

Understanding Traffic Decryption

The following topics provide an overview of Transport Layer Security/Secure Sockets Layer (TLS/SSL) inspection, discuss the prerequisites for TLS/SSL inspection configuration, and detail deployment scenarios.

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

The exception is SSL policies. Because the FMC configuration option is **Policies** > **Access Control** > **SSL**, we use the term *SSL policies* although these policies are used to define rules for TLS and SSL traffic.

For more information about SSL and TLS protocols, see a resource such as SSL vs. TLS - What's the Difference?.

- Traffic Decryption Explained, on page 1
- TLS/SSL Handshake Processing, on page 3
- TLS Crypto Acceleration, on page 6
- TLS/SSL Best Practices, on page 9
- How to Configure TLS/SSL Policies and Rules, on page 19
- TLS/SSL Inspection Appliance Deployment Scenarios, on page 21
- History for TLS/SSL, on page 29

Traffic Decryption Explained

By default, the Firepower System cannot inspect traffic encrypted with the Secure Socket Layer (SSL) protocol or its successor, the Transport Layer Security (TLS) protocol. *TLS/SSL inspection* enables 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.

TLS/SSL inspection is a policy-based feature. In the Firepower System, an access control policy is a main configuration that invokes subpolicies and other configurations, including an SSL policy. If you associate an SSL policy with access control, the system uses that SSL policy to handle encrypted sessions before it evaluates them with access control rules. If you do not configure TLS/SSL inspection, or your devices do not support it, access control rules handle all encrypted traffic.

Access control rules also handle encrypted traffic when your TLS/SSL inspection configuration allows it to pass. However, some access control rule conditions require unencrypted traffic, so encrypted traffic might match fewer rules. Also, by default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improves performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

If the system detects a TLS/SSL 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
- Block the encrypted traffic and reset the TCP connection
- Not decrypt the encrypted traffic

If the system cannot decrypt the traffic, it blocks the traffic without further inspection, evaluates undecrypted traffic with access control; otherwise, the system decrypts it using one of the following methods:

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

Note The Firepower System does not support mutual authentication; that is, you cannot upload a client certificate to the FMC and use it for either **Decrypt - Resign** or **Decrypt - Known Key** TLS/SSL rule actions. For more information, see Decrypt and Resign (Outgoing Traffic), on page 11. and Known Key Decryption (Incoming Traffic), on page 12.

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; Cisco Advanced Malware Protection (Cisco AMP); and discovery. If the system does not block the decrypted traffic post-analysis, it re-encrypts the traffic before passing it to the destination host.

Note Set up decrypt rules *only* if your managed device handles encrypted traffic. Decryption rules require processing overhead that can impact performance.

The Firepower System does not currently support TLS version 1.3 encryption or decryption. When users visit a web site that negotiates TLS 1.3 encryption, users might see errors similar to the following in their web browser:

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

For more information about how to control this behavior, contact Cisco TAC.

If you set the value of TCP maximum segment size (MSS) using FlexConfig, the observed MSS could be less than your setting. For more information, see About the TCP MSS.

TLS/SSL Handshake Processing

In this documentation, the term *TLS/SSL handshake* represents the two-way handshake that initiates encrypted sessions in both the SSL protocol and its successor protocol, TLS.

In an inline deployment, the Firepower System processes the TLS/SSL handshake, potentially modifying the ClientHello message and acting as a TCP proxy server for the session.

After the client establishes a TCP connection with the server (after it successfully completes the TCP three-way handshake), the managed device monitors the TCP session for any attempt to initiate an encrypted session. The TLS/SSL handshake establishes an encrypted session via the exchange of specialized packets between client and server. In the SSL and TLS protocols, these specialized packets are called *handshake messages*. The handshake messages communicate which encryption attributes both the client and server support:

- ClientHello—The client specifies multiple supported values for each encryption attribute.
- ServerHello—The server specifies a single supported value for each encryption attribute, which determines which encryption method the system uses during the secure session.

Although the data transmitted in the session is encrypted, the handshake messages are not.

After a TLS/SSL handshake completes, the managed device caches encrypted session data, which allows session resumption without requiring the full handshake. The managed device also caches server certificate data, which allows faster handshake processing in subsequent sessions.

ClientHello Message Handling

The client sends the ClientHello message to the server that acts as the packet destination if a secure connection can be established. The client sends the message to initiate the TLS/SSL handshake or in response to a Hello Request message from the destination server.

If you configure TLS/SSL decryption, when a managed device receives a ClientHello message, the system attempts to match the message to TLS/SSL rules that have the **Decrypt - Resign** or **Decrypt - Known Key** action. The match relies on data from the ClientHello message and from cached server certificate data. Possible data includes:

Table 1: Data Availability for TLS/SSL Rule Conditions

TLS/SSL Rule Condition	Data Present In
Zones	ClientHello
Networks	ClientHello
VLAN Tags	ClientHello
Ports	ClientHello
Users	ClientHello
Applications	ClientHello (Server Name Indicator extension)

TLS/SSL Rule Condition	Data Present In
Categories	ClientHello (Server Name Indicator extension)
Certificate	server Certificate (potentially cached)
Distinguished Names	server Certificate (potentially cached)
Certificate Status	server Certificate (potentially cached)
Cipher Suites	ServerHello
Versions	ServerHello

If the ClientHello message does not match a **Decrypt - Resign** or **Decrypt - Known Key** rule, the system does not modify the message. It then determines whether the message passes access control evaluation (which can include deep inspection). If the message passes, the system transmits it to the destination server.

If the message matches a **Decrypt - Resign** or **Decrypt - Known Key** rule, the system modifies the ClientHello message as follows:

- Compression methods—Strips the `compression_methods` element, which specifies the compression methods the client supports. The Firepower System cannot decrypt compressed sessions. This modification reduces the Compressed Session type of undecryptable traffic.
- Cipher suites—Strips cipher suites from the `cipher_suites` element if the Firepower System does not support them. If the Firepower System does not support any of the specified cipher suites, the system transmits the original, unmodified element. This modification reduces the Unknown Cipher Suite and Unsupported Cipher Suite types of undecryptable traffic.
- Session identifiers—Strips any value from the `Session Identifier` element and the SessionTicket extension that does not match cached session data. If a ClientHello value matches cached data, an interrupted session can resume without the client and server performing the full TLS/SSL handshake. This modification increases the chances of session resumption and reduces the Session Not Cached type of undecryptable traffic.
- Elliptic curves—Strips elliptic curves from the Supported Elliptic Curves extension if the Firepower System does not support them. If the Firepower System does not support any of the specified elliptic curves, the managed device removes the extension and strips any related cipher suites from the `cipher_suites` element.
- ALPN extensions—Strips any value from the Application-Layer Protocol Negotiation (ALPN) extension that is unsupported in the Firepower System (for example, the SPDY and HTTP/2 protocols).
- Other Extensions—Strips the Next Protocol Negotiation (NPN) and TLS Channel IDs extensions.

  SSL rules with a **Decrypt - Resign** or **Decrypt - Known Key** action now natively support the Extended Master Secret (EMS) extension during ClientHello negotiation, enabling more secure communications. The EMS extension is defined by RFC 7627.

Note The system performs these ClientHello modifications by default. If your SSL policy is configured correctly, this default behavior results in more frequent decryption of traffic. To tune the default behavior for your individual network, contact Cisco TAC.

Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. Do not use **Cipher Suite** and **Version** with **Decrypt - Resign** or **Decrypt - Known Key** rule actions. These conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

After the system modifies the ClientHello message, it determines whether the message passes access control evaluation (which can include deep inspection). If the message passes, the system transmits it to the destination server.

Direct communication between the client and server is no longer possible during the TLS/SSL handshake, because after message modification the Message Authentication Codes (MACs) computed by the client and server no longer match. For all subsequent handshake messages (and for the encrypted session once established), the managed device acts as a man-in-the-middle (MITM). It creates two TLS/SSL sessions, one between client and managed device, one between managed device and server. As a result, each session contains different cryptographic session details.

