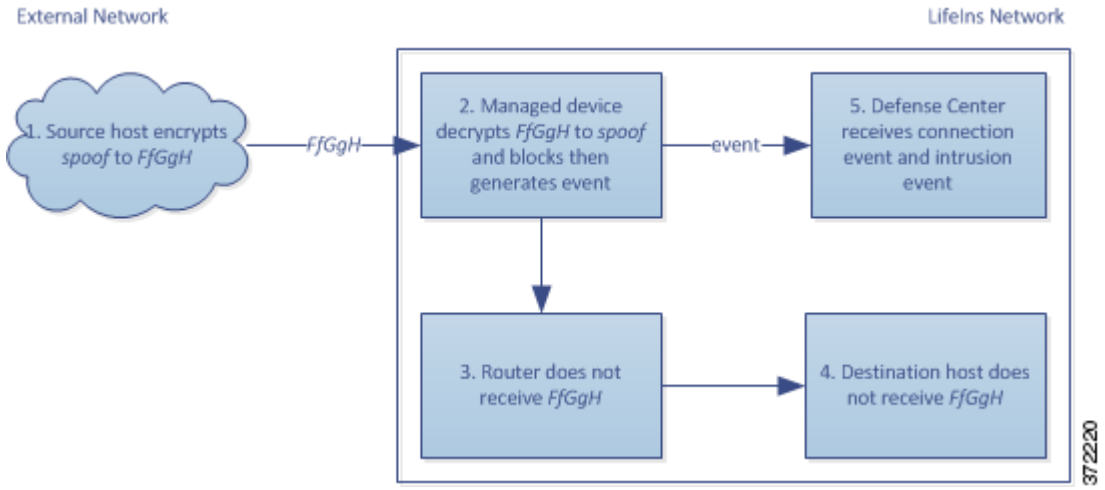


The following steps occur:

1. The user submits the plain text request (`stats`). The client encrypts this (`AaBbC`) and sends the encrypted traffic to the Underwriting department server.
2. The external router receives the traffic and routes it to the Underwriting department server.
3. The managed device uses the session key obtained with the uploaded known private key to decrypt this traffic to plain text (`stats`).

   The access control policy continues to process the decrypted traffic with the custom intrusion policy and does not find a spoof attempt. The device passes the encrypted traffic (`AaBbC`), then generates a connection event after the session ends.
4. The internal router receives the traffic and routes it to the Underwriting department server.
5. The Underwriting department server receives the encrypted information (`AaBbC`) and decrypts it to plain text (`stats`).
6. The Defense Center receives the connection event with information about the encrypted and decrypted traffic.

In contrast, any decrypted traffic that is a spoof attempt is dropped. The system logs the connection and the spoof attempt. The following diagram illustrates the system decrypting encrypted traffic with a known private key, then inspecting the traffic with an access control policy and blocking the decrypted traffic.



The following steps occur:

1. The user submits the plain text request (`spoof`), altering the traffic to appear to originate from MedRepo, LLC. The client encrypts this (`FfGgH`) and sends the encrypted traffic to the Underwriting department server.
2. The managed device uses the session key obtained with the uploaded known private key to decrypt this traffic to plain text (`spoof`).

   The access control policy continues to process the decrypted traffic with the custom intrusion policy and finds a spoof attempt. The device blocks the traffic, then generates an intrusion event. It generates a connection event after the session ends.
3. The internal router does not receive the blocked traffic.
4. The Underwriting department server does not receive the blocked traffic.
5. The Defense Center receives a connection event with information about the encrypted and decrypted traffic, and an intrusion event for the spoofing attempt.

Inspecting Specific Users' Encrypted Traffic with a Re-signed Certificate in an Inline Deployment

