Rule-Based Decryption Rules

The following topics discuss how to manage rule-based decryption rules.

About rule-based decryption

Decryption rules provide a granular method of handling encrypted traffic across multiple managed devices, whether blocking the traffic without further inspection, not decrypting the traffic and inspecting it with access control, or decrypting the traffic for access control analysis.

This information applies only to rule-based decryption policies and rules.

Requirements and prerequisites for rule-based decryption rules

Supported domains

Any

User roles

- Admin
- Access Admin
- Network Admin

rule-based decryption rules guidelines and limitations

Keep the following points in mind when setting up your rule-based decryption rule . Properly configuring rule-based decryption rule is a complex task, but one that is essential to building an effective deployment that handles encrypted traffic. Many factors influence how you configure rules, including certain application behavior that you cannot control.

In addition, rules can preempt each other, require additional licenses, or contain invalid configurations. Thoughtfully configured rules can also reduce the resources required to process network traffic. Creating overly complex rules and ordering rules the wrong way can adversely affect performance.

For detailed information, see Best practices for access control rules.

For guidelines related specifically to TLS crypto acceleration, see TLS crypto acceleration.

Related Topics

- Rule and Other Policy Warnings
- Best practices for access control rules
- Guidelines for using TLS/SSL decryption, on page 2
- rule-based decryption rules unsupported features, on page 3
- TLS/SSL Do Not Decrypt guidelines, on page 3
- TLS/SSL incoming traffic decryption guidelines, on page 5
- TLS/SSL Decrypt - Resign guidelines, on page 6
- TLS/SSL Block guidelines, on page 8
- TLS/SSL certificate pinning guidelines, on page 8
- TLS/SSL heartbeat guidelines, on page 9
- TLS/SSL anonymous cipher suite limitation, on page 9
- TLS/SSL normalizer guidelines, on page 9
- Other Rule-based decryption rule guidelines, on page 9
- Decryption policy Rule Order

Guidelines for using TLS/SSL decryption

General guideline

rule-based decryption rules require processing overhead that can impact performance. Determine which traffic must be decrypted and subjected to deep inspection before you set up any policies or rules.

You cannot decrypt traffic on a device that uses any of the following:

- Passive interface
- Inline or inline tap interface
- TCP state bypass

Guidelines for undecryptable traffic

We can determine that certain traffic is not decryptable either because the website itself is not decryptable or because the website uses TLS/SSL pinning, which effectively prevents users from accessing a decrypted site without errors in their browser.

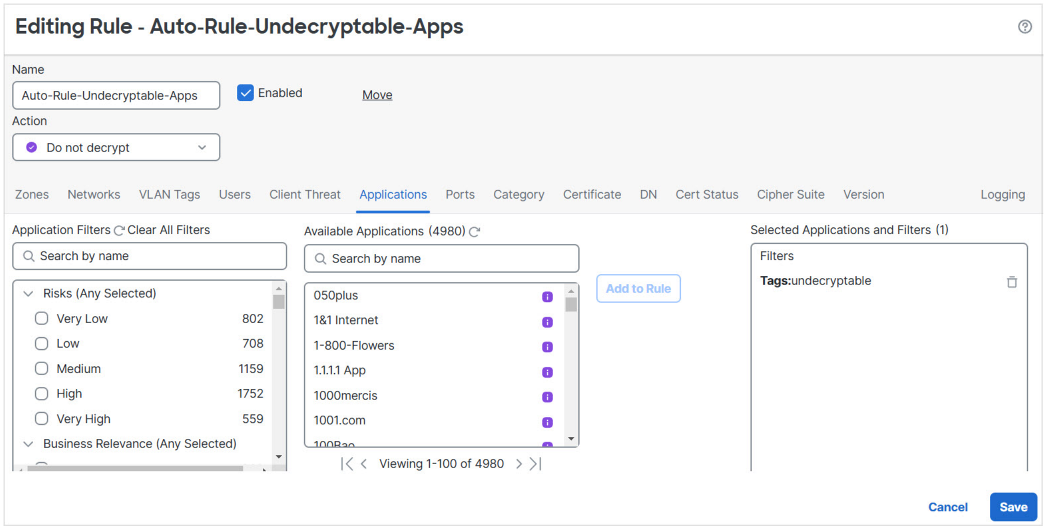
For more information about certificate pinning, see About TLS/SSL pinning, on page 44.

We maintain the list of these sites as follows:

- A Distinguished Name (DN) group named **Cisco-Undecryptable-Sites**
- The **pinned certificate** or **undecryptable** application filter

If you are decrypting traffic and you do not want users to see errors in their browsers when going to these sites, we recommend you set up a **Do Not Decrypt** rule toward the bottom of your decryption rules.

If you use the decryption policy wizard to create a policy for outbound traffic protection, a **Do Not Decrypt** rule for pinned certificates is created for you as the following example shows.


Editing Rule - Auto-Rule-Undecryptable-Apps

Name: Auto-Rule-Undecryptable-Apps ✓ Enabled

Action: Do not decrypt

Application Filters: Risks (Any Selected)

Very Low	802
Low	708
Medium	1159
High	1752
Very High	559

Business Relevance (Any Selected)

Available Applications (4980): 050plus, 1&1 Internet, 1-800-Flowers, 1.1.1.1 App, 1000mercis, 1001.com, 100Bao

Viewing 1-100 of 4980

Selected Applications and Filters (1)

Filters

Tags:undecryptable

rule-based decryption rules unsupported features

Passive, inline tap mode, and SPAN interfaces not supported

TLS/SSL traffic cannot be decrypted on passive, inline tap mode, or SPAN interfaces.

DES and RC4 ciphers not unsupported

The Rivest Cipher 4 (also referred to as *RC4* or *ARC4*) and the Data Encryption Standard (DES) ciphers are known to have vulnerabilities and are considered unsecure.

Configure the **Unsupported Cipher Suite** action in the decryption policies policy's **Undecryptable Actions** page to match your organization’s requirements. For more information, see Default handling options for undecryptable traffic.

TLS/SSL Do Not Decrypt guidelines

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

Encrypted traffic can be allowed or blocked on any decryption rule condition, including, but not limited to:

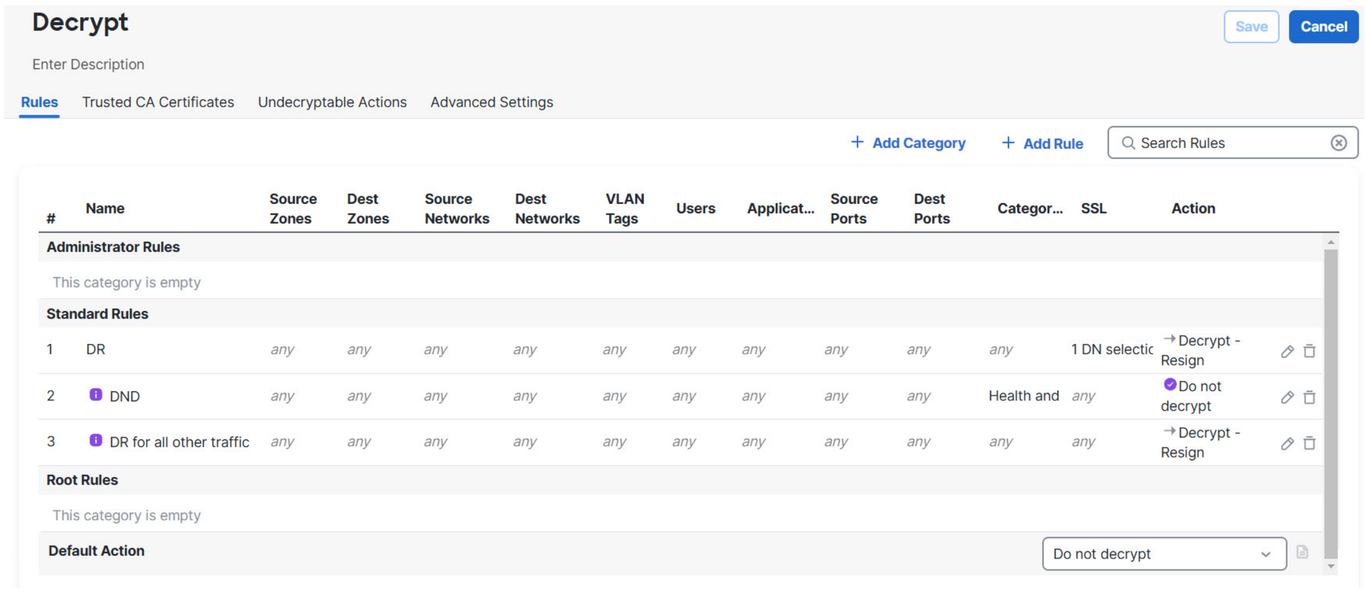
- Certificate status (for example, expired or invalid certificate)
- Protocol (for example, the nonsecure SSL protocol)
- Network (security zone, IP address, VLAN tag, and so on)
- URL category and reputation
- Port
- User group

Limitations of categories in Do Not Decrypt rules

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security. While we strive to continuously update and improve URL filtering categories, it is not an exact science. Some websites are not categorized at all and it's possible some websites might be improperly categorized.

Avoid overusing categories in do not decrypt rules to avoid decrypting traffic without a reason; for example, the Health and Medicine category includes the WebMD website, which does not threaten patient privacy.

Following is a sample decryption policy that can prevent decryption for websites in the Health and Medicine categories but allows decryption for WebMD and everything else. General information about decryption rules can be found in Guidelines for using TLS/SSL decryption, on page 2.



Decrypt

Enter Description

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	Categor...	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DR	any	any	any	any	any	any	any	any	any	any	1 DN selectic	Decrypt - Resign
2	DND	any	any	any	any	any	any	any	any	any	Health and	any	Do not decrypt
3	DR for all other traffic	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													Do not decrypt

Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control.

TLS/SSL incoming traffic decryption guidelines

You can associate only one server certificate and paired private key with a **Decrypt - Replace Cert** rule action. To decrypt TLS 1.2 traffic, the public key type used in the rule must match the internal server's public key type. (For example, if the internal server uses an RSA public key type, the public key type used in the decryption rule must also be RSA). This restriction doesn't apply to decrypting TLS 1.3 traffic.

You can associate one or more server certificates and paired private keys with a **Decrypt - Known Key** rule action.

If traffic matches the rule, and the certificate used to encrypt the traffic matches the certificate associated with the action, the system uses the appropriate private key to obtain the session encryption and decryption keys. Because you must have access to the private key, this action is best suited to decrypt traffic incoming to servers your organization controls.

Also note the following:

Anonymous cipher suite unsupported

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign**, **Decrypt - Replace Cert** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

Cannot match on Distinguished Name or Certificate

You cannot match on **Distinguished Name** or **Certificate** rule conditions when creating a decryption rule with a **Decrypt - Known Key** action. The assumption is that if this rule matches traffic, the certificate, subject DN, and issuer DN already match the certificate associated with the rule.

Do not use Version or Cipher Suite rule conditions

Important *Never* use either **Cipher Suite** or **Version** rule conditions in a rule with a **Decrypt - Resign**, **Decrypt - Replace Cert**, or **Decrypt - Known Key** rule action. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Elliptic Curve Digital Signature Algorithm (*ECDSA*) certificate results in blocked traffic

(TLS 1.3 decryption enabled only.) If you use an ECDSA certificate with a **Decrypt - Known Key** rule action, matching traffic will be blocked. To avoid this, use a certificate with another type of certificate.

TLS/SSL Decrypt - Resign guidelines

You can associate one internal Certificate Authority (CA) certificate and private key with the **Decrypt - Resign** action. If traffic matches this rule, the system re-signs the server certificate with the CA certificate, then 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. Each session contains different cryptographic session details, and allows the system to decrypt and reencrypt traffic.

Best practices

We recommend the following:

- Use the **Decrypt - Resign** rule action for decrypting *outgoing* traffic, as opposed to incoming traffic for which we recommend the **Decrypt - Known Key** or **Decrypt - Replace Cert** rule action.

  For more information about **Decrypt - Known Key** or **Decrypt - Replace Cert**, see TLS/SSL incoming traffic decryption guidelines, on page 5.

- Always check the **Replace Key Only** check box when you set up a **Decrypt - Resign** rule action.

  When a user browses to a web site that uses a *self-signed* certificate, the user sees a security warning in the web browser and is aware that they are communicating with an unsecure site.

  When a user browses to a web site that uses a trusted certificate, the user does not see a security warning.

