



Decryption Rules Best Practices

- [Decryption Rules Best Practices, on page 1](#)
- [Use the Decryption Policy Wizard, on page 3](#)
- [Do Not Decrypt Best Practices, on page 5](#)
- [Decrypt - Resign and Decrypt - Known Key Best Practices, on page 6](#)
- [Decryption Rules to Put First, on page 6](#)
- [Decryption Rules to Put Before the Decrypt - Resign Rule, on page 7](#)
- [Logging Best Practices and Recommendations, on page 7](#)
- [Use Security Zones in Access Control Rules, on page 7](#)
- [Bypass Inspection with Prefilter and Flow Offload, on page 9](#)

Decryption Rules Best Practices

This chapter provides an example decryption policy with decryption rules that illustrates our best practices and recommendations. First we'll discuss settings for the decryption policies and access control policies and then walk through all the rules and why we recommend they be ordered in a particular way.

Some general guidelines:

- Decrypting traffic requires processing and memory; decrypting too much traffic can impact performance. Before you set up decryption policies and rules, see [When to Decrypt Traffic, When Not to Decrypt](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- Among the types of traffic you should exclude from decryption is traffic that is by nature undecryptable; typically, undecryptable traffic uses TLS/SSL certificate pinning. The decryption policy wizard assists you by automatically creating **Do Not Decrypt** rules for traffic determined to be undecryptable according to distinguished name or category. For more information, see [Create a Decryption Policy with Outbound Connection Protection](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Following are the decryption rules we'll discuss in this chapter.

Decryption Policy Example

Enter Description

Rules Trusted CA Certificates Undecryptable Actions Advanced Settings

+ Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND - internal source netw	any	any	Internal	any	any	any	any	any	any	any	any	Do not decrypt
2	Decrypt test site	any	any	any	any	any	any	any	any	any	Astrology (Any re	any	Decrypt - Resign
3	Auto-Rule-Undecrypta	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
4	Auto-Rule-URL-Categories	any	any	any	any	any	any	any	any	any	Finance (Any rep Health and Medic Online Trading (A	any	Do not decrypt
5	Auto-Rule-Undecryptable-	any	any	any	any	any	any	Tags: undecrypte	any	any	any	any	Do not decrypt
6	Block bad cert status	any	any	any	any	any	any	any	any	any	any	1 Cert Status sele	Block
7	Block SSL 3.0, TLS 1.0	any	any	any	any	any	any	any	any	any	any	2 Protocol Version	Block
8	Auto-Rule-IntCA	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action												Do not decrypt	

In the preceding example, the decryption policy wizard creates all rules whose name starts with **Auto-Rule** (that is, rules 3, 4, 5, and 8). You must create the other decryption rules shown in this example and order them manually.

We recommend you add the rules in this order to allow the most intensive operation (decryption) to occur last and also to take advantage of TLS certificate caching, which is defined in [RFC 7924](#).

The managed device that evaluates the traffic uses TLS server certificate caching wherever possible to dramatically improve subsequent certificate matching connections and can *dramatically* improve throughput and performance.

- Rule 1 matches traffic on source network so no TLS certificate is required.
- Rules 2 through 5 match on the TLS certificate, but if there is no certificate in the cache when the managed device sees the ClientHello, the system attempts to fall back to the server name indication (SNI). If the TLS probe connection is successful, the device should have the certificate in the cache for the next connection.
- Rule 6 requires a TLS certificate. If no certificate is in the cache and the TLS probe was successful, the certificate is cached for the next connection.
- Rule 7 is matched on negotiated protocol version, so no TLS certificate is required. The negotiated protocol version waits until we receive the ServerHello.

The preceding recommended rule order also has the advantage of starting with a rule that doesn't need a TLS certificate at all and is followed by rules (2 through 6) that can cache the TLS certificate with the ClientHello. Rules (like rule 7) that require ServerHello should be later in the policy because those take longer to evaluate.

The adaptive TLS server identity probe is a recommended advanced decryption policy option that is discussed in more detail in [Decryption Policy Advanced Options](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

The following topics provide more information.

Use the Decryption Policy Wizard

If you intend to decrypt any outbound or inbound traffic, we strongly recommend you use the decryption policy wizard. Among other reasons, the wizard creates a set of decryption rules ordered the recommended way, not just an empty policy with no rules.

If you choose to protect outbound traffic, the policy contains one **Decrypt - Resign** rules and three **Do Not Decrypt** rules for undecryptable traffic.

If you choose to protect inbound traffic, the policy contains one **Decrypt - Known Key** rules and three **Do Not Decrypt** rules but these rules are all disabled initially. We disable the **Do Not Decrypt** rules because we assume all traffic to inbound servers is trusted but we provide the flexibility for you to enable those rules later if you wish.

