Deploy Decryption Rules With Examples 7.6

First Published: 2024-09-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 1

Decryption Rules Best Practices

Decryption Rules Best Practices

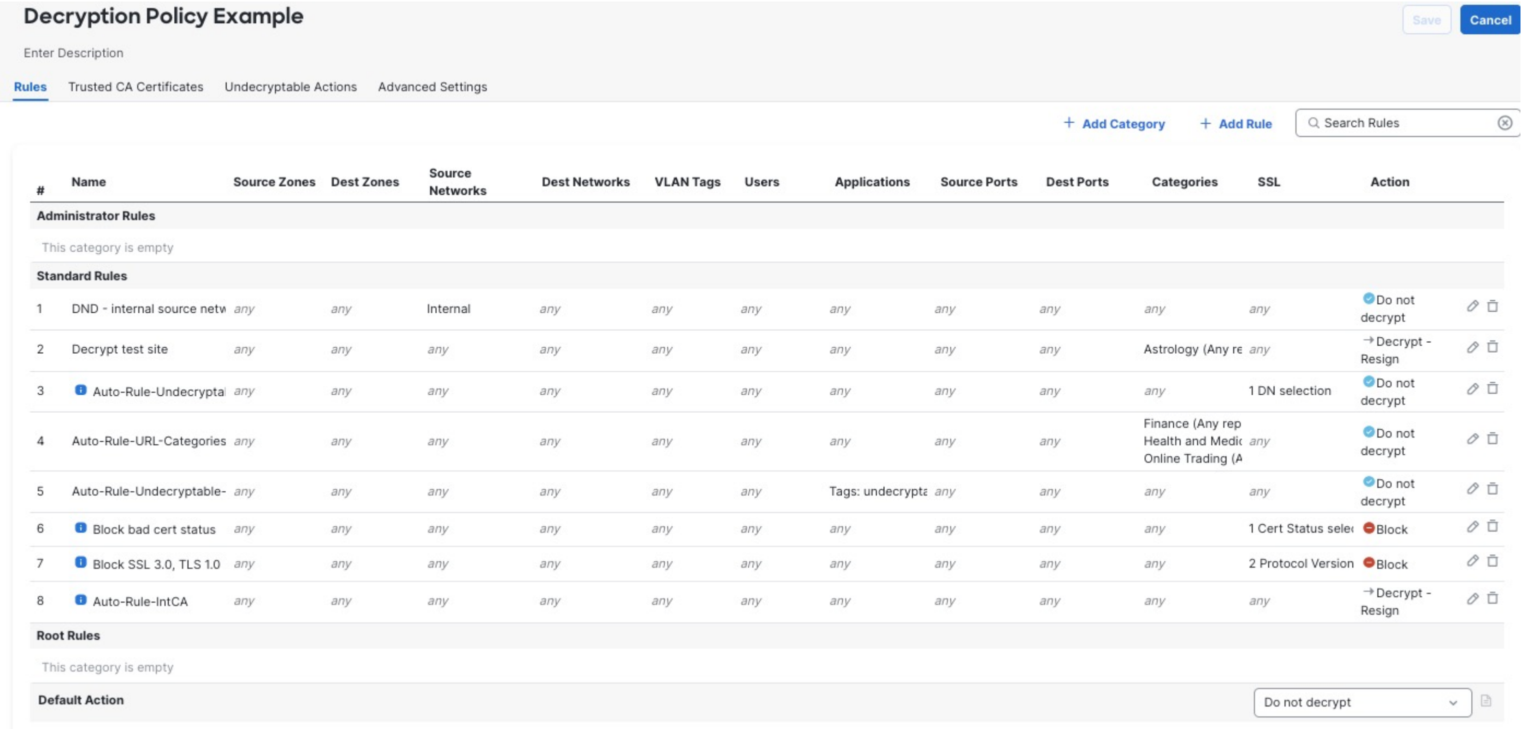
This chapter provides an example decryption policy with decryption rules that illustrates our best practices and recommendations. First we'll discuss settings for the decryption policies and access control policies and then walk through all the rules and why we recommend they be ordered in a particular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

#	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-Undecryptal	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: undecrypta	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 selec	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.

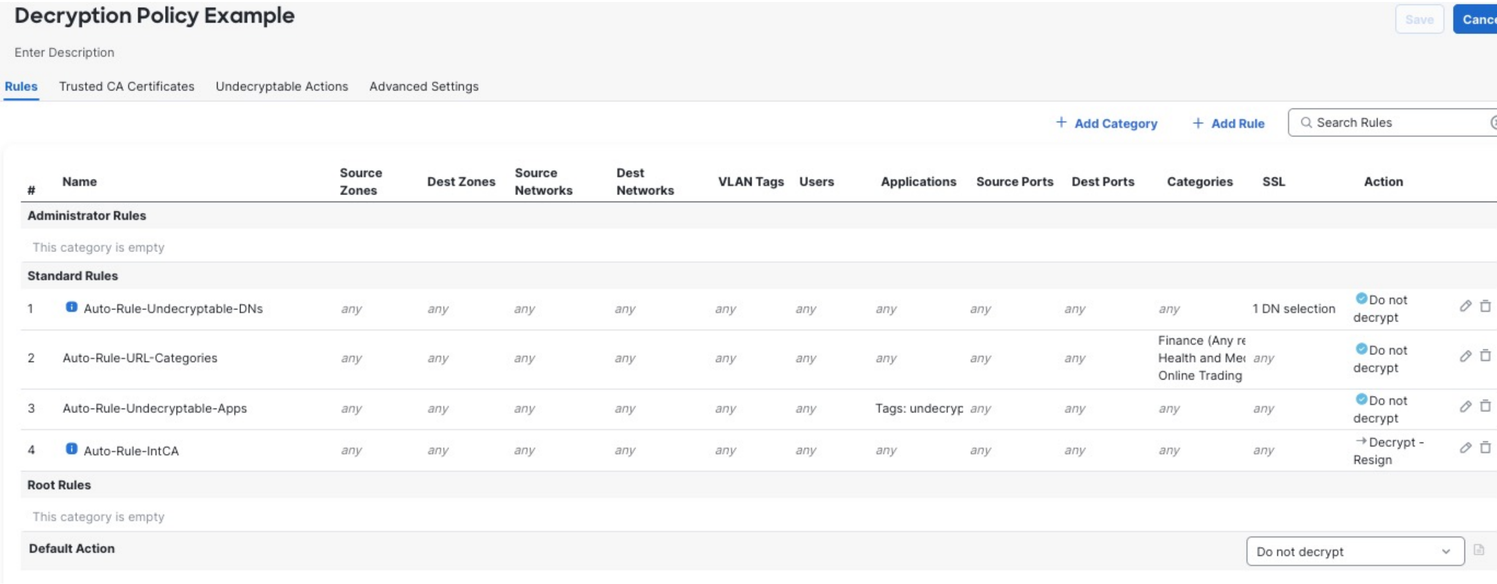
Use the Decryption Policy Wizard

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.