Details

If you configure a rule with the **Decrypt - Resign** action, the rule matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions. Because you associate one CA certificate with a **Decrypt - Resign** action, you cannot create a decryption rule that decrypts multiple types of outgoing traffic encrypted with different signature algorithms. In addition, any external certificate objects and cipher suites you add to the rule must match the associated CA certificate encryption algorithm type.

For example, outgoing traffic encrypted with an elliptic curve (EC) algorithm matches a **Decrypt - Resign** rule only if the action references an EC-based CA certificate; you must add EC-based external certificates and cipher suites to the rule to create certificate and cipher suite rule conditions.

Similarly, a **Decrypt - Resign** rule that references an RSA-based CA certificate matches only outgoing traffic encrypted with an RSA algorithm; outgoing traffic encrypted with an EC algorithm does not match the rule, even if all other configured rule conditions match.

Guidelines and limitations

Also note the following:

Anonymous cipher suite unsupported

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

Do not use Version or Cipher Suite rule conditions

Important *Never* use either **Cipher Suite** or **Version** rule conditions in a rule with a **Decrypt - Resign**, **Decrypt - Replace Cert**, or **Decrypt - Known Key** rule action. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Decrypt - Resign rule action and a Certificate Signing Request

To use a **Decrypt - Resign** rule action, you should create a Certificate Signing Request (CSR) and have it signed by a trusted certificate authority. (You can use the FMC to create a CSR: **Objects** > **PKI** > **Internal Certs**.)

To be used in a **Decrypt - Resign** rule, your certificate authority (CA) must have at least one of the following extensions:

- **CA: TRUE**

  For more information, see the discussion of Basic Constraints in RFC3280, section 4.2.1.10.

- **KeyUsage=CertSign**

  For more information see RFC 5280, section 4.2.1.3.

To verify your CSR or CA has at least one of the preceding extensions, you can use the **openssl** command as discussed in a reference such as the openssl documentation.

This is necessary because for **Decrypt - Resign** inspection to work, the certificate that used in the decryption policy generates certificates on-the-fly and signs them so as to act as man-in-the middle and proxy all TLS/SSL connections.

Certificate pinning

If the customer's browser uses certificate pinning to verify a server certificate, you cannot decrypt this traffic by re-signing the server certificate. To allow this traffic, configure a decryption rule with the **Do Not Decrypt** action to match the server certificate common name or distinguished name.

The decryption policy wizard creates such rules for you; see Create a rule-based decryption policy with outbound connection protection .

Non-matching cipher suite

The following error is displayed if you attempt to save a decryption rule with a cipher suite that does not match the certificate. To resolve the issue, see Verify TLS/SSL cipher suites, on page 49.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

Untrusted Certificate Authority

If the client does not trust the Certificate Authority (CA) used to re-sign the server certificate, it warns the user that the certificate should not be trusted. To prevent this, import the CA certificate into the client trusted CA store. Alternatively, if your organization has a private PKI, you can issue an intermediate CA certificate signed by the root CA which is automatically trusted by all clients in the organization, then upload that CA certificate to the device.

HTTP proxy limitation

The system cannot decrypt traffic if an HTTP proxy is positioned between a client and your managed device, and the client and server establish a tunneled TLS/SSL connection using the CONNECT HTTP method. The **Handshake Errors** undecryptable action determines how the system handles this traffic.

Upload signed CA

If you create an internal CA object and choose to generate a certificate signing request (CSR), you cannot use this CA for a **Decrypt - Resign** action until you upload the signed certificate to the object.

Mismatched signature algorithm

If you configure a rule with the **Decrypt - Resign** action, and mismatch signature algorithm type for one or more external certificate objects or cipher suites, the policy editor displays an **Information**(ℹ) next to the rule. If you mismatch signature algorithm type for all external certificate objects, or all cipher suites, the policy displays a warning icon **Warning** (⚠) next to the rule, and you cannot deploy the access control policy associated with the decryption policy.

TLS/SSL Block guidelines

If your decryption rule is associated with an access control policy that has a rule with an action of either **Interactive Block** or **Interactive Block with reset**, the system displays a customizable response page.

Provided you enabled logging in your rule, two connection events are displayed (in **Events & Logs** > **+ Show more** > **Connection** > **Events**): One event for the interactive block and another event to indicate whether or not the user chose to continue to the site or not.

Related Topics

Configure HTTP Response Pages

TLS/SSL certificate pinning guidelines

Some applications use a technique referred to as *TLS/SSL pinning* or *certificate pinning*, which embeds the fingerprint of the original server certificate in the application itself. As a result, if you configured a decryption rule with a **Decrypt - Resign** action, when the application receives a resigned certificate from a managed device, validation fails and the connection is aborted.

Because TLS/SSL pinning is used to avoid man-in-the-middle attacks, there is no way to prevent or work around it. We recommend adding a **Do Not Decrypt** rule before the **Decrypt - Resign** rule so pinning traffic is excluded from being decrypted. The decryption policy wizard does this for you.

- Create a **Do Not Decrypt** for those applications rule ordered before **Decrypt - Resign** rules.
- Instruct users to access the applications using a web browser.

For more information about rule ordering, see Decryption policy Rule Order.

To determine whether applications are using TLS/SSL pinning, see Troubleshoot TLS/SSL pinning, on page 45.

TLS/SSL heartbeat guidelines

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.

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.

For more information, see About TLS heartbeat, on page 42.

TLS/SSL anonymous cipher suite limitation

By nature, anonymous cipher suites are not used for authentication and do not use key exchanges. There are limited uses for anonymous cipher suites; for more information, see RFC 5246, appendix F.1.1.1. (Replaced for TLS 1.3 by RFC 8446 appendix C.5.)

You cannot use the **Decrypt - Resign** or **Decrypt - Known Key** action in the rule because anonymous cipher suites are not used for authentication.

You can add an anonymous cipher suite to the **Cipher Suite** condition in a decryption rule, but the system automatically strips anonymous cipher suites during ClientHello processing. For the system to use the rule, you must also configure your decryption rules in an order that prevents ClientHello processing. For more information, see Decryption policy Rule Order.

TLS/SSL normalizer guidelines

If you enable the **Normalize Excess Payload** option in the inline normalization preprocessor, when the preprocessor normalizes decrypted traffic, it might drop a packet and replace it with a trimmed packet. This does not end the TLS/SSL session. If the traffic is allowed, the trimmed packet is encrypted as part of the TLS/SSL session.

Other Rule-based decryption rule guidelines

Users and groups

If you add a group or user to a rule, then change your realm settings to exclude that group or user, the rule has no effect. (The same applies to disabling the realm.) For more information about realms, see Create an LDAP realm or an Active Directory realm and realm directory.

Categories in decryption rules

If your decryption policy has a **Decrypt - Resign** action but web sites are not being decrypted, check **Category** page on rules associated with that policy.

In some cases, a web site redirects to another site for authentication or other purposes and the redirected site might have a different URL categorization than the site you're trying to decrypt. For example, `gmail.com` (**Web based email** category) redirects to `accounts.gmail.com` (**Internet Portals** category) for authentication. Be sure to include all relevant categories in the SSL rule.

Note In order to fully process traffic based on URL category, you must also configure URL filtering. See the URL Filtering Rules chapter.

Query for URLs not in the local database

If you create a **Decrypt - Resign** rule and users browse to a web site whose category and reputation are not in the local database, data might not be decrypted. Some web sites are not categorized in the local database and, if not, data from those web sites is not decrypted by default.

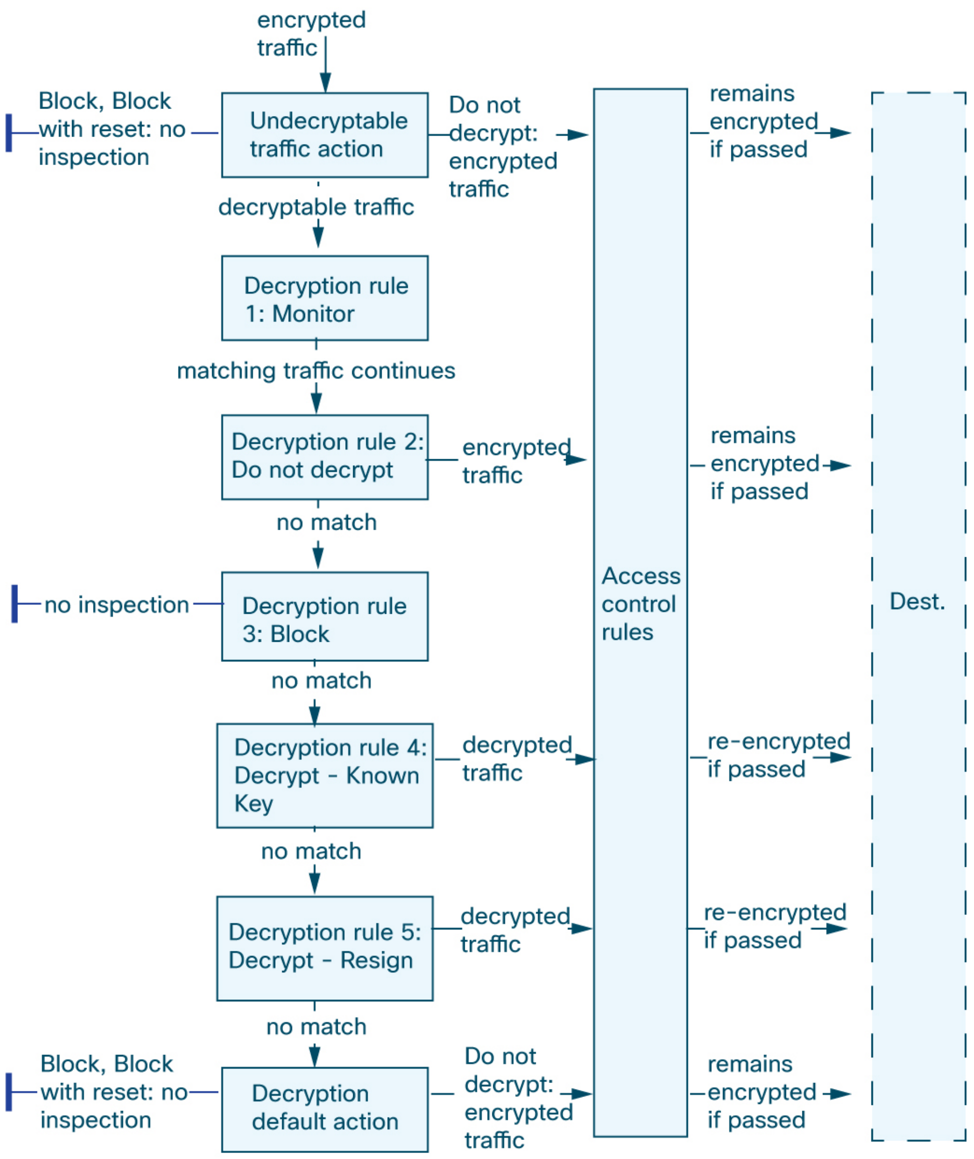
You can control this behavior with the **Query Cisco cloud for unknown URLs** setting in **Integrations** > **Cloud Services**

Rule-based decryption rule traffic handling

The system matches traffic to rule-based decryption rules in the order you specify. In most cases, the system handles encrypted traffic according to the *first* decryption rule where *all* the rule's conditions match the traffic. 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 inspect encrypted and undecryptable traffic with access control. 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.

The following scenario summarizes the ways that decryption 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
Decryption rule 1: Monitor
matching traffic continues
Decryption rule 2: Do not decrypt
encrypted traffic
remains encrypted if passed
no match
no inspection
Decryption rule 3: Block
Access control rules
Dest.
no match
Decryption rule 4: Decrypt - Known Key
decrypted traffic
re-encrypted if passed
no match
Decryption rule 5: Decrypt - Resign
decrypted traffic
re-encrypted if passed
no match
Block, Block with reset: no inspection
Decryption 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.
- **Decryption 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.
- **Decryption 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.

- **Decryption rule 3: Block** evaluates encrypted traffic fourth. Matching traffic is blocked without further inspection. Traffic that does not match continues to the next rule.
- **Decryption 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 decryption rule continues to the next rule.
- **Decryption 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 decryption rule rule continues to the next rule.
- **Decryption policy Default Action** handles all traffic that does not match any of the decryption rules. The default action either blocks encrypted traffic without further inspection or does not decrypt it, passing it for access control inspection.

Encrypted traffic inspection configuration

You must create reusable public key infrastructure (PKI) objects to control encrypted traffic based on encrypted session characteristics and decrypt encrypted traffic. You can add this information on the fly when uploading trusted certificate authority (CA) certificates to the a decryption policy and creating decryption rule, creating the associated object in the process. However, configuring these objects ahead of time reduces the chance of improper object creation.