Note The cipher suites that the Firepower System can decrypt are frequently updated and do not correspond directly to the cipher suites you can use in TLS/SSL rule conditions. For the current list of decryptable cipher suites, contact Cisco TAC.

Related Topics

Default Handling Options for Undecryptable Traffic

Encrypted Traffic Inspection with a Re-signed Certificate in an Inline Deployment, on page 27

ServerHello and Server Certificate Message Handling

The ServerHello message is the response to a ClientHello message in a successful TLS/SSL handshake.

After a managed device processes a ClientHello message and transmits it to the destination server, the server determines whether it supports the decryption attributes the client specified in the message. If it does not support those attributes, the server sends a handshake failure alert to the client. If it supports those attributes, the server sends the ServerHello message. If the agreed-upon key exchange method uses certificates for authentication, the server Certificate message immediately follows the ServerHello message.

When the managed device receives these messsages, it attempts to match them with TLS/SSL rules. These messages contain information that was absent from either the ClientHello message or the session data cache. Specifically, the system can potentially match these messages on Distinguished Names, Certificate Status, Cipher Suites, and Versions conditions.

If the messages do not match any TLS/SSL rules, the managed device performs the default action for the SSL policy. For more information, see SSL Policy Default Actions.

If the messages match an SSL rule, the managed device continues as appropriate:

Action: Monitor
The TLS/SSL handshake continues to completion. The managed device tracks and logs but does not decrypt encrypted traffic.

Action: Block or Block with Reset

The managed device blocks the TLS/SSL session. If appropriate, it also resets the TCP connection.

Action: Do Not Decrypt

The TLS/SSL handshake continues to completion. The managed device does not decrypt the application data exchanged during the TLS/SSL session.

Action: Decrypt - Known Key

The managed device attempts to match the server certificate data to an Internal Certificate object previously imported into the Firepower Management Center. Because you cannot generate an Internal Certificate object, and you must possess its private key, we assume you own the server on which you're using known key decryption.

If the certificate matches a known certificate, the TLS/SSL handshake continues to completion. The managed device uses the uploaded private key to decrypt and reencrypt the application data exchanged during the TLS/SSL session.

If the server changes its certificate between the initial connection with the client and subsequent connections, you must import the new server certificate in the Firepower Management Center for future connections to be decrypted.

Action: Decrypt - Resign

The managed device processes the server certificate message and re-signs the server certificate with the previously imported or generated certificate authority (CA). The TLS/SSL handshake continues to completion. The managed device then uses the uploaded private key to decrypt and reencrypt the application data exchanged during the TLS/SSL session.

Note The Firepower System does not support mutual authentication; that is, you cannot upload a client certificate to the FMC and use it for either **Decrypt - Resign** or **Decrypt - Known Key** TLS/SSL rule actions. For more information, see Decrypt and Resign (Outgoing Traffic), on page 11. and Known Key Decryption (Incoming Traffic), on page 12.

TLS Crypto Acceleration

TLS crypto acceleration accelerates the following:

- TLS/SSL encryption and decryption
- VPN, including TLS/SSL and IPsec

Supported Hardware

The following hardware models support TLS crypto acceleration:

- Firepower 2100 with Firewall Threat Defense
- Firepower 4100/9300 with Firewall Threat Defense

  For information about TLS crypto acceleration support on Firepower 4100/9300 Firewall Threat Defense, see the *FXOS Configuration Guide*.

TLS crypto acceleration is *not* supported on any virtual appliances or on any hardware except for the preceding.



Note For more information about TLS crypto acceleration and the 4100/9300, see the *FXOS Configuration Guide*.

Features Not Supported by TLS crypto acceleration

Features *not* supported by TLS crypto acceleration include the following:

- Managed devices where Firewall Threat Defense is enabled.
- If the inspection engine is configured to preserve connections and the inspection engine fails unexpectedly, TLS/SSL traffic is dropped until the engine restarts.

  This behavior is controlled by the **configure snort preserve-connection {enable | disable}** command.

TLS Crypto Acceleration Guidelines and Limitations

Keep the following in mind if your managed device has TLS crypto acceleration enabled.

HTTP-only performance

Using TLS crypto acceleration on a managed device that is not decrypting traffic can affect performance.

Federal Information Processing Standards (FIPS)

If TLS crypto acceleration and Federal Information Processing Standards (FIPS) are both enabled, connections with the following options fail:

- RSA keys less than 2048 bytes in size
- Rivest cipher 4 (RC4)
- Single Data Encryption Standard (single DES)
- Merkle–Damgard 5 (MD5)
- SSL v3

FIPS is enabled when you configure the and managed devices to operate in a security certifications compliance mode. To allow connections when operating in those modes, you can configure web browsers to accept more secure options.

For more information:

- Ciphers supported by FIPS: About SSL Settings.
- Security Certifications Compliance Modes.
- Common Criteria.

TLS heartbeat

Some applications use the *TLS heartbeat* extension to the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols defined by RFC6520. TLS heartbeat provides a way to confirm

the connection is still alive—either the client or server sends a specified number of bytes of data and requests the other party echo the response. If this is successful, encrypted data is sent.

When a managed device with TLS crypto acceleration enabled encounters a packet that uses the TLS heartbeat extension,the managed device takes the action specified by the setting for **Decryption Errors** in the SSL policy's **Undecryptable Actions**:

- Block
- Block with reset

For more information, see Default Handling Options for Undecryptable Traffic.

To determine whether applications are using TLS heartbeat, see Troubleshoot TLS Heartbeat.

You can configure a **Max Heartbeat Length** in a Network Analysis Policy (NAP) to determine how to handle TLS heartbeats. For more information, see The SSL Preprocessor.

TLS/SSL oversubscription

TLS/SSL oversubscription is a state where a managed device is overloaded with TLS/SSL traffic. Any managed device can experience TLS/SSL oversubscription but only managed devices that support TLS crypto acceleration provide a configurable way to handle it.

When a managed device with TLS crypto acceleration enabled is oversubscribed, any packet received by the managed device is acted on according to the setting for **Handshake Errors** in the SSL policy's **Undecryptable Actions**:

- Inherit default action
- Do not decrypt
- Block
- Block with reset

If the setting for **Handshake Errors** in the SSL policy's **Undecryptable Actions** is **Do Not decrypt** and the associated access control policy is configured to inspect the traffic, inspection occurs; decryption does *not* occur.

If a significant amount of oversubscription is occurring, you have the following options:

- Upgrade your managed devices to increase TLS/SSL processing capacity.
- Change your SSL policies to add **Do Not Decrypt** rules for traffic that is not a high priority to decrypt.

View the status of TLS crypto acceleration

This topic discusses how you can determine if TLS crypto acceleration is enabled.

Perform the following task in the FMC.

Procedure

Step 1 Log in to the FMC.

Step 2 Click **Devices** > **Device Management**.

Step 3 Click **Edit** ( ) to edit a managed device.

Step 4 Click **Device** page. TLS crypto acceleration status is displayed in the General section.

TLS/SSL Best Practices

This section discusses information you should keep in mind when creating your decryption policies and rules.

Note Because TLS and SSL are often used interchangeably, we use the expression *TLS/SSL* to indicate that either protocol is being discussed. The SSL protocol has been deprecated by the IETF in favor of the more secure TLS protocol, so you can usually interpret *TLS/SSL* as referring to TLS only.

The exception is SSL policies. Because the FMC configuration option is **Policies** > **Access Control** > **SSL**, we use the term *SSL policies* although these policies are used to define rules for TLS and SSL traffic.

For more information about SSL and TLS protocols, see a resource such as SSL vs. TLS - What's the Difference?.