Decryption Policy Example

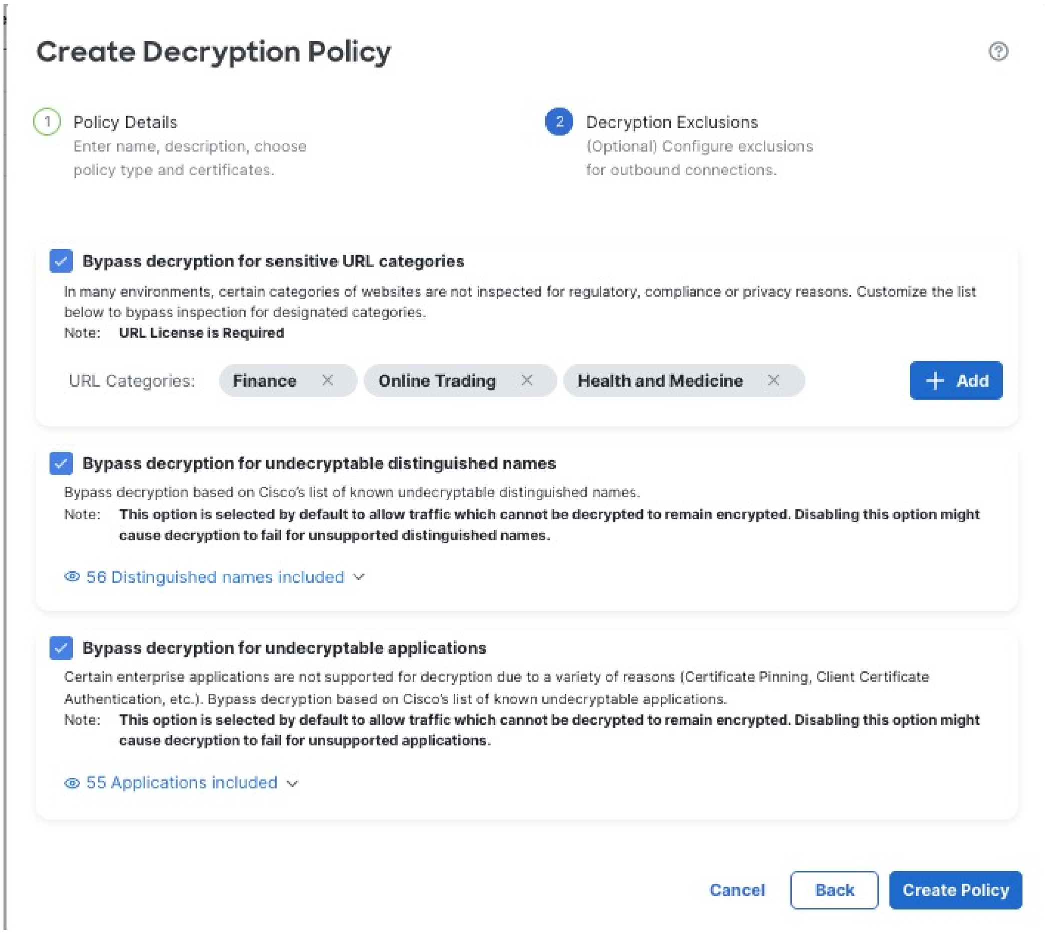
Enter Description

#	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

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

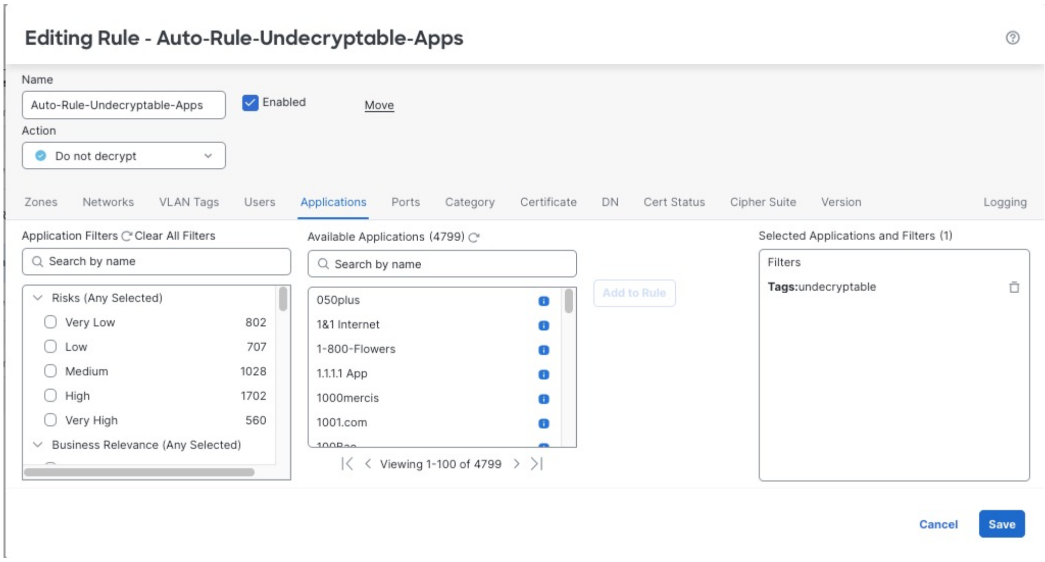
We can determine that certain traffic is not decryptable either because the website itself is not decryptable or because the website uses TLS/SSL pinning, which effectively prevents users from accessing a decrypted site without errors in their browser.

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.



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	707
○ Medium	1028
○ High	1702
○ Very High	560

Business Relevance (Any Selected)

Available Applications (4799)

050plus
1&1 Internet
1-800-Flowers
1.1.1.1 App
1000mercis
1001.com

Viewing 1-100 of 4799

Selected Applications and Filters (1)

Filters

Tags:undecryptable

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, on page 21

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/SSLcertificate 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* .

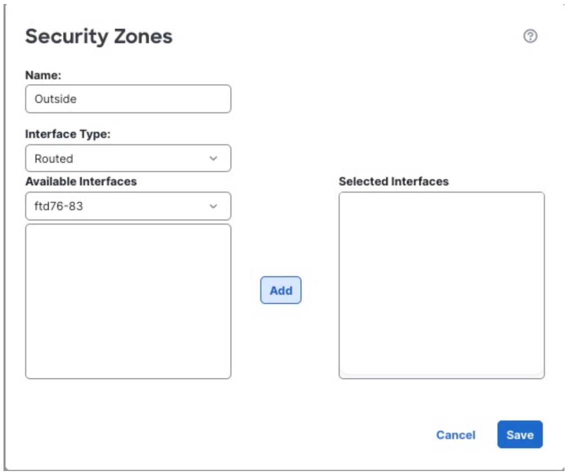
Step 1: Create a security zone

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.



Security Zones

Name: Outside

Interface Type: Routed

Available Interfaces: ftd76-83

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, on page 26.

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

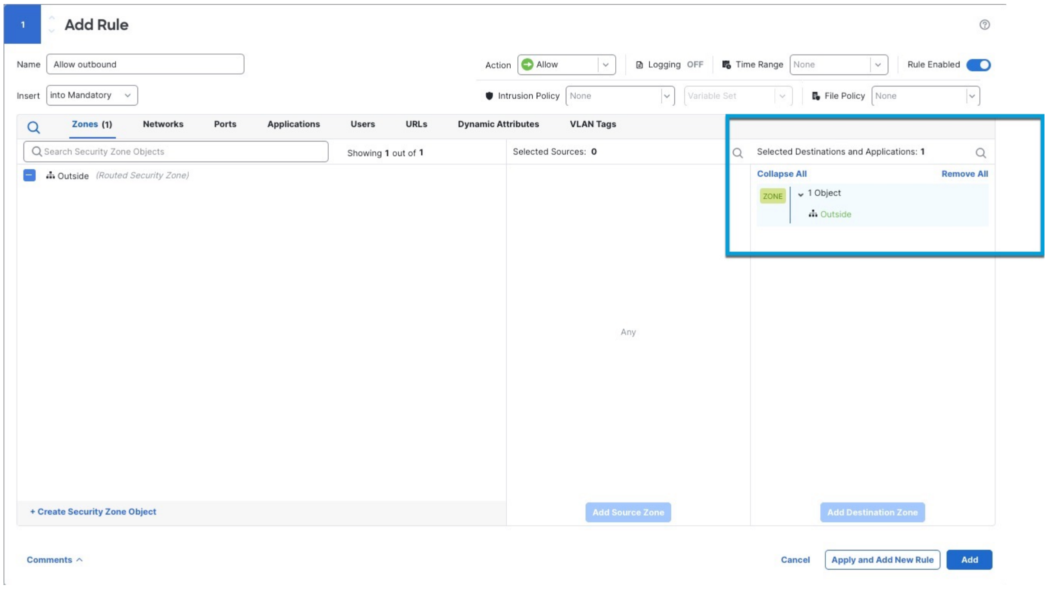
In your access control policy, create a rule with an Allow action that is matched by traffic going to your security zone.

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.



Add Rule

Name: Allow outbound

Insert: into Mandatory

Action: Allow

Logging: OFF

Time Range: None

Rule Enabled

Intrusion Policy: None

Variable Set

File Policy: None

Showing 1 out of 1

Outside (Routed Security Zone)

Selected Sources: 0

Any

Selected Destinations and Applications: 1

ZONE — 1 Object — Outside

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.

CHAPTER 2

Recommended Policy and Rule Settings

Recommended Policy and Rule Settings

We recommend the following policy settings:

- Decryption policy:
  - Default action **Do Not Decrypt**.
  - Enable logging.
  - Set **Undecryptable Actions** to **Block** for both **SSL v2 Session** and **Compressed Session**.
  - Enable TLS 1.3 decryption and adaptive TLS server identity probe in the policy's advanced settings.
- Decryption rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)
- Access control policy:
  - Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
  - Set the default policy action to **Intrusion Prevention: Balanced Security and Connectivity**.
  - Enable logging.

Related Topics

Decryption Policy Settings, on page 12

Decryption Rule Settings, on page 28

Access Control Policy Settings, on page 14

Decryption Policy Settings

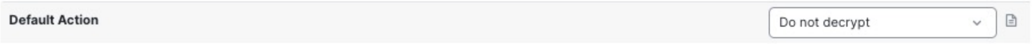
How to configure recommended the following best practice settings for your decryption policy:

- Default action **Do Not Decrypt**.
- Enable logging.
- Set **Undecryptable Actions** to **Block** for both **SSL v2 Session** and **Compressed Session**.
- Enable TLS 1.3 decryption and adaptive TLS server identity probe in the policy's advanced settings.

Step 1 Click **Policies** > **Access Control** > **Decryption**.

Step 2 Click **Edit** (✎) next to your decryption policy.