Decrypting Encrypted Traffic with Certificates and Paired Keys

The system can decrypt incoming encrypted traffic if you configure an internal certificate object by uploading the server certificate and private key used to encrypt the session. If you reference that object in a decryption policy rule with an action of **Decrypt - Known Key** and traffic matches that rule, the system uses the uploaded private key to decrypt the session.

The system can also decrypt outgoing traffic if you configure an internal CA object by uploading a CA certificate and private key. If you reference that object in a decryption rule with an action of **Decrypt - Resign** and traffic matches that rule, the system re-signs the server certificate passed to the client browser, then acts as a man-in-the-middle to decrypt the session. You can optionally replace the self-signed certificate key only and not the entire certificate, in which case users see a self-signed certificate key notice in the browser.

Controlling Traffic Based on Encrypted Session Characteristics

The system can control encrypted traffic based on the cipher suite or server certificate used to negotiate the session. You can configure one of several different reusable objects and reference the object in a decryption rule condition to match traffic. The following table describes the different types of reusable objects you can configure:

If you configure...	You can control encrypted traffic based on whether...
A cipher suite list containing one or more cipher suites	The cipher suite used to negotiate the encrypted session matches a cipher suite in the cipher suite list

If you configure...	You can control encrypted traffic based on whether...
A trusted CA object by uploading a CA certificate your organization trusts	The trusted CA trusts the server certificate used to encrypt the session, whether: • The CA issued the certificate directly • The CA issued a certificate to an intermediate CA that issued the server certificate
An external certificate object by uploading a server certificate	The server certificate used to encrypt the session matches the uploaded server certificate
A distinguished name object containing a certificate subject or issuer distinguished name	The subject or issuer common name, country, organization, or organizational unit on the certificate used to encrypt the session matches the configured distinguished name

Related Topics

Cipher Suite List
Distinguished Name
PKI

Rule-based decryption rule order evaluation

This information applies only to rule-based decryption policies and rules.

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

In most cases, the system handles network traffic according to the *first* decryption 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 category and reputation, 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 decryption 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
Decryption policy Rule Order

Rule-based decryption rule conditions

A rule-based decryption rule ’s conditions identify the type of encrypted traffic the rule handles. Conditions can be simple or complex, and you can specify more than one condition type per rule. Only if traffic meets all the conditions in a rule does the rule apply to the traffic.

If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion. For example, a rule with a certificate condition but no version condition evaluates traffic based on the server certificate used to negotiate the session, regardless of the session SSL or TLS version.

Every rule-based decryption policy has an associated action that determines the following for matching encrypted traffic:

- Handling: Most importantly, the rule action governs whether the system will monitor, trust, block, or decrypt encrypted traffic that matches the rule’s conditions
- Logging: The rule action determines when and how you can log details about matching encrypted traffic.

Your TLS/SSL inspection configuration handles, inspects, and logs decrypted traffic:

- The decryption policy’s undecryptable actions handle traffic that the system cannot decrypt.
- The policy’s default action handles traffic that does not meet the condition of any non-Monitor decryption rule.

You can log a connection event when the system blocks or trusts an encrypted session. 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. Connection logs for encrypted sessions contain details about the encryption, such as the certificate used to encrypt that session. You can log only end-of-connection events, however:

- For blocked connections (Block, Block with reset), the system immediately ends the sessions and generates an event
- For Do Not Decrypt connections, the system generates an event when the session ends

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Caution Adding the first or removing the last active authentication rule when TLS/SSL decryption is disabled (that is, when the access control policy does not include a decryption policy) restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the assigned device handles traffic. See Snort Restart Traffic Behavior for more information.

Note that an active authentication rule has either an **Active Authentication** rule action, or a **Passive Authentication** rule action with **Use active authentication if passive or VPN identity cannot be established** selected.

Related Topics

Security zone rule conditions, on page 15
Network rule conditions
VLAN tags rule conditions
User rule conditions
Application rule conditions
Port rule conditions
Category rule conditions, on page 19
Server certificate-based rule conditions, on page 19

Security zone rule conditions

Security zones segment your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices.

Security zones control or decrypt traffic by its source and destination security zones. If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

Just as all interfaces in a zone must be of the same type (all inline, passive, switched, or routed), all zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device’s interfaces, that rule does not affect that device's performance.

Security zone conditions and multitenancy

In a multidomain deployment, a zone created in an ancestor domain can contain interfaces that reside on devices in different domains. When you configure a zone condition in an descendant domain, your configurations apply to only the interfaces you can see.

Network rule conditions

Networks control or decrypt traffic by its source and destination IP address, using inner headers. Tunnel rules, which use outer headers, have tunnel endpoint conditions instead of network conditions.

You can use predefined objects to build network conditions.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Note You *cannot* use FDQN network objects in identity rules.

VLAN tags rule conditions

Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

VLAN rule conditions control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic. The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note the following Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

User rule conditions

Matches traffic based the user who initiates the connection, or the group to which the user belongs. For example, you could configure a Block rule to prohibit anyone in the Finance group from accessing a network resource.

You can configure user rule conditions for users in Microsoft Active Directory realms only.

In addition to configuring users and groups for configured realms, you can set policies for the following Special Identities users:

- Failed Authentication: User that failed authentication with the captive portal.
- Guest: Users configured as guest users in the captive portal.
- No Authentication Required: Users that match an identity **No Authentication Required** rule action.
- Unknown: Users that cannot be identified; for example, users that are not downloaded by a configured realm.

For access control rules only, you must first associate an identity policy with the access control policy as discussed in Associating other policies with access control.

Client threat rule conditions

The threat confidence levels of the client processes are determined by the Encrypted Visibility Engine (EVE), and represent the likelihood that the incoming traffic is malicious. The client threat confidence levels range from very low to very high, and the levels can be specified as rule conditions for decryption policy rules. When the client threat confidence levels and server URL category reputation are configured, they act as a powerful combination in decryption policies. We highly recommend that you specify a URL Category Reputation rule condition for rules that specify a Client Threat rule condition. When Client Threat and URL Category Reputation conditions are both specified for a decryption policy rule, the reputations of both the client and the server are utilized to make more accurate decryption policy decisions. We recommend that you do not specify a Client Threat rule condition alone without specifying a URL Category Reputation rule condition because this rule configuration only acts on information about the client and lacks information about the server.

Prerequisites for configuring client threat rule conditions

- The EVE must be enabled in the corresponding access control policy.
- The management center and threat defense devices must be Version 7.7.
- Snort 3 must be enabled on the device.
- Valid IPS and URL Filtering licenses must be installed on the managed device.

We recommend that you bypass decryption for very low-risk clients connecting to trusted servers based on the client threat determined by EVE and URL Category Reputation. To do so, create a new decryption policy rule, or edit an existing rule with the following configurations:

1. Choose the decryption policy rule action as **Do not decrypt**.
2. In the **Client Threat** tab, choose the client threat level as **Very Low**.
3. In the **Category** tab, choose the category as **All** and the reputation as **Trusted**.

Application rule conditions

When the system analyzes IP traffic, it can identify and classify the commonly used applications on your network. This discovery-based *application awareness* is the basis for *application control*—the ability to control application traffic.

System-provided *application filters* help you perform application control by organizing applications according to basic characteristics: type, risk, business relevance, category, and tags. You can create reuseable user-defined filters based on combinations of the system-provided filters, or on custom combinations of applications.

At least one detector must be enabled for each application rule condition in the policy. If no detector is enabled for an application, the system automatically enables all system-provided detectors for the application; if none exist, the system enables the most recently modified user-defined detector for the application. For more information about application detectors, see Application Detector Fundamentals.

You can use both application filters and individually specified applications to ensure complete coverage. However, understand the following note before you order your access control rules.

Benefits of application filters

Application filters help you quickly configure application control. For example, you can easily use system-provided filters to create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the system blocks the session.

Using application filters simplifies policy creation and administration. It assures you that the system controls application traffic as expected. Because Cisco frequently updates and adds application detectors via system and vulnerability database (VDB) updates, you can ensure that the system uses up-to-date detectors to monitor application traffic. You can also create your own detectors and assign characteristics to the applications they detect, automatically adding them to existing filters.

Application characteristics

The system characterizes each application that it detects using the criteria described in the following table. Use these characteristics as application filters.

Table 1: Application characteristics

Characteristic	Description	Example
Type	Application protocols represent communications between hosts. Clients represent software running on a host. Web applications represent the content or requested URL for HTTP traffic.	HTTP and SSH are application protocols. Web browsers and email clients are clients. MPEG video and Facebook are web applications.
Risk	The likelihood that the application is being used for purposes that might be against your organization's security policy.	Peer-to-peer applications tend to have a very high risk.
Business Relevance	The likelihood that the application is being used within the context of your organization's business operations, as opposed to recreationally.	Gaming applications tend to have a very low business relevance.
Category	A general classification for the application that describes its most essential function. Each application belongs to at least one category.	Facebook is in the social networking category.
Tag	Additional information about the application. Applications can have any number of tags, including none.	Video streaming web applications often are tagged `high bandwidth` and `displays ads`.

Port rule conditions

Port conditions allow you to control traffic by its source and destination ports.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Best Practices for Port-Based Rules

Specifying ports is the traditional way to target applications. However, applications can be configured to use unique ports to bypass access control blocks. Thus, whenever possible, use application filtering criteria rather than port criteria to target traffic.

Application filtering is also recommended for applications, like Firewall Threat Defense, that open separate channels dynamically for control vs. data flow. Using port-based access control rules can prevent these kinds of applications from performing correctly, and could result in blocking desirable connections.

Using Source and Destination Port Constraints

If you add both source and destination port constraints, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

If you add only source ports or only destination ports, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

Category rule conditions

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security.

For more information, see URL Filtering Overview.

If you are using category rule conditions in decryption policies in a rule with the **Do Not Decrypt** rule action, see Rule-based decryption rule Do Not Decrypt action, on page 33.

Server certificate-based rule conditions

decryption rules can handle and decrypt encrypted traffic based on server certificate characteristics. You can configure decryption rules based on the following server certificate attributes:

- Distinguished name conditions allow you to handle and inspect encrypted traffic based on the CA that issued a server certificate, or the certificate holder. Based on the issuer distinguished name, you can handle traffic based on the CA that issued a site's server certificate.
- Certificate conditions in decryption rules allow you to handle and inspect encrypted traffic based on the server certificate used to encrypt that traffic. You can configure a condition with one or more certificates; traffic matches the rule if the certificate matches any of the condition's certificates.

- Certificate status conditions in decryption rules allow you to handle and inspect encrypted traffic based on the status of the server certificate used to encrypt the traffic, including whether a certificate is valid, revoked, expired, not yet valid, self-signed, signed by a trusted CA, whether the Certificate Revocation List (CRL) is valid; whether the Server Name Indication (SNI) in the certificate matches the server in the request.
- Cipher suite conditions in decryption rules allow you to handle and inspect encrypted traffic based on the cipher suite used to negotiate the encrypted session.
- Session conditions in decryption rules allow you to inspect encrypted traffic based on the SSL or TLS version used to encrypt the traffic.

To detect multiple cipher suites in a rule, the certificate issuer, or the certificate holder, you can create reusable cipher suite list and distinguished name objects and add them to your rule. To detect the server certificate and certain certificate statuses, you must create external certificate and external CA objects for the rule.

Related Topics

Certificate rule conditions, on page 20
Certificate Status Decryption rule Conditions, on page 26
Trusting external certificate authorities, on page 25
Matching Traffic on Certificate Status
Cipher suite rule conditions, on page 29
Encryption protocol version rule conditions, on page 32

Certificate rule conditions

When you build a certificate-based decryption rule condition, you can upload a server certificate; you save the certificate as an external certificate *object*, which is reusable and associates a name with a server certificate. Alternately, you can configure certificate conditions with existing external certificate objects and object groups.

You can search the **Available Certificates** field in the rule condition based for external certificate objects and object groups based on the following certificate distinguished name characteristics:

- Subject or issuer common name (CN), or if the URL is contained in the certificate's Subject Alternative Name (SAN)

  The URL the user enters in the browser matches the Common Name (CN)
- Subject or issuer organization (O)
- Subject or issuer organizational unit (OU)

You can choose to match against multiple certificates in a single certificate rule condition; if the certificate used to encrypt the traffic matches any of the uploaded certificates, the encrypted traffic matches the rule.

You can add a maximum of 50 external certificate objects and external certificate object groups to the **Selected Certificates** in a single certificate condition.