Related Topics

The Case for Decryption, on page 9
When to Decrypt Traffic, When Not to Decrypt, on page 10
Other TLS/SSL Rule Actions, on page 12
TLS/SSL Rule Components, on page 15
TLS/SSL Rule Order Evaluation, on page 16

The Case for Decryption

Only decrypted traffic takes advantage of the Firepower System's threat defense and policy enforcement features. Traffic that is encrypted when it passes through the Firepower System can be allowed or blocked only but it *cannot* be subjected to deep inspection or the full range of policy enforcement (such as intrusion prevention).

All encrypted connections are:

- Sent through the TLS/SSL decryption policy to determine if they should be decrypted or blocked.

  You can also configure TLS/SSL decryption rules to block encrypted traffic of types you know you do not want on your network, such as traffic that uses the nonsecure SSL protocol or traffic with an expired or invalid certificate.

- Any unblocked connections, whether or not decrypted, then go through the access control policy for a final allow or block decision.

Keep in mind that decrypting and then re-encrypting traffic adds a processing load on the device, which can reduce overall system performance.

In summary:

- Encrypted traffic can be allowed or blocked by policy; encrypted traffic *cannot* be inspected
- Decrypted traffic is subject to threat defense and policy enforcement; decrypted traffic can be allowed or blocked by policy

Related Topics

Deep Inspection Using File and Intrusion Policies

When to Decrypt Traffic, When Not to Decrypt

This section provides guidelines on when you should decrypt traffic and when you should allow it to pass through the firewall encrypted.

When not to decrypt traffic

You should not decrypt traffic if doing so is forbidden by:

- Law; for example, some jurisdictions forbid decrypting financial information
- Company policy; for example, your company might forbid decrypting privileged communications
- Privacy regulations
- Traffic that uses certificate pinning (also referred to as *TLS/SSL pinning*) must remain encrypted to prevent breaking the connection

If you elect to bypass decryption for certain types of traffic, no processing is done on the traffic. The encrypted traffic is first evaluated by SSL policy and then proceeds to the access control policy, where a final allow or block decision is made. Encrypted traffic can be allowed or blocked on any TLS/SSL rule condition, including, but not limited to:

- Certificate status (for example, expired or invalid certificate)
- Protocol (for example, the nonsecure SSL protocol)
- Network (security zone, IP address, VLAN tag, and so on)
- Exact URL or URL category
- Port
- User group

SSL policies provide a **Do Not Decrypt** action for this traffic; for more information, see TLS/SSL Rule Do Not Decrypt Action.

Note Neither TLS server identity discovery nor the decryption of TLS 1.3 traffic is supported on 8000 Series devices.

Note The related information links at the end of this topic explain how some aspects of rule evaluation work. Conditions such as URL and application filtering have limitations with respect to encrypted traffic. Make sure you understand those limitations.

When to decrypt traffic

All encrypted traffic must be decrypted to take advantage of the Firepower System's threat protection and policy enforcement features. To the extent your managed device allows traffic to be decrypted (subject to its memory and processing power), you should decrypt traffic that is not protected by law or regulation. If you must decide what traffic to decrypt, base your decision on the risk of allowing the traffic on your network. The Firepower System provides a flexible framework for classifying traffic using rule conditions, which include URL reputation, cipher suite, protocol, and many other factors.

The Firepower System provides two methods of decryption, which are discussed in the following sections.

Related Topics

Decrypt and Resign (Outgoing Traffic), on page 11
Known Key Decryption (Incoming Traffic), on page 12
TLS/SSL Rule Guidelines and Limitations
SSL Rule Order
URL Conditions (URL Filtering)
Application Rule Order

Decrypt and Resign (Outgoing Traffic)

The **Decrypt - Resign** TLS/SSL rule action enables the Firepower System to act as a man in the middle, intercepting, decrypting, and (if the traffic is allowed) inspecting, and re-encrypting it. The **Decrypt - Resign** rule action is used with outgoing traffic; that is, the destination server is outside your protected network.

The FTD device negotiates with the client using an internal Certificate Authority (CA) object specified in the rule and builds an SSL tunnel between the client and the FTD device. At the same time, the device connects to the destination web site and creates an SSL tunnel between the server and the FTD device.

Thus, the client sees the CA certificate configured for the SSL decryption rule instead of the certificate from the destination server. The client must trust the certificate to complete the connection. The FTD device then performs decryption/re-encryption in both directions for traffic between the client and the destination server.

Prerequisite

To use the **Decrypt - Resign** rule action, you must create an internal CA object using a CA file and paired private key file. You can generate a CA and private key in the Firepower System if you don't already have them.



Note The Firepower System does not support mutual authentication; that is, you cannot upload a client certificate to the FMC and use it for either **Decrypt - Resign** or **Decrypt - Known Key** TLS/SSL rule actions. For more information, see Decrypt and Resign (Outgoing Traffic), on page 11. and Known Key Decryption (Incoming Traffic), on page 12.

Related Topics

TLS/SSL Rule Decrypt Actions
External Certificate Objects

Known Key Decryption (Incoming Traffic)

The **Decrypt - Known Key** TLS/SSL rule action uses a server's private key to decrypt traffic. The **Decrypt - Known Key** rule action is used with incoming traffic; that is, the destination server is inside your protected network.

The main purpose of decrypting with a known key is to protect your servers from external attacks.

Prerequisite

To use the **Decrypt - Known Key** rule action, you must create an internal certificate object using the server's certificate file and paired private key file.

Note The Firepower System does not support mutual authentication; that is, you cannot upload a client certificate to the FMC and use it for either **Decrypt - Resign** or **Decrypt - Known Key** TLS/SSL rule actions. For more information, see Decrypt and Resign (Outgoing Traffic), on page 11. and Known Key Decryption (Incoming Traffic), on page 12.

Related Topics

TLS/SSL Rule Decrypt Actions
Internal Certificate Objects

Other TLS/SSL Rule Actions

The following sections discuss other TLS/SSL rule actions.

Related Topics

TLS/SSL Rule Blocking Actions
TLS/SSL Rule Monitor Action

TLS 1.3 Server Identity Discovery

The latest version of the Transport Layer Security (TLS) protocol 1.3, defined by RFC 8446, is the preferred protocol for many web servers to provide secure communications. Because the TLS 1.3 protocol encrypts the server's certificate for additional security, and the certificate is needed to match application and URL filtering criteria in access control rules, the Firepower System provides a way to extract the server certificate *without* decrypting the entire packet.

You can enable this feature, referred to as *TLS server identity discovery*, when you either:

- Associate an SSL policy with an access control policy
- Configure advanced settings for an access control policy

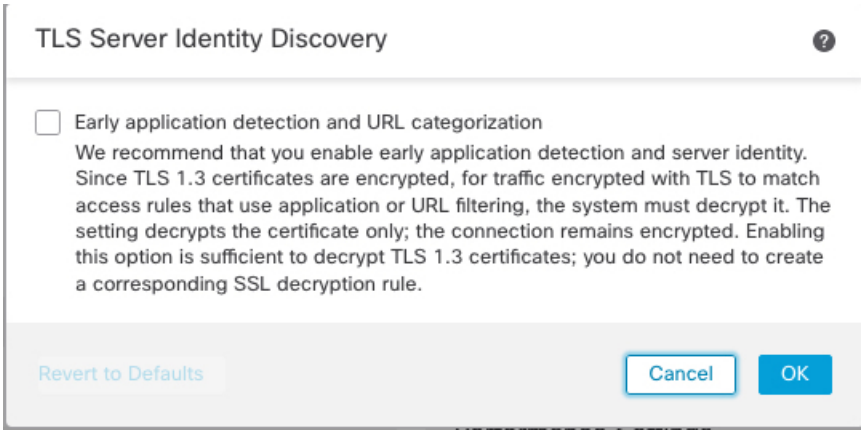
Note Neither TLS server identity discovery nor the decryption of TLS 1.3 traffic is supported on 8000 Series devices.