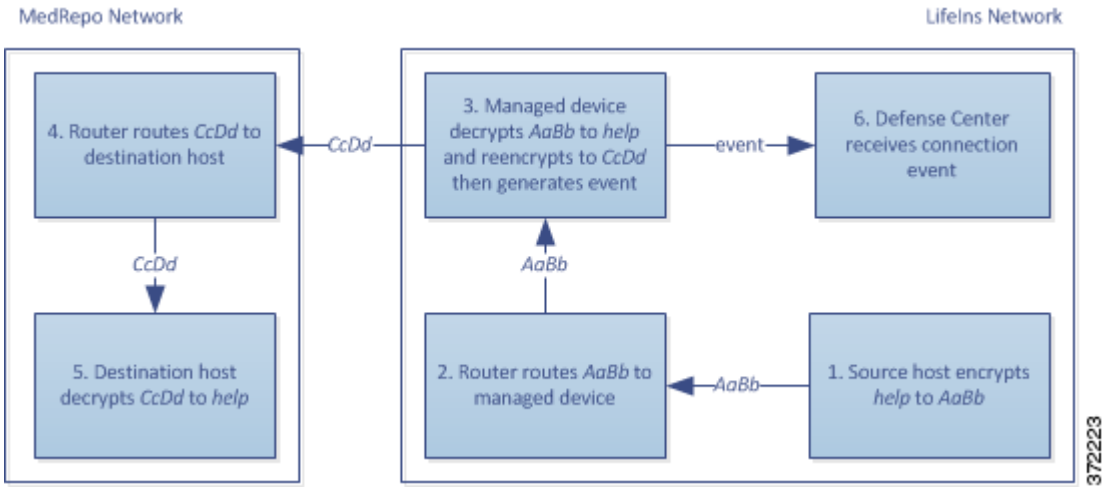
License: Control

Supported Devices: Series 3

For all SSL-encrypted traffic sent from the new and junior underwriters to MedRepo's requests department, the system uses a re-signed server certificate to obtain session keys, then decrypts the traffic and logs the connection. Legitimate traffic is allowed and reencrypted before being sent to MedRepo.

Note When decrypting traffic in an inline deployment by re-signing the server certificate, the device acts as a man-in-the-middle. It creates two SSL sessions, one between client and managed device, one between managed device and server. As a result, each session contains different cryptographic session details.

The following diagram illustrates the system decrypting encrypted traffic with a re-signed server certificate and private key, then inspecting the traffic using access control and allowing the decrypted traffic.



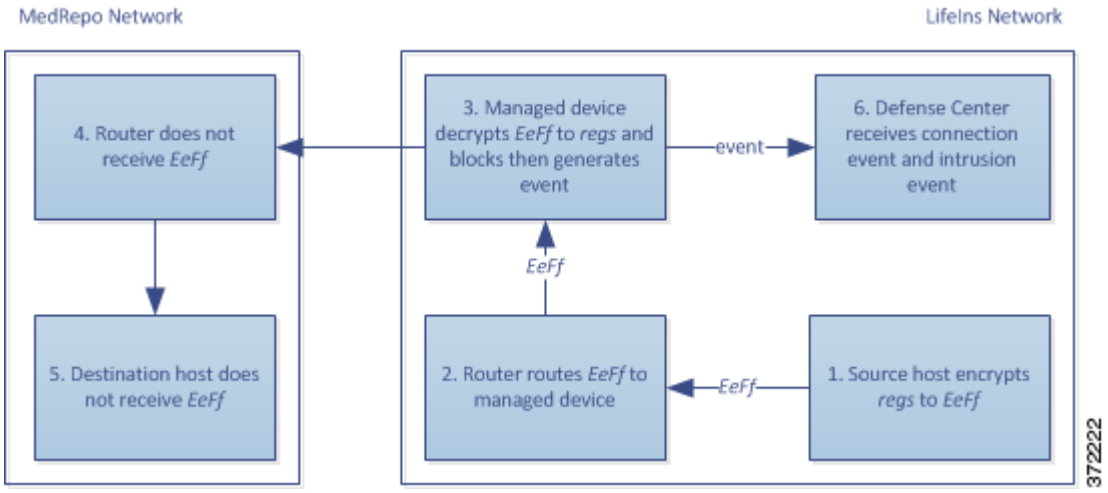
The following steps occur:

1. The user submits the plain text request (`help`). The client encrypts this (`AaBb`) and sends the encrypted traffic to the Requests department server.
2. The internal router receives the traffic and routes it to the Requests department server.
3. The managed device uses the session key obtained with a re-signed server certificate and private key to decrypt this traffic to plain text (`help`).

   The access control policy continues to process the decrypted traffic with the custom intrusion policy and does not find an improper request. The device reencrypts the traffic (`CcDd`), allowing it to pass. It generates a connection event after the session ends.
4. The external router receives the traffic and routes it to the Requests department server.
5. The Requests department server receives the encrypted information (`CcDd`) and decrypts it to plain text (`help`).
6. The Defense Center receives the connection event with information about the encrypted and decrypted traffic.

Note Traffic encrypted with a re-signed server certificate causes client browsers to warn that the certificate is not trusted. To avoid this, add the CA certificate to the organization's domain root trusted certificates store or the client trusted certificates store.

In contrast, any decrypted traffic that contains information that does not meet regulatory requirements is dropped. The system logs the connection and the non-conforming information. The following diagram illustrates the system decrypting encrypted traffic with a re-signed server certificate and private key, then inspecting the traffic with an access control policy and blocking the decrypted traffic.



The following steps occur:

1. The user submits the plain text request (`regs`), which does not comply with regulatory requirements. The client encrypts this (`EeFf`) and sends the encrypted traffic to the Requests department server.
2. The internal router receives the traffic and routes it to the Requests department server.
3. The managed device uses the session key obtained with a re-signed server certificate and private key to decrypt this traffic to plain text (`regs`).

   The access control policy continues to process the decrypted traffic with the custom intrusion policy and finds an improper request. The device blocks the traffic, then generates an intrusion event. It generates a connection event after the session ends.
4. The external router does not receive the blocked traffic.
5. The Requests department server does not receive the blocked traffic.
6. The Defense Center receives a connection event with information about the encrypted and decrypted traffic, and an intrusion event for the improper request.