Note the following:

- You cannot configure a certificate condition if you also select the **Decrypt - Known Key** action. Because that action requires you to select a server certificate to decrypt traffic, the implication is that the certificate already matches the traffic.

- If you configure a certificate condition with an external certificate object, any cipher suites you add to a cipher suite condition, or internal CA objects you associate with the **Decrypt - Resign** action, must match the external certificate's signature algorithm type. For example, if your rule's certificate condition references an EC-based server certificate, any cipher suites you add, or CA certificates you associate with the **Decrypt - Resign** action, must also be EC-based. If you mismatch signature algorithm types in this case, the policy editor displays a warning next to the rule.
- The first time the system detects an encrypted session to a new server, certificate data is not available for ClientHello processing, which can result in an undecrypted first session. After the initial session, the managed device caches data from the server Certificate message. For subsequent connections from the same client, the system can match the ClientHello message conclusively to rules with certificate conditions and process the message to maximize decryption potential.

Distinguished Name (DN) rule conditions

This topic discusses how to use distinguished name conditions in a decryption rule. If you're not sure, you can find a certificate's Subject Alternative Name (SAN) and Common Name using a web browser, then you can add those values to a decryption rule as distinguished name conditions.

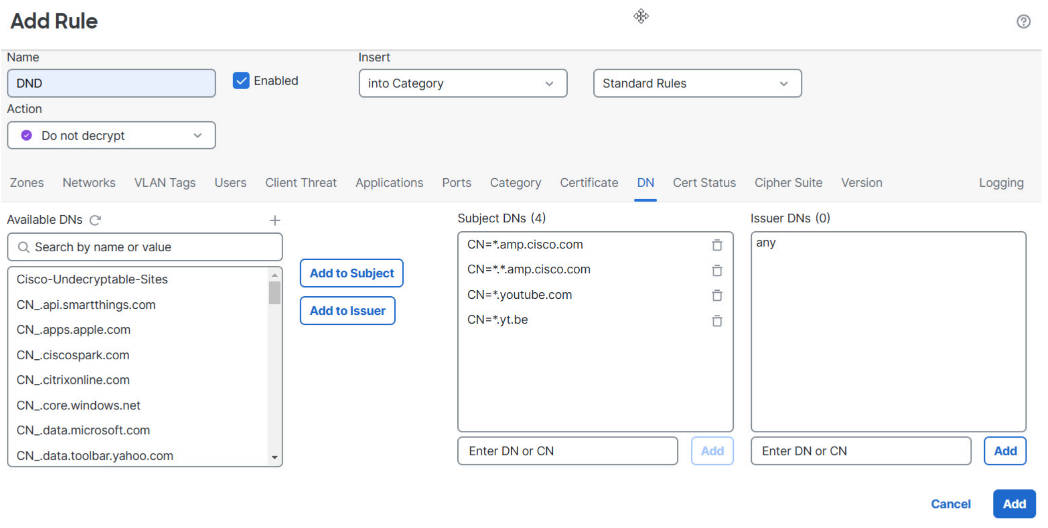
For detailed information about SANs, see RFC 528, section 4.2.1.6.

The following sections discuss:

- DN rule matching example
- How the system uses the SNIs and SANs
- How to find a certificate's Common Name and Subject Alternative Names
- How to add a DN rule condition

DN rule matching example

Following is an example of DN rule conditions in a Do Not Decrypt rule. Suppose you want to make sure to *not* decrypt traffic going to `amp.cisco.com` or to YouTube. You could set up your DN conditions as follows:


Add Rule

Name: DND
Enabled ✓
Insert: into Category | Standard Rules
Action: Do not decrypt

Zones | Networks | VLAN Tags | Users | Client Threat | Applications | Ports | Category | Certificate | DN | Cert Status | Cipher Suite | Version | Logging

Available DNs
Search by name or value
Cisco-Undecryptable-Sites
CN_.api.smartthings.com
CN_.apps.apple.com
CN_.ciscospark.com
CN_.citrixonline.com
CN_.core.windows.net
CN_.data.microsoft.com
CN_.data.toolbar.yahoo.com

Add to Subject
Add to Issuer

Subject DNs (4)
CN=*.amp.cisco.com
CN=*.*.amp.cisco.com
CN=*.youtube.com
CN=*.yt.be
Enter DN or CN | Add

Issuer DNs (0)
any
Enter DN or CN | Add

Cancel | Add

The preceding DN rule conditions would match the following URLs and therefore, the traffic would be undecrypted an earlier rule prevented it:

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com
- kids.youtube.com
- www.yt.be

The preceding DN rule conditions would *not* match any of the following URLs and therefore, the traffic would not match the Do Not Decrypt rule but might match any other decryption rules in the same decryption policy.

- amp.cisco.com
- youtube.com
- yt.be

To match any of the preceding host names, add more CNs to the rule (for example, adding `CN=yt.be` would match that URL.)

How the system uses the SNI and SANs

The host name portion of the URL in the client request is the Server Name Indication (SNI). The client specifies which hostname they want to connect to (for example, `auth.amp.cisco.com`) using the SNI extension in the TLS handshake. The server then selects the corresponding private key and certificate chain that are required to establish the connection while hosting all certificates on a single IP address.

If there's a match between the SNI and the CN or a SAN in the certificate, we use the SNI when comparing against the DNs listed in the rule. If there is no SNI or if it doesn't match the certificate, we use the certificate's CN when comparing against the DNs listed in the rule.

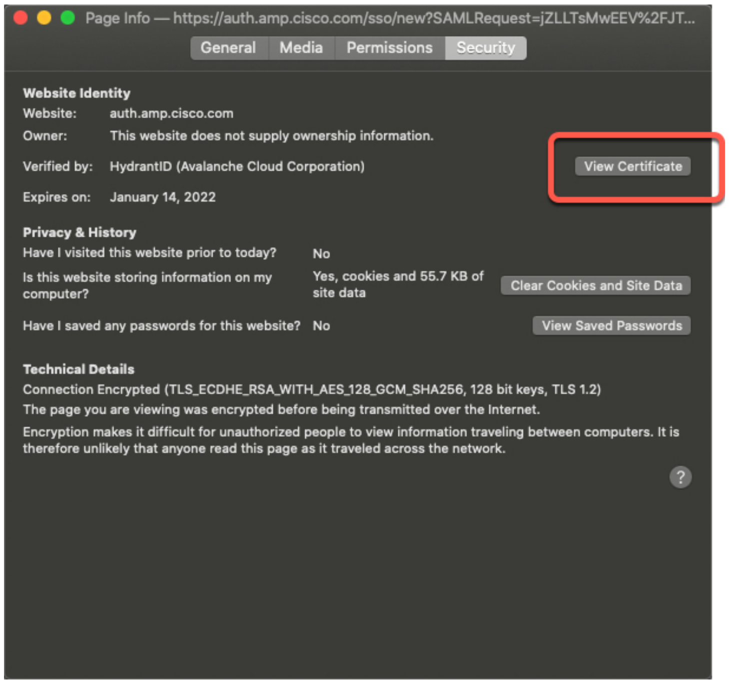
How to find a certificate's Common Name and subject alternative names

To find any certificate's Common Name, use the following steps. You can even use these steps to find the common name and SANs for a self-signed certificate.

These steps are for Firefox but other browsers are similar. The following procedure uses `amp.cisco.com` as an example.

1. Browse to `amp.cisco.com` in Firefox.
2. In the browser's location bar, to the left of the URL, click 🔒.
3. Click **Connection secure** > **More Information**.

   (For a non-secure or self-signed certificate, click **Connection not secure** > **More Information**.)
4. On the Page Info dialog box, click **View Certificate**.


Page Info — https://auth.amp.cisco.com/sso/new?SAMLRequest=jZLLTsMwEEV%2FJT...
General
Media
Permissions
Security
View Certificate
Clear Cookies and Site Data
View Saved Passwords

Website Identity

Website:	auth.amp.cisco.com
Owner:	This website does not supply ownership information.
Verified by:	HydrantID (Avalanche Cloud Corporation)
Expires on:	January 14, 2022

Privacy & History

Have I visited this website prior to today?	No
Is this website storing information on my computer?	Yes, cookies and 55.7 KB of site data
Have I saved any passwords for this website?	No

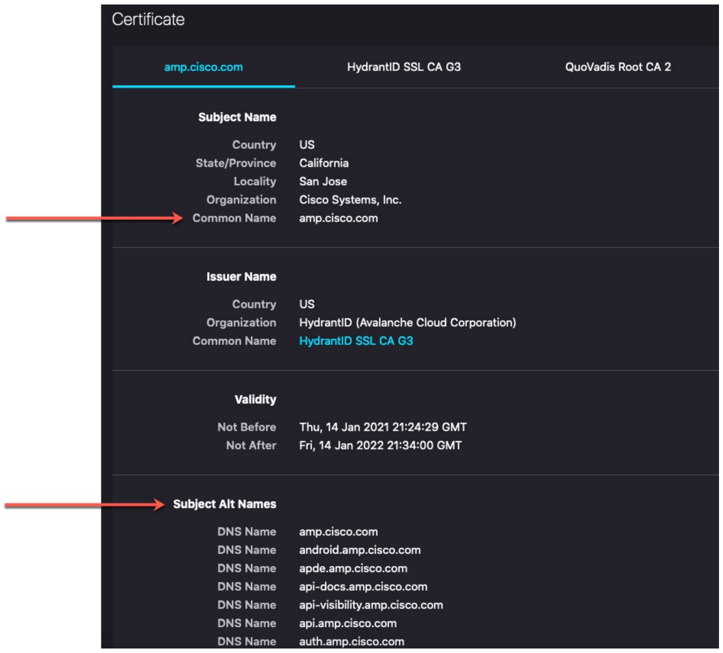
Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

5. The next page shows certificate details.



Subject Name

Country	US
State/Province	California
Locality	San Jose
Organization	Cisco Systems, Inc.
Common Name	amp.cisco.com

Issuer Name

Country	US
Organization	HydrantID (Avalanche Cloud Corporation)
Common Name	HydrantID SSL CA G3

Validity

Not Before	Thu, 14 Jan 2021 21:24:29 GMT
Not After	Fri, 14 Jan 2022 21:34:00 GMT

Subject Alt Names

DNS Name	amp.cisco.com
DNS Name	android.amp.cisco.com
DNS Name	apde.amp.cisco.com
DNS Name	api-docs.amp.cisco.com
DNS Name	api-visibility.amp.cisco.com
DNS Name	api.amp.cisco.com
DNS Name	auth.amp.cisco.com

Note the following:

- `CN=auth.amp.cisco.com`, if used as a DN rule condition, would match *only* that host name (that is, SNI). The SNI `amp.cisco.com` would *not* match.
- To match as many domain name fields as possible, use wildcards.

For example, to match `auth.amp.cisco.com`, use `CN=*.amp.cisco.com`. To match `auth.us.amp.cisco.com`, use `CN=*.*.amp.cisco.com`.

A DN like `CN=*.example.com` matches `www.example.com` but *not* `example.com`. To match both SNIs, use two DNs in the rule condition.

- Don't go overboard with wildcards though. For example, a DN object like `CN=*.google.com` matches a very large number of SANs. Instead of `CN=*.google.com`, use a DN object like `CN=*.youtube.com` as the DN object so it matches names like `www.youtube.com`.

  You can also use variations of the SNI that match SANs like `CN=*.youtube.com`, `CN=youtu.be`, `CN=*.yt.be`, and so on.

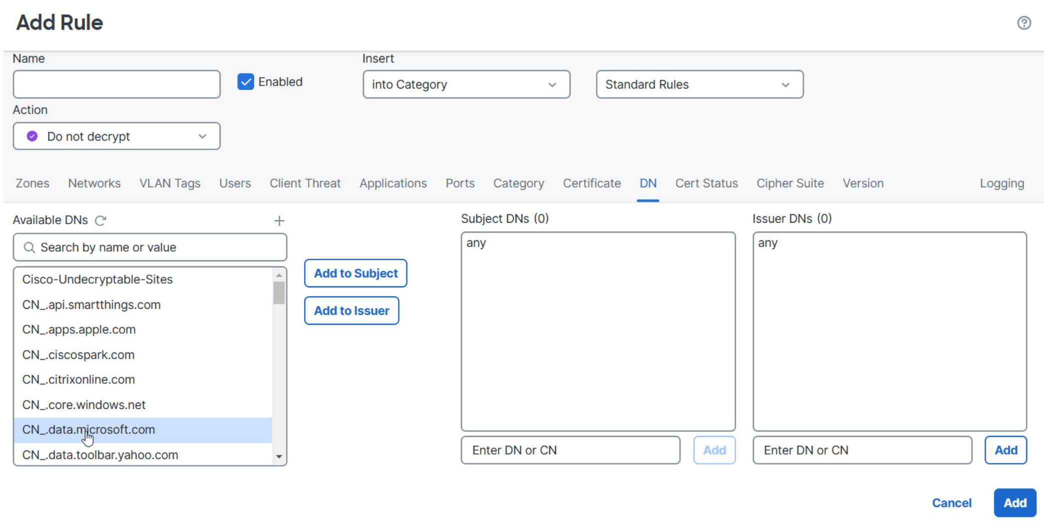
- A self-signed certificate should work the same way. You can confirm it's a self-signed certificate by the fact the issuer DN is the same as the subject DN.