We strongly recommend enabling it for any traffic you want to match on application or URL criteria, especially if you want to perform deep inspection of that traffic. An SSL policy is not required because *traffic is not decrypted* in the process of extracting the server certificate.

Note

- Because the certificate is decrypted, TLS server identity discovery can reduce performance depending on the hardware platform.
- TLS server identity discovery is not supported in inline tap mode or passive mode deployments.

The following figure shows an example of enabling TLS server identity discovery in an access control policy's advanced settings.



Related Topics

Create Basic SSL Policies
Associating Other Policies with Access Control

TLS/SSL Rule Examples

The following sections provide examples of setting up recommended TLS/SSL rules.

Related Topics

Block Nonsecure Protocols, on page 13

Block Nonsecure Protocols

This example shows how to block TLS and SSL protocols on your network that are no longer considered secure, such as TLS 1.0, TLS 1.1, and SSLv3.

You should exclude nonsecure protocols from your network because they are all exploitable. In this example:

- You can block some protocols using **Version** page on the SSL rule.
- Because the Firepower System considers SSLv2 as undecryptable, you can block it using the **Undecryptable Actions** on the SSL policy.

Procedure

Step 1 Log in to the Firepower Management System if you have not already done so.

Step 2 Click **Policies** > **Access Control** > **SSL**.

Step 3 Add or edit an SSL policy.

Step 4 Click **Add Rule**.

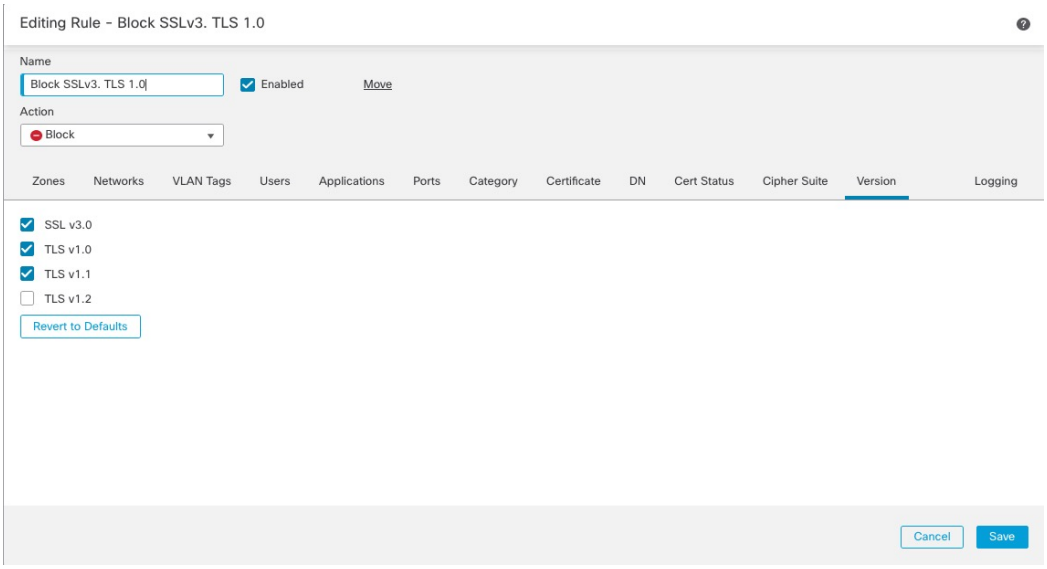
Step 5 In the **Name** field, enter a name for the rule.

Step 6 From the **Action** list, click **Block** or **Block with reset**.

Step 7 Click **Version** page.

Step 8 Check the check boxes for protocols that are no longer secure, such as **SSL v3.0**, **TLS 1.0**, and **TLS 1.1**. Clear the check boxes for any protocols that are still considered secure.

The following figure shows an example.

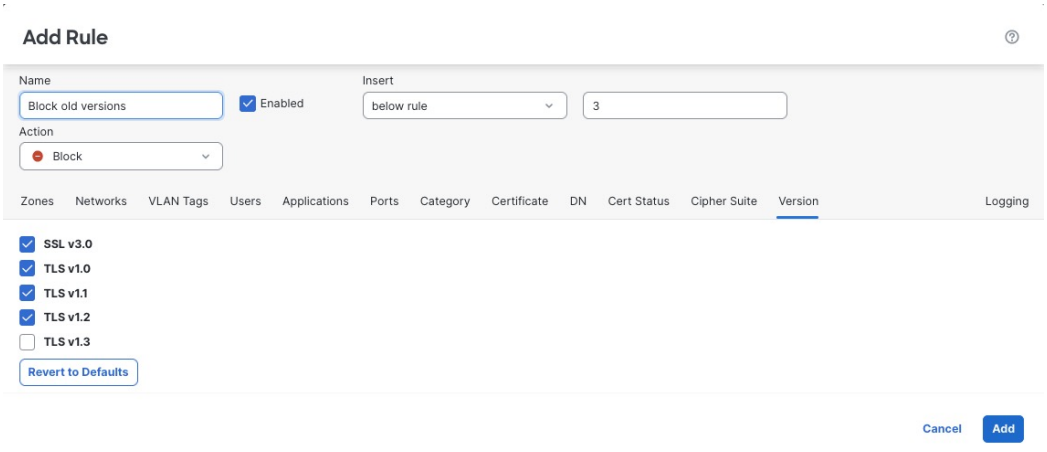


Step 9 Choose other rule conditions as needed.

Step 10 Save the rule.

Step 11 On the SSL policy page, click **Undecryptable Actions**.

Step 12 From the **SSLv2 Session** list, click **Block** or **Block with reset**. The following figure shows an example.



Step 13 Click **Save**.

Step 14 Because this is a specific rule, order it earlier in your policy than more general rules such as application-matching rules.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

TLS/SSL Rule Conditions

TLS/SSL Rule Components

Each TLS/SSL rule has the following components.

State

By default, rules are enabled. If you disable a rule, the system does not use it to evaluate network traffic, and stops generating warnings and errors for that rule.

Position

Rules in an SSL policy are numbered, starting at 1. The system matches traffic to rules in top-down order by ascending rule number. With the exception of Monitor rules, the first rule that traffic matches is the rule that handles that traffic.

Conditions

Conditions specify the specific traffic the rule handles. Conditions can match traffic by security zone, network or geographical location, VLAN, port, application, requested URL, user, certificate, certificate subject or issuer, certificate status, cipher suite, or encryption protocol version. The use of conditions can depend on target device licenses.

Action

A rule's action determines how the system handles matching traffic. You can monitor, allow, block, or decrypt encrypted matching traffic. Decrypted and allowed encrypted traffic is subject to further inspection. Note that the system does **not** perform inspection on blocked encrypted traffic.

Logging

A rule's logging settings govern the records the system keeps of the traffic it handles. You can keep a record of traffic that matches a rule. You can log a connection when the system blocks an encrypted session or allows it to pass without decryption, according to the settings in an SSL policy. You can also force the system to log connections that it decrypts for further evaluation by access control rules, regardless of how the system later handles or inspects the traffic. You can log connections to the Firepower Management Center database, as well as to the system log (syslog) or to an SNMP trap server.

For more information about logging, see Best Practices for Connection Logging.

Tip Properly creating and ordering TLS/SSL rules is a complex task. If you do not plan your policy carefully, rules can preempt other rules, require additional licenses, or contain invalid configurations. To help ensure that the system handles traffic as you expect, the SSL policy interface has a robust warning and error feedback system for rules.

Related Topics

Interface Conditions
Network Conditions
VLAN Conditions
Port and ICMP Code Conditions
Application Conditions (Application Control)
URL Conditions (URL Filtering)
User, Realm, and ISE Attribute Conditions (User Control)
Best Practices for Access Control Rules
TLS/SSL Rule Guidelines and Limitations

TLS/SSL Rule Order Evaluation

When you create the TLS/SSL rule in an SSL policy, you specify its position using the **Insert** list in the rule editor. TLS/SSL rules in an SSL policy are numbered, starting at 1. The system matches traffic to TLS/SSL rules in top-down order by ascending rule number.