Step 3 From the **Default Action** list at the bottom of the page, click **Do Not Decrypt**.
The following figure shows an example.

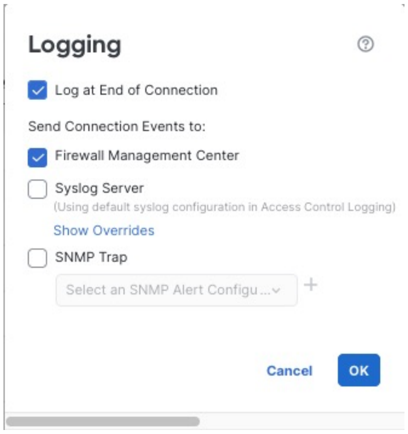


Default Action   Do not decrypt

Step 4 At the end of the row, click **Logging** (🗎).

Step 5 Select the **Log at End of Connection** check box.

The following figure shows an example.



Logging

☑ Log at End of Connection

Send Connection Events to:

☑ Firewall Management Center

☐ Syslog Server
(Using default syslog configuration in Access Control Logging)
Show Overrides

☐ SNMP Trap
Select an SNMP Alert Configu...

Step 6 Click **OK**.

Step 7 Click **Save**.

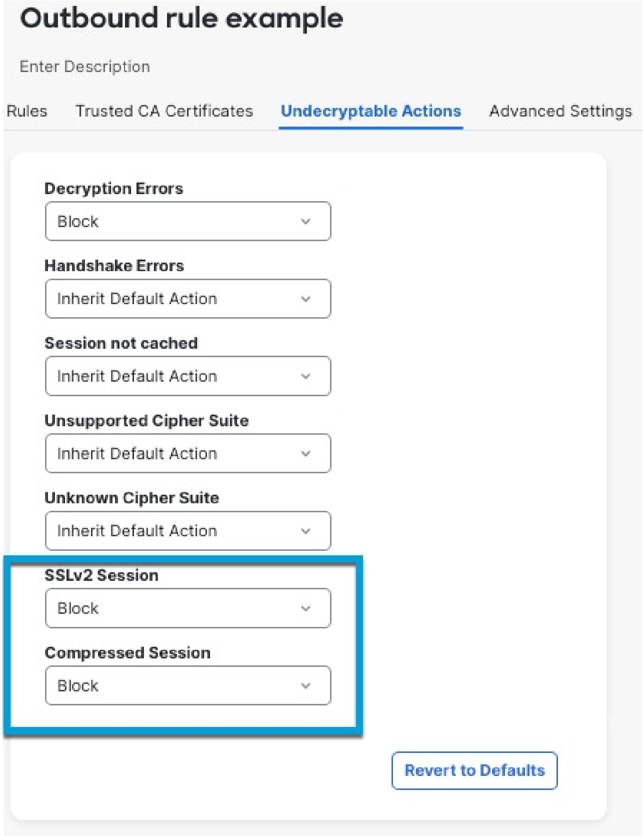
Step 8 Click the **Undecryptable Actions** tab.

Step 9 We recommend setting the action for **SSLv2 Session** and **Compressed Session** to **Block**.

You shouldn't allow SSL v2 on your network and compressed TLS/SSL traffic is not supported so you should block that traffic as well.

See Default Handling Options for Undecryptable Traffic in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information about setting each option.

The following figure shows an example.



Outbound rule example

Enter Description

Decryption Errors: Block

Handshake Errors: Inherit Default Action

Session not cached: Inherit Default Action

Unsupported Cipher Suite: Inherit Default Action

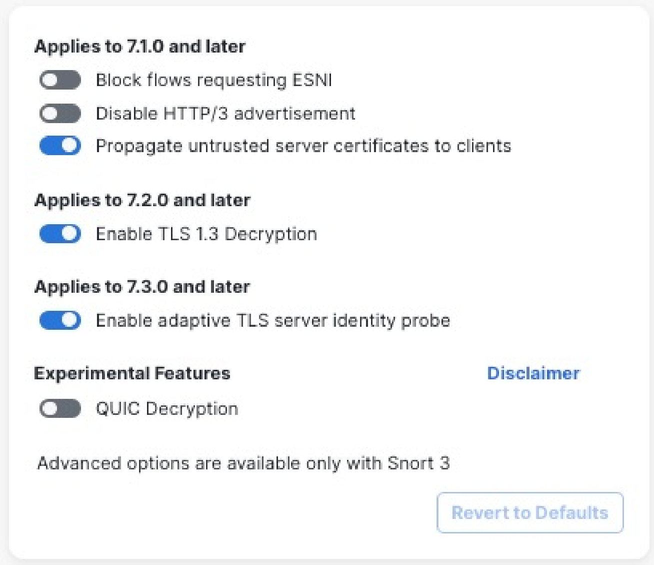
Unknown Cipher Suite: Inherit Default Action

SSLv2 Session: Block

Compressed Session: Block

Step 10 Click the **Advanced Settings** tab page.

Step 11 Select the **Enable TLS 1.3 Decryption** check box.



Applies to 7.1.0 and later

- ○ Block flows requesting ESNI
- ○ Disable HTTP/3 advertisement
- ● Propagate untrusted server certificates to clients

Applies to 7.2.0 and later

- ● Enable TLS 1.3 Decryption

Applies to 7.3.0 and later

- ● Enable adaptive TLS server identity probe

Experimental Features

- ○ QUIC Decryption

Advanced options are available only with Snort 3

Step 12 For more information about QUIC decryption, see Decryption Policy Advanced Options in the *Cisco Secure Firewall Management Center Device Configuration Guide* .

Step 13 At the top of the page, click **Save**.

What to do next

Configure decryption rules and set each one as discussed in Decryption Rule Settings, on page 28.

Access Control Policy Settings

How to configure recommended the following best practice settings for your access control policy:

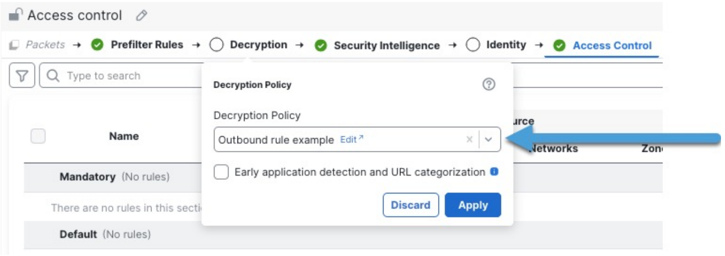
- Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
- Set the default policy action to **Intrusion Prevention: Balanced Security and Connectivity**.
- Enable logging.

Step 1 Click **Policies** > **Access Control**.

Step 2 Click **Edit** (✎) next to your access control policy.

Step 3 (If your decryption policy is not set up yet, you can do this later.)

a) Click the **Decryption** link at the top of the page as the following figure shows.



Decryption Policy: Outbound rule example

☐ Early application detection and URL categorization

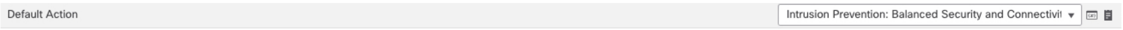
Access control
Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control
Type to search
Name
Mandatory (No rules)
There are no rules in this secti
Default (No rules)
Decryption Policy
Edit
urce
Networks
Zon
Discard
Apply

b) From the list, click the name of your decryption policy.

c) Click **Apply**.

d) At the top of the page, click **Save**.

Step 4 From the **Default Action** list at the bottom of the page, click **Intrusion Prevention: Balanced Security and Connectivity**. The following figure shows an example.



Default Action: Intrusion Prevention: Balanced Security and Connectivit

Step 5 Click **Logging** (▤).

Step 6 Select the **Log at End of Connection** check box and click **OK**.

Step 7 Click **Save**.

What to do next

See Decryption Rule Examples, on page 15.

CHAPTER 3

Decryption Rule Examples

Decryption Rule Examples

This chapter provides an example of decryption rule that illustrate our best practices.

Run the Decryption Policy Wizard

This task discusses how to run the decryption policy wizard for outbound traffic protection. This policy has four rules:

1. **Do Not Decrypt** rule for distinguished names that are known to be undecryptable, most likely because they use TLS/SSL pinning.

2. **Do Not Decrypt** rule for URL categories that we classify as sensitive based on their content (for example, medical and financial).

3. **Do Not Decrypt** rule for applications that are known to be undecryptable, most likely because they use TLS/SSL pinning.

4. **Decrypt - Resign** rule that uses a certificate authority object named **IntCA** to decrypt the remainder of the traffic.

You can then edit the rules if you want and also manually add:

- **Decrypt - Resign** rules for traffic to monitor and determine whether the traffic should be blocked in the future.

- **Do Not Decrypt** rules for other types of traffic

- **Block** or **Block with Reset** rules for bad certificates and unsecure cipher suites.