How to add a DN rule condition

After you know the CN you want to match, edit the decryption rule in one of the following ways:

- Use an existing DN.

  Click the name of a DN and then click either **Add to Subject** or **Add to Issuer**. (**Add to Subject** is much more common.) To view the value of a DN object, hover the mouse pointer over it.)

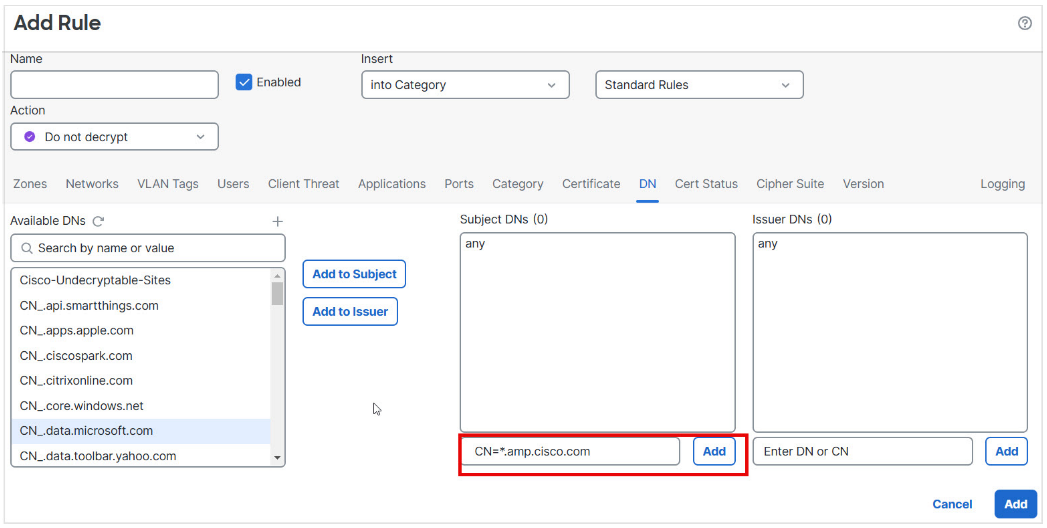


- Create a new DN object.

  Click **Add** (+) to the right of Available DNs. The DN object must consist of a name and a value.

- Add the DN directly.

  Enter the DN in the field at the bottom of the **Subject DNs** field or the **Issuer DNs** field. (**Subject DNs** is more common.) After you enter the DN, click **Add**.



Name

Enabled

Insert: into Category, Standard Rules

Action: Do not decrypt

Available DNs

Search by name or value

Cisco-Undecryptable-Sites
CN_.api.smartthings.com
CN_.apps.apple.com
CN_.ciscospark.com
CN_.citrixonline.com
CN_.core.windows.net
CN_.data.microsoft.com
CN_.data.toolbar.yahoo.com

Subject DNs (0): any

CN=*.amp.cisco.com

Issuer DNs (0): any

Enter DN or CN

Related Topics

Distinguished Name

Trusting external certificate authorities

You can trust CAs by adding root and intermediate CA certificates to your decryption policy, then use these trusted CAs to verify server certificates used to encrypt traffic.

If a trusted CA certificate contains an uploaded certificate revocation list (CRL), you can also verify whether a trusted CA revoked the encryption certificate.

Tip Upload all certificates in a root CA's chain of trust to the list of trusted CA certificates, including the root CA certificate and all intermediate CA certificates. Otherwise, it is more difficult to detect trusted certificates issued by intermediate CAs. Also, if you configure certificate status conditions to trust traffic based on the root issuer CA, all traffic within a trusted CA's chain of trust can be allowed without decryption, rather than unnecessarily decrypting it.

For more information, see Trusted CA Object.

Note When you create a decryption policy, the policy's **Trusted CA Certificate** tab page is populated with several trusted CA certificates, including the **Cisco-Trusted-Authorities** group, which is added to the **Select Trusted CAs** list.

Procedure

Step 1 Log in to the Firewall Management Center if you haven't already done so.

Step 2 Click **Policies** > **Security policies** > **Decryption**.

Step 3 Click **Edit** (✎) next to the decryption policy to edit.

Step 4 Click **Add Rule** to add a new decryption rule or click **Edit** (✎) to edit an existing rule.

Step 5 Click the **Certificates** tab.

Step 6 Find the trusted CAs you want to add from the **Available Certificates**, as follows:

- To add a trusted CA object on the fly, which you can then add to the condition, click **Add** (+) above the **Available Certificates** list.
- To search for trusted CA objects and groups to add, click the **Search by name or value** prompt above the **Available Certificates** list, then enter either the name of the object, or a value in the object. The list updates as you type to display matching objects.

Step 7 To select an object, click it. To select all objects, right-click and then **Select All**.

Step 8 Click **Add to Rule**.

Tip
You can also drag and drop selected objects.

Step 9 Add or continue editing the rule.

What to do next

- Add a certificate status decryption rule condition to your SSL rule. See Matching Traffic on Certificate Status for more information.
- Deploy configuration changes; see Deploy Configuration Changes.

Certificate Status Decryption rule Conditions

For each certificate status decryption rule you configure, you can match traffic against the presence or absence of a given status. You can select several statuses in one rule condition; if the certificate matches any of the selected statuses, the rule matches the traffic.

You can choose to match against the presence or absence of multiple certificate statuses in a single certificate status rule condition; the certificate needs to match only one of the criteria to match the rule.

You should consider, when setting this parameter, whether you're configuring a decrypt rule or a block rule. Typically, you should click **Yes** for a block rule and **No** for a decrypt rule. Examples:

- If you're configuring a **Decrypt - Resign** rule, the default behavior is to decrypt traffic with an expired certificate. To change that behavior, click **No** for **Expired** so traffic with an expired certificate is not decrypted and resigned.
- If you're configuring a **Block** rule, the default behavior is to allow traffic with an expired certificate. To change that behavior click **Yes** for **Expired** so traffic with an expired certificate is blocked.

The following table describes how the system evaluates encrypted traffic based on the encrypting server certificate’s status.

Table 2: Certificate Status Rule Condition Criteria

Status Check	Status Set to Yes	Status Set to No
Revoked	The policy trusts the CA that issued the server certificate, and the CA certificate uploaded to the policy contains a CRL that revokes the server certificate.	The policy trusts the CA that issued the certificate, and the CA certificate uploa policy does not contain a CRL that rev certificate.
Self-signed	The detected server certificate contains the same subject and issuer distinguished name.	The detected server certificate contains subject and issuer distinguished names
Valid	All of the following are true: • The policy trusts the CA that issued the certificate. • The signature is valid. • The issuer is valid. • None of the policy's trusted CAs revoked the certificate. • The current date is between the certificate Valid From and Valid To date.	At least one of the following is true: • The policy does not trust the CA t certificate. • The signature is invalid. • The issuer is invalid. • A trusted CA in the policy revoke certificate. • The current date is before the cert From date. • The current date is after the certifi date.
Invalid signature	The certificate's signature cannot be properly validated against the certificate's content.	The certificate's signature is properly va the certificate's content.
Invalid issuer	The issuer CA certificate is not stored in the policy's list of trusted CA certificates.	The issuer CA certificate is stored in th of trusted CA certificates.
Expired	The current date is after the certificate Valid To date.	The current date is before or on the cer To date.
Not yet valid	The current date is before the certificate Valid From date.	The current date is after or on the certi From date.

Status Check	Status Set to Yes	Status Set to No
Invalid certificate	The certificate is not valid. At least one of the following is true: • Invalid or inconsistent certificate extension; that is, a certificate extension had an invalid value (for example, an incorrect encoding) or some value inconsistent with other extensions. • The certificate cannot be used for the specified purpose. • The Basic Constraints path length parameter has been exceeded. For more information, see RFC 5280, section 4.2.1.9. • The certificate's value for Not Before or Not After is invalid. These dates can be encoded as UTCTime or GeneralizedTime For more information, see RFC 5280 section 4.1.2.5. • The format of the name constraint is not recognized; for example, an email address format of a form not mentioned in RFC 5280, section 4.2.1.10. This could be caused by an improper extension or some new feature not currently supported. An unsupported name constraint type was encountered. OpenSSL currently supports only directory name, DNS name, email, and URI types. • The root certificate authority is not trusted for the specified purpose. • The root certificate authority rejects the specified purpose.	The certificate is valid. All of the followin • Valid certificate extension. • The certificate can be used for the spe purpose. • Valid Basic Constraints path length. • Valid values for Not Before and Not • Valid name constraint. • The root certificate is trusted for the s purpose. • The root certificate accepts the specifie

Status Check	Status Set to Yes	Status Set to No
Invalid CRL	The Certificate Revocation List (CRL) digital signature is not valid. At least one of the following is true: • The value of the CRL's Next Update or Last Update field is invalid. • The CRL is not yet valid. • The CRL has expired. • An error occurred when attempting to verify the CRL path. This error occurs only if extended CRL checking is enabled. • CRL could not be found. • The only CRLs that could be found did not match the scope of the certificate.	The CRL is valid. All of the following • Next Update and Last Update fiel • The CRL's date is valid. • The path is valid. • The CRL was found. • The CRL matches the certificate's
Server mismatch	The server name does not match the server's Server Name Indication (SNI) name, which could indicate an attempt to spoof the server name.	The server name matches the SNI name to which the client is requesting access

Note that even though a certificate might match more than one status, the rule causes an action to be taken on the traffic only once.

Checking whether a CA issued or revoked a certificate requires uploading root and intermediate CA certificates and associated CRLs as objects. You then add these trusted CA objects to an decryption policy's list of trusted CA certificates.

Cipher suite rule conditions

The system provides predefined cipher suites you can add to a cipher suite rule condition for Block or Block with Reset rule actions. You can also add cipher suite list objects containing multiple cipher suites.

Important Cipher suite rule conditions can be used only to *block* traffic, they cannot be used to *decrypt* traffic.

Note You cannot add new cipher suites. You can neither modify nor delete predefined cipher suites.

You can add a maximum of 50 cipher suites and cipher suite lists to the **Selected Cipher Suites** in a single cipher suite condition. The system supports adding the following cipher suites to a cipher suite condition:

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

Note the following:

- If you add cipher suites not supported for your deployment, you cannot deploy your configuration. For example, passive deployments do not support decrypting traffic with the any of the ephemeral Diffie-Hellman (DHE) or ephemeral elliptic curve Diffie-Hellman (ECDHE) cipher suites. Creating a rule with these cipher suites prevents you from deploying your access control policy.
- You can add an anonymous cipher suite to the **Cipher Suite** condition in decryption policy to use the rule, you must also configure your in an order that prevents ClientHello processing. For more information, see Decryption policy Rule Order.
- When specifying a cipher suite as a rule condition, consider that the rule matches on the negotiated cipher suite in the ServerHello message, rather than on the full list of cipher suites specified in the ClientHello message. During ClientHello processing, the managed device strips unsupported cipher suites from the ClientHello message. However, if this results in all specified cipher suites being stripped, the system retains the original list. If the system retains unsupported cipher suites, subsequent evaluation results in an undecrypted session.