In most cases, the system handles network traffic according to the *first* TLS/SSL rule where *all* the rule's conditions match the traffic. Except in the case of Monitor rules (which log traffic but do not affect traffic flow), the system does *not* continue to evaluate traffic against additional, lower-priority rules after that traffic matches a rule. Conditions can be simple or complex; you can control traffic by security zone, network or geographical location, VLAN, port, application, requested URL, user, certificate, certificate distinguished name, certificate status, cipher suite, or encryption protocol version.

Each rule also has an *action*, which determines whether you monitor, block, or inspect matching encrypted or decrypted traffic with access control. Note that the system does *not* further inspect encrypted traffic it blocks. It does subject encrypted and undecryptable traffic to access control. However, access control rule conditions require unencrypted traffic, so encrypted traffic matches fewer rules.

Rules that use *specific* conditions (such as network and IP addresses) should be ordered *before* rules that use general conditions (such as applications). If you're familiar with the Open Systems Interconnect (OSI) model, use similar numbering in concept. Rules with conditions for layers 1, 2, and 3 (physical, data link, and network) should be ordered first in your rules. Conditions for layers 5, 6, and 7 (session, presentation, and application) should be ordered later in your rules. For more information about the OSI model, see this Wikipedia article.

Tip Proper TLS/SSL rule order reduces the resources required to process network traffic, and prevents rule preemption. Although the rules you create are unique to every organization and deployment, there are a few general guidelines to follow when ordering rules that can optimize performance while still addressing your needs.

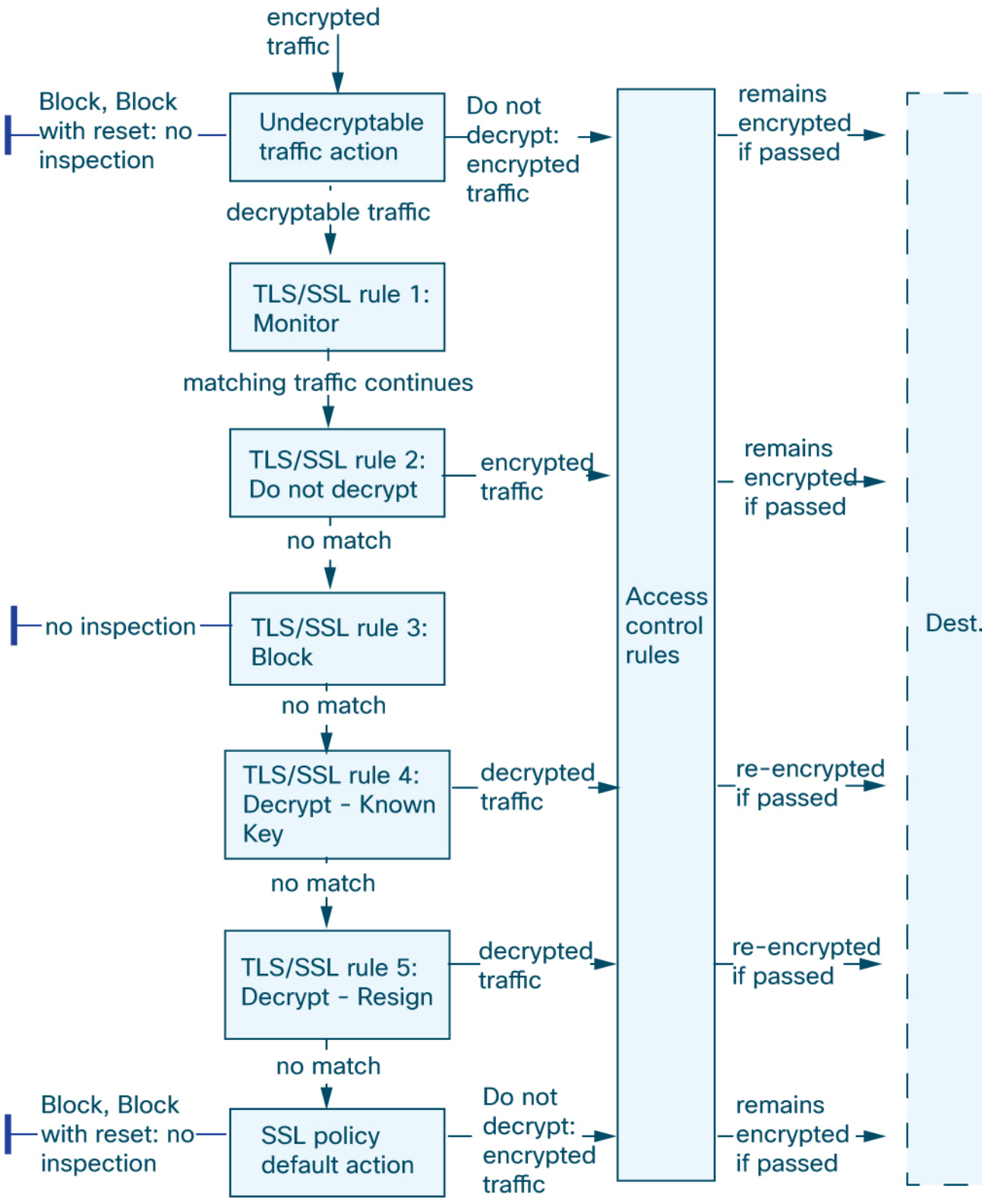
In addition to ordering rules by number, you can group rules by category. By default the system provides three categories: Administrator, Standard, and Root. You can add custom categories, but you cannot delete the system-provided categories or change their order.

Related Topics

Best Practices for Access Control Rules
Default Handling Options for Undecryptable Traffic
SSL Rule Order

Multi-Rule Example

The following scenario summarizes the ways that SSL rules handle traffic in an inline deployment.


encrypted traffic
Block, Block with reset: no inspection
Undecryptable traffic action
Do not decrypt: encrypted traffic
remains encrypted if passed
decryptable traffic
TLS/SSL rule 1: Monitor
matching traffic continues
TLS/SSL rule 2: Do not decrypt
encrypted traffic
remains encrypted if passed
no match
no inspection
TLS/SSL rule 3: Block
Access control rules
Dest.
no match
TLS/SSL rule 4: Decrypt - Known Key
decrypted traffic
re-encrypted if passed
no match
TLS/SSL rule 5: Decrypt - Resign
decrypted traffic
re-encrypted if passed
no match
Block, Block with reset: no inspection
SSL policy default action
Do not decrypt: encrypted traffic
remains encrypted if passed

In this scenario, traffic is evaluated as follows:

- **Undecryptable Traffic Action** evaluates encrypted traffic first. For traffic the system cannot decrypt, the system either blocks it without further inspection or passes it for access control inspection. Encrypted traffic that does not match continues to the next rule.
- **TLS/SSL Rule 1: Monitor** evaluates encrypted traffic next. Monitor rules track and log encrypted traffic but do not affect traffic flow. The system continues to match traffic against additional rules to determine whether to permit or deny it.
- **TLS/SSL Rule 2: Do Not Decrypt** evaluates encrypted traffic third. Matching traffic is not decrypted; the system inspects this traffic with access control, but not file or intrusion inspection. Traffic that does not match continues to the next rule.
- **TLS/SSL Rule 3: Block** evaluates encrypted traffic fourth. Matching traffic is blocked without further inspection. Traffic that does not match continues to the next rule.
- **TLS/SSL Rule 4: Decrypt - Known Key** evaluates encrypted traffic fifth. Matching traffic incoming to your network is decrypted using a private key you upload. The decrypted traffic is then evaluated against access control rules. Access control rules handle decrypted and unencrypted traffic identically. The system can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the SSL rule continues to the next rule.
- **TLS/SSL Rule 5: Decrypt - Resign** is the final rule. If traffic matches this rule, the system re-signs the server certificate with an uploaded CA certificate, then acts as a man-in-the-middle to decrypt traffic. The decrypted traffic is then evaluated against access control rules. Access control rules treat decrypted and unencrypted traffic identically. The system can block traffic as a result of this additional inspection. All remaining traffic is reencrypted before being allowed to the destination. Traffic that does not match the SSL rule continues to the next rule.
- **SSL Policy Default Action** handles all traffic that does not match any of the TLS/SSL rules. The default action either blocks encrypted traffic without further inspection or does not decrypt it, passing it for access control inspection.