If you enabled Change Management, you must create and assign a ticket before you can create a decryption policy. Before the decryption policy can be used, the ticket and all associated objects (like certificate authorities) must be approved. For more information, see Creating Change Management Tickets and Policies and Objects that Support Change Management.

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

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

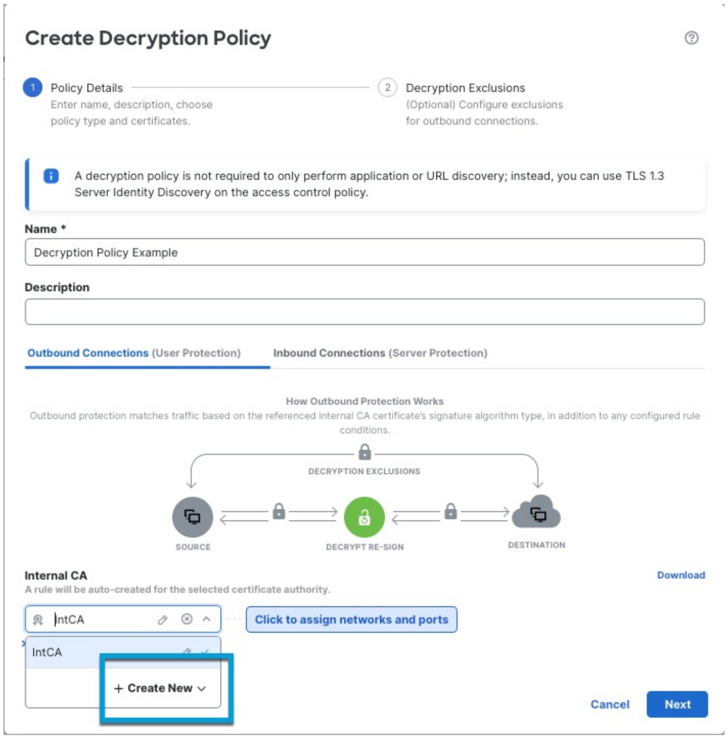
Step 3 Click **Create Decryption Policy**.

Step 4 Give the decryption policy a **Name** and optionally a **Description**.

Step 5 Click the **Outbound Protection** tab.

Step 6 From the **Internal CA** list, click the name of an internal certificate authority object or click **Create New** to upload or generate one.

The following figure shows an example.



Create Decryption Policy

1 Policy Details
Enter name, description, choose policy type and certificates.

2 Decryption Exclusions
(Optional) Configure exclusions for outbound connections.

A decryption policy is not required to only perform application or URL discovery; instead, you can use TLS 1.3 Server Identity Discovery on the access control policy.

Name *: Decryption Policy Example

Description:

How Outbound Protection Works

Outbound protection matches traffic based on the referenced internal CA certificate's signature algorithm type, in addition to any configured rule conditions.

Internal CA
A rule will be auto-created for the selected certificate authority.

Internal CA: IntCA

Outbound Connections (User Protection)
Inbound Connections (Server Protection)
DECRYPTION EXCLUSIONS
SOURCE
DECRYPT RE-SIGN
DESTINATION
Download
Click to assign networks and ports
IntCA
+ Create New
Cancel
Next

For more information about creating or uploading an internal certificate authority object, see:

- Upload an Internal CA for Outbound Protection in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- Generate an Internal CA for Outbound Protection in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 7 (Optional.) To restrict traffic to source and destination networks, click **Click to assign networks and ports**.

Step 8 Click **Next**.

Step 9 Complete the wizard as discussed in Decryption Policy Exclusions, on page 17.

Decryption Policy Exclusions

This task discusses how to exclude from decryption certain types of traffic. We create **Do Not Decrypt** rules in your decryption policy for these although the rules are initially enabled only for an outbound decryption policy (that is, one that uses the **Decrypt - Resign** policy action).

Step 1 Complete the tasks discussed in:

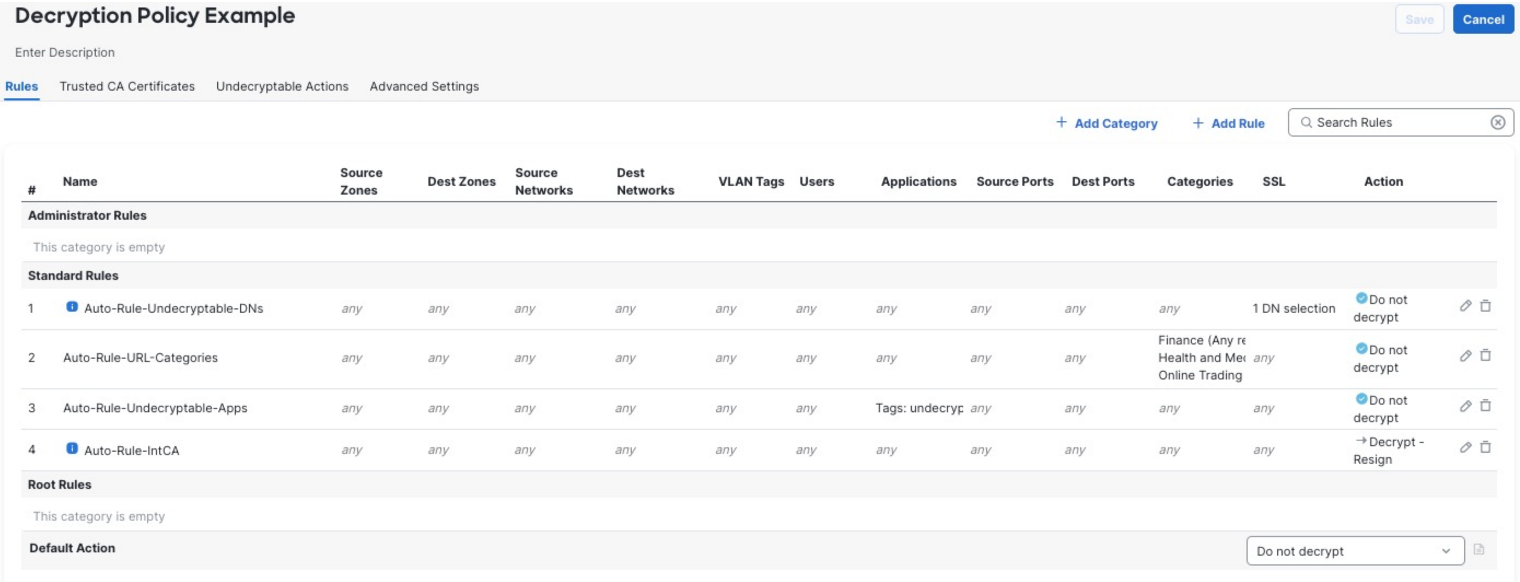
- Run the Decryption Policy Wizard, on page 15

Step 2 The exclusions page provides the following options. All options are *enabled* for an outbound protection policy (**Decrypt - Resign** rule action) and *disabled* for all other decryption policy actions.

Item	Description
Bypass decryption for sensitive URL categories	Check the box to not decrypt traffic from the indicated categories. Depending on the laws in your area, decryption certain traffic, such as finance or health-related, might be prohibited. Consult an authority in your area for more information. Click **Add** to add more categories. Click **Delete** (✕) to remove categories.
Bypass decryption for undecryptable distinguished names	Check the box to not decrypt traffic when re-signing the certificate is likely to cause the connection to fail. Typically, this behavior is associated with *certificate pinning*, which is discussed in Certificate Pinning Guidelines in the *Cisco Secure Firewall Management Center Device Configuration Guide*. The list of undecryptable distinguished names is maintained by Cisco.
Bypass decryption for undecryptable applications	Check the box to not decrypt traffic when re-signing the certificate is likely to cause the connection to fail. Typically, this behavior is associated with *certificate pinning*, which is discussed in Certificate Pinning Guidelines in the *Cisco Secure Firewall Management Center Device Configuration Guide*. Undecryptable applications are updated automatically in the Vulnerability Database (VDB). You can find a list of all applications on the Secure Firewall Application Detectors page; the **undecryptable** tag identifies applications Cisco determines are undecryptable. The list of undecryptable applications is maintained by Cisco.

Step 3 Click **Create Policy**.

The following figure shows an example of the resulting decryption policy.