Encryption protocol version rule conditions

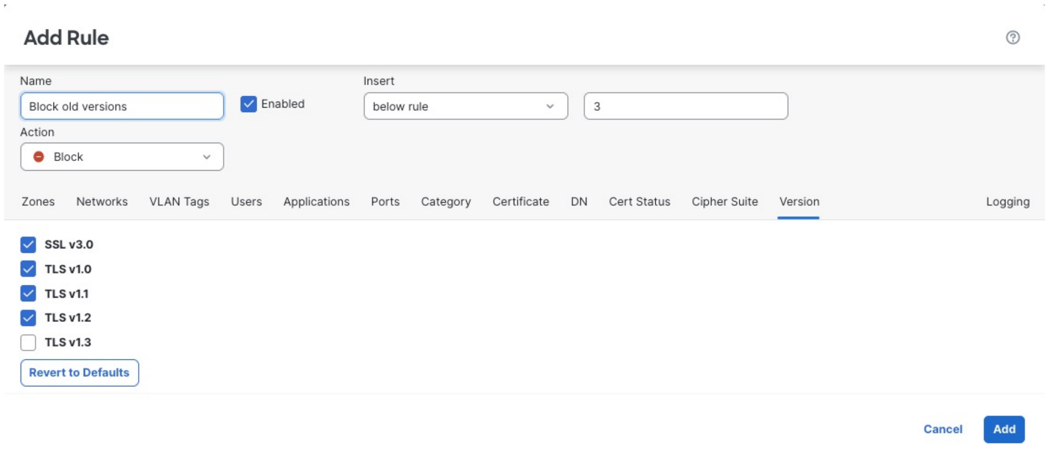
You can choose to match against traffic encrypted with SSL version 3.0, or TLS version 1.0, 1.1, or 1.2. By default, all protocol versions are selected when you create a rule; if you select multiple versions, encrypted traffic that matches any of the selected versions matches the rule. You must select at least one protocol version when saving the rule condition.

You can use SSL 3.0 in a Do Not Decrypt, Block, or Block with Reset rule action.

You *cannot* select SSL v2.0 in a version rule condition; the system does not support decrypting traffic encrypted with SSL version 2.0. You can configure an undecryptable action to allow or block this traffic without further inspection. For more information, see Set default handling for undecryptable traffic.

Important Protocol version rule conditions can be used *only* to *block* traffic, they cannot be used to *decrypt* traffic.

For example, to block all SSL v3.0, TLS v1.0, TLS v1.1, and TLS v1.2 traffic, set the options as follows:


Add Rule

Name: Block old versions
Enabled: ✓
Insert: below rule 3
Action: Block

- [✓] SSL v3.0
- [✓] TLS v1.0
- [✓] TLS v1.1
- [✓] TLS v1.2
- [ ] TLS v1.3

Rule-based decryption rule actions

The following sections discuss the actions available with rule-based decryption rule .

Rule-based decryption rule monitor action

The **Monitor** action is not designed to permit or deny traffic. Rather, its primary purpose is to force connection logging, regardless of how matching traffic is eventually handled. The ClientHello message is not modified if traffic matches a **Monitor** rule condition.

Traffic is then matched against additional rules, if present, to determine whether to trust, block, or decrypt it. The first non-Monitor rule matched determines traffic flow and any further inspection. If there are no additional matching rules, the system uses the default action.

Because the primary purpose of Monitor rules is to track network traffic, the system automatically logs end-of connection events for monitored traffic to the Secure Firewall Management Center database, regardless of the logging configuration of the rule or default action that later handles the connection.

Rule-based decryption rule Do Not Decrypt action

The **Do Not Decrypt** action passes encrypted traffic for evaluation by the access control policy's rules and default action. Because some access control rule conditions require unencrypted traffic, this traffic might match fewer rules. The system cannot perform deep inspection on encrypted traffic, such as intrusion or file inspection.

Typical reasons for a **Do Not Decrypt** rule action include:

- When decrypting TLS/SSL traffic is prohibited by law.
- Sites you know you can trust.
- Sites you can disrupt by inspecting traffic (such as Windows Update).
- To view the values of TLS/SSL fields using connection events. (You do not need to decrypt traffic to view connection event fields.) For more information, see *Requirements for Populating Connection Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide*.

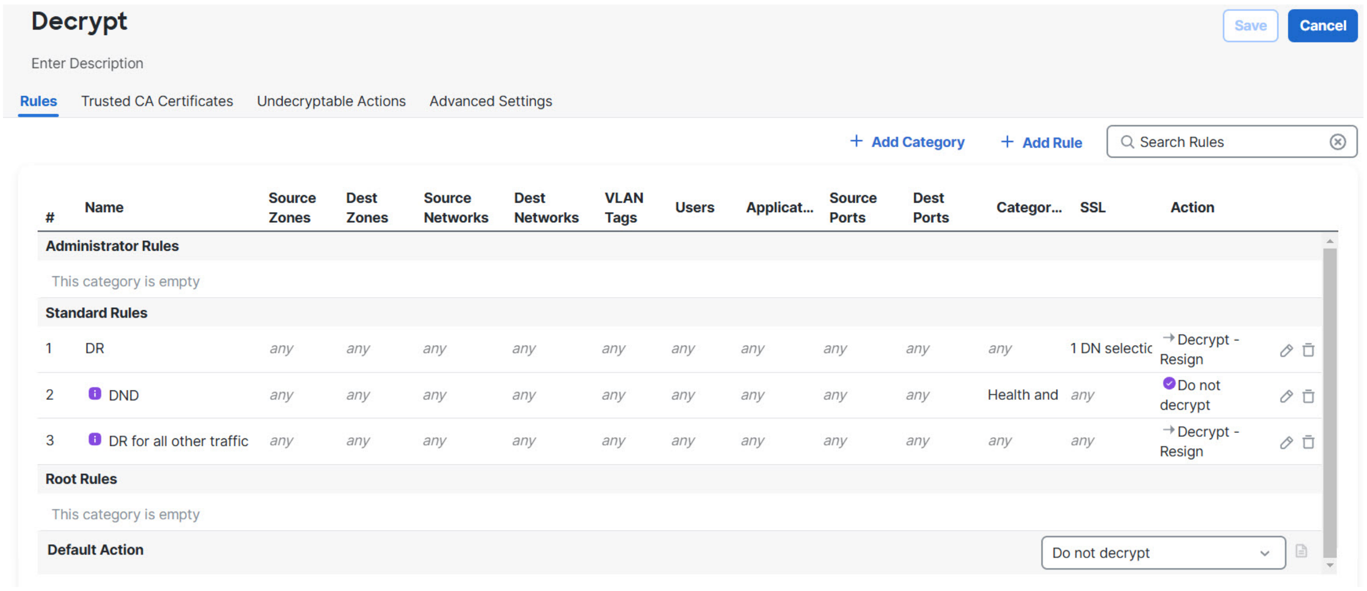
For more information, see Default handling options for undecryptable traffic

Limitations of categories in Do Not Decrypt rules

You can optionally choose to include categories in your decryption policies. These categories, also referred to as *URL filtering*, are updated by the Cisco Talos intelligence group. Updates are based on machine learning and human analysis according to content that is retrievable from the website destination and sometimes from its hosting and registration information. Categorization is *not* based on the declared company vertical, intent, or security. While we strive to continuously update and improve URL filtering categories, it is not an exact science. Some websites are not categorized at all and it's possible some websites might be improperly categorized.

Avoid overusing categories in do not decrypt rules to avoid decrypting traffic without a reason; for example, the Health and Medicine category includes the WebMD website, which does not threaten patient privacy.

Following is a sample decryption policy that can prevent decryption for websites in the Health and Medicine categories but allows decryption for WebMD and everything else. General information about decryption rules can be found in Guidelines for using TLS/SSL decryption, on page 2.



#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	Categor...	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DR	any	any	any	any	any	any	any	any	any	any	1 DN selectic	Decrypt - Resign
2	DND	any	any	any	any	any	any	any	any	any	Health and	any	Do not decrypt
3	DR for all other traffic	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													Do not decrypt

Note Don't confuse URL filtering with application detection, which relies on reading some of the packet from a website to determine more specifically what it is (for example, Facebook Message or Salesforce). For more information, see Recommendations for application control.

Rule-based decryption rule blocking actions

The system provides the following decryption rule actions for traffic you do not want to pass through the system:

- **Block** to terminate the connection, resulting in an error in the client browser.

  The error message does not indicate the site was blocked due to policy. Instead, errors might indicate that there are no common encryption algorithms. It is not obvious from this message that you blocked the connection on purpose.

- **Block with reset** to terminate and reset the connection, resulting in an error in the client browser.

  The error indicates the connection was reset but does not indicate why.

Tip You cannot use the **Block** or **Block with reset** action in a passive or inline (tap mode) deployment because the device does not directly inspect the traffic. If you create a rule with the **Block** or **Block with reset** action that contains passive or inline (tap mode) interfaces within a security zone condition, the policy editor displays a warning (⚠) next to the rule.

Rule-based decryption rule decrypt actions

The **Decrypt - Replace Cert**, **Decrypt - Known Key**, and **Decrypt - Resign** actions decrypt encrypted traffic. The system inspects decrypted traffic with access control. Access control rules handle decrypted and unencrypted traffic identically — you can inspect it for discovery data as well as detect and block intrusions, prohibited files, and malware. The system reencrypts allowed traffic before passing it to its destination.

We recommend you use a certificate from a trusted Certificate Authority (CA) to decrypt traffic. This prevents **Invalid Issuer** from being displayed in the SSL Certificate Status column in connection events.

For more information about adding trusted objects, see Trusted Certificate Authority Objects.

Related topic: TLS 1.3 decryption best practices.

Related Topics

TLS 1.3 decryption best practices

Incoming traffic decryption actions

Both the **Decrypt - Replace Cert** and **Decrypt - Known Key** decryption actions enable you to decrypt *incoming* traffic to a server you want to protect from malicious attacks.

We provide the **Decrypt - Replace Cert** decryption action as an alternative to **Decrypt - Known Key** for the following reasons:

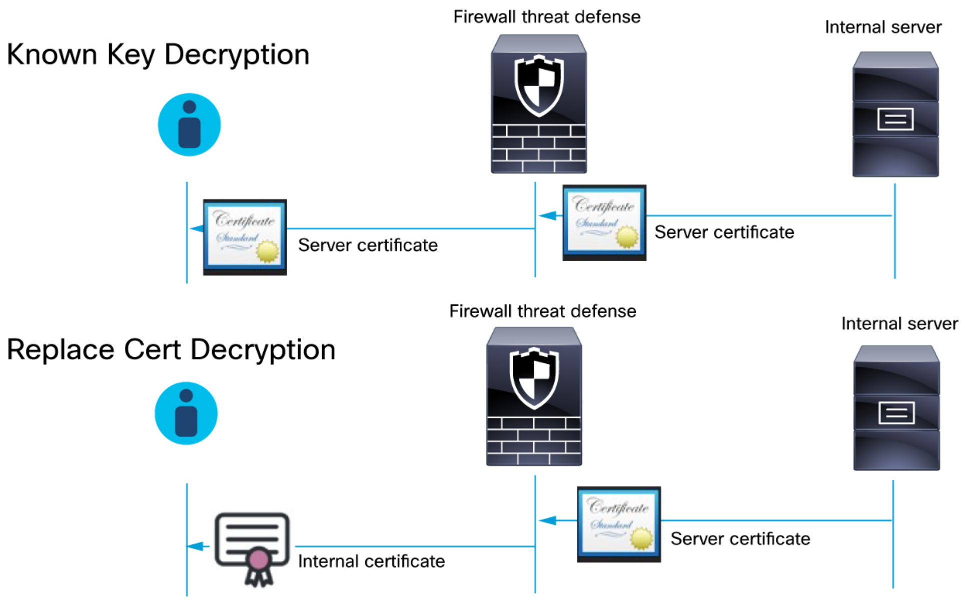
- Certificates can expire or need to be replaced anytime.

  If you choose the **Decrypt - Known Key** action, decryption can stop and the rule can stop functioning when a certificate is replaced for any reason.

- With **Decrypt - Replace Cert**, the connection matches and traffic is decrypted, and deploying the certificate hours or days later on the device is not an issue.

- **Decrypt - Replace Cert** gives you the flexibility to have separate internal and external facing certificates. For example, you could use `payroll.example.local` as an internal server hostname, but use `payroll.example.com` as an externally-facing hostname. You can also use an Enterprise PKI certificate for an internal server but use DigiCert or some other public provider for my external certificate.

The following figure shows the difference between **Decrypt - Replace Cert** and **Decrypt - Known Key** decryption actions.



The following table provides more information.

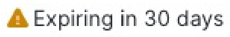
	Known Key	**Replace Cert**
Must match certificate installed on internal server or resource	Yes	No
The device must trust the internal certificate (that is, it must be chained to Trusted CAs list in the decryption policy)	No	No
Certificate hostnames can be different between device-installed certificate and that on the internal server	No, certificates must be identical. (Although multiple SANs can be on the certificates to accommodate different internal and external host names.)	Yes, certificates and certificate host names can be completely different, as long as the internal certificate is trusted by the user's device.
Works if the internal server certificate is expired	Yes – As long as it matches the certificate installed on the device.	No – an expired certificate causes broken trust, and therefore a mismatch.