The following figure shows an example of a decryption rule to protect outbound traffic.

The screenshot shows the 'Decryption Policy Example' configuration page. It includes a search bar, navigation tabs for 'Rules', 'Trusted CA Certificates', 'Undecryptable Actions', and 'Advanced Settings', and buttons for '+ Add Category' and '+ Add Rule'. The main area displays a table of rules with columns for #, Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applications, Source Ports, Dest Ports, Categories, SSL, and Action.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	Auto-Rule-Undecryptable-DNs	any	any	any	any	any	any	any	any	any	any	1 DN selection	Do not decrypt
2	Auto-Rule-URL-Categories	any	any	any	any	any	any	any	any	any	Finance (Any re Health and Me Online Trading	any	Do not decrypt
3	Auto-Rule-Undecryptable-Apps	any	any	any	any	any	any	Tags: undecryp	any	any	any	any	Do not decrypt
4	Auto-Rule-IntCA	any	any	any	any	any	any	any	any	any	any	any	Decrypt - Resign
Root Rules													
This category is empty													
Default Action													
													Do not decrypt

The wizard created the following rules:

1. **Auto-Rule Undecryptable-DNs**, a **Do Not Decrypt** rule for distinguished names that are known to be undecryptable, most likely because they use TLS/SSL pinning.
2. **Auto-Rule-URL-Categories**, a **Do Not Decrypt** rule for URL categories that we categorize based on their content (such as medical or financial sites).
3. **Auto-Rule-Undecryptable-Apps**, a **Do Not Decrypt** rule for applications that are known to be undecryptable, most likely because they use TLS/SSL certificate pinning.
4. **Auto-Rule-IntCA**, a **Decrypt - Resign** rule that uses an internal certificate authority object named **IntCA** to decrypt the remainder of the traffic and then re-sign the traffic with IntCA before evaluation by the associated access control policy.

Rules 1 through 3 are created by the following choices on the second page of the decryption policy wizard.

Create Decryption Policy ?

1 Policy Details

Enter name, description, choose policy type and certificates.

2 Decryption Exclusions

(Optional) Configure exclusions for outbound connections.

Bypass decryption for sensitive URL categories

In many environments, certain categories of websites are not inspected for regulatory, compliance or privacy reasons. Customize the list below to bypass inspection for designated categories.

Note: **URL License is Required**

URL Categories: Finance Online Trading Health and Medicine + Add

Bypass decryption for undecryptable distinguished names

Bypass decryption based on Cisco's list of known undecryptable distinguished names.

Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported distinguished names.**

[56 Distinguished names included](#) ▼

Bypass decryption for undecryptable applications

Certain enterprise applications are not supported for decryption due to a variety of reasons (Certificate Pinning, Client Certificate Authentication, etc.). Bypass decryption based on Cisco's list of known undecryptable applications.

Note: **This option is selected by default to allow traffic which cannot be decrypted to remain encrypted. Disabling this option might cause decryption to fail for unsupported applications.**

[55 Applications included](#) ▼

Cancel Back Create Policy

After the wizard is finished, you can:

- Add rules (for example, block rules shown in this example)
- Edit rules to modify any of these parameters.
- Delete rules you don't need.
- Disable rules you don't need.
- Add categories.
- Move rules to reorder them.

If you choose to reorder rules, make sure to review:

- [Decryption Rules to Put First, on page 6](#)
- [Decryption Rules to Put Before the Decrypt - Resign Rule, on page 7](#)

Do Not Decrypt Best Practices

Log traffic during evaluation period

Do Not Decrypt rules generally should disable logging but if you're not sure what traffic matches your rules, you can temporarily enable logging. After you confirm the correct traffic is being matched, disable logging for those rules.