Decryption Policy Example

Enter Description

#	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

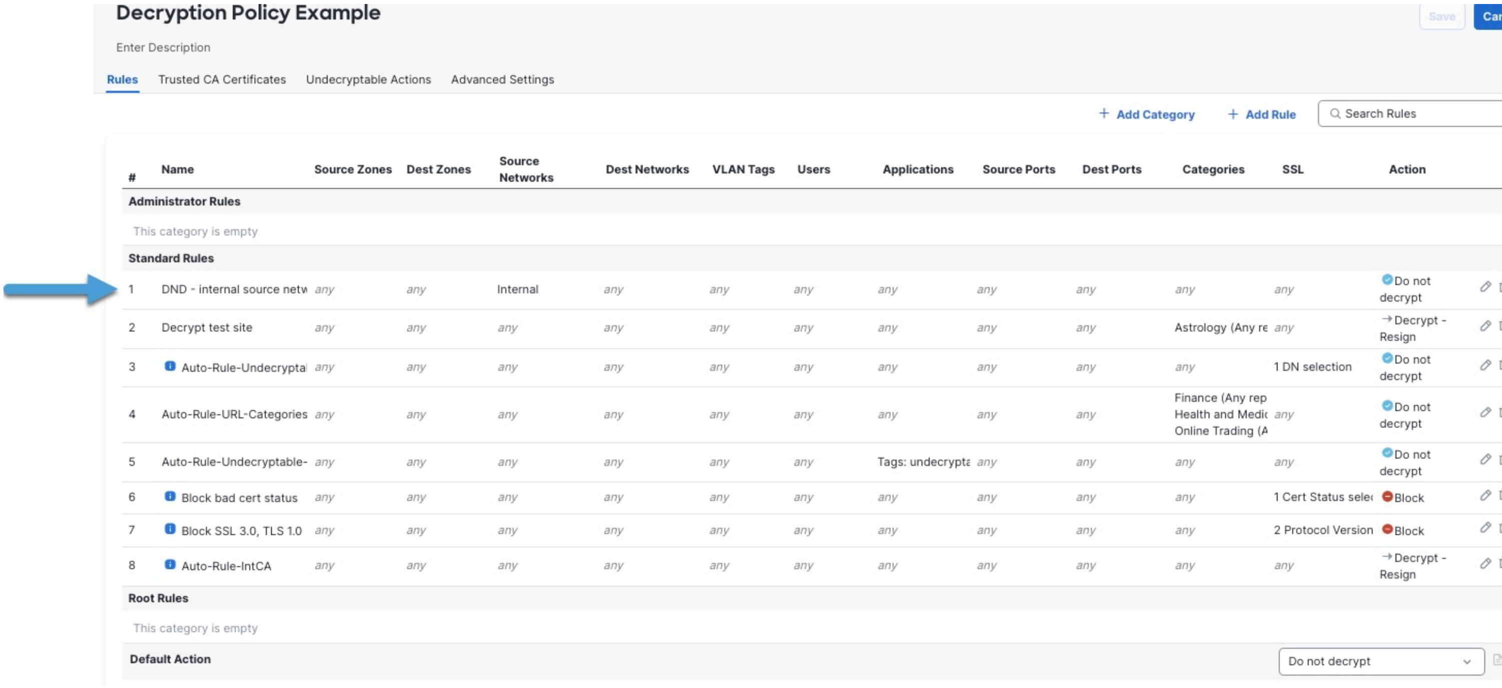
The preceding example shows the **Do Not Decrypt** rules corresponding to your choices for rule exclusions are automatically added before the **Decrypt - Resign** rule. Later in this guide you'll add additional rules manually.

Step 4 Click **Create Policy**.

First Manual Do Not Decrypt Rule: Specific Traffic

The first decryption rule in the example does not decrypt traffic that goes to an internal network (defined as **internal**). **Do Not Decrypt** rule actions are matched during ClientHello so they are processed very fast.

After you run the decryption policy wizard, edit the policy to add the following rule. Drag it to the top of the list of rules so it's evaluated first.



Decryption Policy Example

Enter Description

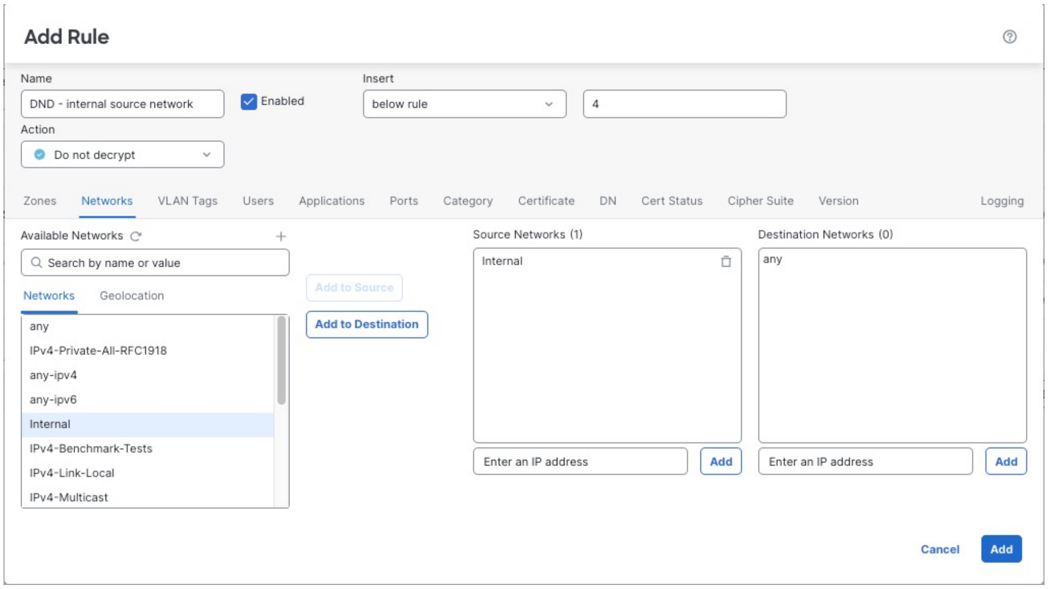
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND - internal source netw	any	any	Internal	any	any	any	any	any	any	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: undecrypta	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

Note

If you have traffic going from internal DNS servers to internal DNS resolvers (such as Cisco Umbrella Virtual Appliances), you can add **Do Not Decrypt** rules for them as well. You can even add those to prefiltering policies if the internal DNS servers do their own logging.

However, we strongly recommend you *do not* use **Do Not Decrypt** rules or prefiltering for DNS traffic that goes to the internet, such as internet root servers (for example, Microsoft internal DNS resolvers built into Active Directory). In those cases, you should fully inspect the traffic or even consider blocking it.

Rule detail:



Add Rule

Name: DND - internal source network ☑ Enabled

Insert: below rule 4

Action: Do not decrypt

Available Networks

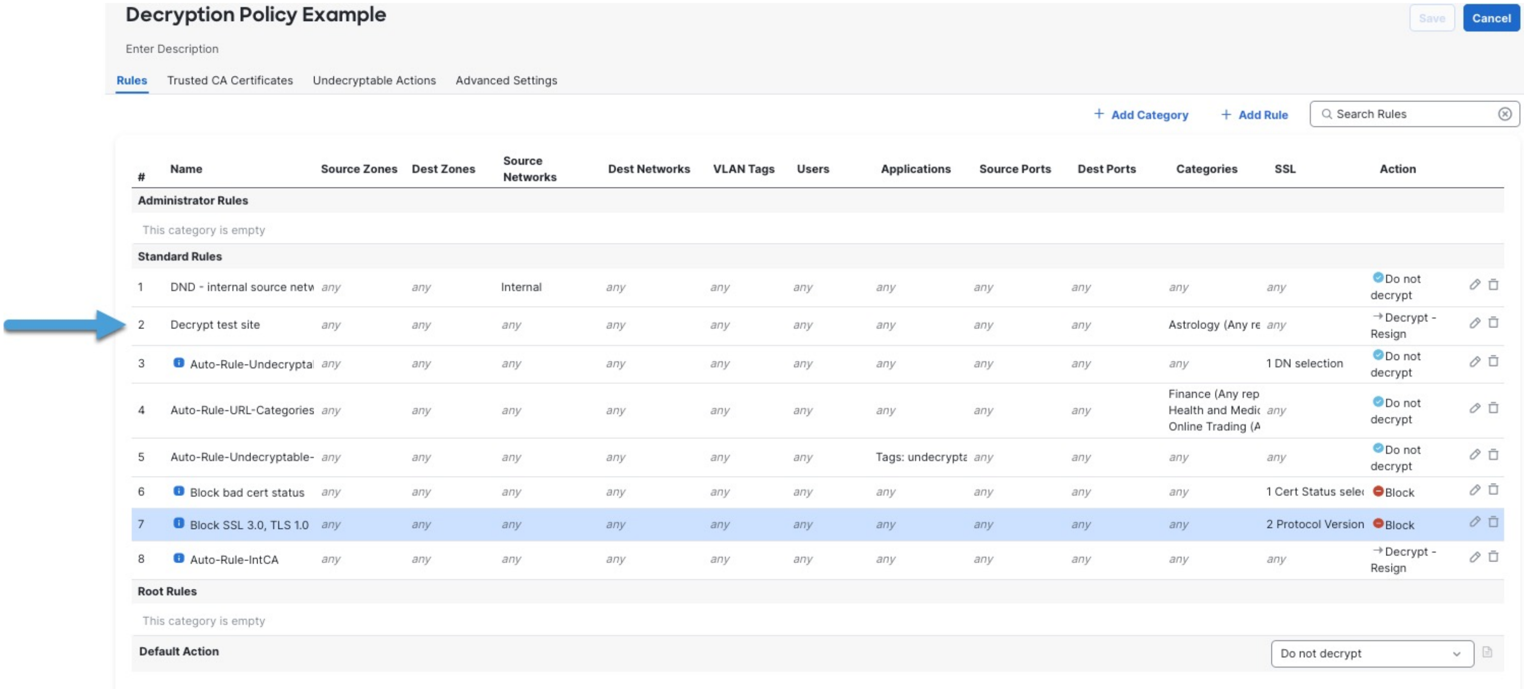
Source Networks (1): Internal

Destination Networks (0): any

Next Manual Rule: Decrypt Specific Test Traffic

The next rule is *optional* in the example; use it to decrypt and monitor limited types of traffic before determining whether or not to allow it on your network.