How to Configure TLS/SSL Policies and Rules

This topic provides a high-level overview of tasks you must complete to configure SSL policies and TLS/SSL rules in those policies to block, monitor, or allow TLS/SSL traffic on your network.

You must be an Admin, Access Admin, or Network Admin to perform this task. You can configure SSL policies on any device type except NGIPSv.

Procedure

	Command or Action	Purpose
Step 1	Create an SSL policy.	An SSL policy is a container for one or more rules. To use an SSL policy and its rules for access control, you must later associate the SSL policy with an access control policy. For more information, see See Create Basic SSL Policies.

	Command or Action	Purpose
Step 2	Set a default action for your SSL policy.	The default action is taken when traffic matches no rules defined by the SSL policy. See SSL Policy Default Actions.
Step 3	Specify how undecryptable traffic should be handled.	Traffic can be undecryptable for a number of reasons, including unsecure protocols, uses and unknown cipher suite, or in the event of errors with the handshake or decryption. See Default Handling Options for Undecryptable Traffic.
Step 4	For **Decrypt - Known Key** (to decrypt inbound traffic to a server in your network) TLS/SSL rules, create an internal certificate object.	The internal certificate object uses your server's certificate and private key. See Internal Certificate Objects.
Step 5	For **Decrypt - Resign** (to decrypt outbound traffic to a server outside of your network) TLS/SSL rules, create an internal certificate authority (CA) object.	The internal CA object uses a CA and private key. See Internal Certificate Authority Objects.
Step 6	Create your TLS/SSL rules:	• **Block, Block with reset, Interactive block**: Configuring TLS/SSL Rule Actions. • **Do Not Decrypt**, see Configuring TLS/SSL Rule Actions. • **Decrypt - Resign**, see Configuring a Decrypt - Resign Action. • **Decrypt - Known Key**, see Configuring a Decrypt - Known Key Action. • **Monitor**, see Configuring TLS/SSL Rule Actions.
Step 7	Associate the SSL policy with an access control policy.	Unless you associate your SSL policy with an access control policy, it has no effect. After you do this, you can choose to allow or block traffic that matches the access control rule and take other actions. See Associating Other Policies with Access Control.
Step 8	Configure your access control rules to allow or block decrypted traffic.	See Access Control Policy Components.
Step 9	Deploy the access control policy to managed devices.	Before your policy can take effect, it must be deployed to managed devices. See Deploy Configuration Changes.

TLS/SSL Inspection Appliance Deployment Scenarios

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 FTD device in an inline deployment for the Underwriting Department
- one Firepower Management 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.

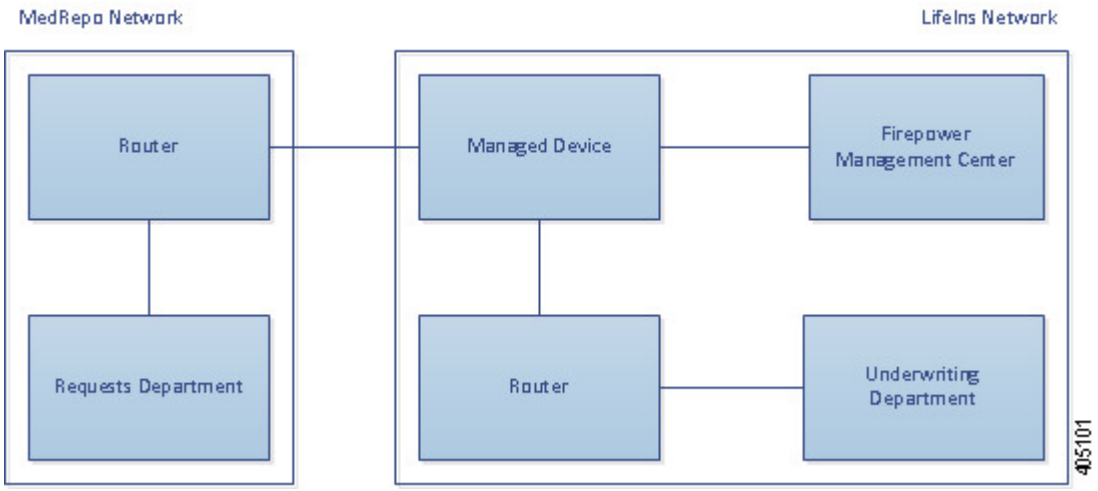
LifeIns places junior underwriters on six-month training periods. Lately, these underwriters have been incorrectly submitting encrypted medical regulation requests to MedRepo's customer service department. MedRepo has submitted multiple complaints to LifeIns in response. LifeIns plans on extending their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

Traffic Decryption in an Inline Deployment

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.



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 Firepower Management Center. LifeIns's router routes traffic to the destination host.

On the managing Firepower Management Center, a user in the Access Control and SSL Editor custom role configures an SSL access control rule 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.

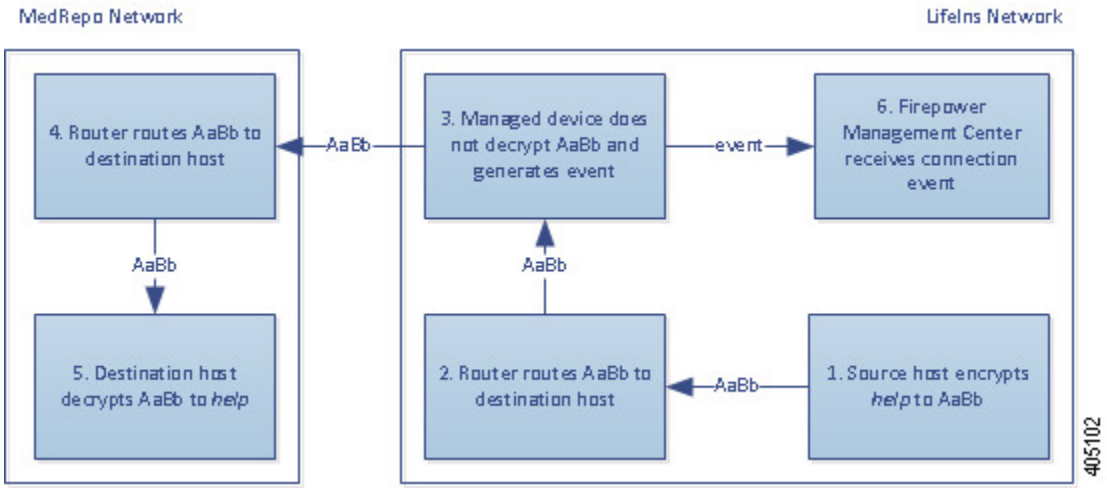
You can also cause the system to decrypt and resign the traffic using a TLS/SSL control rule with the action **Decrypt - Resign** or **Decrypt - Known Key**. If traffic matches the TLS/SSL rule, after the system modifies the ClientHello message, it determines whether the message passes access control evaluation (which can include deep inspection). If the message passes, the system transmits it to the destination server. For more information, see ClientHello Message Handling, on page 3

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.

Encrypted Traffic Monitoring in an Inline Deployment

For all SSL-encrypted traffic sent to and from the Underwriting department, the system logs the connection.