Replace an internal certificate (Decrypt - Replace Cert only)

This task discusses how to replace the internal certificate used in an incoming decryption rule using the Secure Firewall Management Center (**Objects** > **PKI** > **Internal Certs**).

You can also replace the certificate using the API as discussed in *Cisco Secure Firewall Threat Defense REST API Guide*.

The system indicates that an internal certificate is *expiring* when today's date is within 30 days of its expiration date. The following figure shows an example.


Expiring in 30 days

Before you begin

You must choose the **Decrypt - Replace Cert** decryption rule action in any of the following ways:

- In a rule-based decryption policy by clicking the action from the rule's **Action** list.
- Create a standard decryption policy, which always uses the **Decrypt - Replace Cert** rule action.

Procedure

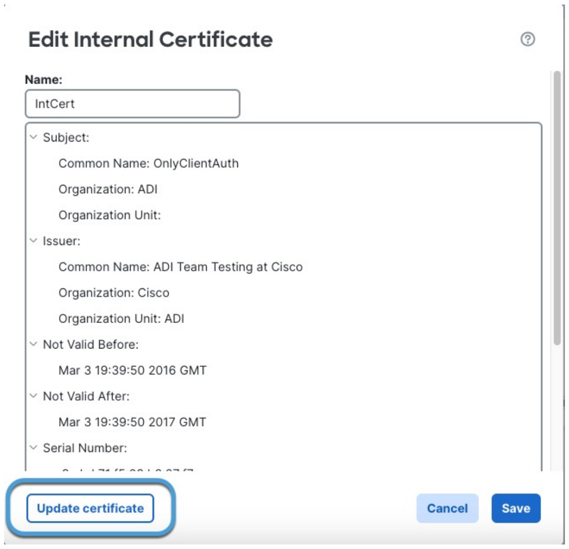
Step 1 Log in to Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Objects** > **PKI** > **Internal Certs**.

Step 3 Locate the internal certificate that is expired or expiring (for example, an expired certificate is indicated by ❗ Expired).

Step 4 Click **Edit** (✎).

Step 5 Click **Update Certificate** as the following figure shows.



Edit Internal Certificate

Name:
IntCert

Subject:
Common Name: OnlyClientAuth
Organization: ADI
Organization Unit:
Issuer:
Common Name: ADI Team Testing at Cisco
Organization: Cisco
Organization Unit: ADI
Not Valid Before:
Mar 3 19:39:50 2016 GMT
Not Valid After:
Mar 3 19:39:50 2017 GMT
Serial Number:

Step 6 Enter the requested information; see Upload an internal certificate for inbound protection for more information.

Step 7 Follow the prompts on your screen to complete the action.

Decrypt - Resign rule action

The **Decrypt - Resign** rule action enables you to decrypt *outgoing* traffic so the traffic can be subjected to deep inspection.

Select internal certificate objects

Before you begin

To create a decryption rule with a **Decrypt - Known Key** action, you must add internal certificates for the servers to decrypt traffic. For more information, see Internal Certificate Objects.

For important guidelines, see TLS/SSL incoming traffic decryption guidelines, on page 5.

Procedure

Step 1 Click **Edit** (🖉) in the field next to the decryption rule **Action**.

Step 2 In the Select Internal Certificate Objects dialog box, do the following:
Available Certificates list: Click the name of a certificate and click **Add to Rule** to use it in this rule. You can add one or more certificates to the rule.

Selected Certificates list: Displays internal certificates used in the rule. To remove a certificate, click **Delete** (🗑).

Step 3 To save these changes, click **OK**.

Monitor TLS/SSL hardware acceleration

The following topics discuss how to monitor the status of TLS/SSL

Informational counters

If a system under load is working well, you should see large counts for the following counters. Because there are 2 sides to the tracker process per connection, you can see these counters increase by 2 per connection. The PRIV_KEY_RECV and SECU_PARAM_RECV counters are the most important, and are highlighted. The CONTEXT_CREATED and CONTEXT_DESTROYED counters relate to the allocation of cryptographic chip memory.

```
> show counters
Protocol      Counter                          Value   Context
SSLENC        CONTEXT_CREATED                 258225   Summary
SSLENC        CONTEXT_DESTROYED               258225   Summary
TLS_TRK       OPEN_SERVER_SESSION             258225   Summary
TLS_TRK       OPEN_CLIENT_SESSION             258225   Summary
TLS_TRK       UPSTREAM_CLOSE                  516450   Summary
TLS_TRK       DOWNSTREAM_CLOSE                516450   Summary
TLS_TRK       FREE_SESSION                    516450   Summary
TLS_TRK       CACHE_FREE                      516450   Summary
TLS_TRK       PRIV_KEY_RECV                   258225   Summary
TLS_TRK       NO_KEY_ENABLE                   258225   Summary
TLS_TRK       SECU_PARAM_RECV                 516446   Summary
TLS_TRK       DECRYPTED_ALERT                 258222   Summary
TLS_TRK       DECRYPTED_APPLICATION         33568976   Summary
TLS_TRK       ALERT_RX_CNT                    258222   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT           258222   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY            258222   Summary
TCP_PRX      OPEN_SESSION                     516450   Summary
TCP_PRX      FREE_SESSION                     516450   Summary
TCP_PRX      UPSTREAM_CLOSE                   516450   Summary
TCP_PRX      DOWNSTREAM_CLOSE                 516450   Summary
TCP_PRX      FREE_CONN                        258222   Summary
TCP_PRX      SERVER_CLEAN_UP                  258222   Summary
TCP_PRX      CLIENT_CLEAN_UP                  258222   Summary
```

Alert counters

We implemented the following counters according to the TLS 1.2 specification. FATAL or BAD alerts could indicate issues; however, ALERT_RX_CLOSE_NOTIFY is normal.

For details, see RFC 5246 section 7.2.

```
TLS_TRK      ALERT_RX_CNT                                311   Summary
TLS_TRK      ALERT_TX_CNT                                  2   Summary
TLS_TRK      ALERT_TX_IN_HANDSHAKE_CNT                     2   Summary
TLS_TRK      ALERT_RX_IN_HANDSHAKE_CNT                     2   Summary
TLS_TRK      ALERT_RX_WARNING_ALERT                      308   Summary
TLS_TRK      ALERT_RX_FATAL_ALERT                          3   Summary
TLS_TRK      ALERT_TX_FATAL_ALERT                          2   Summary
TLS_TRK      ALERT_RX_CLOSE_NOTIFY                       308   Summary
TLS_TRK      ALERT_RX_BAD_RECORD_MAC                       2   Summary
TLS_TRK      ALERT_TX_BAD_RECORD_MAC                       2   Summary
TLS_TRK      ALERT_RX_BAD_CERTIFICATE                      1   Summary
```

Error counters

These counters indicate system errors. These counts should be low on a healthy system. The BY_PASS counters indicate packets that have been passed directly to or from the inspection engine (Snort) process (which runs in software) without decryption. The following example lists some of the bad counters.

Counters with a value of 0 are not displayed. To view a complete list of counters, use the command **show counters description | include TLS_TRK**

```
> show counters
Protocol     Counter                           Value   Context
TCP_PRX      BYPASS_NOT_ENOUGH_MEM              2134   Summary
TLS_TRK      CLOSED_WITH_INBOUND_PACKET            2   Summary
TLS_TRK      ENC_FAIL                             82   Summary
TLS_TRK      DEC_FAIL                            211   Summary
TLS_TRK      DEC_CKE_FAIL                      43194   Summary
TLS_TRK      ENC_CB_FAIL                        4335   Summary
TLS_TRK      DEC_CB_FAIL                         909   Summary
TLS_TRK      DEC_CKE_CB_FAIL                     818   Summary
TLS_TRK      RECORD_PARSE_ERR                    123   Summary
TLS_TRK      IN_ERROR                          44948   Summary
TLS_TRK      ERROR_UPSTREAM_RECORD             43194   Summary
TLS_TRK      INVALID_CONTENT_TYPE                123   Summary
TLS_TRK      DOWNSTREAM_REC_CHK_ERROR            123   Summary
TLS_TRK      DECRYPT_FAIL                      43194   Summary
TLS_TRK      UPSTREAM_BY_PASS                    127   Summary
TLS_TRK      DOWNSTREAM_BY_PASS                  127   Summary
```

Fatal counters

The fatal counters indicate serious errors. These counters should be at or near 0 on a healthy system. The following example lists the fatal counters.

```
> show counters
Protocol     Counter                          Value   Context
CRYPTO       RING_FULL                            1   Summary
CRYPTO       ACCELERATOR_CORE_TIMEOUT             1   Summary
CRYPTO       ACCELERATOR_RESET                    1   Summary
CRYPTO       RSA_PRIVATE_DECRYPT_FAILED           1   Summary
```

The RING_FULL counter is not a fatal counter, but indicates how often the system overloaded the cryptographic chip. The ACCELERATOR_RESET counter is the number of times the TLS crypto acceleration process failed unexpectedly, which also causes the failure of pending operations, which are the numbers you see in ACCELERATOR_CORE_TIMEOUT and RSA_PRIVATE_DECRYPT_FAILED.

If you have persistent problems, disable TLS crypto acceleration (or **config hwCrypto disable**) and work with Cisco TAC to resolve the issues.

Note You can do additional troubleshooting using the **show snort tls-offload** and **debug snort tls-offload** commands. Use the **clear snort tls-offload** command to reset the counters displayed in the **show snort tls-offload** command to zero.

Troubleshoot rule-based decryption rules

The following topics discuss how to troubleshoot rule-based decryption rules .

About 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 decryption policy's **Undecryptable Actions**:

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

If the setting for **Handshake Errors** in the decryption 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.

Troubleshoot TLS/SSL oversubscription

If your managed device has TLS crypto acceleration enabled, you can view connection events to determine whether or not the devices are experiencing SSL oversubscription. You must add at least the **SSL Flow Flags** event to the table view of connection events.

Before you begin

- Configure a decryption policy with a setting for **Handshake Errors** on **Undecryptable Actions** page.

  For more information, see Set default handling for undecryptable traffic.

- Enable logging for your SSL rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

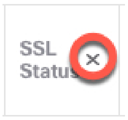
Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

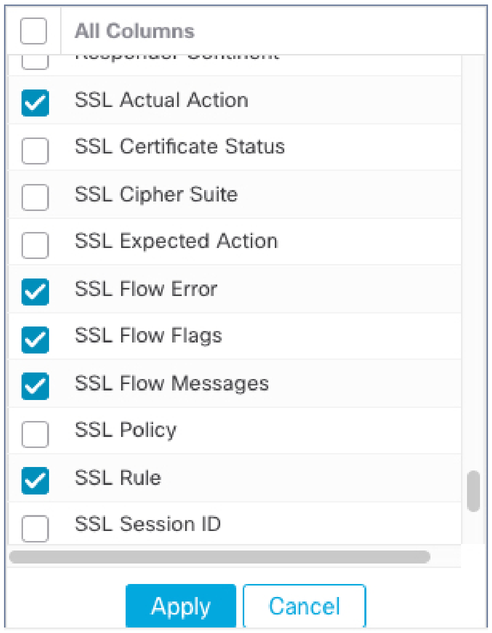
Step 2 Click **Events & Logs** > **+ Show more** > **Connection** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events. (Look in the Disabled Columns section of the dialog box.)



The columns are added in the order discussed in *Connection and Security Intelligence Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide* .

Step 5 Click **Apply**.

TLS/SSL oversubscription is indicated by the values of `ERROR_EVENT_TRIGGERED` and `OVER_SUBSCRIBED` in the **SSL Flow Flags** column.

Step 6 If TLS/SSL oversubscription is occurring, log in to the managed device and enter any of the following commands:

Command	Result
show counters	If the value of **TCP_PRX BYPASS_NOT_ENOUGH_MEM** is large, consider upgrading your device to one with a larger capacity for SSL traffic or use **Do Not Decrypt** rules for lower priority encrypted traffic.
show snort tls-offload	If the value of **BYPASS_NOT_ENOUGH_MEM** is large, consider upgrading your device to one with a larger capacity for SSL traffic or use **Do Not Decrypt** rules for lower priority encrypted traffic.

About 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 decryption policy's **Undecryptable Actions**:

- Block
- Block with reset

Related Topics

Troubleshoot TLS heartbeat, on page 43

Troubleshoot TLS heartbeat

If your managed device has TLS crypto acceleration enabled, you can view connection events to determine whether or not the devices are seeing traffic with the TLS heartbeat extension. You must add at least the **SSL Flow Messages** event to the table view of connection events.