After you run the decryption policy wizard, edit the policy to add the following rule. Drag it to the second position in the list of rules.



Decryption Policy Example

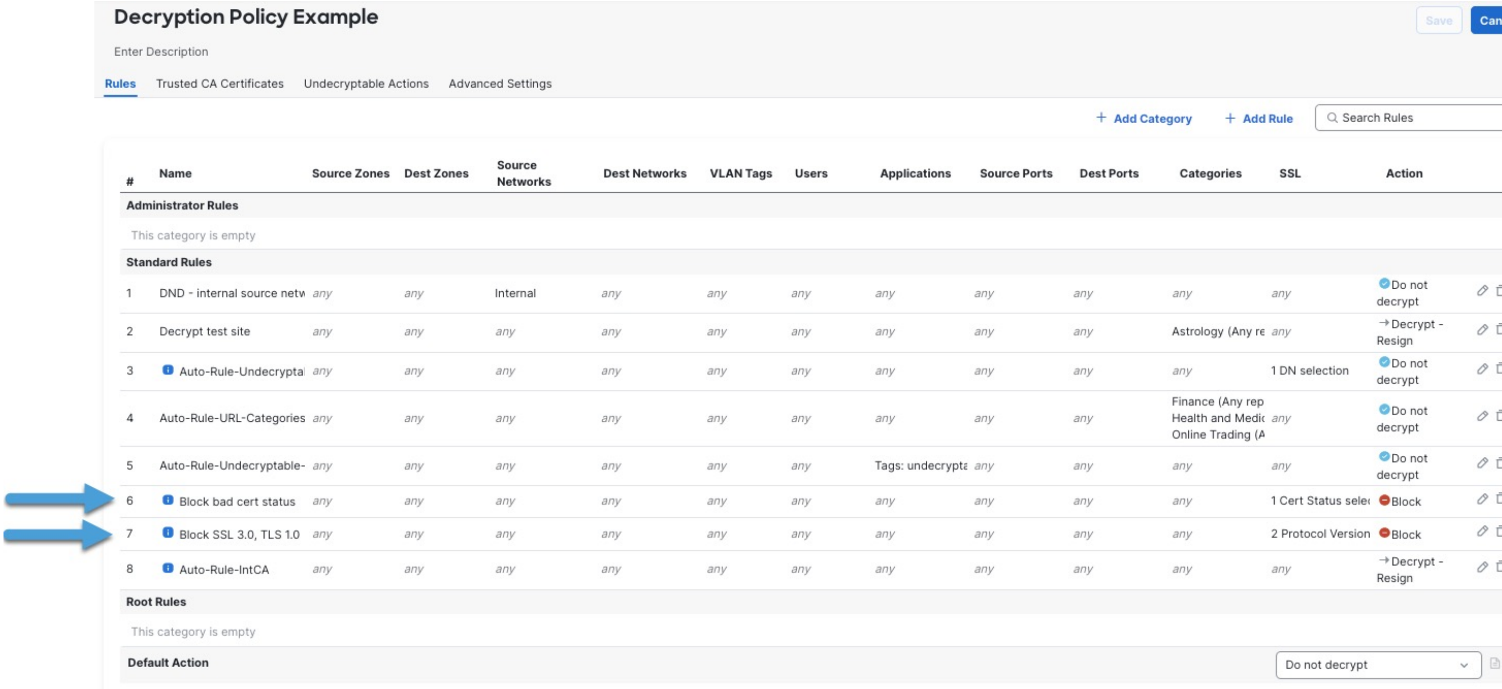
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	Categories	SSL	Action
Administrator Rules													
This category is empty													
Standard Rules													
1	DND - internal source netw	any	any	Internal	any	any	any	any	any	any	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-Undecryptal	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: undecrypta	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 selec	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

Rule detail:

Last Manual Decryption Rules: Block or Monitor Certificates and Protocol Versions

The last decryption rules, because they are the most specific and require the most processing, are rules that either monitor or block bad certificates and unsecure protocol versions.

After you run the decryption policy wizard, edit the policy to add the following rules. Drag them to a position *before* the **Decrypt - Resign** rule.



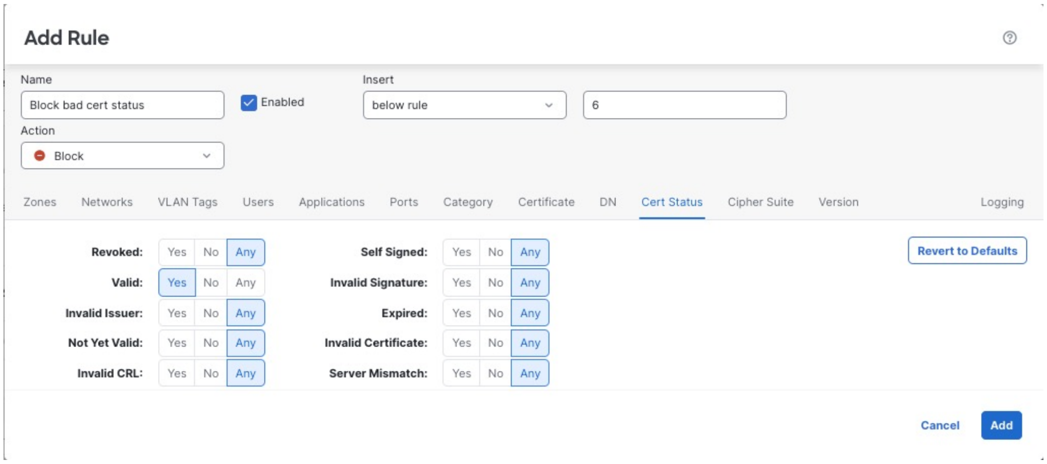
Decryption Policy Example

Enter Description

Rules | Trusted CA Certificates | Undecryptable Actions | Advanced Settings

#	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-Undecryptal	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: undecrypta	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 selec	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

Rule details:



Add Rule

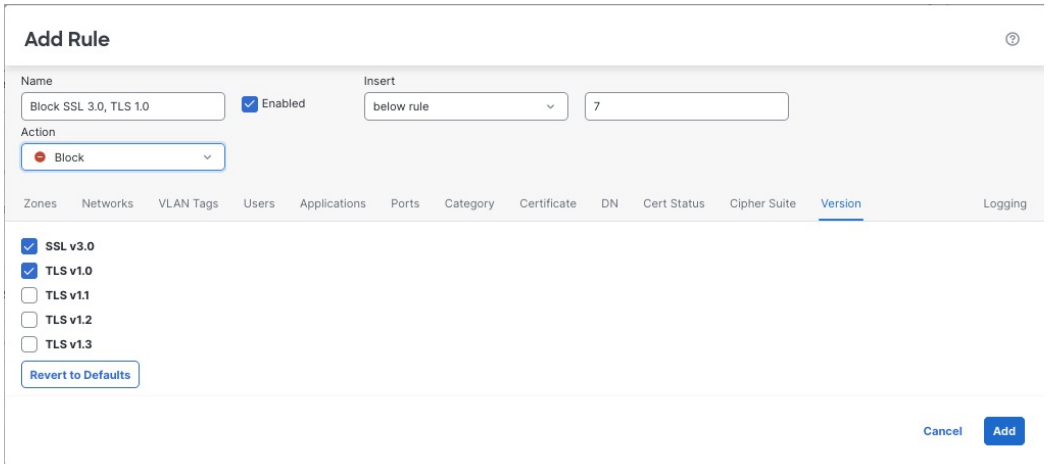
Name: Block bad cert status

☑ Enabled

Insert: below rule | 6

Action: Block

Revoked:	Any
Valid:	Yes
Invalid Issuer:	Any
Not Yet Valid:	Any
Invalid CRL:	Any
Self Signed:	Any
Invalid Signature:	Any
Expired:	Any
Invalid Certificate:	Any
Server Mismatch:	Any



Add Rule

Name: Block SSL 3.0, TLS 1.0 — ☑ Enabled

Insert: below rule — 7

Action: Block

☑ SSL v3.0
☑ TLS v1.0
☐ TLS v1.1
☐ TLS v1.2
☐ TLS v1.3

Example: Decryption Rule to Monitor or Block Certificate Status

The last decryption rules, because they are the most specific and require the most processing, are rules that either monitor or block bad certificates and unsecure protocol versions. The example in this section shows how to monitor or block traffic by certificate status.

Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

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

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

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

Step 4 Click **Edit** (✎) next to a decryption rule.

Step 5 Click **Add Rule**.

Step 6 n the Add Rule dialog box, in the **Name** field, enter a name for the rule.

Step 7 Click **Cert Status**.

Step 8 For each certificate status, you have the following options:

- Click **Yes** to match against the *presence* of that certificate status.
- Click **No** to match against the *absence* of that certificate status.
- Click **Any** to skip the condition when matching the rule. In other words, choosing **Any** means the rule matches whether the certificate status is present or absent.

Step 9 From the **Action** list, click either **Monitor** to only monitor and log traffic that matches the rule or click **Block** or **Block with Reset** to block the traffic and optionally reset the connection.

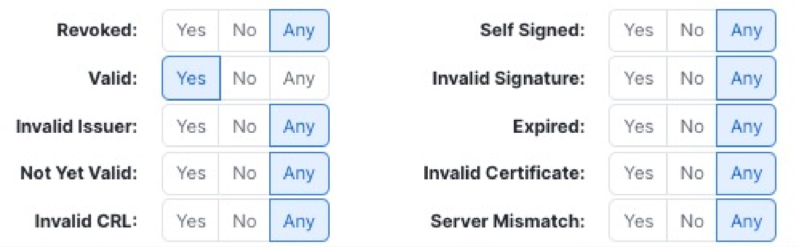
Step 10 To save changes to the rule, at the bottom of the page, click **Add**.

Step 11 To save changes to the policy, at the top of the page, click **Save**.

Example

The organization trusts the Verified Authority certificate authority. The organization does not trust the Spammer Authority certificate authority. The system administrator uploads the Verified Authority certificate and an intermediate CA certificate issued by Verified Authority to the system. Because Verified Authority revoked a certificate it previously issued, the system administrator uploads the CRL that Verified Authority provided.

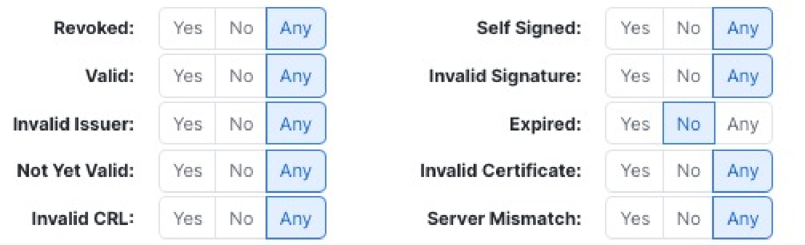
The following figure shows a certificate status rule condition checking for valid certificates, those issued by a Verified Authority, are not on the CRL, and still within the Valid From and Valid To date. Because of the configuration, traffic encrypted with these certificates is not decrypted and inspected with access control.



Revoked: Yes No [✓ Any]
Valid: [✓ Yes] No Any
Invalid Issuer: Yes No [✓ Any]
Not Yet Valid: Yes No [✓ Any]
Invalid CRL: Yes No [✓ Any]

Self Signed: Yes No [✓ Any]
Invalid Signature: Yes No [✓ Any]
Expired: Yes No [✓ Any]
Invalid Certificate: Yes No [✓ Any]
Server Mismatch: Yes No [✓ Any]

The following figure shows a certificate status rule condition checking for the absence of a status. In this case, because of the configuration, it matches against traffic encrypted with a certificate that has not expired.

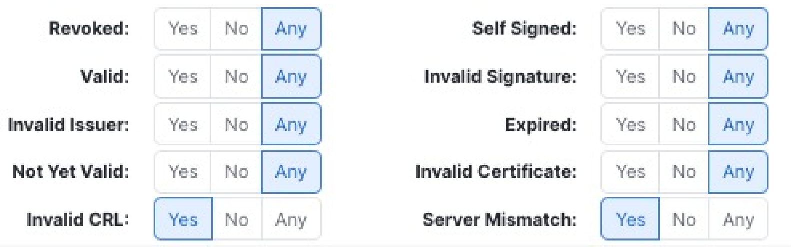


Revoked: Yes No [✓ Any]
Valid: Yes No [✓ Any]
Invalid Issuer: Yes No [✓ Any]
Not Yet Valid: Yes No [✓ Any]
Invalid CRL: Yes No [✓ Any]

Self Signed: Yes No [✓ Any]
Invalid Signature: Yes No [✓ Any]
Expired: Yes [✓ No] Any
Invalid Certificate: Yes No [✓ Any]
Server Mismatch: Yes No [✓ Any]

In the following example, traffic would match this rule condition if the incoming traffic is using a certificate that has an invalid issuer, is self-signed, expired, and it is an invalid certificate.

The following graphic illustrates a certificate status rule condition that matches if the SNI of the request matches the server name or if the CRL is not valid.



Revoked: Yes No [✓ Any]
Valid: Yes No [✓ Any]
Invalid Issuer: Yes No [✓ Any]
Not Yet Valid: Yes No [✓ Any]
Invalid CRL: [✓ Yes] No Any

Self Signed: Yes No [✓ Any]
Invalid Signature: Yes No [✓ Any]
Expired: Yes No [✓ Any]
Invalid Certificate: Yes No [✓ Any]
Server Mismatch: [✓ Yes] No Any

Example: Decryption Rule to Monitor or Block Protocol Versions

This example shows how to block TLS and SSL protocols on your network that are no longer considered secure, such as TLS 1.0, TLS 1.1, and SSLv3. It's included to give you a little more detail about how protocol version rules work.

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

- You can block some protocols using **Version** page on the decryption rule.
- Because the system considers SSLv2 as undecryptable, you can block it using the **Undecryptable Actions** on the decryption policy.
- Similarly, because compressed TLS/SSL is not supported, you should block it as well.

Important Use the **Cipher Suite** and **Version** rule conditions *only* in rules with either the **Block** or **Block with reset** rule actions. The use of these conditions in rules with other rule actions can interfere with the system's ClientHello processing, resulting in unpredictable performance.

Step 1 Click **Policies** > **Access Control** > **Decryption**.

Step 2 Click **Edit** (✎) next to your decryption policy.

Step 3 Click **Edit** (✎) next to a decryption rule.

Step 4 Click **Add Rule**.

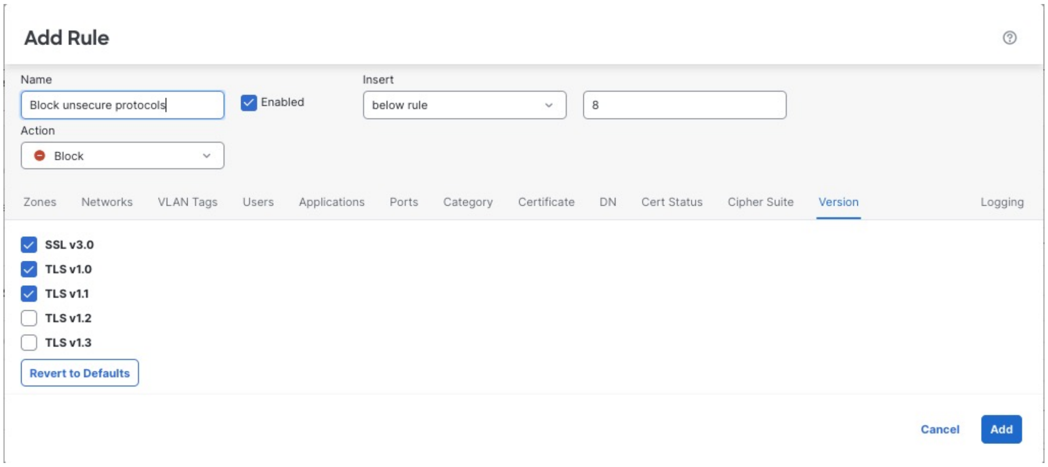
Step 5 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

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

Step 7 Click **Version** page.

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

The following figure shows an example.



Name: Block unsecure protocols
☑ Enabled
Insert: below rule, 8
Action: Block

☑ SSL v3.0
☑ TLS v1.0
☑ TLS v1.1
☐ TLS v1.2
☐ TLS v1.3

Step 9 Choose other rule conditions as needed.

Step 10 Click **Add**.

Optional Example: Manual Decryption Rule to Monitor or Block Certificate Distinguished Name

This rule is included to give you an idea about how to monitor or block traffic based on the server certificate's distinguishedname. It's included to give you a little more detail.