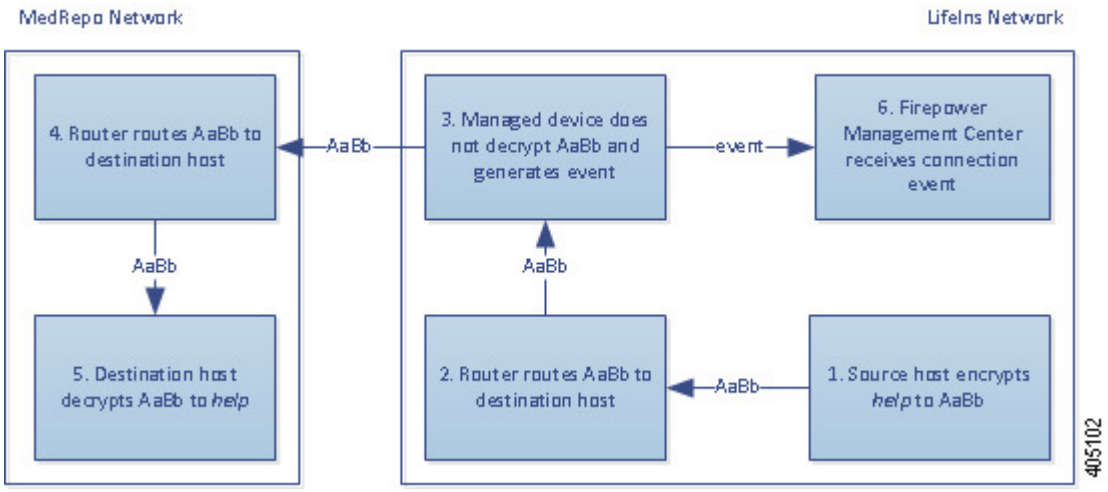
The following steps occur:

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 Firepower Management Center receives the connection event.

Undecrypted Encrypted Traffic in an Inline Deployment

For all TLS/SSL-encrypted traffic originating from the senior underwriters, the managed device allows the traffic without decrypting it and logs the connection.



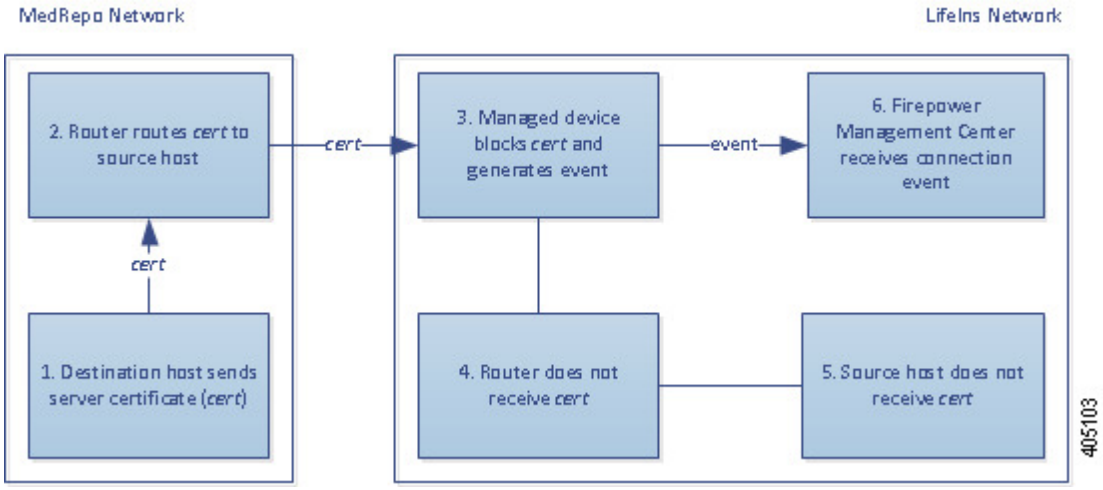
The following steps occur:

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 Firepower Management Center receives the connection event.

Encrypted Traffic Blocking in an Inline Deployment

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.

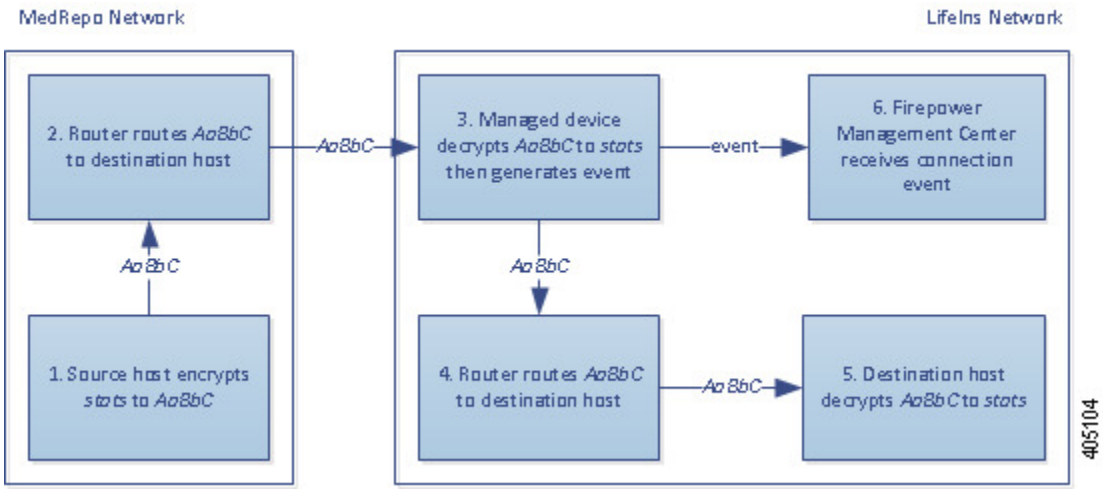


The following steps occur:

1. Having received the request to establish a TLS/SSL handshake from a client's browser, the Customer Service department server sends the server certificate (`cert`) as the next step in the TLS/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 Firepower Management Center receives the connection event.

Encrypted Traffic Inspection with a Private Key in an Inline Deployment

For all TLS/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.

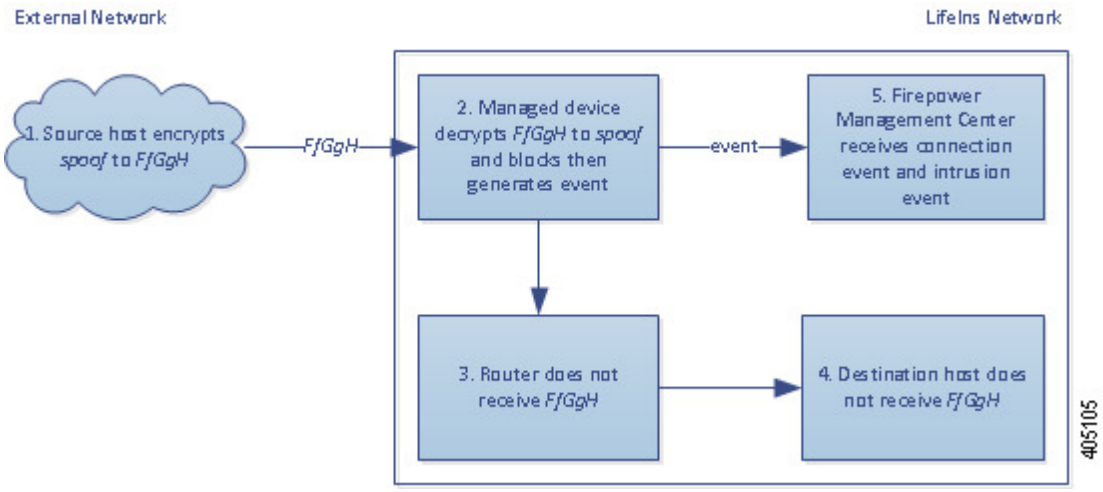


The following steps occur:

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 Firepower Management 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 steps occur:

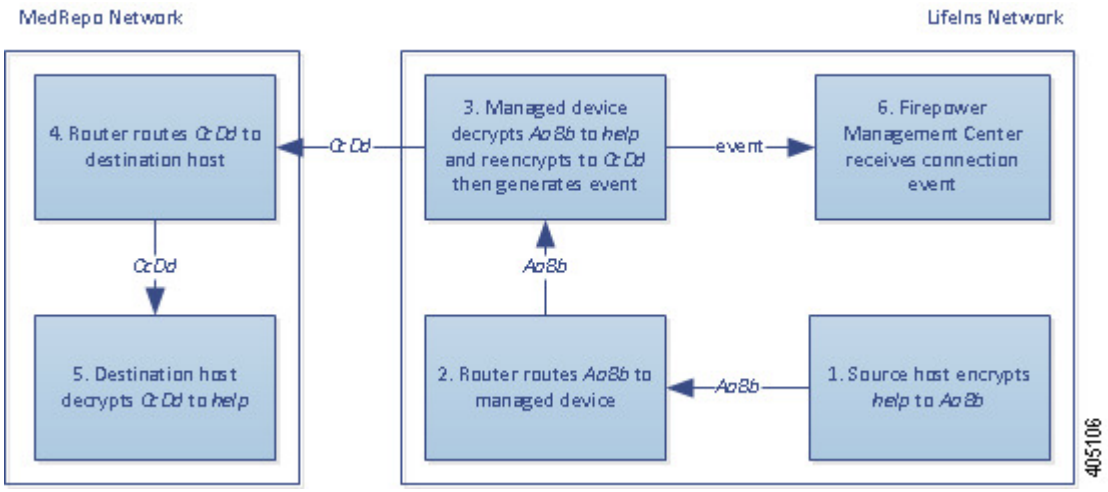
1. The user submits the plain text request (`spoof`), altering the traffic to appear to originate from MedRepo, LLC. The client encrypts this (`FfGgH`) and sends the encrypted traffic to the Underwriting department server.
2. The managed device uses the session key obtained with the uploaded known private 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 Firepower Management Center receives a connection event with information about the encrypted and decrypted traffic, and an intrusion event for the spoofing attempt.

Encrypted Traffic Inspection with a Re-signed Certificate in an Inline Deployment

For all TLS/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 TLS/SSL sessions, one between client and managed device, one between managed device and server. As a result, each session contains different cryptographic session details.



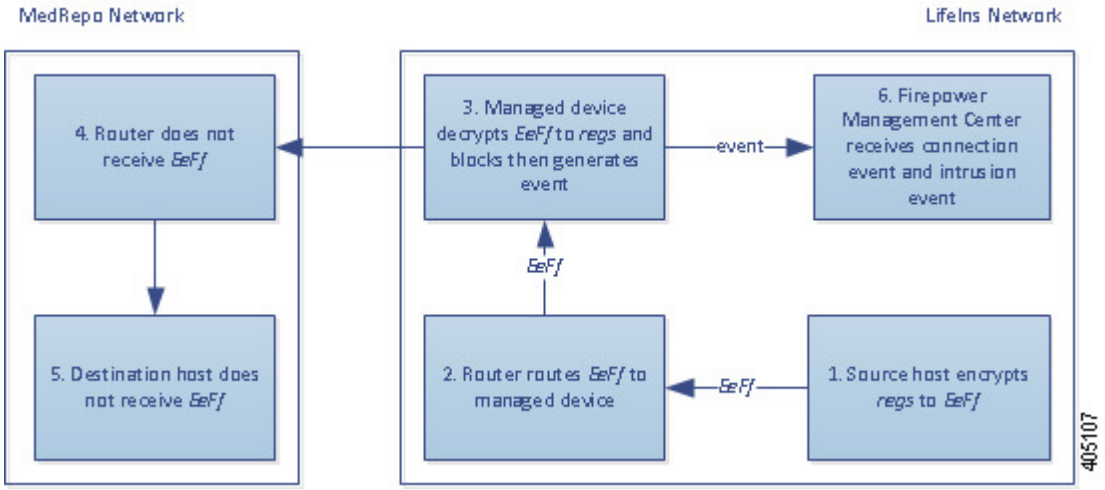
The following steps occur:

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 Firepower Management 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 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 Firepower Management Center receives a connection event with information about the encrypted and decrypted traffic, and an intrusion event for the improper request.

History for TLS/SSL

Feature	Version	Details
Ability to specify handling of URLs having unknown reputation	6.7	For details, see History for URL Filtering.
ClientHello modification for **Decrypt - Known** key rules	6.7	For details, see ClientHello Message Handling, on page 3.
Ability to extract the certificate in TLS 1.3 traffic to enable traffic to match URL and application criteria in access control rules.	6.7	New/modified screen: **Policies** > **Access Control** > **(edit an access control policy)** > **Advanced** link. For details, see TLS 1.3 Server Identity Discovery, on page 12

Feature	Version	Details
Changes to category- and reputation- based URL Filtering	6.5	For details, see History for URL Filtering.
TLS crypto acceleration cannot be disabled	6.4	TLS crypto acceleration is enabled on all supported devices. On a managed device with native interfaces, TLS crypto acceleration cannot be disabled. Support for TLS crypto acceleration on FTD container instances is limited as discussed in the next row of this table. Removed commands: **system support ssl-hw-accel enable** **system support ssl-hw-accel disable** **system support ssl-hw-status**
Support for TLS crypto acceleration on one FTD container instance on a Firepower 4100/9300 module/security engine	6.4	You can now enable TLS crypto acceleration for one FTD container instance on a module/security engine. TLS crypto acceleration is disabled for other container instances, but enabled for native instances. New/Modified commands: **config hwCrypto enable** **show crypto accelerator status** replaces **system support ssl-hw-status**)
TLS/SSL hardware acceleration is now referred to as *TLS crypto acceleration*	6.4	The name change reflects that TLS/SSL encryption and decryption acceleration is supported on more devices. Depending on the device, acceleration might be performed in software or in hardware. Affected screen: To view the status of TLS crypto acceleration, **Devices** > **Device Management** > **Device**, General page.
Extended Master Secret extension supported (see RFC 7627)	6.3.0.1	The TLS Extended Master Secret extension is supported for SSL policies; specifically, policies with a rule action of **Decrypt - Resign** or **Decrypt - Known Key**.
Extended Master Secret extension not supported	6.3	The extension is stripped during ClientHello modification for **Decrypt - Resign** rules.
TLS/SSL hardware acceleration enabled by default	6.3	TLS/SSL hardware acceleration is enabled by default on all supported devices but can be disabled if desired.
Extended Master Secret extension supported (see RFC 7627)	6.2.3.9	The TLS Extended Master Secret extension is supported for SSL policies; specifically, policies with a rule action of **Decrypt - Resign** or **Decrypt - Known Key**.
Aggressive TLS 1.3 downgrade	6.2.3.7	Using the **system support ssl-client-hello-enabled aggressive_tls13_downgrade {true|false}** CLI command, you can determine the behavior for downgrading TLS 1.3 traffic to TLS 1.2. For details, see the *Command Reference for Firepower Threat Defense*.

Feature	Version	Details
TLS/SSL hardware acceleration introduced	6.2.3	Certain managed device models perform TLS/SSL encryption and decryption in hardware, improving performance. By default, the feature is enabled. Affected screen: To view the status of TLS/SSL hardware acceleration, **Devices** > **Device Management** > **Device**, General page.
Category and reputation conditions supported	6.2.2	Access control rules or SSL rules with category/reputation conditions.
SafeSearch supported	6.1.0	• The system displays an HTTP response page for connections decrypted by the SSL policy, then blocked (or interactively blocked) either by access control rules or by the access control policy default action. In these cases, the system encrypts the response page and sends it at the end of the reencrypted SSL stream. • SafeSearch filters objectionable content and stops people from searching adult sites.