Before you begin

SSL heartbeat is indicated by the value of `HEARTBEAT` in the **SSL Flow Messages** column in the table view of connection events. To determine if applications in your network use SSL heartbeat, first perform the following tasks:

- Configure an decryption policy with a setting for **Decryption Errors** on **Undecryptable Actions** page.

  For more information, see Set default handling for undecryptable traffic.

- Enable logging for your SSL rules as discussed in Secure Firewall Management Center and Threat Defense Management Network Administration.

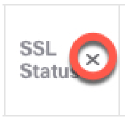
Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

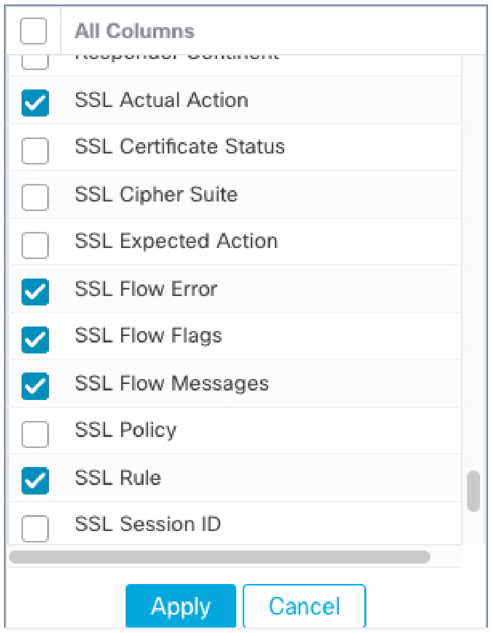
Step 2 Click **Events & Logs** > **+ Show more** > **Connection** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events.



The columns are added in the order discussed in *Connection and Security Intelligence Event Fields* in the *Cisco Secure Firewall Management Center Administration Guide* .

Step 5 Click **Apply**.
TLS heartbeat is indicated by the value of `HEARTBEAT` in the **SSL Flow Messages** column.

Step 6 If applications in your network use SSL heartbeat, see rule-based decryption rules guidelines and limitations, on page 2.

About TLS/SSL pinning

Some applications use a technique referred to as *TLS/SSL pinning* or *certificate pinning*, which embeds the fingerprint of the original server certificate in the application itself. As a result, if you configured a decryption rule with a **Decrypt - Resign** action, when the application receives a resigned certificate from a managed device, validation fails and the connection is aborted.

To confirm that TLS/SSL pinning is occurring, attempt to log in to a mobile application like Facebook. If a network connection error is displayed, log in using a web browser. (For example, you *cannot* log in to a Facebook mobile application but *can* log in to Facebook using Safari or Chrome.) You can use Firepower Management Center connection events as further proof of TLS/SSL pinning

Note TLS/SSL pinning is not limited to mobile applications.

If applications in your network use SSL pinning, see TLS/SSL certificate pinning guidelines, on page 8.

Related Topics

Troubleshoot TLS/SSL pinning, on page 45

Troubleshoot TLS/SSL pinning

You can view connection events to determine whether or not the devices are experiencing SSL pinning. You must add at least the **SSL Flow Flags** and **SSL Flow Messages** columns to the table view of connection events.

Before you begin

- Enable logging for your decryption rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.
- Log in to a mobile application like Facebook; if a network connection error displays, log in to Facebook using Chrome or Safari. If you *can* log in using a web browser but not the native application, SSL pinning is likely occurring.

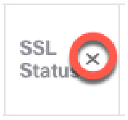
Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

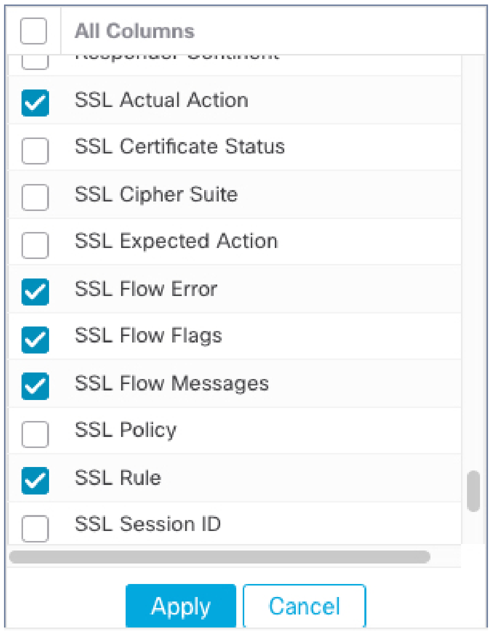
Step 2 Click **Events & Logs** > **+ Show more** > **Connection** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events.



The columns are added in the order discussed in the section on connection and security intelligence event fields in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Step 5 Click **Apply**.

Step 6 The following paragraphs discuss how you can identify SSL pinning behavior.

Step 7 If you determine that applications in your network use SSL pinning, see rule-based decryption rules guidelines and limitations, on page 2.

What to do next

You can use TLS/SSL connection events to confirm TLS/SSL pinning is occurring by looking for any of the following:

- Applications that send an SSL ALERT Message as soon as the client receives the SERVER_HELLO, SERVER_CERTIFICATE, SERVER_HELLO_DONE message from the server, followed by a TCP Reset, exhibit the following symptoms. (The alert, `Unknown CA (48)`, can be viewed using a packet capture.)
  - The SSL Flow Flags column displays `ALERT_SEEN` but *not* `APP_DATA_C2S` or `APP_DATA_S2C`.
  - If your managed device has SSL hardware acceleration enabled, the SSL Flow Messages column typically displays: `CLIENT_ALERT`, `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`.
  - If your managed device doesn't support SSL hardware acceleration or if the feature is disabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`.
  - `Success` is displayed in the SSL Flow Error column.

- Applications that send no alerts but instead send TCP Reset after the SSL handshake is finished exhibit the following symptoms:
  - The SSL Flow Flags column does *not* display `ALERT_SEEN`, `APP_DATA_C2S`, or `APP_DATA_S2C`.
  - If your managed device has SSL hardware acceleration enabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`, `SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`.
  - If your managed device doesn't support SSL hardware acceleration or if the feature is disabled, the SSL Flow Messages column typically displays: `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`,`SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`.
  - `Success` is displayed in the SSL Flow Error column.

Related Topics

Troubleshoot unknown or bad certificates or certificate authorities, on page 47

Troubleshoot unknown or bad certificates or certificate authorities

You can view connection events to determine whether or not the devices are experiencing unknown certificate authorities, bad certificates, or unknown certificates. This procedure can also be used if a TLS/SSL certificate has been pinned. You must add at least the **SSL Flow Flags** and **SSL Flow Messages** columns to the table view of connection events.

Before you begin

- Set up a decryption rule.
- Enable logging for your decryption rules as discussed in the section on logging decryptable connections in decryption rules in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

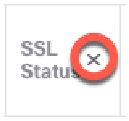
Procedure

Step 1 If you haven't done so already, log in to the Firewall Management Center.

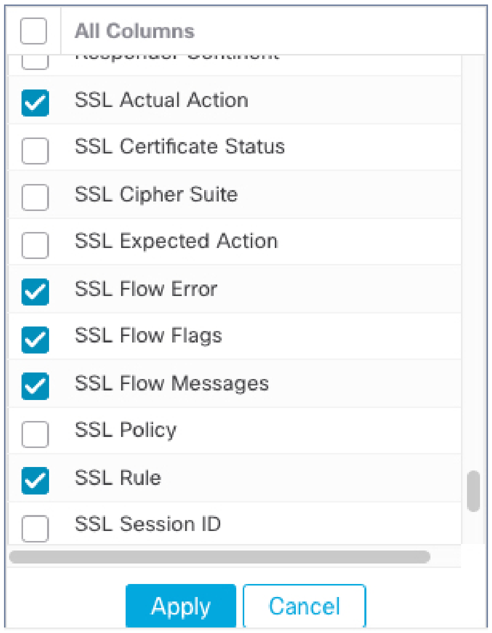
Step 2 Click **Events & Logs** > **+ Show more** > **Connection** > **Events**.

Step 3 Click **Table View of Connection Events**.

Step 4 Click **x** on any column in the connection events table to add additional columns for at least **SSL Flow Flags** and **SSL Flow Messages**.



The following example shows adding the **SSL Actual Action**, **SSL Flow Error**, **SSL Flow Flags**, **SSL Flow Messages**, **SSL Policy**, and **SSL Rule** columns to the table of connection events.



The columns are added in the order discussed in the section on connection and security intelligence event fields in the Secure Firewall Management Center and Threat Defense Management Network Administration guide.

Step 5 Click **Apply**.

Step 6 The following table discusses how you can determine if a certificate or certificate authority is bad or missing.

SSL flow flag	Meaning
CLIENT_ALERT_SEEN_UNKNOWN_CA	Indicates a valid certificate chain or partial chain was received by an SSL client application, but the certificate was not accepted because the CA certificate could not be located or could not be matched with a known, trusted CA. This message always indicates an unrecoverable error.
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	A certificate was corrupt, contained signatures that did not verify correctly, or had other problems.
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	Some other (unspecified) issue arose in processing the certificate, rendering it unacceptable.

Verify TLS/SSL cipher suites

Before you begin

This topic discusses actions you must take if you see the following error when saving a decryption rule that has cipher suite conditions:

```
Traffic cannot match this rule; none of your selected cipher suites contain a signature
algorithm that matches the resigning CA's signature algorithm
```

The error indicates that one or more of the cipher suites you chose for the decryption rule condition are incompatible with the certificate used in the decryption rule. To resolve the issue, you must have access to the certificate you're using.

Note The tasks in this topic assume knowledge of how TLS/SSL encryption works.

Procedure

Step 1 When you attempt to save a decryption rule rule with either **Decrypt - Resign**, **Decrypt - Replace Cert**, or **Decrypt - Known Key** with specified cipher suites, the following error is displayed:

Example:

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

Step 2 Locate the certificate you're using to decrypt traffic and, if necessary, copy the certificate to a system that can run openssl commands.

Step 3 Run the following command to display the signature algorithm used by the certificate:

openssl x509 -in *CertificateName* **-text -noout**

The first few lines of output are displayed similar to the following:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

Step 4 The **Signature algorithm** tells you the following:

- The cryptographic function used (in the preceding example, **ECDSA** means Elliptic Curve Digital Signature Algorithm).
- The hash function used to create a digest of the encrypted message (in the preceding example, **SHA256**).

Step 5 Search a resource such as *OpenSSL at University of Utah* for cipher suites that match those values. The cipher suite must be in RFC format.
You can also search a variety of other sites, such as Server Side TLS at the Mozilla wiki or Appendix C of RFC 5246. Cipher Suites in TLS/SSL (Schannel SSP) in Microsoft documentation has a detailed explanation of cipher suites.

Step 6 If necessary, translate the OpenSSL name to an RFC name that the Firepower Management System uses.

See the RFC mapping list on the on the `https://testssl.sh` site.

Step 7 The previous example, **ecdsa-with-SHA256**, can be found in the Modern Compatibility List on the Mozilla wiki.

a) Choose only cipher suites that have **ECDSA** and **SHA-256** in the name. These cipher suites follow:

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) Find the corresponding RFC cipher suite on RFC mapping list. These cipher suites follow:

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

Step 8 Add the preceding cipher suites to your decryption rule.

Troubleshooting using crypto archives

About Crypto Archives

Crypto issues are difficult to triage. Crypto archives help you to troubleshoot these issues. A crypto archive contains crypto session information about the crypto request, peer information, the component that sent the crypto request, and the timed-out crypto session information. Threat defense does not save keys and initialization vectors (IVs) for the session. For SSL and IPsec, you can also view the following information:

- For SSL: Session SSL version, source, destination IP addresses, and ports.
- For IPsec: IPsec security association information.

A ring can hold 2000 crypto command entries. Threat defense pushes the crypto command in one of the rings and pulls out the result after completing the crypto request. Crypto archive files now have the timed-out crypto request's ring and entry index. The ring and its entry index help in troubleshooting problematic crypto commands.

The crypto archive has two formats: a text file and a binary file. You can use the **debug menu ctm 103** command to decode the binary file. The crypto archive files are available at disk0:/crypto_archive.

For example:

```
FTD# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443
```

In the above example, the highlighted information shows the timeout ring, the crash time (timeout entry), and SSL session information.

Supported Devices for Crypto Archives

The following devices with Nitrox V crypto accelerator support crypto archives:

- Cisco Firepower 3105, 3110, 3120, 3130, 3140
- Cisco Firepower 4112, 4115, 4125, 4145
- Cisco Firepower 9300 SM-40, SM-48 and SM-56
- Cisco Secure Firewall 4200