The distinguished name can consist of country code, common name, organization, and organizational unit, but typically consists of a common name only. For example, the common name in the certificate for `https://www.cisco.com` is `cisco.com`. (However, it's not always this simple; Distinguished Name Rule Conditions in the *Cisco Secure Firewall Management Center Device Configuration Guide* shows how to find common names.)

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.

Step 1 Click **Policies** > **Access Control** > **Decryption**.

Step 2 Click **Edit** (✎) next to your decryption policy.

Step 3 Click **Edit** (✎) next to a decryption rule.

Step 4 Click **Add Rule**.

Step 5 In the Add Rule dialog box, in the **Name** field, enter a name for the rule.

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

Step 7 Click **DN**.

Step 8 Find the distinguished names you want to add from the **Available DNs**, as follows:

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

Step 9 To select an object, click it. To select all objects, right-click and then **Select All**.

Step 10 Click **Add to Subject** or **Add to Issuer**.

Tip You can also drag and drop selected objects.

Step 11 Add any literal common names or distinguished names that you want to specify manually. Click the **Enter DN or CN** prompt below the **Subject DNs** or **Issuer DNs** list; then type a common name or distinguished name and click **Add**.

Although you can add a CN or DN to either list, it's more common to add them to the **Subject DNs** list.

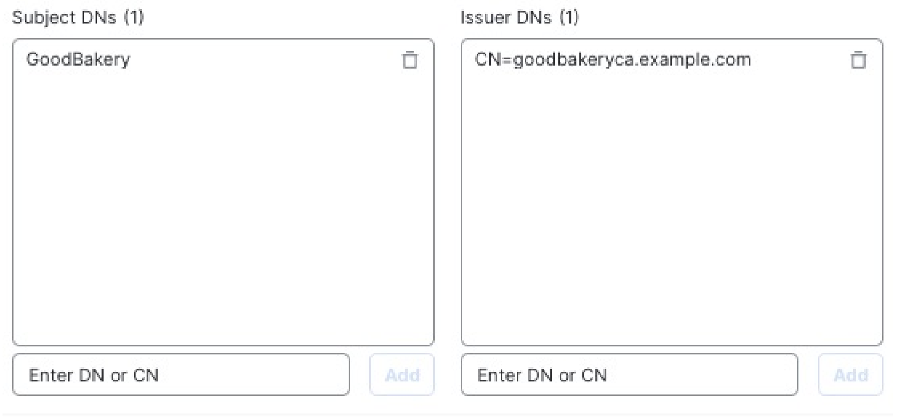
Step 12 Add or continue editing the rule.

Step 13 When you're done, to save changes to the rule, click **Add** at the bottom of the page.

Step 14 To save changes to the policy, click **Save** at the top of the page.

Example

The following figure shows a distinguished name rule condition searching for certificates issued to goodbakery.example.com or issued by goodca.example.com. Traffic encrypted with these certificates is allowed, subject to access control.



Subject DNs (1)

GoodBakery

Issuer DNs (1)

CN=goodbakeryca.example.com

Associate the Decryption Policy with an Access Control Policy and Advanced Settings

This task discusses how to associate the decryption policy with an access control policy and setting recommended advanced settings for the access control policy.

For your decryption policy to be used by the system, you *must* associate it with an access control policy.

Before you begin

Create the sample decryption policy as discussed in this guide.

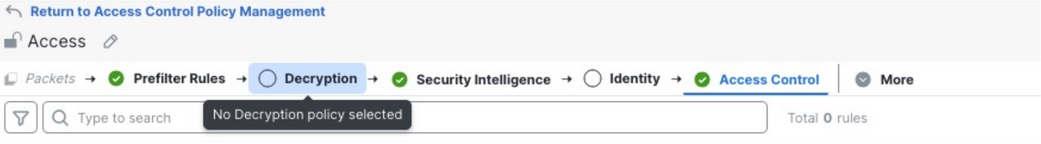
For more information about decryption policy advanced options, see Decryption Policy Advanced Options in the *Cisco Secure Firewall Management Center Device Configuration Guide*..

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

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

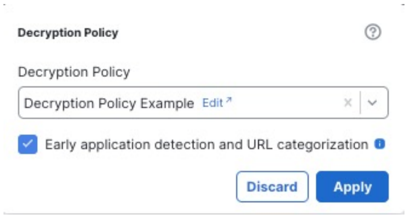
Step 3 Either create a new access control policy or click **Edit** (✎) to edit an existing one.

Step 4 Click the word Decryption as the following figure shows.



No Decryption policy selected

Step 5 From the list, click the name of your decryption policy and also check **Early application detection and URL categorization** as the following figure shows.



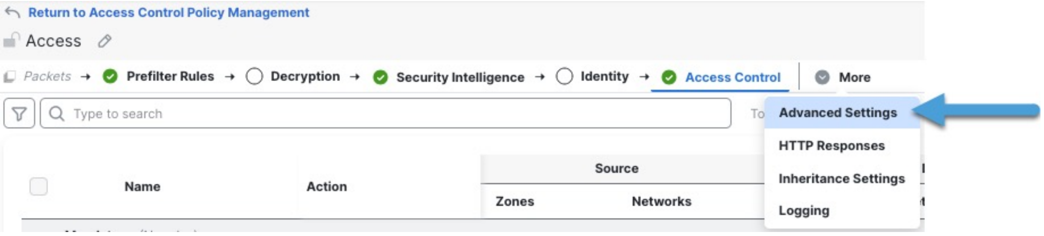
Decryption Policy

Decryption Policy: Decryption Policy Example Edit

☑ Early application detection and URL categorization

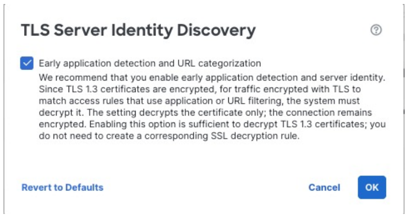
Step 6 Click **Apply**.

Step 7 Click **More** > **Advanced Settings** as the following figure shows.



Step 8 Click **Edit** (✎) next to **TLS Server Identity Discovery**.

Step 9 Select the check box as the following figure shows.



TLS Server Identity Discovery

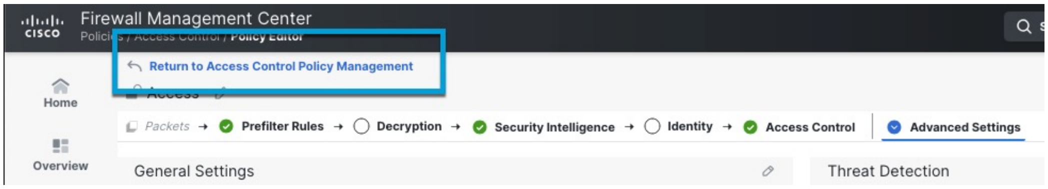
☑ Early application detection and URL categorization

We recommend that you enable early application detection and server identity. Since TLS 1.3 certificates are encrypted, for traffic encrypted with TLS to match access rules that use application or URL filtering, the system must decrypt it. The setting decrypts the certificate only; the connection remains encrypted. Enabling this option is sufficient to decrypt TLS 1.3 certificates; you do not need to create a corresponding SSL decryption rule.

Step 10 Click **OK**.

Step 11 At the top of the page, click **Save**.

Step 12 At the top of the page, click **Return to Access Control Policy Management**, as the following figure shows



Step 13 Click **Edit** (✎) to edit the access control rule.

Step 14 At the bottom of the page, next to the default action, click ⚙ (Default Logging and Inspection).

Step 15 Check **Log at beginning of connection** and any other options you choose.

For more information, see Logging Settings for Access Control Policies in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 16 Click **Apply**.

Step 17 At the top of the page, click **Save**.

What to do next

- Add rule conditions: Decryption Rule Conditions
- Add a default policy action: Decryption Policy Default Actions
- Configure logging options for the default action .
- Set advanced policy properties: Decryption Policy Advanced Options.
- Associate the decryption policy with an access control policy as described in Associating Other Policies with Access Control.
- Deploy configuration changes.

Traffic to Prefilter

Prefiltering is the first phase of access control, before the system performs more resource-intensive evaluation. Prefiltering is simple, fast, and early compared to subsequent evaluation, which uses inner headers and has more robust inspection capabilities.

Based on your security needs and traffic profile, you should consider prefiltering and therefore excluding from any policy and inspection the following:

- Common intraoffice applications such as Microsoft Outlook 365
- Elephant flows, such as server backups

Decryption Rule Settings

How to configure recommended best practice settings for your decryption rules.

Decryption rules: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)

Step 1 Click **Policies** > **Access Control** > **Decryption**.

Step 2 Click **Edit** (✎) next to your decryption policy.

Step 3 Click **Edit** (✎) next to a decryption rule.

Step 4 Click the **Logging** tab.

Step 5 Click **Log at End of Connection**.

Step 6 Click **Save**.

Step 7 Click **Save** at the top of the page.