Guidelines for undecryptable traffic

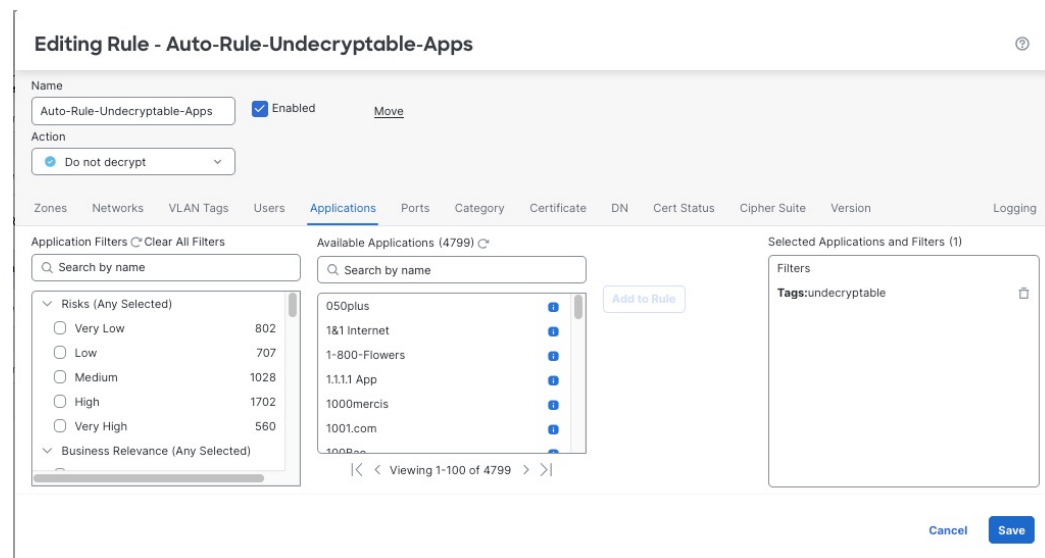
We can determine that certain traffic is not decryptable either because the website itself is not decryptable or because the website uses TLS/SSL pinning, which effectively prevents users from accessing a decrypted site without errors in their browser.

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.



Related Topics

[Bypass Inspection with Prefilter and Flow Offload](#), on page 9

[Do Not Decrypt Best Practices](#), on page 5

[Decrypt - Resign and Decrypt - Known Key Best Practices](#), on page 6

[Decryption Rules to Put First](#), on page 6

[Last Manual Decryption Rules: Block or Monitor Certificates and Protocol Versions](#)

[Use the Decryption Policy Wizard](#), on page 3

Decrypt - Resign and Decrypt - Known Key Best Practices

This topic discusses best practices for **Decrypt - Resign** and **Decrypt - Known Key** decryption rule.

Use the decryption policy wizard

The decryption policy wizard creates a decryption policy for protecting either inbound or outbound traffic. We strongly recommend you use the wizard to create the policy because we automatically create **Do Not Decrypt** rules and put them in the recommended order in the policy. For more information, see [Use the Decryption Policy Wizard, on page 3](#).

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** 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 best practices with certificate 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.

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.

For more information about certificate pinning, see [About TLS/SSL Pinning](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Decrypt - Known Key best practices

Because a **Decrypt - Known Key** rule action is intended to be used for traffic going to an internal server, you should always add either a destination network to the TBD rule rules (**Networks** rule condition) or add a security zone to the access control rule (**Zones** tab page). That way the traffic goes directly to the network or interface on which the server is located, thereby reducing traffic on the network.

Decryption Rules to Put First

Put first any rules that can be matched by the first part of the packet; an example is a rule that references IP addresses (**Networks** rule condition).

Decryption Rules to Put Before the Decrypt - Resign Rule

Rules with the following rule conditions should be ordered immediately before the **Decrypt - Resign** rule because those rules require traffic to be examined for the longest amount of time by the system:

- Applications
- Category
- Certificate
- Distinguished Name (DN)
- Cert Status
- Cipher Suite
- Version

Logging Best Practices and Recommendations

This topic discusses our best practices and recommendations for logging in decryption policies.

Always log rules with decryption actions

Always enable logging for any decryption rule that performs a decryption action (that is, a rule action of **Decrypt - Resign** or **Decrypt - Known Key**).

Do not log rules for undecryptable applications

Undecryptable applications can generate a lot of noise so you can disable logging in rule actions where the **Applications** tab page filter setting includes the **undecryptable** tag. For example, Apple mobile devices typically contact the Apple site repeatedly. This traffic typically uses TLS/SSL certificate pinning and therefore isn't decryptable.

Decryption policy logging settings override access control policy logging settings

Even if your access control policy is not set to log anything, enabling logging for decryption policies or rules enables a decryption associated with the access control policy to log.

Decryption policy logs are appended to access control policy logs

If both your access control policy and decryption policies and rules enable logging, the log messages are appended to the same log.

Enable logging for Do Not Decrypt rules to test, then disable logging

To save resources, there's normally no reason to enable logging for **Do Not Decrypt** rules; however, you can choose to enable logging temporarily as you fine-tune decryption rule rule conditions. For example, you can test how a **Do Not Decrypt** rule works in a particular security zone then either change the rule or disable logging if you're happy with the results.

Use Security Zones in Access Control Rules

You must associate a decryption policy with an access control policy for the decryption policy to have any effect; when you do that, set up your access control rule to use security zones to segment traffic to certain interfaces. For example, if your decryption policy has rules protecting outbound traffic, create a security zone of interfaces to the outside and add that to the access control rule.

For more information about security zones, see [Security Zones and Interface Groups](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 1: Create a security zone

Create a security zone that contains at least one device that is on an inside or outside routed interface. In the following example, the security zone is for an outside interface.

Create a security zone:

1. Click **Objects > Object Management**
2. Click **Interface**.
3. Click **Add > Security Zone**.
4. Enter the required information.

The following figure shows an example of a security zone named **Outside** with one managed device.

The screenshot displays the 'Security Zones' configuration window. It includes the following fields and controls:

- Name:** A text input field containing 'Outside'.
- Interface Type:** A dropdown menu set to 'Routed'.
- Available Interfaces:** A dropdown menu set to 'ftd76-83'.
- Selected Interfaces:** An empty rectangular box.
- Add:** A blue button located between the 'Available Interfaces' and 'Selected Interfaces' boxes.
- Cancel:** A light blue button at the bottom right.
- Save:** A blue button at the bottom right.

Step 2: Associate a decryption policy with an access control policy

Associate a decryption policy with an access control policy; otherwise, the decryption policy will have no effect.

For more information, see [Associate the Decryption Policy with an Access Control Policy and Advanced Settings](#).

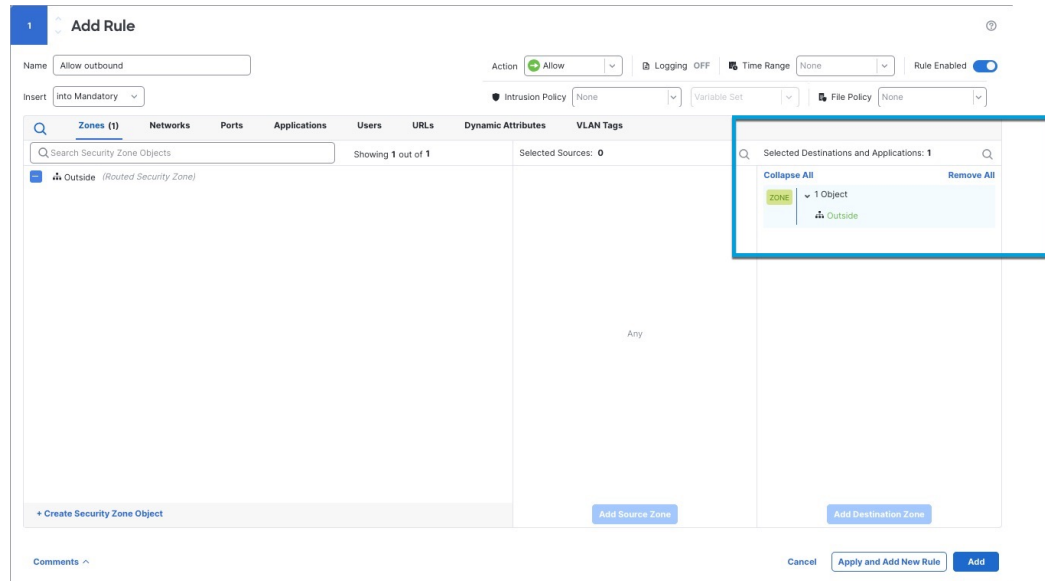
Step 3: Create an access control Allow rule that includes the security zone

In your access control policy, create a rule with an Allow action that is matched by traffic going to your security zone.

1. Click **Policies > Access Control**.
2. Click **Edit** (✎) next to the access control policy to edit.
3. Click **Add Rule** and optionally give the rule a name.
4. From the **Action** list, click **Allow**.

5. Click the **Zones** tab.
6. On the Zones tab page, select the check box next to your outside security zone and click **Add to Destination Zone**.

The following figure shows an example.



7. Set up the access control rule as desired.
8. Follow the prompts on your screen to complete the change to the access control policy.
9. Deploy configuration changes as discussed in [Deploy Configuration Changes](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Bypass Inspection with Prefilter and Flow Offload

Prefiltering is the first phase of access control, before the system performs more resource-intensive evaluation. Prefiltering is simple, fast, and early. Prefiltering uses limited outer-header criteria to quickly handle traffic. Compare this to subsequent evaluation, which uses inner headers and has more robust inspection capabilities.

Configure prefiltering to:

- Improve performance— The sooner you exclude traffic that does not require inspection, the better. You can fastpath or block certain types of plaintext, passthrough tunnels based on their outer encapsulation headers, without inspecting their encapsulated connections. You can also fastpath or block any other connections that benefit from early handling.
- Tailor deep inspection to encapsulated traffic—You can rezone certain types of tunnels so that you can later handle their encapsulated connections using the same inspection criteria. Rezoning is necessary because after prefiltering, access control uses inner headers.

If you have a Firepower 4100/9300 or Secure Firewall 3100 available, you can use *large flow offload*, a technique where trusted traffic can bypass the inspection engine for better performance. You can use it, for example, in a data center to transfer server backups.

